Journal of Networks

ISSN 1796-2056

Volume 9, Number 12, December 2014

Contents

Special Issue on Selected Best Papers from ICCIT 2012

Guest Editorial

The domain of computer networks is evolving and expanding fast in recent years. New technologies, protocols, services and usage patterns have contributed to the major research interests in this area of computer science. We aim at bringing forward some of these interesting developments that are being pursued by researchers at present in different parts of the globe through the current special issue. Our objective is to provide the readership with some insight into the latest innovations in computer networking through this.

This Special Issue presents selected papers from the fifteenth conference of the ICCIT (International Conference on Computer and Information Technology) series, i.e., ICCIT 2012, held during December 22-24, 2012 at the University of Chittagong, Bangladesh. The first ICCIT was held in Dhaka, Bangladesh, in 1998. Since then the conference has grown to be one of the largest computer and IT related research conferences in the South Asian region, with participation of academics and researchers from many countries around the world. Since 2008 the proceedings of ICCIT has been included in IEEExplore.

In 2012, a total of 491 papers were submitted to the conference. After initial scrutiny, 318 papers were shortlisted for review. After a double blind review process, 126 papers were selected for presentation at the conference and subsequent publication in the conference proceedings. This was tantamount to an acceptance rate of 26%. From these 126 papers, ten highly ranked manuscripts were invited for this Special Issue. In addition, a couple of manuscripts originally submitted for the special issue of the AP Journal of Communications have been transferred for consideration in this special issue because of the relevance of their content. The authors of all the manuscripts were advised to enhance their papers significantly and submit them to undergo review for suitability of inclusion into this publication. Of those, six papers survived the review process and have been selected for inclusion in this Special Issue. These papers address issues concerning different domains of networks namely, channel estimation in OFDM system, performance of decode and forward relaying for wireless uplink, design of LDPC decoders for wireless sensor networks, performance of RFID tags in millimeter wave band, partial coverage algorithm for cluster based wireless sensor network and VoIP quality of service for wireless local area network.

The paper titled “Efficient Scheme for Channel Estimation in OFDM System” deals with devising an efficient channel estimation scheme for OFDM systems. The authors, Md. Nazmul Islam Khan and Md. Jobayer Alam notice that the existing schemes like Least Square (LS) method and Minimum Mean-Square-Error (MMSE) estimator have either performance or computational complexity issues. They devise two new schemes called Simplified Least Square (SLS) and Simplified Minimum Mean-Square-Error (SMMSE) to overcome these issues. They show that SLS is robust against situations where LS had performance problems and that SMMSE is computationally much less complex than MMSE.

The author M.M. Kamruzzaman reports his research findings on the performance of relay in the uplink wireless communication in the manuscript titled “Performance of Decode and Forward Relaying with Space Diversity using STBC for Wireless Uplink”. The author takes the advantages of virtual MIMO for uplink communication into account. He evaluates the performance of relay for uplink wireless communication where source is equipped with single transmit antenna, relay is equipped with multiple transmit and receive antennas and destination is equipped with multiple receive antennas. The results are expected to serve as guidelines for power efficient solution in achieving spatial diversity over wireless fading channels.

The article titled “On Efficient Designing FPGA based LDPC Decoders for Wireless Sensor Networks” deals with reducing the complexity of designing LDPC decoders. The authors Duc Minh Pham and Syed Mahfuzul Aziz present an efficient automated high level approach to designing LDPC decoders using a collection of high level modeling tools. The proposed methodology is being used in the design and implementation of resource efficient LDPC decoders for wireless sensor networks.

The authors A. K. M. Baki and Nemai Chandra Karmakar of the paper “Performance Comparison of RFID Tag at UHF Band and Millimeter-Wave Band” present a novel approach to improve data throughput, range resolution and multiuser capability of RFID systems using millimeter wave band rather than conventional UHF bands. The authors have developed a technically better method for beam forming at 60 GHz by implementing a concept of staircase power distribution (SPD). The proposed method minimizes interference and allows fabrication of a large number of antenna elements within smaller area.

The manuscript “Keeping Desired QoS by a Partial Coverage Algorithm for Cluster-Based Wireless Sensor Networks” has been authored by Lei Wang, Jui-Yu Yang, Yu-Yun Lin, and Wei-Jun Lin. The authors propose a new topology control algorithm for cluster based wireless sensor networks (WSN) to ensure predefined QoS coverage as long as the sensor nodes can stand. The algorithm consists of a novel cluster head competition mechanism and proper transmission of power settings. The method dynamically organizes sensor nodes into clusters to achieve the required connectivity so long as the battery power permits.

doi:10.4304/jnw.9.12.3189-3191

The final title is “Achieving VoIP Guarantee in Wireless Local Area Networks”. It has been contributed by Wen-Li Li, Chunhung Richard Lin, and Chih-Heng Ke. The authors address the issue of quality of Voice over IP (VoIP) services on a wireless local area network (WLAN) environment. Sometimes, voice traffic from high rate stations (HR-STA) gets affected by the traffic from low priority (LP-STA) or low rate (LR-STA) stations. The authors therefore, propose an extension of the EDCA scheme which they name as Voice Differentiation-EDCA (VD-EDCA). Simulation results show that with appropriate maximal delay threshold, the proposed scheme well protects all of the VoIP calls transmitted by HR-STAs from LP-STAs and LR-STAs.

Finally, the Guest Editors would like to express their sincere gratitude to the 13 reviewers besides the guest editors themselves (Abdelrahman Desoky, Fahmida Rahman, Srimathi Chandrasekaran, Atiur R Siddique, Shaila Pervin, Akbar Hossain, Rony Hasinur Rahman, Martin Macuha, Amr Yusef, Yenumula B Reddy, Mohammad Abdus Salam, Qinghai Gao, M. Nazrul Islam) from several countries (Australia, Japan, India, New Zealand and USA) who have given immensely to this process. They have responded to the Guest Editors in the shortest possible time and dedicated their valuable time to ensure that the Special Issue contains high-quality papers with significant novelty contributions.

Guest Editors:

Salahuddin Muhammad Salim Zabir, Orange Labs, Japan, Keio Shinjuku Oiwake Building 9F, 3-1-13 Shinjuku, Shinjuku-ku, Tokyo 160-0022, Japan

J. H. Abawajy, Deakin University, School of Engineering and Information Technology, Geelong, VIC, 3072, AUSTRALIA

Farid Ahmed, Applied Information Sciences Department, Johns Hopkins University Applied Physics Laboratory, Laurel, MD 20723, USA

Joarder Kamruzaman, Gippslans School of IT, Faculty of IT, Monash University, Gippsland Campus, Churchill Vic 3842, Australia

Mohammad A. Karim, University of Massachusetts Dartmouth 285 Old Westport Road Dartmouth, MA 02747-2300
Tel: 508-999-8024, E-mail: mkarim@umassd.edu

Nurul I. Sarkar, School of Computing and Mathematical Science, Auckland University of Technology, Room: WY106, Private Bag 92006, Auckland 1142, New Zeland

Salahuddin Muhammad Salim Zabir is leading research and development on smart cities, e-health, machine to machine (M2M), wellness and disabilities at Orange Labs, Japan. He had his PhD and an MS in information science from Tohoku University, Japan. Before that, he obtained his MSc Engineering and BSc Engineering degrees in Computer Science and Engineering from Bangladesh University of Engineering and Technology. Prior to his current appointment, he has served at Tohoku University, Japan, Kyushu University, Japan, Kyung Hee University, Korea and Bangladesh University of Engineering and Technology. He also worked with Panasonic R&D headquarters in Osaka, Japan. His research interests include computer networks, networking protocols, performance evaluations, ubiquitous computing, applications of ICT for development etc. Dr. Zabir has been serving in the program/technical committees of various international conferences and is guest editing special issues of scholarly journals. He is a senior member of the IEEE.

Jemal H. Abawajy is a professor, Deakin University, Australia. Prof. Abawajy is the director of the "Parallel and Distributed Computing Lab" at Deakin University and a senior member of IEEE. Prof. Abawajy is actively involved in funded research in robust, secure and reliable resource management. He has published more than 200 research articles in refereed international conferences and journals as well as a number of technical reports. Prof. Abawajy has given keynote/invited talks at many international and national conferences. Prof. Abawajy has guest-edited several international journals and served as an associate editor of international conference proceedings. In addition, he is on the editorial board of several international journals (e.g., IEEE Transaction on Cloud Computing). Prof. Abawajy has been a member of the organizing committee for over 200 international conferences serving in various capacity including chair, general co-chair, vice-chair, best paper award chair, publication chair, session chair and program committee. He is also a frequent reviewer for international research journals (e.g., FGCS, TPDS and JPDC), research grant agencies, and PhD examinations.

Farid Ahmed is currently with the Applied Information Sciences Department at Johns Hopkins University Applied Physics Laboratory at Laurel, MD. Prior to this position, he had been associate professor of electrical engineering and computer science at the Catholic University of America, Washington, DC. Dr. Ahmed's professional background includes signal/image processing, computer networks, information security, digital watermarking, cryptography, and optical information processing. He has a publication record of over fifty peer-reviewed journal articles and conference papers combined in these areas and holds 5 US patents. Dr. Ahmed is an associate editor of the EURASIP Journal of Wireless Communications and Networking. He has also been serving on the technical program committee of SPIE conference, ICISST, IFIP N2S, IEEE NAECON, and ICCIT etc. Dr. Ahmed is a member of SPIE and Computer Security Institute, and a senior member of IEEE.

Joarder Kamruzzaman is currently an Associate Professor in the Faculty of Science Technology, Federation University Australia and Deputy Director of the Centre for Multimedia Computing, Communications and Applications Research hosted by the faculty. Prior to joining Federation University, he worked in Monash University, Australia (2000-2013) as an Associate Professor and Bangladesh University of Engineering and Technology, Bangladesh. His research interests include computational intelligence, wireless sensor networks and Internet of Things. His research outcomes are published in top-tier journals and conferences. So far, he has published over 190 articles which include over 45 journal publications. He has edited 2 books that present cutting-edge research on neural network theory and innovative applications in healthcare and finance. Two of his conference papers were awarded best papers in mainstream IEEE conferences. He has attracted over 0.5M research grant from Australian Research Council and industry.

Mohammad Ataul Karim is Provost, Executive Vice Chancellor of Academic and Student Affairs, and Chief Operating Officer of University of Massachusetts Dartmouth. Previously, he served as vice president for research of Old Dominion University in Virginia (2004-2013) and as dean of engineering at the City College of New York of the City University of New York (2000-2004). His research interests include computing, displays, and electro-optical systems, information processing, and pattern recognition. Professor Karim is author of 19 books, 8 book chapters, over 360 articles, 3 patents, and numerous reports. He is Editor of Optics & Laser Technology and an Associate Editor of the IEEE Transactions on Education and has served as guest editor for over 33 journal special issues. Professor Karim is an elected fellow of the Institute of Electrical and Electronics Engineers (IEEE), Optical Society of America (OSA), Society of Photo-Instrumentation Engineers (SPIE), the Institute of Physics (InstP), the Institution of Engineering & Technology (IET), and Bangladesh Academy of Sciences (BAS). He received his BS in physics in 1976 from the University of Dacca, Bangladesh, and MS degrees in both physics and electrical engineering, and a Ph.D. in electrical engineering from the University of Alabama respectively in 1978, 1979, and 1981.

Nurul I. Sarkar (nurul.srakar@aut.ac.nz) holds a PhD from the University of Auckland and is currently associate professor and leader of the Network and Security Research Group at the Auckland University of Technology, New Zealand. He is a member of many professional organizations and societies. Dr Sarkar is a regularly invited keynote speaker, chair, and committee member for various national and international forums. He has published over 120 refereed articles and served on the editorial review boards of several prestigious journals. "Improving the Performance of Wireless LANs: A Practical Guide," his second book has been published by Taylor & Francis in January 2014. Dr. Sarkar is a senior member of IEEE.

Efficient Scheme for Channel Estimation in OFDM System

Md. Nazmul Islam Khan
Department of Electrical & Electronics Engineering, Southeast University, Dhaka, Bangladesh
Email: mnislam@seu.ac.bd

Md. Jobayer Alam
Department of Signal Processing, Blekinge Institute of Technology, Karlskrona, Sweden
Email: farhan2222@gmail.com

***Abstract*—The choice of channel estimation is of fundamental importance in OFDM receiver designs, which further involves a trade-off between complexity and estimation accuracy. In pilot-symbol-aided OFDM system, the Least Square (LS) estimator suffers from inherent additive Gaussian noise and Inter Carrier Interference (ICI), although the estimator exhibits lower complexity and requires implicit knowledge of the channel. In comparison, the Minimum Mean-Square-Error (MMSE) estimator shows much better performance than the LS. However, a major drawback of the MMSE is its higher computational overhead, which further grows with increasing the number of pilots. Accordingly, the optimal design of channel estimators has remained an area of ongoing research. This study performs modifications to both existing LS and MMSE algorithms, followed by proposing two new channel estimators, namely Simplified Least Square (SLS) and Simplified Minimum Mean Square Error (SMMSE). Mathematical analyses and simulation results show that the proposed SLS method is more robust against the additive Gaussian noise and outperforms the original LS estimator. Moreover, this method can perform almost similar to the MMSE for a range of SNRs. Meanwhile, in our study the proposed SMMSE method requires only a minimum knowledge of the Channel Impulse Response (CIR) to efficiently estimate the channel. Additionally, the SMMSE exhibits computational complexity to be significantly lower than that of the original MMSE estimator.**

***Index Terms*—OFDM; Channel Estimation; LS; MMSE**

I. Introduction

Orthogonal Frequency Division Multiplexing (OFDM) [1] system has become increasingly popular due to its bandwidth efficiency, high speed transmission capability and robustness to multipath fading. OFDM has already been successfully implemented in Digital Audio Broadcasting (DAB) system, Digital Video Broadcasting (DVB) system and Wireless LAN standards such as the American IEEE 802.11 (Wi-Fi) [17]. Lately, it has gained a broad interest as a promising technique for wideband radio communication that requires a very high speed for transmission.

For wideband mobile communication system, the radio channel is usually frequency selective and time variant. Therefore, the transfer function of the radio channel for any OFDM system appears to be unequal in both frequency and time domains. Consequently, a dynamic estimation of the channel is necessary when demodulating the OFDM signals. The block-type-pilot estimation technique is widely used to correct the received signal. However, a number of imperative challenges are to be taken into consideration when designing such estimator in any wireless OFDM system. One of those includes accurate arrangement and insertion of the pilot information into all subcarriers of OFDM symbol. Aside from this, modeling an estimator both with higher accuracy and minimum complexity has also become a major concern for the designers [2].

The channel estimation for the block-type-pilot arrangement can be based on Least Square (LS) [14] or Minimum Mean Square Error (MMSE) [15] method. Contemporary research shows that the MMSE estimator can provide 5-10 dB gain in signal to noise ratio (SNR) for the same mean square error of channel estimation over LS estimator [3]. The MMSE method uses the channel statistical properties including the channel autocorrelation matrix and the noise variance. However, in practical wireless environments the channel statistical properties cannot be measured accurately. On top of that, computational complexity of the MMSE estimator is relatively higher than that of the LS estimator. Therefore, in practical OFDM systems the LS method is widely implemented due to its low complexity and minimum requirements of knowing the channel state information. Nevertheless, the LS estimator suffers from inherent Additive White Gaussian Noise (AWGN) and Inter Carrier Interference (ICI), which subsequently results in degradation on the receiver performance [8]. As a matter of fact, estimator design can be viewed as a trade-off between achieving a desired level of performance and maintaining a low complexity.

Following the above background and problem statements, one of the major aims of the paper is to gain a thorough understanding of existing LS and MMSE algorithms, followed by proposing a revised algorithm both for LS and MMSE to minimize their existing limitations. It is worthwhile to mention that the paper is

doi:10.4304/jnw.9.12.3192-3199

an extended version of the previous research carried out in [11]. While, the former had not incorporated the issue of minimizing the computational overhead associated with the existing methods, the current study develops low complexity algorithms to yield optimal or near-optimal designs for the estimators. This study begins by conducting a comprehensive performance evaluation of LS and MMSE algorithms for the OFDM system. Subsequently, we propose a new estimator, which is based on conventional LS algorithm and named as Simplified Least Square (SLS) estimator in our study. The proposed estimator mainly utilizes a modified weighting matrix and establishes no dependency on the original transmitted signal. The SLS can reduce the noise and the interference significantly by performing autocorrelation operation between the derived weighting factor and the channel attenuation.

One of the other important contributions of the paper is to perform a modification to the original MMSE estimator in order to reduce the computational complexity. The proposed estimator is named as Simplified Minimum Mean Square Error (SMMSE) estimator, which exploits the fact that most of the channel energy is contained within a small number of time-domain samples. And, by lowering the sample size it is possible to reduce the complexity for any estimator despite a negligible amount of information about the channel may be lost. To what follows, the SMMSE includes the taps of significant energy only while the taps corresponding to low energy are approximated by zero. Based on such low-rank approximation concept, three versions of the proposed estimator are implemented in this study, i.e., SMMSE-8, SMMSE-14 and SMMSE-20. All three versions of estimator presented in this paper have different computational complexities, and the design variations offer them to have different performances as well. More specifically, there exists performance and complexity trade-off in the choice of one among the algorithms. The simulator used in this study is MATLAB and the performance results are validated on basis of the analysis of two parameters, i.e., Mean Square Error (MSE) and Symbol Error Rate (SER).

The rest of the paper is organized as follows. Section II of this paper describes the related research work for channel estimation. Section III describes the basic baseband OFDM model. Section IV discusses the algorithm of the channel estimators, while the computational complexities of the estimators are documented in section V. Section VI presents a discussion on the results obtained upon running the simulation experiments. Finally, the conclusions are drawn in section VII.

II. Related Work

A number of researches have been carried out on evaluating the performance of LS and MMSE methods; however, not much research has been conducted on aspects relating to any improvement on performance accuracy of the estimators. Besides, very few studies had previously addressed the issue of the computational overhead associated with individual estimators. Some studies had been conducted to develop the conventional LS and MMSE algorithms in order to reduce the noise and the interference [4] [5] [6]. Similarly, it was shown in [7] that the LS estimator can be modified by setting the channel impulse response to zero in time domain. However, the method was incapable of mitigating the edge effect caused by the virtual carriers of the OFDM system. Meanwhile, the authors in [8] proposed a DFT-based noise reduction algorithm that appears to be susceptible to the edge effect of the virtual subcarriers. However, the differences among the channel coefficients on the virtual carriers are neglected in their study. Hence, the performance results for such algorithm could be highly degraded for frequency selective channels. Research in [9] employed a low-pass filter in a transform domain to reduce the noise in the estimation. However, the performance of the algorithm depends on the number of the coefficients of the pilot subcarriers and the frequency selectivity of the channel. Research in [10] states that the accuracy of the channel estimation vector can be significantly improved by using the Q matrix from QR decomposition and the zero-forcing processing. However, the scope of the study was limited to its performance measurement; the associated complexity measurement had not been incorporated.

In [13], a low rank Wiener filter based channel estimator is proposed to reduce the complexity. This optimal estimator avoids large-scale inverse matrix operation of MMSE method, which in turn reduces the computational complexities. Moreover this estimator transmits two training blocks instead of one training block of data and pre-calculates the Singular Value Decomposition (SVD) of the channel correlation matrix. Ref. [12] proposes a modified MMSE, which calculates the predicted channel coefficient vector from the current and past received vector. This predictor memory allows exploiting the temporal channel correlations. In [15], a pilot–aided TD MMSE channel estimator is developed for channel estimation. In this method, pilots are multiplexed with data symbols in different sub-carriers within the OFDM symbol. The TD operation is a simple linear operation and the input signal is directly linked to output samples. The computational complexity is found to be lower because neither DFT nor IDFT operations are required. The separated smoothing and interpolation estimator (SINE) is another proposed method to reduce the MMSE estimator complexity, as described in [16]. The smoothing operation is employed using a low rank estimator based on the singular value decomposition (SVD), while the interpolation technique is implemented using a Wiener interpolation filter (WIF).

III. System Model

The baseband model of a pilot-based OFDM system is depicted in Fig. 1, where we use the following variables: y the received signal vector, x the transmitted signal vector, g the Channel Impulse Response (CIR), and n the AWGN vector. An N-point IDFT is used to modulate the OFDM signal, followed by the insertion of the cyclic

prefix between two consecutive OFDM symbols (Which are not shown in Fig.1). A cyclic extension, longer than the CIR is inserted to avoid inter-carrier interferences [4].

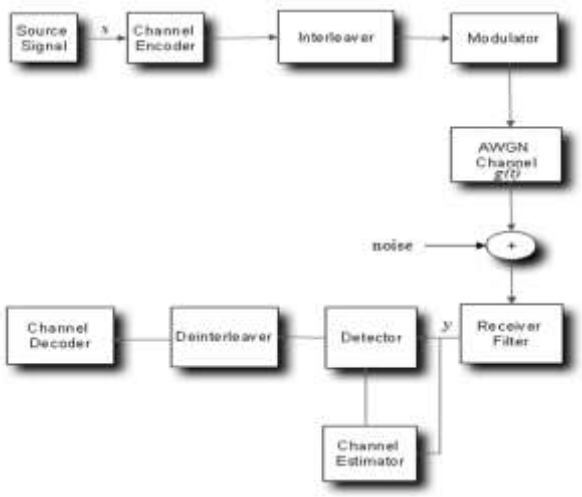


Figure 1. Baseband model of an OFDM system

The channel is modeled as an impulse response *g(t):*

$$g(t)=\sum_{m=0}^{N-1} i_m \delta\left(\tau-\tau_m T_s\right) \tag{1}$$

where we have considered the following variables: i_m the zero mean complex Gaussian variable, *g(t)* the time limited pulse train of length *N*, T_s the sampling period, and τ_m the delay of *N*-th impulse. Except the *N*-th delay, all other remaining ones, i.e., τ_1 through τ_{N-1}, generated by the respective impulses, are uniformly distributed over the total length of the given cyclic prefix.

At the receiver, the cyclic prefix is removed and an *N*-point DFT is used to analyze the signal in frequency domain .The original signal is then obtained back through detection and channel decoding operations. The signal in frequency domain at the receiver can be expressed by:

$$y=DFT_N\left[\, IDFT_N(x)\otimes\frac{g}{\sqrt{N}}+\tilde{n}\,\right] \tag{2}$$

The variables used in (2) are: the transmitted pilot symbols, $x=[x_0,x_1.x_2...x_{N-1}]^T$, the received symbols $y=[y_0,y_1,y_2.....y_{N-1}]^T$, the complex AWGN vector $n=[n_0,n_1,n_2.....n_{N-1}]^T$, and the CIR $g=[g_0,g_1,g_2.....g_{N-1}]^T$. A cyclic convolution, i.e. $\otimes$, requires to be performed additionally in part of the total modeling processes, as it is shown in (2). Further, a term called channel attenuation or channel transfer function is used to substitute the vector $\frac{g}{\sqrt{N}}$ of (2). The transfer function is nothing but an observable channel coefficient obtained by means of sampling of the CIR. Meanwhile, to calculate g the following expression is used:

$$g_k=\frac{1/\sqrt{N}\sum_{m=0}^{N-1} i_m e^{-j\frac{\pi}{N(K+(N-1)\tau_m)\sin(\pi\tau_m)}}}{\sin(\frac{\pi}{N}(\tau_m-k))} \tag{3}$$

If τ_m is found to be an integer in (3), all energy will be mapped to taps g_k. However, the energy will be leaked to taps g_k, in case τ_m is not an integer. Usually most of the energy is located near the original pulse location. For mathematical modeling of the system, the expression can be finally derived as:

$$y_k=x_k h_k+n_k \tag{4}$$

where n_k represents a set of independent Gaussian channels, and *k = 0,1, …. N-1*. Meanwhile, h_k denotes the channel attenuation vector and can be expressed as:

$$h_k=\left[h_0,h_1,h_2.....h_{N-1}\right]^T=DFT(g_k)$$

For simplicity we can rewrite (4) as:

$$y=xF_g+n \tag{5}$$

where *F* represents the DFT matrix.

IV. MMSE, LS, SLS AND SMMSE ESTIMATORS

This section continues with an analytical discussion of the channel estimation strategies used in OFDM system. Both the existing and the proposed methods are incorporated in the discussion.

A. MMSE Estimator

The task of the channel estimator is to estimate the channel attenuations *h* from the observations, given that the channel and noise statics are known. The estimator employs the second-order statistics of the channel conditions to minimize the error. The technique is one of the simplest techniques of estimation.

$$g_{MMSE}=R_{gy}R_{yy}^{-1}y \tag{6}$$

where

$$g_{MMSE}=R_{gy}R_{yy}^{-1}y$$

and $R_{yy}=E\{yy^H\}=xFR_{gg}x^HF^H+\delta_n^2 I_n$

R_{gg} and R_{yy} represent the auto-covariance matrices of g and y, respectively. Meanwhile, the cross-covariance of g and y is denoted by R_{gy}. The columns in F are orthogonal and I is the identity matrix. The channel impulse response h_{MMSE} is defined as:

$$h_{MMSE}=Fg_{MMSE}=FQ_{MMSE}F^HX^Hy \tag{7}$$

where

$$Q_{MMSE}=R_{gg}\left[(F^Hx^HxF)\delta_n^2+R_{gg}\right]^{-1}\left(F^Hx^HxF\right)^{-1}$$

and the noise variance $E\{(|n|)^2\}$ is denoted by δ_n^2.

B. LS Estimator

The LS estimator for the cyclic impulse response *g* minimizes $(xFg)(y-xFg)^{H}$ and generates the channel attenuation as bellow

$$h_{LS} = FQ_{LS}F^{H}x^{H}y \tag{8}$$

$Q_{LS} = \left(F^{H}x^{H}Fx\right)^{-1}$ and $(y-xFg)^{(H)}$ are the conjugate transpose operations. Hence,

$$h_{LS} = x^{-1}y \tag{9}$$

where h_{LS} is the channel attenuation for LS.

C. Proposed Estimator, SLS

We proposed the following SLS estimator, which is based on the LS algorithm. Equation (9) can be alternatively written as:

$$h_{LS} = h + n \tag{10}$$

where *h* is the transfer function, *n* is the Gaussian noise, *F* is the DFT matrix, and *g* is the channel impulse response in time domain. Making a comparison between (10) and (5), we can write the value of h as:

$$h = F_g \tag{11}$$

The LS estimation is noisy observation of the channel attenuation which can be smoother using some autocorrelation operation with the channel attenuation h_{LS}. If the channel transfer function is *h*, the received signal y and the transmitted symbol *x*, then the SLS channel estimator will be

$$h_{SLS} = W_x h_{LS} \tag{12}$$

where W_x is called weighted matrix and is defined by

$$W_x = R_{hh}\left[R_{hh} + \sigma_n^2\{x(x)^{-1}\}^{-1}\right]^{-1} \tag{13}$$

The auto-covariance matrix of h is defined as

$$R_{hh} = E\{hh^{H}\} \tag{14}$$

The weighting matrix W_x of size $N \times N$ depends on the transmitted signal *x*. As a step towards the low-complexity estimators we want to find a weighting matrix which does not depend on the transmitted signal *x*. The weighting matrix can be obtained from the auto-covariance matrix of h and auto-correlation of transmitted signal *x*. Consider that the transmitted signal *x* to be stochastic with independent and uniformly distributed constellation points. In that case the auto-covariance matrix of noise becomes:

$$R_{nn} = \frac{\alpha}{SNR} I \tag{15}$$

where α is constellation factor and $E\left\{\left|x_i\right|^2\right\}$ $E\left\{\left|\frac{1}{\left|x_i\right|^2}\right|\right\}$ is the mathematical expression of α. The value of α is $\frac{17}{6}$ for 16-QAM. SNR is a per-symbol signal to noise ratio and equals to $E\left\{\frac{\left|x_i\right|^2}{\delta_n^2}\right\}$. The SLS estimator becomes:

$$h_{SLS} = W_{\mathrm{mod}ified} h_{LS} \tag{16}$$

where

$$W_{\mathrm{mod}ified} = R_{hh}\left(R_{hh} + R_{nn}\right)^{-1}$$

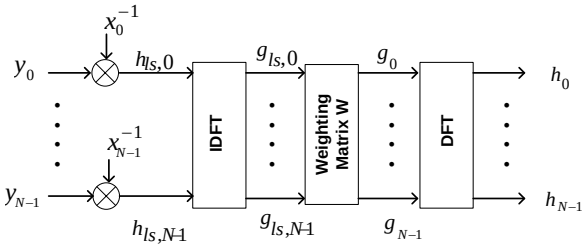


Figure 2. Block diagram of SLS estimator

Fig. 2 represents the block diagram of h_{SLS} estimator, where x_n is the input signal with 0 to (*N-1)* samples, y_n is the output signal with 0 to (*N-1)* samples, g_n is the channel impulse response in the time domain, and h_n is the channel transfer function in the frequency domain.

D. Proposed Estimator, SMMSE

The proposed SMMSE estimator is developed based on the original MMSE algorithm that uses the assumption of a finite length impulse response. In (1), most of the energy in *g* lies usually in the first *L* no. of samples, where *L* is a small fraction of *g*. To find such energy contained samples, *L* is calculated by performing a multiplication between *N* (the total DFT size) and the $\frac{T_G}{T_S}$, where T_G and T_s represent cyclic extension and sampling interval of the OFDM system, respectively. The ideal value of $\frac{T_G}{T_S}$ is often chosen, as recommended by IEEE 802.11 and IEEE 802.16, among $\{\frac{1}{32}, \frac{1}{16}$ and $\frac{1}{8}\}$ [7]. For example, if the DFT size is 64 and $\frac{T_G}{T_S}$ is set to $\frac{1}{8}$, then *L* is found to be as small as 8. This implies that the significant portion of the channel energy is contained in first eight samples, while the remaining samples are mostly filled with unwanted noise. To what follows, the proposed SMMSE excludes all the low energy taps for channel estimation and reduces the size of the Q'_{SMMSE} to

an ($L \times L$) matrix. The first L column of F is represented by A. By taking only the significant energy samples of g into account and $R^{'}_{gg}$ is set to zero for all taps outside the first L samples, the SMMSE estimator becomes:

$$h_{SMMSE} = Ag_{SMMSE} = AQ^{/}_{SMMSE} A^H X^H y \qquad (17)$$

where

$$Q^{/}_{SMMSE} = R^{"}_{gg}\left[(A^H x^H xA)\delta_n^2 + R^{"}_{gg}\right]^{-1}\left(A^H x^H xA\right)^{-1}$$

Using (17), three modified estimations are presented in this study, namely SMMSE-8, SMMSE-14 and SMMSE-20. Fig. 3 shows the general structure of SMMSE estimator where x_n is the input signal, y_n is output signal and h_n is the transfer function. As can be seen, part of the channel is set to the null signal and does not belong to the modified Q. A smaller dimension of Q represents a lower computational complexity and still lets the estimator describe the channel with no significant loss.

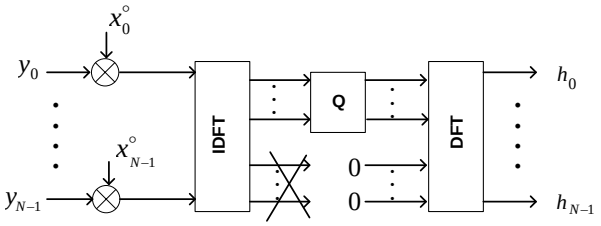


Figure 3. Block diagram of SMMSE estimator

V. Computational Complexities

To determine the computational complexity of the channel estimators, the conventional matrix calculation procedures are used. In all the calculations, capital notation O represents the computational complexity and n represents the matrix size.

A. MMSE Estimator

Complexity of DFT matrix F:

O (F) = O (DFT) = n (log n),

where F is a matrix of $n \times n$ size.

Complexity of R_{gy}:

$$O(R_{yy}) = O(xFR_{gg}x^H F^H + \delta_n^2 I_n)$$

where R_{gy} is an $n \times n$ matrix, F is an $n \times n$ matrix, x is an $1 \times n$ matrix. Number of operations needed for square matrix *(n × n)* (n × n)* is *[O (n^3)]* and matrix multiplication of *(n × n) * (n ×1)* is *O (n * n * 1)* or *[O (n^2)]*. So the computational complexity for R_{gy} becomes $n^2(n+1)$.

Complexity of R_{yy}:

$$O(R_{yy}) = O(xFR_{gg}x^H F^H + \delta_n^2 I_n)$$

$$= n^2 + n^3 + n^3 + n^2 + n^2 = n^2(2n+3)$$

Number of operations needed for square matrix *(n × n)* (n × n)* is *[O (n^3)]* and matrix multiplication of *(n × n) * (n ×1)* is *O (n * n * 1)* or *[O (n^2)]*.

Complexity of g_{MMSE}:

$$O(g_{MMSE}) = O(R_{gy}R_{yy}^{-1}y)$$

$$= n^3 + n^2 + n^3 = n^2(2n+1)$$

Number of operations needed for square *matrix (n × n)* (n × n)* is *[O (n^3)]* and matrix multiplication of *(n × n) * (n ×1)* is *O (n * n * 1)* or *[O (n^2)]* and for inverse operation that is n^3.

Complexity of h_{MMSE}:

$$O(h_{MMSE}) = O(DFT(h_{MMSE})) = n(\log n)$$

Complexity of 'for loop':

$$O(for\_loop) = n+1$$

TABLE I. Computational complexities of MMSE estimator

Variables	Number of Operation
F	115
R_{gy}	266240
R_{yy}	536576
g_{MMSE}	528384
h_{MMSE}	115
'for' loop	65
Total	1,331,495

B. LS Estimator

From (9), we can write

$$O(h_{LS}) = O(x^{-1}y) = n + n^2 = n(1+n)$$

For the above calculation, one inverse operation and one multiplication operation are required. For inverse operation we need to consider n operation because matrix size of $n \times 1$, and for multiplication operation we need total n^2 operation. Thus, the computational complexity for h_{LS} is $n(1+n)$. Here, n = 64, thus total computational complexity for the LS estimator becomes 4160.

C. Proposed Estimator, SLS

Complexity of DFT matrix F:

O (F) = O (DFT) = n (log n),

where F is a matrix of n ×n size.

Complexity of R_{gy}:

$$O(R_{hh}) = O(F^* R_{gy} * F^{-1})$$

$$= n^3 + n^3 + n^2 = n^2(2n+1)$$

Number of operations needed for square matrix *(n × n)* (n × n)* is *[O (n^3)]* and matrix multiplication of *(n × n) * (n ×1)* is *O (n * n * 1)* or *[O (n^2)]*. For inverse multiplication the number of required operation is n^3.

Complexity of R_{hh}:

$$O(R_{yy}) = O(xFR_{gg}x^H F^H + \delta_n^2 I_n)$$

$$= n^2 + n^3 + n^3 + n^2 + n^2 = n^2(2n+3)$$

Number of operations needed for square matrix *(n × n)* (n × n)* is *[O (n^3)]* and matrix multiplication of *(n × n) * (n ×1)* is *O (n * n * 1)* or *[O (n^2)]*.

Complexity of h_{LS}:

$$O(h_{LS}) = O(x^{-1}y) = n + n^2 = n(1+n)$$

Complexity of h_{SLS}:

$h_{SLS} = W * h_{LS}$

where

$$O(W) = O(R_{hh}(R_{hh} + \frac{\alpha}{SNR} * I)^{-1})$$

$$= n^3 + n^2 + n$$

Thus

$$O(h_{SLS}) = n^2$$

For W, we need to consider one inverse operation, one multiplication operation and one multiplication operation between $\frac{\alpha}{SNR}$ and *I*. For inverse operation we need to consider n^2 operation. The matrix multiplication of *(n × n) * (n ×1)* is *O (n * n * 1)* or *[O(n)^2]* and for multiplication between $\frac{\alpha}{SNR}$ and *I* the required number of operation is *n*. The total complexity required to determine *O (W)* is $= n^3 + n^2 + n$.

Table II shows the overall computational complexity of the SLS estimator with *n* = 64. The total computational complexity for SLS is 803,059, which is greater than that of the original LS method (i.e. 4160). In addition, the complexity of SLS is found to be about 40 % lower than that of the original MMSE (i.e. 1,331,495).

TABLE II. COMPUTATIONAL COMPLEXITIES OF SLS ESTIMATOR

Variables	Number of Operation
F	115
R_{hh}	528384
h_{LS}	4160
W	266304
h_{SLS}	4096
Total	803059

TABLE III. COMPUTATIONAL COMPLEXITIES OF SMMSE ESTIMATOR

Variables	Number of Operations		
	SMMSE-8	SMMSE-14	SMMSE-20
F	7	16	26
R_{gy}	576	2940	8400
R_{yy}	1153	5881	16801
g_{SMMSE}	1088	5684	16400
h_{SMMSE}	7	16	26
'for' loop	9	15	21
Total	2,840	14,552	41,674

D. Proposed Estimator, SMMSE

The complexity results of SMMSE-8, SMMSE-14 and SMMSE-20 are summarized in Table II. From the numerical experiments it is evident that all of the proposed versions can result in substantial reductions in computational complexity by utilizing a low-rank approximation strategy. The matrix calculation procedures used to determine the proposed estimators' complexity are quite similar to those of the one done for the MMSE in this paper. The SMMSE-8, SMMSE-14 and SMMSE-20 perform total 2,840, 14,552 and 41,674 no. of calculations, respectively, which is approximately 98, 98.5 and 96.5 percent, respectively, lower than that of the original MMSE. An interesting observation is that total number of computations the SMMSE-8 performs during the estimation is lower even than that of the LS (i.e. 4160).

VI. SIMULATION RESULTS

This section outlines how well the existing (i.e. LS and MMSE) and the proposed (i.e. SLS and SMMSE) estimator respond to the performance differentials (i.e. MSE and SER) when subjected to different SNR values. We considered the maximum value of SNR as 30 dB over which the performance statistics of MSE and SER are collected. To evaluate the performance of existing and proposed estimators, an OFDM system with a bandwidth 500 kHz is considered in our study. The parameters of the system include, among others: the FFT size is 64, the number of the used subcarriers is 64, the sampling rate is 500 kHz, the total symbol period is 138 μs, cyclic prefix is 10 μs and the modulation scheme on every subcarrier is 16-QAM modulation.

A. Mean Square Error

In Fig. 4, the MSE results of LS, MMSE and SLS estimators over an SNR range are shown. For different SNRs, the MSE is found between 10^{-4} to $10^{-1.5}$ for the MMSE, between $10^{-3.5}$ to $10^{-0.5}$ for the LS and between $10^{-2.5}$ to $10^{-1.5}$ for the SLS. The MMSE is appeared to be more susceptible to noise since the method uses the channel statistical properties including the channel autocorrelation matrix and the noise variance. Compared with the LS method, the proposed SLS method can obtain better performance up to 16 dB of SNRs, while the performance between SLS and MMSE appears to be almost same up to 8 dB of SNRs.

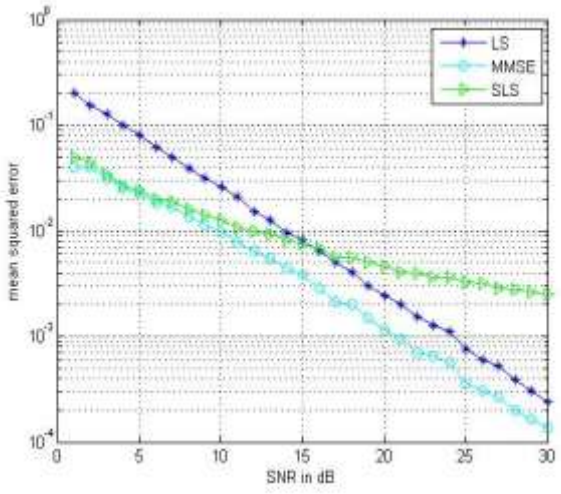


Figure 4. MSE vs. SNRs for channel estimators

Fig. 5 shows the MSE versus SNR results for the MMSE, SMMSE-8, SMMSE-14 and SMMSE-20. All the existing and modified estimators presented in this study have different computational complexities, and the design variations offer them to have different performances as

well. The performance of the low-complexity estimators, especially for low SNRs, depends strongly on the number of included taps. As can be observed, the SMMSE-8 has the lowest complexity but it has relatively higher MSE, because only small parts of the channel statistics are taken into the account when designing such estimator. Meanwhile, the SMMSE-20 yields the best performance among all the modified versions. However, the MSE of SMMSE-20 is yet higher than the MMSE due to the fact the rank of the channel correlation matrix is reduced in the proposed one. However, as the SNR range increases, the MSE result tends to be close to the MMSE.

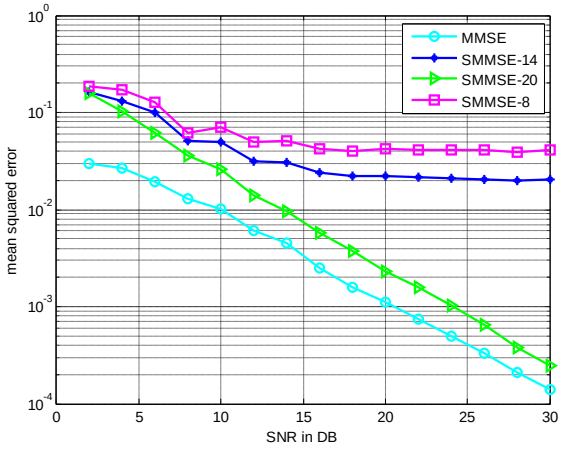


Figure 5. MSE vs. SNRs for channel estimators

B. Symbol Error Rate

Fig. 6 illustrates the SER versus SNRs for LS, MMSE and SLS methods. The MMSE achieves the SER between 10^{-2} to $10^{-1.1}$, the LS achieves between 10^{-2} to $10^{-0.8}$ and the SLS achieves between 10^{-2} to $10^{-1.2}$. The performance of SLS method is found to be considerably better than that of the LS up to the SNRs of 17 dB. A gain in SNR up to about 4 dB can be obtained for certain SNRs when using the proposed estimator instead of the original LS estimator. Meanwhile, the SER of the proposed method is about the same as that of the MMSE for all SNRs.

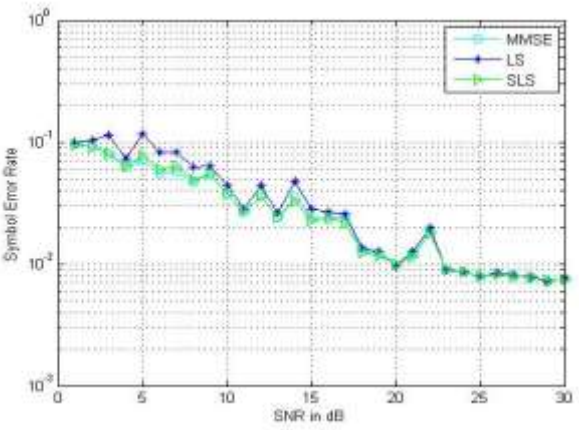


Figure 6. SER vs. SNRs for channel estimators

In Fig. 7, the SER results are plotted for MMSE and different SMMSE estimation schemes over a range of SNRs. The SER value of MMSE lies between $10^{-2.5}$ to $10^{-1.5}$, while it is found to be in the range of $10^{-0.5}$ and $10^{-1.5}$ for all other proposed versions. The SER of SMMSE-8, SMMSE-14 and SMMSE-20 appears to be slightly higher than that of the MMSE as only the part of the channel is considered for the estimation. The irreducible error floor is introduced for the modified estimators due to the loss of channel information; although the performance tends to show improvement at higher SNRs. Among the proposed estimators, the SMMSE-8 includes only a minimum number of energy taps and therefore experiences more SER floor. Meanwhile, a relatively larger dimension of Q'_{SMMSE} allows the SMMSE-20 to attain a lower SER for all SNRs.

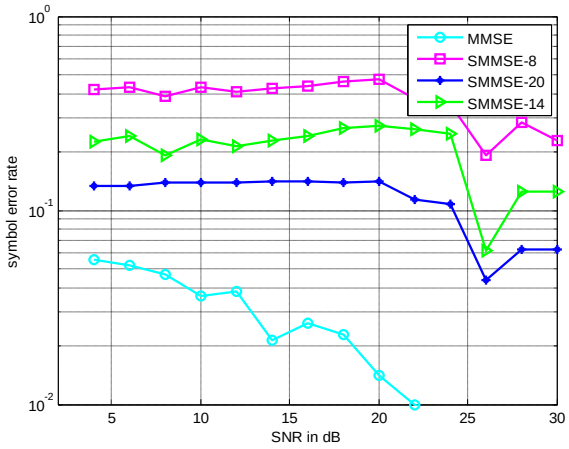


Figure 7. SER vs. SNRs for channel estimators

VII. CONCLUSION

This paper reviews pilot-symbol-aided channel estimation strategies in OFDM systems and proposes two new estimation methods for use in such system. The implementation complexity and system performance of different estimators are studied and compared in this paper. The study finds that the LS estimator cannot outperform the MMSE in terms of their MSE and SER results. Meanwhile, computational complexity associated with the MMSE method is found to be much higher than the LS. Following that, this paper presents the analytical expressions of the proposed SLS and SMMSE methods, and shows their efficiency and improvement over the existing ones through simulation result and mathematical analysis. The result shows that the SLS outperforms the conventional LS method for a range of SNRs. Moreover, the performance of SLS is found to be almost equal, if compared with the MMSE estimator. Although, the proposed method experiences relatively higher computational complexity than the original one, the complexity is yet to be achieved about 40 % lower than the MMSE. Meanwhile, the proposed SMMSE utilizes the low-rank approximation technique and reduces the complexity significantly at the expense of certain

performance loss. Among three SMMSE versions, the most satisfactory performance is achieved by the SMMSE-20, followed by the SMMSE-14 and the SMMSE-8. In terms of computational overhead, the SMMSE-8 demonstrates its superiority both over the modified versions as well as the original one. The complexity results of SMMSE-8 could be further rewarding, if compared with the LS estimator, because the total number of computations the SMMSE-8 performs during the estimation is found to be lower even than that of the LS. Finally, the SMMSE-14 offers the most effective trade-off between performance and complexity among the three SMMSE estimators presented in this paper.

REFERENCES

[1] Su Wei and Pan Zhiwen, "Iterative LS channel estimation for OFDM systems based on transform-domain processing", International Conference on Wireless Communications, Networking and Mobile Computing, vol. 1, pp. 416-419, September 2007.

[2] Dongxu Shesn, Zhifeng Diao, Kai-Kit Wong and Victor O.K.Li, "Analysis of pilot assisted channel estimators' for OFDM systems with transmit diversity", IEEE Transactions on Broadcasting, vol. 52, no. 2, June 2006.

[3] Carlos Ribeiro and Atilio Gameiro, "An OFDM symbol design for reduced complexity MMSE channel estimation", Journal of Communications, vol. 3, no. 4, September 2008.

[4] Gunther Auer and Eleftherious Karipidis, "Pilot aided channel estimation for OFDM: a separated approach for smoothing and interpolation", IEEE International Conference on Communications, vol. 4, pp 2173-2178, August 2005.

[5] Yi Gong and K.B Lataief, "Low rank channel estimation for space-time coded wide band OFDM systems", IEEE Vehicular Technology Conference, vol. 2, pp. 772-776, 2001.

[6] Dieter Schafhuber and Gerald Matz, "MMSE and adaptive prediction of time-varying channels for OFDM systems", IEEE Transactions on Wireless Communications, vol. 4, no 2, March 2005.

[7] J.-J. van de Beek, M. Sandell, S. K. Wilson, and P. O. Börjesson, "On channel estimation in OFDM systems", in Proceedings of the IEEE VTC'95, vol. 2, pp. 815-819, July 1995.

[8] Xiaolin Hou, Zhan Zhang, and Kayama, H., "Low-complexity enhanced DFT-based channel estimation for OFDM systems with virtual subcarriers", in Proceedings of the 18th IEEE Conference on Vehicular Technology, pp. 521-525, June 2008.

[9] Zhao Yuping, and Huang Aiping. "A novel channel estimation method for OFDM mobile communication systems based on pilot signals and transform-domain processing", in Proceedings of the IEEE VTC' 97, pp. 2089 – 2093, July 1997.

[10] Lihua Yang, Guangliang Ren, and Zhiliang Qiu, "Novel noise reduction algorithm for LS channel estimation in OFDM system with frequency selective channels", International Conference on Communication Systems, vol. 10, pp. 478-483, January 2011.

[11] Khan M.N.I. and Alam M. J., "Noise reduction algorithm for LS channel estimation in OFDM system," In Proceedings of 15th International Conference on Computer and Information Technology (ICCIT 2012), pp. 310- 315, December 2012.

[12] N. Geng, X. Yuan, and L. Ping, "Dual-diagonal LMMSE channel estimation for OFDM systems," IEEE Transaction on Signal Processing, Vol. 60, no. 9, September 2012.

[13] F. Gao, T Cui, and A. Nallanathan, "On channel estimation and optimal training design for amplify and forward relay networks," IEEE Transactions on Wireless Communications, Vol. 7, no. 5, January 2008.

[14] X. Liao, L. Fan, and F. Gao, "Blind channel estimation for OFDM modulated two-way relay network," in Proceedings of IEEE Wireless Communications and Networking Conference, Australia, April 2010.

[15] O. Rabaste and T. Chonavel, "Estimation of multipath channels with long impulse response at low SNR via an MCMC method," IEEE Transaction on Signal Processing, vol. 55, pp. 1312–1325, April 2007.

[16] R. Otnes and M. Tuchler, "Iterative channel estimation for turbo equalization of time-varying frequency-selective channels," IEEE Transaction on Wireless Communication, vol. 3, no. 6, pp. 1918–1923, Nov. 2004.

[17] P. Fertl and G. Matz, "Efficient OFDM channel estimation in mobile environments based on irregular sampling," In proceeding of 11th Asilomar Conference on Signals, Systems and Computers, pp. 1777–1781, November 2006.

Md Nazmul Islam Khan was born in Dhaka, Bangladesh in 1985. He obtained his M.Sc degree in electrical engineering from Blekinge Institute of Technology, Sweden in 2010. Currently he is working as a Lecturer at Southeast University, Bangladesh. His research interest includes Wireless communication, OFDM and multicarrier systems, radio propagation, and MANET.

Md Jobayer Alam received his BSc in Computer Engineering from American International University Bangladesh (AIUB), Bangladesh and M Sc in Electrical Engineering with emphasis on Signal Processing from Blekinge Institute of Technology, Sweden. His research interest lies in the areas of adaptive and statistical signal processing and their applications to the wireless communications, signal processing, and information theory.

Performance of Decode and Forward MIMO Relaying using STBC for Wireless Uplink

M. M. Kamruzzaman
Key Lab of Information Coding & Transmission, Southwest Jiatong University, Chengdu, Sichuan, China
E-mail: m.m.kamruzzaman@gmail.com

***Abstract*—This paper compares the performance of a decode and forward relay assisted wireless uplink with direct wireless uplink in the presence of rayleigh fading where source is equipped with single transmit antenna (Tx), relay is equipped with multiple transmit and receive antennas (Rx), and destination has multiple receive antennas. Data are modulated using QPSK or 16 QAM or 64 QAM modulator at source and send to relay which combine and decode the incoming signal using Maximum Likelihood decoding and further encode the symbols using STBC, and the encoded data are split into n streams which are simultaneously transmitted using n transmit antennas of relay. It is observed that relay with 2Tx or 3Tx or 4Tx and 2Rx or 3Rx or 4Rx provides 1 dB to 22 dB gains at 10^{-5} compare to direct link where destination has 2Rx or 3Rx or 4Rx. And there is around 1 dB to 7 dB gains for increasing number of Tx antennas from 2 to 3 or 3 to 4 at relay.**

***Index Terms*—Space Time Block Code; MIMO; Relay; Decode and Forward; Uplink**

I. INTRODUCTION

In recent wireless communication systems, relaying has attracted a lot of research interest due to its ability of improving performance, increasing system capacity, extending coverage without the need of having multiple antennas at the source and/or destination [1-3]. The basic idea of relay is to transmit signals from one terminal to another through a number of relays. There are mainly two types of relays: Amplify and Forward (AF) and Decode and Forward (DF). AF simply amplifies the incoming signal and forwards it to the destination without any attempt to decode it. AF relay is easy to implement but can not achieve high performance gain. On the other hand, DF decodes the incoming signal, re-encodes it, and then retransmits it to the destination. Although the complexity of DF is high but can obtain high performance gain [4]. So we have used DF to show the performance of our system.

Relay assisted wireless communication has been widely studied [5-30]. [5-7] show the performance of relay using amplifying and forwarding. [8-10] show the performance of relay having difference time slot to transmit information. [11-19] show the performance of relay having single antenna at source, relay and destination. [20-22] show the performance of relay having single antenna at source and destination but multiple antennas at relay. [23-30] show the performance of relay having multiple antennas at source, relay and destination. This paper investigate the performance of relay for uplink wireless communication where source is equipped with single transmit antenna, relay is equipped with multiple transmit and receive antennas and destination is equipped with multiple receive antennas. The main reason of considering this configuration is to provide the advantages of virtual MIMO for uplink communication. Because it is not possible to achieve spatial diversity by integrating many antennas onto a small mobile hand set due to size, complexity, power or other constraints. To overcome this problem, multiple users would consider the configuration studied in this paper for relaying with multiple transmit and receive antennas which will provide power efficient solution to achieving spatial diversity in wireless fading channels.

The rest of the paper is organized as follows. In section II, we present the system model with channel characteristics, encoding-decoding techniques of relay and decoding techniques of received signals at destination. The simulation results are presented in section III, and section VI contains the conclusions.

II. SYSTEM MODEL

Fig. 1 shows the relay-assisted wireless uplink communication system in which source is equipped with single transmitte antenna and relay is equipped with multiple transmit antennas and multiple receive antennas. Signal s is transmitted from source using single transmit antenna and receivers of relay receive the signal. r_i is the received signal on the ith receiver antenna of relay. Maximum Likelihood (ML) decoder decodes the received signal, further encodes using STBC encoder and send to destination where destination is also equipped with multiple receiving antennas. We assume that at each time slot t, receiving antennas. We signals S_t^i, i =1, 2, ... n are transmitted simultaneously using n transmit antennas of relay. Data are modulated by a QPSK or 16 QAM or 64 QAM modulator before transmitting. The channel h_i is

Manuscript received August 8, 2013; revised March 21, 2014; accepted June 1, 2014. Part of the results of this paper was presented at the 15th International Conference on Computer and Information Technology (ICCIT2012), December 22-24, 2012 [39].

M.M.Kamruzzaman is with the Key Lab of Information Coding & Transmission, Southwest Jiaotong University, Chengdu, Sichuan, China. E-mail: m.m.kamruzzaman@gmail.com.

doi:10.4304/jnw.9.12.3200-3206

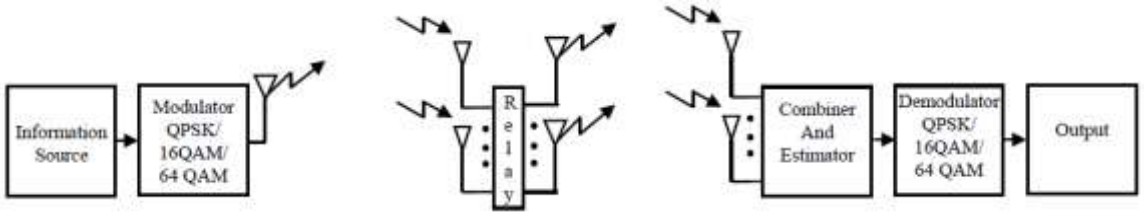


Figure 1. System Block diagram

assumed to be a flat fading channel, channel experienced by each receive antenna is independent from the channel experienced by other receive antennas and the channel is know at the receiver. Finally the signal y_t^j is received on the jth receiver antenna of destination at time *t*. ML decoder decodes the received signal of destination and the detected symbols are demodulated by QPSK or 16 QAM or 64 QAM demodulator to get the output.

A. Received Signal at Relay

If the symbol transmitted by transmit antenna is s, then the signal received by the receiving antennas at relay can be written as:

$$r_i = p_i^{SR} h_i s + n_i \quad (1)$$

where r_i is the received symbol on the ith receiver antenna of relay.

p_i^{SR} is path loss from transmit antenna i of source to receive antenna j of relay and $p_i^{SR} \alpha \frac{1}{d_{SR}^2}$

h_i is the channel on the i[th] receive antenna.

s is the transmitted symbol and

n_i is the noise on i[th] receive antenna. It is assumed that the noise on each receive antenna is independent from the noise on the other receive antennas.

It is considered that $H_i = P_i^{SR} h_i$, then (1) can be written as:

The combiner combines received signals which are then sent to the maximum likelihood detector. The combiner generates the following signals [31- 38]:

$$\tilde{s} = H_1^* r_1 + H_2 r_2^* + H_3^* r_3 + H_4 r_4^* + \ldots\ldots\ldots + H_{n-1}^* r_{n-1} + H_n r_n^* \quad (2)$$

Maximum likelihood decoding of combined signal $\tilde{s}$ can be achieved using the decision metric (3) to detect the symbol s:

$$\sum_{i=2}^{n} \left(\left| r_{i-1} - h_{i-1} s \right|^2 + \left| r_i - h_i s^* \right|^2 \right) \quad (3)$$

over all possible values of s.

We expand the above equation and delete the terms that are independent of the code words. So the above can be rewrite:

$$-\sum_{i=2}^{n} \left[r_{i-1} h_{i-1}^* s^* + r_i^* h_i s \right] + \left| s \right|^2 \sum_{i=1}^{n} \left| h_i \right|^2 \quad (4)$$

which is equivalent to following the decision metric[31-38].

$$\left\| \left[\sum_{i=2}^{n} \left(r_{i-1} h_{i-1}^* + r_i^* h_i \right) \right] - s \right|^2 + \left(-1 + \sum_{i=1}^{n} \left| h_i \right|^2 \right) \left| s \right|^2 \quad (5)$$

Detected symbols are represented as $\hat{s}_1$ and $\hat{s}_2 \ldots \hat{s}_n$.

B. Encoding Using STBC and Retransmitting from relay:

STBC encoder of relay encodes the received symbols of relay according to number of transmit antennas as shown in Table I, Table II and Table III and then at each time slot *t*, signals S_t^i, i =1, 2, … n are transmitted simultaneously using *n* transmit antennas [40,41].

TABLE I. THE ENCODING AND TRANSMISSION SEQUENCE FOR TWO TRANSMIT ANTENNAS OF ALAMOUTI WITH CODE RATE ONE [14].

	Antenna-I	Antenna-II
Time slot-I	$\hat{s}_1$	$\hat{s}_2$
Time slot-II	$-\hat{s}_2^*$	$\hat{s}_1^*$

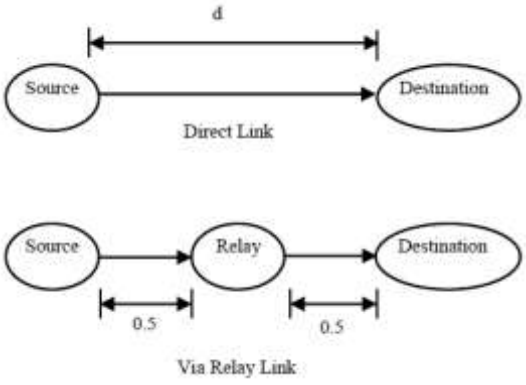


Figure 2. Direct link and via relay link

C. Received Signal at Destination:

At time t the signal y_t^i, received at antenna j of destination, is given by

$$y_t^i = \sum_{i=1}^{n} P_{i,j}^{RD} \alpha_{i,j} \hat{s}_t^i + \eta_t^j \quad (6)$$

where, y_t^j is the received symbol on the j^{th} receiver antenna of destination at time t

$p_{i,j}^{RD}$ is path loss from transmit antenna i of relay to receive antenna j of destination and $p_{i,j}^{RD} \alpha \frac{1}{d_{RD}^2}$

TABLE II. THE ENCODING AND TRANSMISSION SEQUENCE FOR THREE TRANSMIT ANTENNAS OF TAROKH WITH CODE RATE ¾ .

Time slot	Antenna		
	Antenna-I	Antenna-II	Antenna-III
Time slot-I	$\hat{s}_1$	$\hat{s}_2$	$\frac{\hat{s}_3}{\sqrt{2}}$
Time slot-II	$-\hat{s}_2^*$	$\hat{s}_1^*$	$\frac{\hat{s}_3}{\sqrt{2}}$
Time slot-III	$\frac{\hat{s}_3^*}{\sqrt{2}}$	$\frac{\hat{s}_3^*}{\sqrt{2}}$	$\frac{-\hat{s}_1-\hat{s}_1^*+\hat{s}_2-\hat{s}_2^*}{2}$
Time slot-IV	$\frac{s_3^*}{\sqrt{2}}$	$-\frac{s_3^*}{\sqrt{2}}$	$\frac{\hat{s}_2+\hat{s}_2^*+\hat{s}_1-\hat{s}_1^*}{2}$

TABLE III. THE ENCODING AND TRANSMISSION SEQUENCE FOR FOUR TRANSMIT ANTENNAS OF TAROKH WITH CODE RATE ¾

Time slot	Antenna			
	Antenna-I	Antenna-II	Antenna-III	Antenna-IV
Time slot-I	$\hat{s}_1$	$\hat{s}_2$	$\frac{\hat{s}_3}{\sqrt{2}}$	$\frac{\hat{s}_3}{\sqrt{2}}$
Time slot-II	$-\hat{s}_2^*$	$\hat{s}_1^*$	$\frac{\hat{s}_3}{\sqrt{2}}$	$-\frac{\hat{s}_3}{\sqrt{2}}$
Time slot-III	$\frac{\hat{s}_3^*}{\sqrt{2}}$	$\frac{\hat{s}_3^*}{\sqrt{2}}$	$\frac{-\hat{s}_1-\hat{s}_1^*+\hat{s}_2-\hat{s}_2^*}{2}$	$\frac{-\hat{s}_1-\hat{s}_2^*+\hat{s}_1-\hat{s}_1^*}{2}$
Time slot-IV	$\frac{s_3^*}{\sqrt{2}}$	$-\frac{s_3^*}{\sqrt{2}}$	$\frac{\hat{s}_2+\hat{s}_2^*+\hat{s}_1-\hat{s}_1^*}{2}$	$\frac{\hat{s}_1+\hat{s}_1^*+\hat{s}_2-\hat{s}_2^*}{2}$

$\alpha_{i,j}$ is the channel from transmit antenna i to receive antenna j .

$\hat{s}_t^i$ is the transmitted symbol from transmit antenna i at each time slot t .

η_t^j is the noise on j^{th} receive antenna of destination at time slot t .

It is considered that $A_{i,j} = P_{i,j}^{RD}\alpha_{i,j}$, then (6) can be rewrite as:

$$y_t^j = \sum_{i=1}^{n} A_{i,j}\hat{s}_t^i + \eta_t^j \quad (7)$$

D. Decoding at Destination

The combiner combines received signals of destination which are then sent to the maximum likelihood detector. For detecting symbols $\hat{s}_1$ and $\hat{s}_2$ of two transmit antennas, (8) and (9) decision metrics have been used [40, 41]:

$$\left|\left[\sum_{j=1}^{m}\left(y_1^j A_{1,j}^* + \left(y_2^j\right)^* A_{2,j}\right)\right] - \hat{s}_1\right|^2 + \left(-1+\sum_{j=1}^{m}\sum_{i=1}^{2}\left|A_{i,j}\right|^2\right)\left|\hat{s}_1\right|^2 \quad (8)$$

$$\left|\left[\sum_{j=1}^{m}\left(y_1^j A_{2,j}^* - \left(y_2^j\right)^* A_{1,j}\right)\right] - \hat{s}_2\right|^2 + \left(-1+\sum_{j=1}^{m}\sum_{i=1}^{2}\left|A_{i,j}\right|^2\right)\left|\hat{s}_2\right|^2 \quad (9)$$

Similarly, for detecting the symbols of three and four transmit antennas, we can use the decision metrics mentioned in [40, 41]. The detected symbols are demodulated by a QPSK or 16 QAM or 64 QAM demodulator to get the output.

III. SIMULATION RESULTS

In this section, computer simulation is carried out to show the BER performance of the proposed system. The results are evaluated for several combinations of T_x and R_x antennas with and without relay. 64 QAM is used for simulation. It is assumed that the channel is flat fading. The path gains are modeled as samples of independent complex Gaussian random variables with variance 0.5 per real dimension and path gains are constant over a frame of length l and vary from one frame to another. It is assumed that the noise on each receive antenna is independent from the noise on the other receive antennas and noise samples are independent samples of a zero-mean complex Gaussian random variable with variance n/(2SNR) per complex dimension. The average energy of the symbols transmitted from each antenna is normalized to be one.

It is also considered that relay is placed at the middle of source and destination. However, impact of location of relay is also shown in fig. 12. We used two terms in fig.3-fig .11: Direct Link (DL) and Via Relay Link (VRL). DL means that information pass from source to destination without relay. On the other hand, VRL means that information pass from source to relay and then from relay to destination as shown in fig. 2.

Fig. 3 shows the performance of DL and VRL where source has 1 T_x, destination has 2 R_x, relay has 2 T_x and 2 R_x or 3 R_x or 4 R_x .It is observed that VRL provides 13 dB, 18 dB and 20 dB gain compared to DL at 10^{-5} for 2 R_x, 3 R_x, 4R_x of relay respectively. BER of VRL of 1 T_x at source and relay and 1 R_x at relay and destination is also

compared with DL of 1 T_x at source and 1 R_x at destination. There is around 9dB gain for using VRL of the SISO configuration at 10^{-3}compare to DL. And there is around 20-25 dB gain for using MIMO (2 T_x and 2 or 3 or 4 R_x) relaying compare to SISO relaying at 10^{-4}.

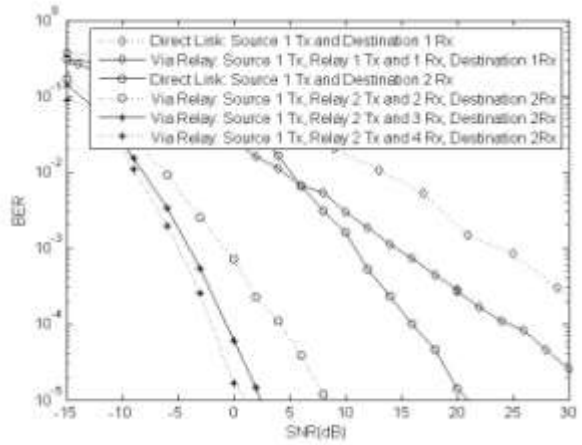


Figure 3. BER performance comparision of direct link and via relay link for 1Tx at source, 1 or 2Rx at destination and 1 T_x or 2T_x & 1 R_x or 2R_x or 3R_x or 4R_x at relay

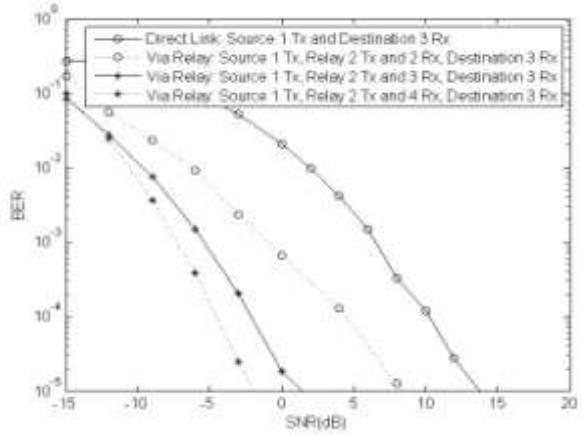


Figure 4. BER performance comparision of direct link and via relay link for 1Tx at source, 3Rx at destination and 2T_x & 2R_x or 3R_x or 4R_x at relay

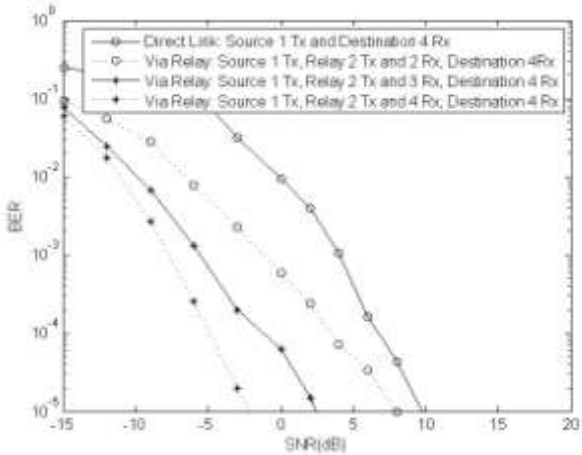


Figure 5. BER performance comparision of direct link and via relay link for 1Tx at source, 4Rx at destination and 2T_x & 2R_x or 3R_x or 4R_x at relay

Fig. 4 shows the performance of DL and VRL where source has 1 T_x, destination has 3 R_x, relay has 2 T_x and 2 R_x or 3 R_x or 4 R_x .It is observed that VRL provides 5 dB, 12 dB and 15 dB gain compared to DL at 10^{-5} for 2 R_x, 3 R_x, 4R_x of relay respectively. And there are around 1-7 dB gains for increasing R_x antennas of destination from 2 to 3 with same diversity of the system.

Fig. 5 shows the performance of DL and VRL where source has 1 T_x, destination has 4 R_x, relay has 2 T_x and 2 R_x or 3 R_x or 4 R_x .It is observed that VRL provides 2 dB, 7 dB and 12 dB gain compared to DL at 10^{-5} for 2 R_x, 3 R_x, 4R_x of relay respectively. And there are around 1- 4 dB gains for increasing R_x antennas of destination from 3 to 4 with same diversity of the system.

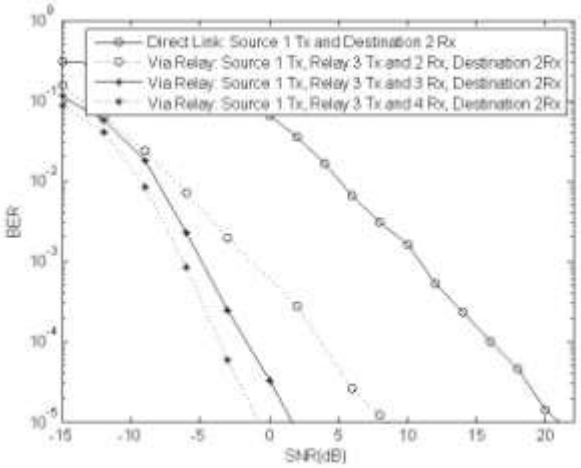


Figure 6. BER performance comparision of direct link and via relay link for 1Tx at source, 2Rx at destination and 3T_x & 2R_x or 3R_x or 4R_x at relay

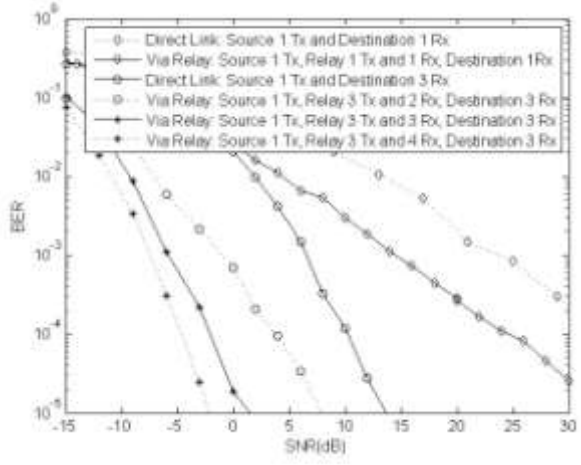


Figure 7. BER performance comparision of direct link and via relay link for 1Tx at source,1 or 3Rx at destination and 1 T_x or 3T_x & 1 R_x or2R_x or 3R_x or 4R_x at relay

Fig. 6 shows the performance of DL and VRL where source has 1 T_x, destination has 2 R_x, relay has 3 T_x and 2 R_x or 3 R_x or 4 R_x. It is observed that VRL provides 13 dB, 19 dB and 22 dB gain compared to DL at 10^{-5} for 2 R_x, 3 R_x, 4R_x of relay respectively.

Fig. 7 shows the performance of DL and VRL where source has 1 T_x, destination has 3 R_x, relay has 3 T_x and 2

R_x or 3 R_x or 4 R_x .It is observed that VRL provides 6 dB, 13 dB and 16 dB gain compared to DL at 10^{-5} for 2 R_x, 3 R_x, 4R_x of relay respectively. And there are around 1-7 dB gains for increasing R_x antennas of destination from 2 to 3 with same diversity of the system. There is around 21-28 dB gain for using MIMO (3 T_x and 2 or 3 or 4 R_x) relaying compare to SISO relaying at 10^{-4}.

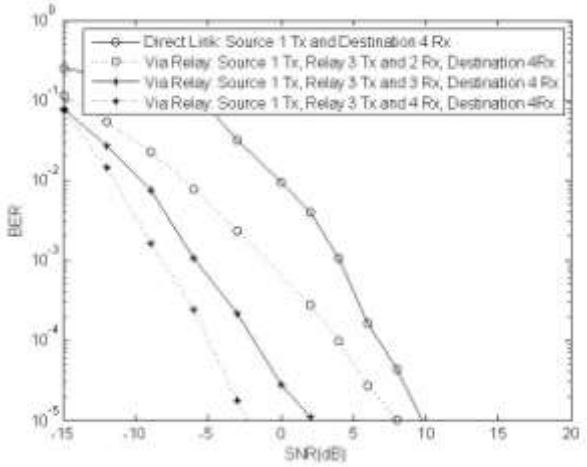


Figure 8. BER performance comparision of direct link and via relay link for 1Tx at source, 4 Rx at destination and 3T_x & 2R_x or 3R_x or 4R_x at relay

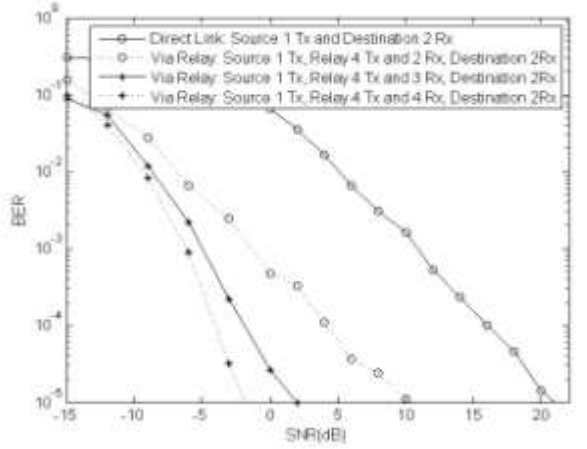


Figure 9. BER performance comparision of direct link and via relay link for 1Tx at source, 2Rx at destination and 4T_x & 2R_x or 3R_x or 4R_x at relay

Fig. 8 shows the performance of DL and VRL where source has 1 T_x, destination has 4 R_x, relay has 3 T_x and 2 R_x or 3 R_x or 4 R_x .It is observed that VRL provides 1 dB, 7 dB and 12 dB gain compared to DL at 10^{-5} for 2 R_x, 3 R_x, 4R_x of relay respectively. And there are around 4-6 dB gains for increasing R_x antennas of destination from 1 to 4 with same diversity of the system.

Fig. 9 shows the performance of DL and VRL where source has 1 T_x, destination has 2 R_x, relay has 4 T_x and 2 R_x or 3 R_x or 4 R_x .It is observed that VRL provides 10 dB, 18 dB and 22 dB gain compared to DL at 10^{-5} for 2 R_x, 3 R_x, 4R_x of relay respectively.

Fig. 10 shows the performance of DL and VRL where source has 1 Tx, destination has 3 Rx, relay has 4 Tx and 2 Rx or 3 Rx or 4 Rx .It is observed that VRL provides 6 dB, 13 dB and 16 dB gain compared to DL at 10^{-5} for 2 Rx, 3 Rx, 4Rx of relay respectively. And there are around 6-7 dB gains for increasing Rx antennas of destination from 1 to 7 with same diversity of the system.

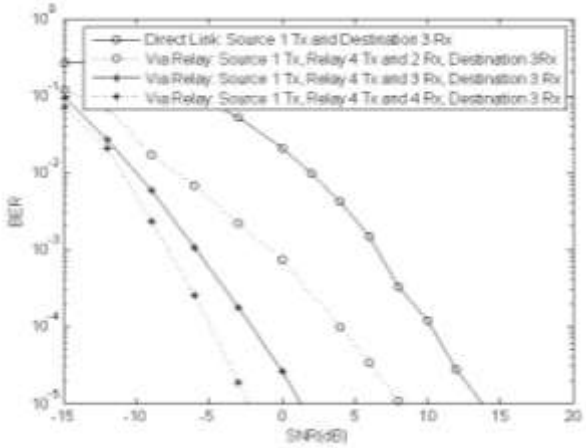


Figure 10. BER performance comparision of direct link and via relay link for 1Tx at source, 4Rx at destination and 3T_x & 2R_x or 3R_x or 4R_x at relay

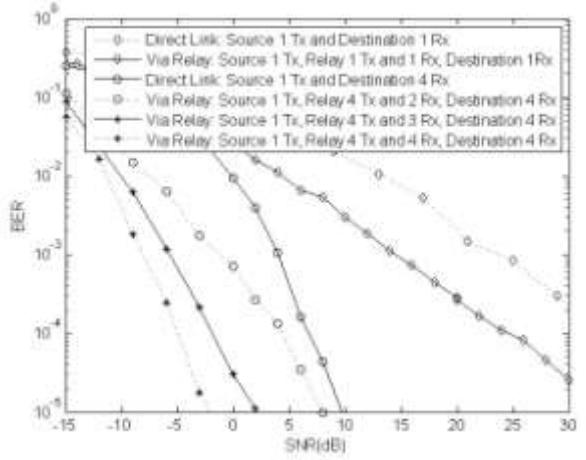


Figure 11. BER performance comparision of direct link and via relay link for 1Tx at source, 1 Rx or 4Rx at destination and 1 T_x or 2T_x & 2R_x or 1 Rx or 3R_x or 4R_x at relay

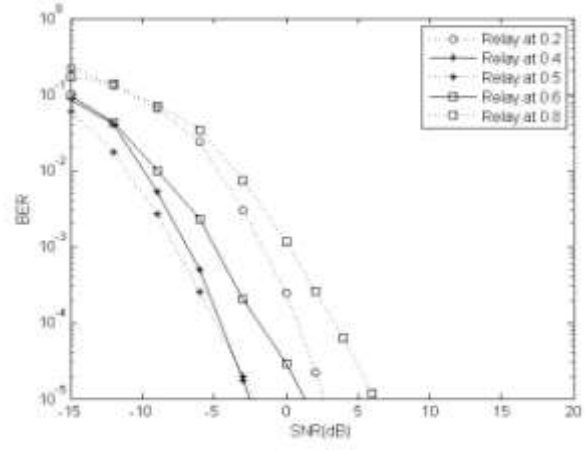


Figure 12. BER performance comparisons of wireless uplink for placing relay at different position where relay is equipped with 2T_x & 4R_x and destination is equipped with 4 Rx

Fig. 11 shows the performance of DL and VRL where source has 1 Tx, destination has 4 Rx, relay has 4 Tx and 2 Rx or 3 Rx or 4 Rx .It is observed that VRL provides 2 dB, 7 dB and 12 dB gain compared to DL at 10^{-5} for 2 Rx, 3 Rx, 4Rx of relay respectively. And there are around 1-4 dB gains for increasing R_x antennas of destination from 3 to 4 with same diversity of the system. There is around 21-28 dB gain for using MIMO (3 T_x and 2 or 3 or 4 R_x) relaying compare to SISO relaying at 10^{-4}.

Fig. 12 shows the performance of wireless uplink for placing relay at different position (at 0.2, 0.4, 0.5, 0.6 and 0.8) where relay is equipped with 2Tx & 4Rx and destination is equipped with 4 Rx .It is observed that relay at 0.8 shows the worst performance. Relay at 0.6, 0.5, 0.4 and 0.2 provides 5 dB, 8 dB, 8 dB and 3 dB gains at 10-5 respectively compared to relay at 0.8. And relay at 0.5 and 0.4 shows the best performance.

IV. CONCLUSION

From the simulations results, it is observed that relay assisted uplink wireless communication makes a significant difference over direct uplink wireless communication. It is also observed that increasing number antennas in relay as well as destination also improve the performance remarkably. It is possible to get 1 dB to 22 dB gains at 10^{-5} by placing relay between source and destination having multiple transmit and receive antennas at relay as well as multiple receiving antennas at destination. There is around 1 dB to 7 dB gains for increasing number of antennas of relay from 2 to 3 or 3 to 4.

ACKNOWLEDGMENT

The author would like to thank the reviewers for the suggestions which help to improve the quality of this paper. In addition, the author is also very thankful to Key Lab of Information Coding & Transmission, Southwest Jiaotong University, Chengdu, Sichuan, China for providing resources.

REFERENCES

[1] J. N. Laneman, D. N. Tse and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behaviour," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[2] P. A. Anghel and M. Kaveh, "Exact symbol error probability of a cooperative network in a Rayleigh-fading environment," *IEEE Trans. Wireless Commun.*, vol. 3, pp 1416–1421, Sept. 2004.

[3] Ribeiro, X. Cai, and G. B. Giannakis, "Symbol error probabilities for general cooperative links," *IEEE Trans. Wireless Commun.*, vol. 4, pp. 1264–1273, May 2005.

[4] Y. -W. Peter Hong, Wan-Jen Huang and C. -C. Jay Kuo, Cooperative Communications and Networking technologies and system design, Springer. 2010.

[5] Canpolat, O..; Uysal, M..; Fareed, M. M.; , "Analysis and Design of Distributed Space–Time Trellis Codes With Amplify-and-Forward Relaying," Vehicular Technology, IEEE Transactions on, vol. 56, no. 4, pp. 1649-1660, July 2007

[6] Berger, S.; Kuhn, M.; Wittneben, A.; Unger, T.; Klein, A.; , "Recent advances in amplify-and-forward two-hop relaying," Communications Magazine, IEEE, vol. 47, no. 7, pp. 50-56, July 2009

[7] Abdaoui, A.; Ikki, S. S.; Ahmed, M. H.; , "Performance Analysis of MIMO Cooperative Relaying System Based on Alamouti STBC and Amplify-and-Forward Schemes," *Communications (ICC), 2010 IEEE International Conference on*, vol., no., pp. 1-6, 23-27 May 2010

[8] Vien, N. H.; Nguyen, H. H.; Le-Ngoc, T.; , "Diversity analysis of smart relaying over Nakagami and Hoyt generalised fading channels," *Communications, IET*, vol. 3, no. 11, pp. 1778-1789, November 2009

[9] Heesun Park; Joohwan Chun; , "Alternate Transmission Relaying Schemes for MIMO Wireless Networks," *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, vol., no., pp. 1073-1078, March 31 2008-April 3 2008

[10] Ho Van Khuong; Tho Le-Ngoc; , "A bandwidth-efficient cooperative relaying scheme with space-time block coding and iterative decoding," *Communications and Electronics, 2008. ICCE 2008. Second International Conference on*, vol., no., pp. 262-267, 4-6 June 2008

[11] Janani, M.; Hedayat, A.; Hunter, T. E.; Nosratinia, A.; , "Coded cooperation in wireless communications: space-time transmission and iterative decoding," *Signal Processing, IEEE Transactions on*, vol. 52, no. 2, pp. 362-371, Feb. 2004

[12] Abouei, J.; Bagheri, H.; Khandani, A.; , "An efficient adaptive distributed space-time coding scheme for cooperative relaying," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 10, pp. 4957-4962, October 2009

[13] Zhang, C.; Zhang, J.; Yin, H.; Wei, G.; , "Selective relaying schemes for distributed space-time coded regenerative relay networks," *Communications, IET*, vol. 4, no. 8, pp. 967-979, May 21 2010

[14] Tourki, K.; Alouini, M. -S.; Deneire, L.; , "Blind Cooperative Diversity Using Distributed Space-Time Coding in Block Fading Channels," *Communications, 2008. ICC '08. IEEE International Conference on*, vol., no., pp. 4596-4600, 19-23 May 2008

[15] Duong, T. Q.; Alexandropoulos, G. C.; Zepernick, H.; Tsiftsis, T. A.; , "Orthogonal Space–Time Block Codes With CSI-Assisted Amplify-and-Forward Relaying in Correlated Nakagami- m Fading Channels," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 3, pp. 882-889, March 2011

[16] Feng Tian; Wei Zhang; Wing-Kin Ma; Ching, P. C.; , "Distributed Space-Time Coding for Two-Path Successive Relaying," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, vol., no., pp. 1-5, 6-10 Dec. 2010

[17] Torabi, M.; Haccoun, D.; , "Performance analysis of cooperative diversity systems with opportunistic relaying and adaptive transmission," *Communications, IET*, vol. 5, no. 3, pp. 264-273, Feb. 11 2011

[18] Le Quang Vinh Tran; Berder, O.; Sentieys, O.; , "Non-regenerative full distributed space-time codes in cooperative relaying networks," *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, vol., no., pp. 1529-1533, 28-31 March 2011

[19] Mimura, T.; Kuwabara, A.; Murata, H.; Yamamoto, K.; Yoshida, S.; , "Packet Transmission Experiments of STBC-Based Multi-Hop Cooperative Relaying," *Communications (ICC), 2011 IEEE International Conference on*, vol., no., pp. 1-5, 5-9 June 2011

[20] Sharma, G. V. V.; Ganwani, V.; Desai, U. B.; Merchant, S. N.;, "Performance Analysis of Maximum Likelihood Detection for Decode and Forward MIMO Relay Channels in Rayleigh Fading," *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, vol., no., pp. 1-6, 5-8 April 2009
[21] Miyano, T.; Murata, H.; Araki, K.;, "Cooperative relaying scheme with space time code for multihop communications among single antenna terminals," *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, vol. 6, no., pp. 3763- 3767 Vol. 6, 29 Nov. -3 Dec. 2004
[22] Mheidat, H.; Uysal, M.;, "Space-Time Coded Cooperative Diversity with Multiple-Antenna Nodes," *Information Theory, 2007. CWIT '07. 10th Canadian Workshop on*, vol., no., pp. 17-20, 6-8 June 2007
[23] Fan, Y.; Thompson, J.; , "MIMO Configurations for Relay Channels: Theory and Practice," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 5, pp. 1774-1786, May 2007
[24] Yang, Q.; Kwak, K. S.; , "Outage performance of cooperative relaying with dissimilar Nakagami-m interferers in Nakagami-m fading," *Communications, IET*, vol. 3, no. 7, pp. 1179-1185, July 2009
[25] In-Ho Lee; Dongwoo Kim; , "Achieving maximum spatial diversity with decouple-and-forward relaying in dual-hop OSTBC transmissions," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 3, pp. 921-925, March 2010
[26] Bastami, A. H.; Olfat, A.; , "Optimal SNR-based selection relaying scheme in multi-relay cooperative networks with distributed space-time coding," *Communications, IET*, vol. 4, no. 6, pp. 619-630, April 16 2010
[27] Maham, B.; Hjorungnes, A.; , "Opportunistic relaying for space-time coded cooperation with multiple antennas terminals," *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, vol., no., pp. 251-255, 13-16 Sept. 2009
[28] Abdaoui, A.; Ikki, S. S.; Ahmed, M. H.; Châtelet, E.; , "On the Performance Analysis of a MIMO-Relaying Scheme With Space–Time Block Codes," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 7, pp. 3604-3609, Sept. 2010
[29] Van Khuong, H.; Le-Ngoc, T.; , "Performance analysis of a decode-and-forward cooperative relaying scheme for MIMO systems," *Communications (QBSC), 2010 25th Biennial Symposium on*, vol., no., pp. 400-403, 12-14 May 2010
[30] Dharmawansa, Prathapasinghe; McKay, Matthew R.; Mallik, Ranjan K.;, "Analytical Performance of Amplify-and-Forward MIMO Relaying with Orthogonal Space-Time Block Codes," *Communications, IEEE Transactions on*, vol. 58, no. 7, pp. 2147-2158, July 2010
[31] Kamruzzaman, M. M.; Azad, M. M., "Single Input Multiple Output (SIMO) Wireless Link with Turbo Coding", International Journal of Advanced Computer Science and Applications, Vol. 1, No. 5, pp. 69-73, November 2010.
[32] Kamruzzaman, M. M., "Performance of Turbo Coded Wireless Link for SIMO Using SC EGC and MRC," Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on, vol., no., pp. 191, 194, 2-4 Nov. 2012
[33] Kamruzzaman, M. M.; Li Hao, "Performance of Turbo-SISO, Turbo-SIMO, Turbo-MISO and Turbo-MIMO system using STBC," Journal of Communications(JCM), Vol. 6, No. 8, Nov 2011 page 633- 639.
[34] M. M. Kamruzzaman, "Performance of relay sssisted STBC coded MIMO wireless downlink communication" International Journal of Informatics and Communication Technology (IJ-ICT) vol. 3, no. 1. 2014.
[35] Kamruzzaman, M. M., "Performance of Turbo Coded Wireless Link for SISO, SIMO, MISO and MIMO System," Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on, vol., no., pp. 187, 190, 2-4 Nov. 2012
[36] Kamruzzaman, M. M. "Performance Comparison of Space Time Block Coding with Code Rate ½ and ¾ for Turbo Coded Multiple Input Multiple Output System. " International Journal of Information and Network Security (IJINS) 2. 6 (2014): 482-491.
[37] Kamruzzaman, M. M., "Performance of Turbo coded wireless link for SISO-OFDM, SIMO-OFDM, MISO-OFDM and MIMO-OFDM system," Computer and Information Technology (ICCIT), 2011 14th International Conference on, vol., no., pp. 185-190, 22.
[38] Ka**mr**uzzaman, M. M.; Li Hao, "Performance of Turbo coded OFDM wireless link for SISO, SIMO, MISO and MIMO system," Journal of Communications (JCM) Volume: 7 Issue: 11 Pages: 795-802, Nov. 2012.
[39] Kamruzzaman, M. M.," Performance of decode and forward MIMO relaying for wireless uplink," Computer and Information Technology (ICCIT), 2012 15th International Conference on, vol., no., pp. 321, 325, 22-24 Dec. 2012.
[40] S. M. Alamouti," A simple transmit diversity scheme for wireless communications," IEEE J. Selected. Areas Commu., vol 16, no. 8, pp. 1451-1458, Oct. 1998.
[41] Vahid Tarokh, Hamid Jafarkhani and A. Robert Calderbank," Sp**a**ce time block coding for wireless communication: performance result," IEEE J. Select Areas Commun., vol. 17, pp. 451-460, Mar. 1999.

M. M. Kamruzzaman was born in Bangladesh in 1978. He received B.E. degree in Computer Science and Engineering from Bangalore University, Bangalore, India in 2001, M.S. degree in Computer Science and Engineering from United International University, Dhaka, Bangladesh in 2009. At present he is studying PhD in the department of Information & Communication Engineering at Southwest Jiaotong University, Chengdu, Sichuan, China.

After completing B.E, he worked several universities as a faculty. He worked in Islamic Institute of Technology, Bangalore, India and Leading University, Dhaka, Bangladesh. And before studying PhD, he was working as a faculty of Presidency University, Dhaka, Bangladesh. He is a member of TPC of several international conferences and reviewer of few international journals and conferences.

His areas of interest include wireless communications, modern coding theory, Turbo coding, Space Time Coding, VBLAST, MIMO, Multiple Access Channel , OFDM, Relay, WCDMA , WiMAX and LTE system.

On Efficient Design of LDPC Decoders for Wireless Sensor Networks

Duc Minh Pham and Syed Mahfuzul Aziz
School of Engineering, University of South Australia, Mawson Lakes, SA 5095, Australia
Email: {duc.pham, mahfuz.aziz}@unisa.edu.au

***Abstract*—Low density parity check (LDPC) codes are error-correcting codes that offer huge advantages in terms of coding gain, throughput and power dissipation in digital communication systems. Error correction algorithms are often implemented in hardware for fast processing to meet the real-time needs of communication systems. However,traditional hardware implementation of LDPC decoders require large amount of resources, rendering them unsuitable for use in energy constrained sensor nodes of wireless sensor networks (WSN). This paper investigates the use of short-length LDPC codes for error correction in WSN. It presents the LDPC decoder designs, implementation, resource requirement and power consumption to judge their suitability for use in the sensor nodes of WSN. Due to the complex interconnections among the variable and check nodes of LDPC decoders, it is very time consuming to use traditional hardware description language (HDL) based approach to design these decoders. This paper presents an efficient automated high-level approach to designing LDPC decoders using a collection of high-level modelingtools. The automated high-level design methodology provides a complete design flow to quickly and automatically generate, test and investigate the optimum (length) LDPC codes for wireless sensor networks to satisfy the energy constraints while providing acceptable bit-error-rate performance.**

***Index Terms*—Error Correction Coding; Wireless Communication; Wireless Sensor Networks; Digital System; FPGA**

I. INTRODUCTION

Low Density Parity-Check (LDPC) codes [1, 2] are known as the most powerful forward error correction codes with a bit-error-rate (BER) performance closed to the Shannon limit. LDPC codes have been proved to have better performance and several advantages over other error correction codes such as Turbo codes, Hamming codes, Reed-Muller and Reed-Solomon codes [2]. Because of excellent BER, LDPC-codes are extensively used in standards such as WiMAX, 10Gigabit Ethernet (10GBaseT), digital video broadcasting (DVB-S2) and expected to be part of many future standards [3, 4].

Although the decoding algorithm of LDPC is simple, hardware implementation faces several significant challenges. One of the challenges in implementation of fully parallel LDPC decoder is the complexity of the interconnections between the nodes inside the decoder [5]. Especially when the LDPC matrix becomes large, it is almost impossible and time consuming to manually connect and check the connections.In this paper, an automated high-level design methodology is introduced. We propose a design methodology that supports programmable logic design starting from high-level modeling all the way up to FPGA implementation using a collection of high-level modeling tools. The methodology has been used to design and implement LDPC decoders of various code lengths on FPGAs. The simulation and FPGA implementation results obtained are then used to determine suitable LDPC decoders for Wireless Sensor Networks (WSN), which consist of severely resource constrained sensor nodes.

In recent years, WSNs have attracted significant research interests [6-8]. A WSN can be defined as a network of a large number of spatially distributed, small, low cost and low power nodes, which can sense the environment and wirelessly communicate the information gathered to other nodes. The collected information is forwarded, normally via multiple hops, to a sink (or controller or monitor) node that uses the information locally or transmits it to other networks (e.g., Internet) through a gateway. WSNs are normally comprised of scalar sensors capable of measuring physical phenomenon such as temperature, pressure, light intensity, humidity etc. [9]. The abovementioned applications do not have a high bandwidth requirement and are delay tolerant. Recently, several research works have been reported to add small sized and low-power CMOS cameras and microphones to the sensor nodes. Such Wireless Multimedia Sensor Network (WMSN), with the ability to gather multimedia information from the surrounding environment, is providing the impetus for extending the capabilities WSNs for many new applications such as advanced environmental monitoring, advanced health care delivery, traffic avoidance, fire prevention and monitoring, object tracking etc. However, in WMSN, with the large volume of multimedia data generated by the sensor nodes, both processing and transmission of data leads to higher levels of energy consumption. Energy consumption in transmitting large volume of multimedia data can be reduced by using energy-efficient and reliable transmission protocols [10] or reducing the amount of multimedia data [11]. Beside these approaches, efficient error correction decoders can be used to reduce the energy required for communication of the multimedia information. However, the amount of energy spent to transmit the redundant information

doi:10.4304/jnw.9.12.3207-3214

required for error correction and the energy used to perform error correction should be less than the energy saved at the transmitter side for retransmission of erroneous information [12].

Several codes have been investigated for error correction in WSN, including Reed–Solomon codes, convolution codes, turbo codes and LDPC codes [13, 14]. Some preliminary results in [12, 15] suggest that LDPC codes are good candidates for WSN applications as they feature a significant coding gain compared with other codes. LDPC codes are known to achieve nearly the Shannon limit with long code length. However, parallel decoders for long LDPC codes require large hardware and energy consumption and therefore partially parallel decoders were introduced [16]. In WSN, the data exchanged between sensor nodes is usually small [10]. This raises the prospect of using short LDPC codes for error correction in WSN for without compromising the *bit-error-rate* (BER) performance significantly.

Most of the previous works proposing error correction codes for WSNs assume that networks contain only two types of nodes: sensing nodes and base stations. Sensing nodes feature lower computational capabilities and lower available energy than base stations. Thus, sensing nodes send coded information to a central node which performs the decoding operations. In this paper, we investigate the possibility of implementing short length LDPC codes in WSNs where sensor nodes can both encode/transmit and receive/decode information. We show that that LDPC codes with small block length are adequate for typical throughput and data transmission requirements of WSNs.

II. LDPC Codes and Decoding Algorithm

LDPC codes can be represented by an M x N sparse matrix, usually called H matrix. The H matrix contains mostly zeros and a small number of 1s [1, 2]. It can also be represented by a graph called bipartite or Tanner graph as shown in Fig. 1.

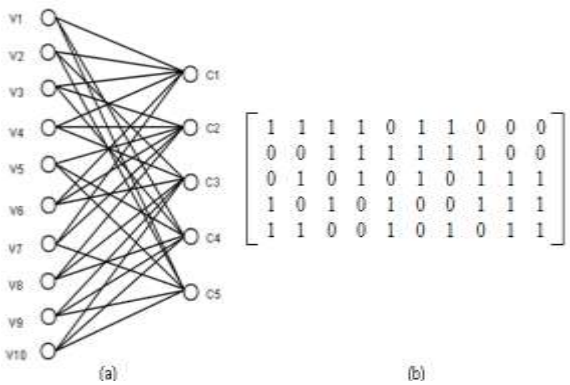


Figure 1. Tanner graph and LDPC matrix of a 5x10 (3,6) code

There are different algorithms which could be used for decoding purposes. We used the min-sum decoding algorithm [17], which is a special case of the sum-product algorithm [18]. Sum-product algorithm reduces the computational complexity and makes the decoder numerically stable [18]. The LDPC decoder consists of a number of variable nodes (v) and check nodes (c). In min-sum decoding algorithm, a variable node performs the operation given in equation (1) and passes the outputs to the check nodes.

$$L_{cv} = \sum_{m \in M(v) \backslash c}^{`} R_{mv} + I_v \qquad (1)$$

where, I_v is the input to variable node v, also known as Log Likelihood ratio (LLR), L_{cv} is the output of variable node v going to check node c, $M(v)\backslash c$ denotes the set of check nodes connected to variable node v excluding the check node c, R_{mv} is the output of check nodes going to variable node v.

A check node receives messages from the variable nodes and performs the operation given by (2):

$$R_{cv} = \prod_{n \in N(c) \backslash v} sign(L_{cv}) \times \min_{n \in N(c) \backslash v} | L_{cv} | \qquad (2)$$

where, R_{cv} is the output of check node c going to variable node v.

Every check node also checks whether the parity condition is satisfied by looking at the sign of the messages coming from the variable nodes. Until the parity conditions are satisfied at all the check nodes the messages are sent back to variable nodes otherwise the decoder stops the process. Min-sum decoding algorithm uses soft decisions. However, hard decision is taken on the new LLR (I_v). If the new LLR is negative then the output bit would be a 1 otherwise a 0.

III. Automated High-Level Design Methodology

The proposed automated high-level design methodology provides a complete design flow to automatically generate and test complex LDPC decoders. As shown in Fig. 2, the methodology has two main parts, namely, automatic generation of decoder models and automatic testing of decoders (presented in Part B of this section).

A. Automatic Generation of LDPC Models and HDL Codes

The automatic LDPC model generation flow shown in Fig. 2 requires two inputs: LDPC library and LDPC matrix. The LDPC library contains two basic hand designed modules, check node (C-node) and variable node (V-node). The LDPC matrix can be preconfigured to any size for (3, 6)-regular LDPC code.

1) Design of Check Node and Variable Node

The C-node has been designed in Simulink using built-in Simulink library blocks. It performs the operation given in (2). The main function of the C-node is to find the minimum of all the inputs to the C-node and to perform parity checks. Several approaches to design the C-node have been evaluated for hardware requirement and speed to choose the most optimized design for the automated design flow. For LDPC (3, 6) code, every C-node has six inputs. First, the C-node was designed using (2), by comparing every set of five inputs separately, to find the minimum. In this approach the hardware

requirement for the C-node is high due to the same comparisons being made multiple times [19]. An optimized *find-minimum-function* is presented in Fig. 3. In this design, a module called *find3min* is used to find the minimum of 3 sets of 4 inputs. For example, *Min1234* is the minimum of input set {1, 2, 3, 4}. Each output of the *find3min* block is then compared with one more input to find the minimum of five inputs. As the outputs of every *fin3min* block are reused, this approach reduces the amount of hardware resources required to implement the *find-minimum-function*. Simulink model of the C-node is shown in Fig. 4. Comparison between the original C-node design in [19] and this optimized C-node design is given in Table I.

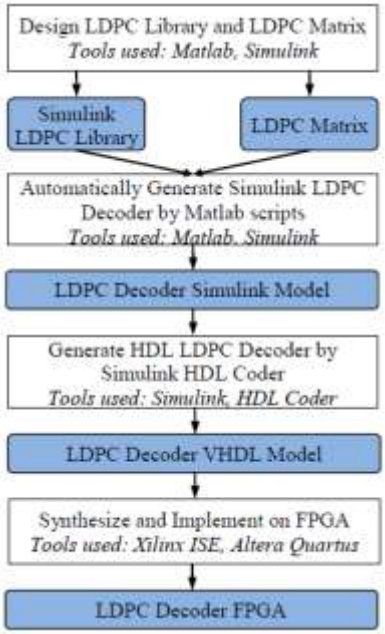


Figure 2. Automated LDPC design flow

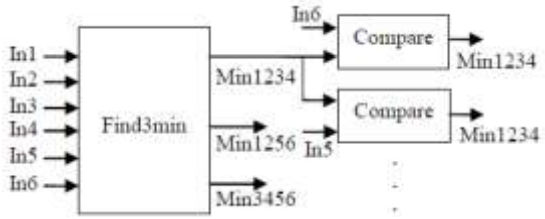


Figure 3. Optimized find-mimimum-function for C-node

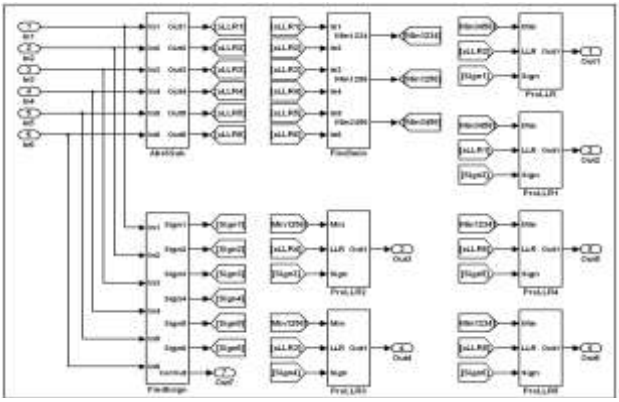


Figure 4. Simulink model of the check node

TABLE I. C-NODE DESIGN COMPARISON

Design	Xilinx XC3S1200E Synthesis Results		
	Slices Used	4-input LUTs Used	Maximum delay
Original C-node	105	186	12.87ns
Optimized C-node	56	98	12.38ns

The V-node has also been designed in Simulink using the basic add block from the Simulink library. The V-node has four inputs, the first three come from various check nodes and the fourth one is the raw LLR, which is an external input supplied by the host communication system. It performs the operation given in (1) and passes the outputs to the C-nodes it is connected to. Simulink model of V-node is shown in Fig. 5.

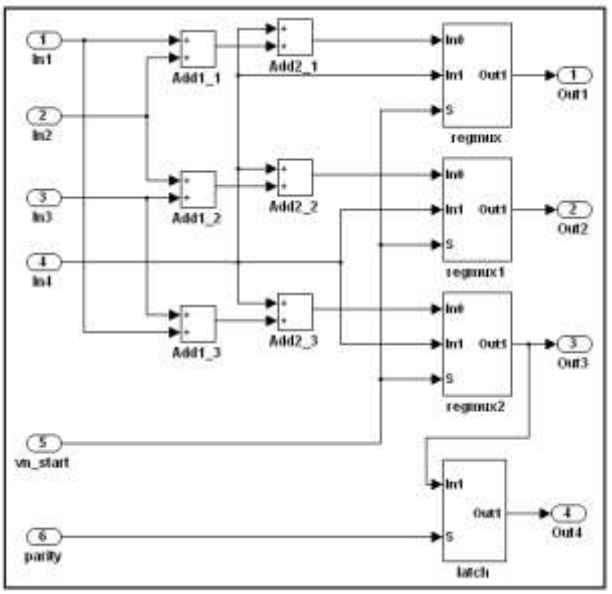
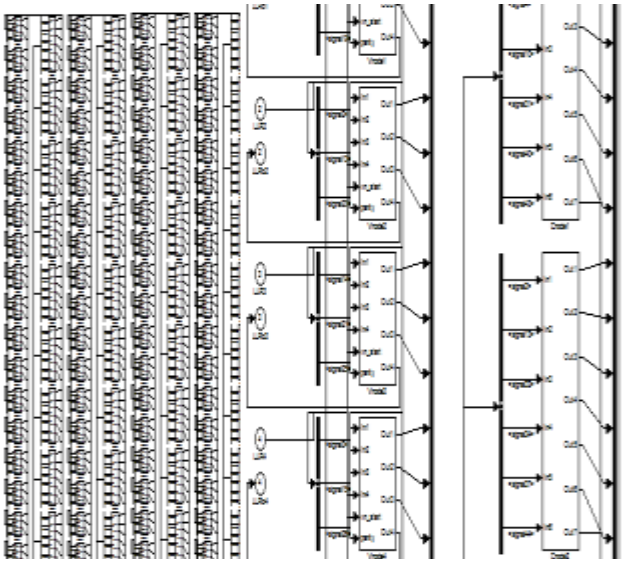


Figure 5. Simulink model of the variable node

2) Auto-generation of Decoder Models

The auto-generation of decoder models is accomplished using Matlab scripts. The Matlab scripts read the LDPC matrix and automatically instantiate the V-nodes and C-nodes to build the corresponding decoder model in Simulink. They also connect the V-nodes and C-nodes according to the LDPC matrix. The routing process is very simple but effective. Each input and output of the V-nodes and C-nodes are marked with a Simulink routing label. The routing labels are specified by the Matlab scripts to build the connections between nodes as required by the LDPC matrix. If a routing label of a V-node input has the same name as that of the routing label of a C-node output then Simulink will understand these two ports to be connected to each other. Fig. 6a shows the layout of the Simulink model of a (200,100) LDPC decoder after it is automatically generated. Fig. 6b shows a zoomed view of the interconnections inside the model.

Once a Simulink decoder model is generated by the Matlab script, it can be used to automatically generate a HDL model using the Simulink HDL Coder tool. Either VHDL or Verilog can be chosen as the target HDL. The generated HDL code is vendor independent, and can be synthesized and implemented on most FPGAs.



(a) (b)

Figure 6. (a) Generated Simulink model of a LDPC decoder. (b) magnified view of the model in (a).

B. Automatic Testing Strategy

The proposed automatic model generation process is complemented with a comprehensive automatic testing strategy. It comprises an automatic process of generating and encoding test data, inserting noise, quantization and application of the final test data to the decoder under test. The Matlab and Simulink environments used in this high-level design methodology provide an efficient and fast mechanism to build a full test system for the entire design. The proposed testing strategy is comprehensive as it allows for testing the decoder at all possible levels of the hierarchy: Simulink model, HDL model and FPGA implementation. Fig. 7 shows the proposed testing strategy.

The Matlab Test Data Generator module generates a sequence of LDPC encoded test data. These test data are written to text files, which are then supplied as inputs while executing the Simulink model, the HDL model as well as to run the decoder implemented on FPGA. After decoding is done in the three environments, the results are written to separate text files. The Matlab LDPC Test Data Analyzer module will compare the results and produce the report on the consistency or otherwise of the results. The Analyzer will also produce performance plot of the decoder, e.g. bit-error-rate (BER) as a function of Eb/N0. This scheme has been used to test and validate the decoder designs presented in this paper.

IV. FPGA IMPLEMENTATION AND TESTING

We have successfully implemented and tested the decoders generated by our automation methodology on Xilinx FPGA boards. Fig. 8 illustrates the arrangement used for testing the designs. The hardware platform contains three modules: the USB communication module for communicating with the PC, the main FPGA module and the I/O module. As described in the automatic testing strategy, the LLRs generated by the MATLAB program are stored in text files. A LabVIEW program running on the PC sends these LLRs to the decoder via the USB module and receives the decoded LLRs back along with the parity information. The decoded LLRs are written into a separate file by the LabVIEW program and analyzed for correctness by a MATLAB program by comparing with the LLRs generated by simulation of the Simulink and/or VHDL models.

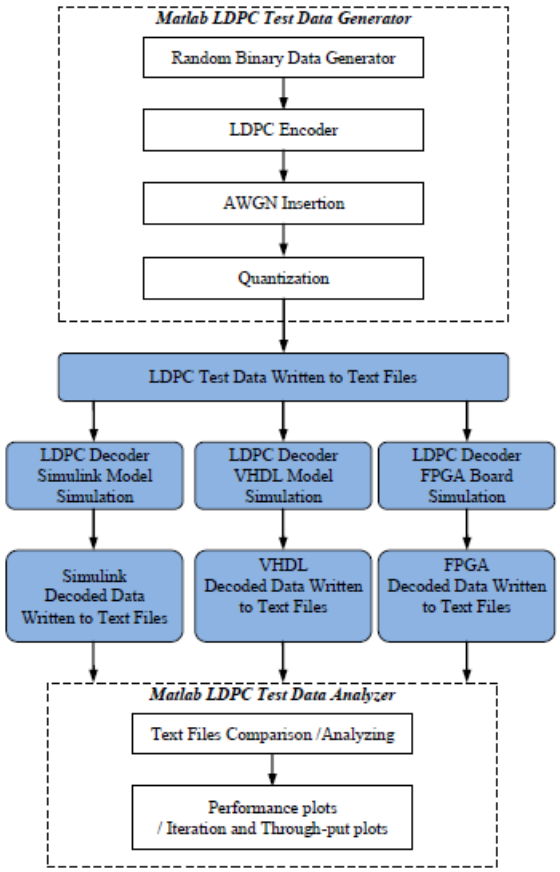


Figure 7. Comprehensive automatic test and simulation flow

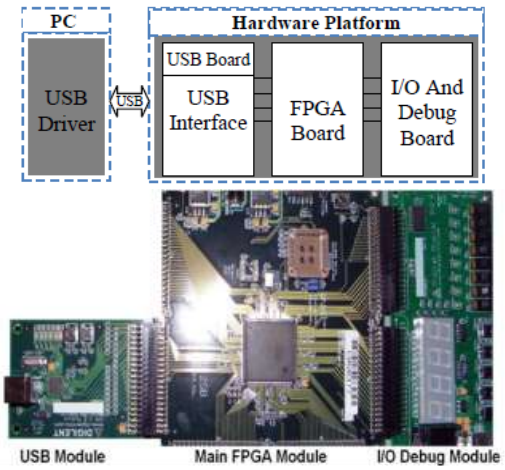


Figure 8. Hardware setup for testing LDPC decoders

V. RESULTSAND ANALYSIS

A. Synthesis Results

All the decoders generated by the proposed automation methodology are synthesizable for implementation on a

range of FPGAs. Table II shows the FPGA resources required for fully parallel architectures of various decoder sizes. Because of the resource constraints of the Spartan 3E FPGA we used, an LDPC decoder with a maximum block length of 200 with 2-bit quantization (LLRs) was implemented and successfully tested. The proposed automated methodology can be used to implement decoders with larger block lengths and higher quantization levels as long as the target FPGA has the required amount of resources. The proposed automated model generation and testing regimes are fully parameterized for block length and quantization, making it a very flexible and efficient design and implementation method for investigating alternative design choices.

TABLE II. SYNTHESIS RESULTS

Design	Xilinx FPGA	Synthesis Results			
		SlicesUsed	LUTs Used	FFs Used	Fmax
(50,25) 4-bit LLRs	XC3S1200E	3478	6423	800	61.34 MHz
(100,50) 4-bit LLRs	XC3S1200E	6445	12591	1600	59.91 MHz
(200,100) 2-bit LLRs	XC3S1200E	4122	9856	800	83.2 MHz
(200,100) 4 bit LLRs	XC5VLX110T	2450	17018	3200	153.45 MHz
(400,200) 4-bit LLRs	XC5VLX110T	4925	34445	6400	152.34 MHz

B. Iteration Convergence Test

The convergence characteristics of LDPC decoders implemented on FPGAs have been plotted. The number of iterations taken by each set of LLR is monitored by a counter on the FPGA and the final iteration count is sent to the PC. A Matlab script reads all iteration counts at each E_b/N_0 and calculates the average iteration count. Fig. 9 shows the spread of the average number of iterations for a (200,100) LDPC decoder versus E_b/N_0 with maximum iteration set to 10.

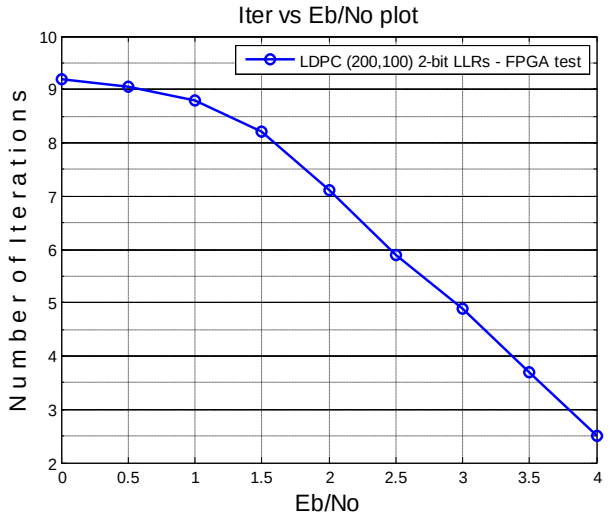


Figure 9. Spread of iterations for a (200,100) LDPC design

C. Throughput and Algorithm Performance Test

Because of the fully parallel architecture, the decoders presented in this paper have very good throughput in comparison with LDPC designs reported in literature [16, 20-24]. The throughput (T) of the decoder is calculated as follows:

$$T = \frac{rate \times blocklengt\ h \times fmax}{Nit * \gamma} \quad (3)$$

We calculate the throughput (at 3.5dB E_b/N_0) of the (200,100) decoder that was implemented on a Spartan 3E FPGA device (XC3S1200E). As per Table II, the block-length is 200, code rate is $1/2$and γ =1, where γ is the number of clock cycles needed to complete one iteration. Fig. 9 shows that at 3.5dB the average number of iterations ($N_{it)}$ is approximately 3.7. From Table II, the maximum clock frequency for the selected FPGA device is 83.2MHz. Using these values in (3), the throughput of the implemented LDPC decoder at 3.5dB is 2.25Gbps. For decoders with higher block lengths implemented on high end FPGAs, much higher throughputs (exceeding 10Gbps) is possible.Fig.10 shows the BER performance obtained from the FPGA test and simulation results of a few LDPC decoders designed using the proposed methodology. As expected, it shows that the BER improves when the code length is increased. However, it is important to ensure that the resource requirement does not increase significantly leading to higher power consumption.

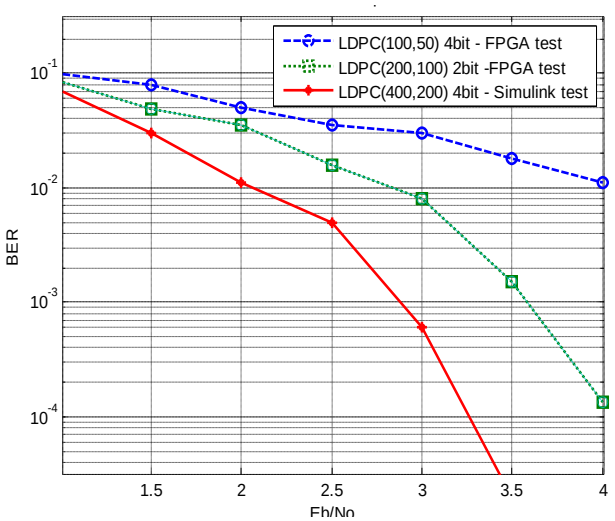


Figure 10. Performance comparison of various LDPC decoders

D. Analysis of theAutomatic High-Level Design Methodology

As the LDPC design gets larger and larger, it becomes very difficult to manually code and connect all the variable and check nodes usinga hardware description language (HDL). The high-level automated design methodology presented in this paper reduces design complexity, effort and time drastically. In comparison with the work introduced in [19], this automation methodology has helped reduce the design time and effort dramatically. Importantly, italso greatly enhances the ability tomanage and reuse complex design blocks. Design reuse requires much less effort because changes are easily made at block level in Simulink. In addition, Matlab is a high-level programming language that is used

much more widely than hardware description languages such as VHDL and Verilog. Therefore, designers without specific skills in HDLs are able to design complex digital systems without much problem. Even software engineers and algorithm developers are able to quickly implement and test their high-level designs due to the ability to automatically generate HDL descriptions from the Simulink models. This will surely offer great flexibility and efficiency in the design and reuse of complex LPDC decoders.

VI. Implications of the Results for WSN

Recent applications of wireless sensor networks have highlighted the importance of energy efficiency in hardware processing in the sensor nodes [25]-[26]. The proposed automation methodology has been used to quickly design, test and analyze the characteristics of LDPC decoders of various code lengths targeting Xilinx FPGAs. The complete design flow, including synthesis, place and route has been performed using Xilinx ISE 14. Xilinx Power Analyzer has been used to estimate the power consumption. The dynamic power consumption results for all the tested decoders have been obtainedat 50 MHz and are shown in Table III. Typical leakage power for Spartan 3E FPGA (XC3S1200E) is 159mW and that for a Virtex 5 device (XC5VL50T) is 591mW.

As per Table III, the largest LDPC code that fits into the low-power Spatan3E FPGA (XC3S1200E) is of length (200,100) with a 2-bit LLR. Its power consumption is lower than that of a decoder of length (100, 50) with a 4-bit LLR. The performance plot in Fig.10 shows that the (200,100) decoder with a 2-bit LLR can achieve higher BER performance than the (100, 50) decoder with a 4-bit LLR. Therefore, for emerging WSN applications [10]-[11], a (200,100) decoder with 2-bit LLR is the most suitable choice among the decoders shown in Table III. Recent techniques on reduced complexity LDPC algorithms [27]-[28] are likely to further improve the energy efficiency by reducing resource requirement and consequently the power consumption for LDPC decoding.

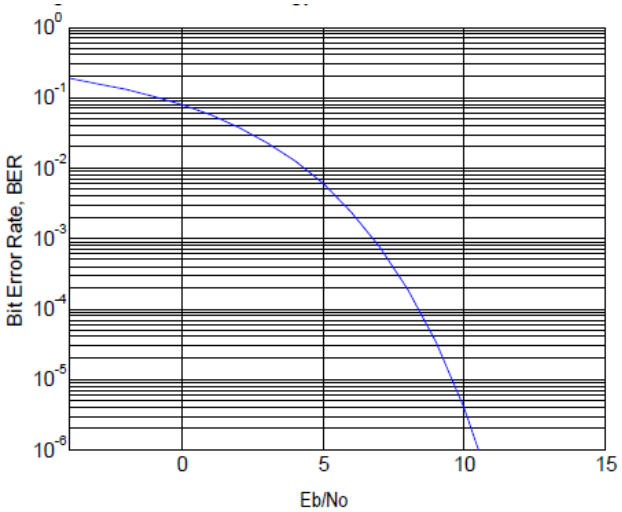


Figure 11. Uncoded WSN data stream with OQPSK

Fig. 10 shows that the BER of the (200,100) decoder with a 2-bit LLR is 10^{-3} at Eb/No=3.6dB. The Eb/No required to achieve this BER in an uncoded data stream (OQPSK) is over 7 dB, as shown in Fig. 11. This means that with LDPC coding the dB value of the transmit signal power can be reduced by half to achieve the same BER as that for an uncoded stream. This will lead to significant savings in transmission energy.

The proposed (200,100) 2-bit LDPC decoder implemented on FPGA has a dynamic power consumption of only 57mW. This is comparable with the power consumption of a larger LDPC decoder of length (1008,504) synthesized on an ASIC [29], the power consumption of the latter being 33.14mW. The difference is that the results presented in this paper are from a practical FPGA implementation, and therefore the real hardware functions and performance have been tested and validated. However, in [29], the reported power consumption is from a synthesized design only. Moreover, ASIC implementations are costly, time consuming and not reprogrammable. Recently, several LDPC decoders have been proposed for wireless sensor networks [15, 29, 30]. However, all of them report results from synthesis of the designs using ASIC design approach, not practical test results from actual ASIC implementation. Therefore, none of them has been validated on hardware.

TABLE III. Power consumption results @25^{O}C, 50MHz

Design	Xilinx FPGA	Dynamic power consumption (mW)
(50,25) 4-bit LLRs	XC3S1200E	38
(100,50) 4-bit LLRs	XC3S1200E	77
(200,100) 2-bit LLRs	XC3S1200E	57
(200,100) 4 bit LLRs	XC5VL50T	159

VII. Conclusions

This paper has presented the designs and practical implementation results of short-length LDPC decoders for wireless sensor networks using a flexible automated methodology. FPGA test results have proved that the design methodology is efficient and error-free. The proposed methodology offers great advantages in terms of reduced design complexity, effort and time. It allows designers to quickly determine the trade-offs between shorter LDPC codes and shorter LLRs versus BER performance. The practical test results presented in the paper have demonstrated that short-length LDPC codes with small LLRs can be used for error correction at low power consumption while providing acceptable bit-error-rate performance. The results of this study are therefore useful to determine optimum LDPC codes for low power applications such as wireless sensor networks.

References

[1] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, pp. 21-28, 1962.

[2] S. J. Johnson, "Introducing low-density parity-check codes," *University of Newcastle, Australia*, 2006.

[3] M. Eroz, F. W. Sun, and L. N. Lee, "DVB-S2 low density parity check codes with near Shannon limit performance," *International Journal of Satellite Communications and Networking*, vol. 22, pp. 269-279, 2004.
[4] T. Mohsenin and B. M. Baas, "Split-Row: A reduced complexity, high throughput LDPC decoder architecture," in *International Conference on Computer Design, ICCD*, San Jose, 2007, pp. 320-325.
[5] A. Darabiha, A. C. Carusone, and F. R. Kschischang, "A bit-serial approximate min-sum LDPC decoder and FPGA implementation," in *IEEE International Symposium onCircuits and Systems, ISCAS, Island of Kos*, 2006.
[6] D. Culler, D. Estrin, and M. Srivastava, "Overview of wireless sensor networks," *IEEE Computer, Special Issue in Sensor Networks*, vol. 37, pp. 41–49, 2004.
[7] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An Overview on Wireless Sensor Networks Technology and Evolution," *Sensors*, vol. 9, p. 6869, 2009.
[8] M. Tubaishat and S. Madria, "Sensor networks: an overview," *IEEE potentials*, vol. 22, pp. 20-23, 2003.
[9] I. Akyildiz, T. Melodia, and K. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks*, vol. 51, pp. 921-960, 2007.
[10] S. M. Aziz and D. M. Pham, "Energy Efficient Image Transmission in Wireless Multimedia Sensor Networks," *IEEE Communications Letters*, vol. 17, pp. 1084 -1087, June 2013.
[11] D. M. Pham and S. M. Aziz, "Object extraction scheme and protocol for energy efficient image communication over Wireless Sensor Networks," *Computer Networks, Elsevier*, Online, July 2013.
[12] E. Sanchez, F. Gandino, B. Montrucchio, and M. Rebaudengo, "Increasing effective radiated power in wireless sensor networks with channel coding techniques," in *International Conference on Electromagnetics in Advanced Applications, ICEAA*, 2007, pp. 403-406.
[13] M. C. Vuran and I. F. Akyildiz, "Error control in wireless sensor networks: a cross layer analysis," *IEEE/ACM Transactions on Networking*, vol. 17, pp. 1186-1199, 2009.
[14] M. Sartipi and F. Fekri, "Source and channel coding in wireless sensor networks using LDPC codes," in *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON*, 2004, pp. 309-316.
[15] A. D. G. Biroli, M. Martina, and G. Masera, "An LDPC Decoder Architecture for Wireless Sensor Network Applications," *Sensors*, vol. 12, pp. 1529-1543, 2012.
[16] V. A. Chandrasetty and S. M. Aziz, "A highly flexible LDPC decoder using hierarchical quasi-cyclic matrix with layered permutation," *Journal of Networks*, vol. 7, pp. 441-449, 2012.
[17] J. Sha, *et al.*, "An FPGA implementation of array LDPC decoder," in *IEEE Asia Pacific Conference on Circuits and Systems, APCCAS*, 2006, pp. 1675-1678.
[18] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*: Pearson-Prentice Hall, 2004.
[19] S. M. Aziz and M. D. Pham, "Implementation of low density parity check decoders using a new high level design methodology," *Journal of Computers*, vol. 5, pp. 81-90, 2010.
[20] T. Zhang and K. K. Parhi, "A 54 mbps (3, 6)-regular FPGA LDPC decoder," in *IEEE Workshop on Signal Processing Systems, SIPS*, 2002, pp. 127-132.
[21] A. J. Blanksby and C. J. Howland, "A 690-mW 1-Gb/s 1024-b, rate-1/2 low-density parity-check code decoder," *IEEE Journal of Solid-State Circuits*, vol. 37, pp. 404-412, 2002.
[22] A. Darabiha, A. C. Carusone, and F. R. Kschischang, "Multi-Gbit/sec low density parity check decoders with reduced interconnect complexity," in *IEEE International Symposium on Circuits and Systems, ISCAS*, 2005, pp. 5194-5197.
[23] V. A. Chandrasetty and S. M. Aziz, "An area efficient LDPC decoder using a reduced complexity min-sum algorithm," *Integration, the VLSI Journal*, vol. 45, pp. 141-148, 2012.
[24] V. A. Chandrasetty and S. M. Aziz, "FPGA implementation of a LDPC decoder using a reduced complexity message passing algorithm," *Journal of Networks*, vol. 6, pp. 36-45, 2011.
[25] D. M. Pham and S. M. Aziz, "FPGA-based image processor architecture for wireless multimedia sensor network," in *IFIP 9th International Conference on Embedded and Ubiquitous Computing, EUC, Melbourne, ,* 2011, pp. 100-105.
[26] D. M. Pham and S. M. Aziz, "An energy efficient image compression scheme for Wireless Sensor Networks," *in IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, ISSNIP, Sydney, 2013, pp. 260-264.
[27] V. A. Chandrasetty and S. M. Aziz, "FPGA implementation of high performance LDPC decoder using modified 2-bit min-sum algorithm," *in Second International Conference on Computer Research and Development*, 2010, pp. 881-885.
[28] V. A. Chandrasetty and S. M. Aziz, "A reduced complexity message passing algorithm with improved performance for LDPC decoding," *in 12th International Conference on Computers and Information Technology, ICCIT*, Dhaka, 2009, pp. 19-24.
[29] M. Ismail, I. Ahmed, and J. Coon, "Low Power Decoding of LDPC Codes," *ISRN Sensor Networks*, vol. 2013, p. 12, 2013.
[30] J. S. Rahhal, "LDPC coding for MIMO wireless sensor networks with clustering," in *The Second International Conference on Digital Information and Communication Technology and it's Applications , DICTAP*, 2012, pp. 58-61.

Duc Minh Pham received B.S. degree in electronic engineering from HCM National University of Technology, Vietnam in 2003 and M.S. degree in micro systems technology from the University of South Australia in 2008. Mr Pham is currently working as a Research Associate and doing his PhD at University of South Australia in the field of wireless multimedia sensor networks. He has strong industry experiences in system design for both FPGA and ASIC platforms. His research interests are in the fields of VLSI implementation of communication systems such as SoC for next generation networking, automation in VLSI design, FEC (Forward Error Correction), APS (Application Specific Processor), wireless sensor networks, coding theory, image and video processing.

Syed Mahfuzul Aziz received Bachelor and Master degrees in electrical and electronic engineering (EEE) from Bangladesh University of Engineering & Technology (BUET) in 1984 and

1986 respectively. He received a Ph.D. degree in electronic engineering from the University of Kent (UK) in 1993 and a Graduate Certificate in higher education from Queensland University of Technology in 2002.

He was a Professor in BUET till 1999. Prof Aziz initiated and led the development of teaching and research programs in integrated circuit (IC) design in Bangladesh. In 1996, he was a visiting scholar at the University of Texas at Austin when he spent time at Crystal Semiconductor Corporation designing advanced CMOS integrated circuits. He joined the University of South Australia in 1999, where he is currently the discipline leader of EEE. He has been involved in many industry projects and has attracted funding from industry as well as reputed bodies such as the Australian Research Council (ARC), Australian Defence Science and Technology Organization (DSTO), and Cooperative Research Centre. He has authored over 120 research papers. His research interests include digital systems and IC design, wireless sensor networks, biomedical instrumentation and engineering education.

Prof Aziz is a senior member of the IEEE and a member of Engineers Australia. He has received numerous professional and teaching awards including the Prime Minister's Award for Australian University Teacher of the Year (2009). He reviews papers for a number of reputed journals including IEEE Transactions and journals published by the IET and Elsevier.

Performance Comparison of RFID Tag at UHF Band and Millimeter-Wave Band

A. K. M. Baki [1,*] and Nemai Chandra Karmakar [2]
1. Dept. of Electrical & Electronic Engineering, Ahsanullah University of Science and Technology 141-142 Love Road, Tejgaon, Dhaka 1208, Bangladesh
2. Dept. of Electrical & Computer Systems Engg., Monash University Bldg. 72, Monash University, Clayton Campus, Clayton, VIC 3800, Australia
*Corresponding author, Email: akalam@daad-alumni.de

***Abstract*—The ultra high frequency (UHF) band spectrum will likely be congested in near future since the next generation wireless as well as Radio Frequency Identification (RFID) system users will witness the use of UHF band technology with increased demand of bandwidth, bit rate, frequency spectrum and power consumption. The alternate solution is the use of millimeter-wave band technology. It is possible to improve data throughput, range resolution and multi-user capability in mm-wave band RFID system. 'Higher power reception efficiency and lower side lobe level (SLL) of radiation pattern' is required for RFID system that will increase the tag range and transmission bit rate. At the same time lower SLL will minimize the interference level. Beam pointing error is another problem of UHF band antenna which reduces the tag range and bit rate. These problems can be minimized by using large number of antenna elements. But with UHF band signal it is practically difficult to construct large array antenna; since the array size becomes tremendously larger with the increase of antenna elements. 'Higher power reception efficiency and lower SLL' can practically be obtained by using non-uniform power distribution of large number of antenna elements in millimeter wave band. A new and technically better method of beam forming by implementing the concept of staircase power distribution (SPD) of antenna elements at 60 GHz has been investigated and presented in the paper. The SPD method is compared with Gaussian edge tapering method. It was found that the maximum SLL (MSLL) is the lowest in case of SPD. The beam efficiency of SPD is also equivalent to that of Gaussian edge tapering method. It is easier to fabricate a larger number of antenna elements within smaller area with SPD at 60 GHz system; since the antenna size is smaller and the number of different power distribution in SPD case is less and stepwise uniform. Uniform and less number of different power distribution of SPD also minimizes other technical errors.**

***Index Terms*—Adaptive Arrays; Antenna Radiation Pattern; Antenna Tapering; Antenna Theory; Beam Steering; Radio Frequency IDentification**

I. INTRODUCTION

Ultra high frequency band spectrum will likely be congested and the use of millimeter (mm) wave technology in the wireless local area network (WLAN) and Radio Frequency Identification (RFID) systems will be witnessed in the near future. The characteristic of mm-wave transmission must be considered carefully in particular the strong attenuation at this frequency spectrum. Free-space propagation loss, as an example, at 60 GHz is higher than the one at 5 GHz under the same condition. Other losses and fading factors, such as rain, foliage, scattering, diffraction loss etc., increasingly affect the mm-wave propagation. Directive antennas are best suited to point-to-point applications because the directive antenna pattern improves the channel multipath profile; by limiting the spatial extent of the transmitting and receiving antenna patterns to the dominant transmission path. The antennas used in some applications, such as automatic cruise control (ACC), collision avoidance radar, and RFID reader antenna must have very low side lobes. This is crucial as side lobes lead to false alarms in a collision avoidance radar system. In RFID applications higher side lobes can lead to false tracking of RFID tags. An RFID tag can be identified automatically at a distant location by exchanging information through RFID system. RFID system has different applications such as animal tagging, authenticity verification**,** inventory tracking and security surveillance [1]. A faster and energy efficient tag reading is needed in some sophisticated applications, particularly for higher number of tags reading [2]. Following frequency bands are generally used in RFID applications:

a. Low frequency (LF): 125-134 KHz;
b. High frequency (HF) : 13.56 MHz;
c. Ultra high frequency (UHF): 433 MHz, 860-960 MHz;
d. Microwave (MW) : 2.4 GHz, 5.8 GHz;
e. Millimetre wave (mm-Wave): e.g., 60 GHz and 77 GHz [3];

RFID reader antenna with very low side lobes in its radiation pattern would maximize the received power and minimize interferences. Higher side lobes result in false alarms in RFID applications. Different RFID reader architecture by using phased array/smart antenna concepts is discussed in details in [4]. It is possible to improve data throughput, range resolution and multi-user capability with mm-wave RFID communication without accepting range limiting RF power restrictions [5]. Beam Collection Efficiency (BCE) and Maximum Side Lobe Level (MSLL) are the indices for the evaluation of

doi:10.4304/jnw.9.12.3215-3220

antenna radiation pattern. BCE is the ratio of power flow that is intercepted by the receiving antenna to the whole transmitted power [6]. Suppression of Grating Lobe (GL) and Side Lobe Level (SLL) is necessary for higher BCE and to avoid interferences. When GL appears and SLL increases, the transmitted power is absorbed into these lobes which cause reduction of received power. These also cause higher interference levels. Though array antennas increase the directivity of the antenna system but if all antennas are uniformly excited then the main beam carries only a part of the total power due to the higher SLL. It is possible to increase BCE and reduce SLL if edge tapering concept can be implemented.

A better method of power distribution of array antennas by incorporating Isosceles Trapezoidal Distribution (ITD) concept is discussed in [6]. In ITD method, only a few edge antenna elements are tapered. Power levels of the remaining middle antennas are uniform. With ITD, which is also technically better than Gaussian or Dolph-Chebyshev power distribution, it is possible to maintain higher BCE and lower SLL. Another method of ITD with Unequal element spacing (ITDU) to achieve lower Maximum Side Lobe Level (MSLL) and higher beam efficiency (BE) is reported in [7]. It is possible to maintain even higher BE and lower MSLL by incorporating ITDU. Methods of designing transmitter outputs by using on-chip power amplifier (PA) stages in each element need good linearity, high efficiency, high power gain and high output power [8-10]. A four-stage PA with at least 3-dB gain in each stage, with the transistor size doubled in each stage, is discussed in [8-9]. It is possible to design on chip power amplifier stages with variable gains for different antenna elements. This way it would be possible to minimize the SLLs even to lower levels. As a result the BE of the array antenna will increase and interference to other communication systems will decrease.

The authors have investigated a comparatively new and technically better method of power distribution of array antenna for 60 GHz system. Instead of using gradual decrement of power distribution of array antenna, the concept of 'staircase' is implemented and named as Staircase Power Distribution (SPD) [11-12]. Fabrication of array antenna with SPD concept is easier and technically better than other kinds of power distributions; since the number of different power distribution in SPD is least and stepwise uniform. Figure 1 shows a conceptual block diagram of an RFID system.

The paper is organized in the following way. General characteristics of radio frequency identification (RFID) tag are discussed in section II. A comparative study of UHF band RFID-system with mm-Wave RFID system is made in section III. A new and technically better method of power distribution of array antenna by implementing SPD concept is described in section IV. A comparative analysis of radiation patterns and power collection efficiency by using SPD and Gaussian edge tapering is made in section V. And finally the conclusion is made in section VI.

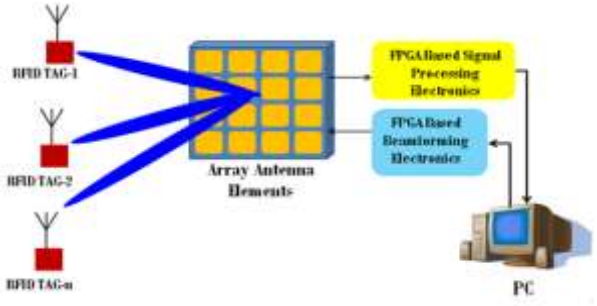


Figure 1. Conceptual block diagram of an RFID system

II. Characteristics of Radio Frequency Identification Tag

The power received by a tag can be expressed by the following Friis transmission formula [11]:

$$P_{tag} = P_T G_T g_t (\frac{\lambda}{4\pi d_t})^2 \quad (1)$$

where,

P_T is the power transmitted by the reader antenna;

G_T is the gain of transmitting antenna;

g_t is the gain tag antenna;

d_t is the distance between the transmitting antenna and the tag;

In equation (1), the term '$(\frac{\lambda}{4\pi d_t})^2$' is the free space loss factor which is a function of operationg frequency and tag distance. Received power by the reader antenna can be expressed as [11]:

$$P_r = P_T G_T G_R g_t \frac{1}{d_t^2 r_b^2} (\frac{\lambda}{4\pi})^4 \xi \quad (2)$$

where,

G_R is the gain of reader antenna;

ξ is the backscatter efficiency of the tag;

r_b is the distance between the reader antenna and the tag;

The sensitivity of the reader, or minimum reader power ($P_{\min r}$), is specified for maximum possible operation range. When $P_{\min r}$ and g_t are fixed, the ranges d_t/r_b can be controlled by controlling G_T and/or G_R.

III. Milli-Meter Wave Band for RFID System

Higher data transfer rate even with gigabit range is achievable [3] at mm-wave (e.g., 60 GHz) band. Signal at mm-wave band can create pencil like main beam with improved gain. Pencil like main beam also occupies smaller surrounding space. Interferences with other communication channels can be minimized with this kind mm-wave signal. The reader can also receive signal through narrower space, thereby reducing the chances of interferences. RFID system at 60 GHz has been reported in [13-14]. The signal at 60 GHz is rapidly absorbed by atmospheric oxygen over long distances. Therefore it can be used for short distance communication and the frequency reuse would be possible. In U. S. A. the maximum limit of power transmission in the 60 GHz band is 40 dBm (10 watt), which is higher than the limit in the UHF band. Beam pointing error is another reason

of lower received power. For N+1 number of antenna elements, beam pointing error can be expressed as [15]:

$$\Delta\theta_{rms} = \frac{2\sqrt{3}\sigma}{\beta d \cos\theta_0 N^{3/2}} \quad (3)$$

where

$\sigma =$ R.M.S. phase error;

$\beta = \frac{2\pi}{\lambda}$ = Phase constant;

d = Spacing between antenna elements;

θ_0 = Main beam steering angle;

Equation (3) shows that if the number of antenna elements is increased then the beam pointing error decreases. It would be possible to create a pencil like beam with higher gain if the number of antenna elements can be increased. Additionally, the use of larger antenna elements will minimize beam pointing error. Figure 2 shows the beam pointing errors with different number of array elements. One is with 9-elements array and the other is with 50-elements array. It is apparent from Figure 2 that the beam pointing error can be brought down near to zero by using even higher number of antenna elements. With UHF band signal, there is a limitation of fabrication using antenna elements larger than 9, since the array size becomes tremendously larger. The nearby transponders also cannot be spatially distinguished at UHF band signal since the reader transmission cannot be efficiently directed. On the other hand radiation from the mm-wave reader can be directed efficiently since larger number of antenna elements can be fabricated on to a smaller area at mm-wave band. Figure 3 shows the radiation patterns for the two different cases, one is with 9 antenna elements and the other is with 50. The simulation was done by using 60 GHz signal. Figure 3 shows that the same transmitted power can be concentrated into smaller spatial area with higher number of antenna elements. This will also help isolate the tag of interest from other tags. Therefore mm-wave antenna would help in finding tag in high-density sensor network such as item level identification. Some advantages of RFID system at mm-wave over UHF band is summarized in Table 1. Since the inter-element spacing (generally$\lambda/2$) for 60 GHz signal is much smaller than that of 900 MHz UHF band signal, a huge number of antenna elements can be fabricated within smaller area for 60 GHz band system. A comparison of antenna size for two different cases is mentioned in Table 1. It was mentioned earlier that the beam pointing error can be minimized (shown in Figure 2) and the main beam can be made narrower (shown in Figure 3) with larger number of mm-wave antenna elements. One example of main beam width for two different cases is also mentioned in Table 1. For 9-elements array the main beam width is about 20° (Figure 3). This is generally the case for UHF band antenna. On the other hand, the main beam width for 50-elements antenna is 4° which can be the case for a 60 GHz system (Figure 3). 'Minimum beam pointing error and narrower main beam' with larger number antenna elements will increase the BCE and reduce the interference level in a mm-wave band system.

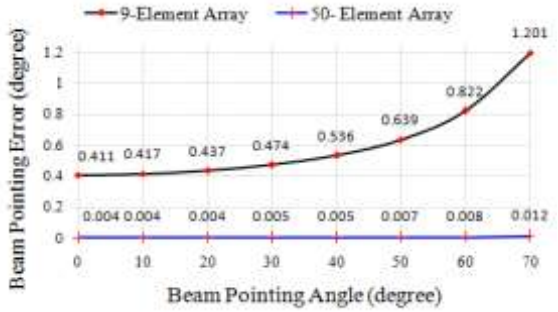


Figure 2. Beam pointing error vs. beam pointing angle with different number of array elements

Radiation patterns with staircase power distribution.

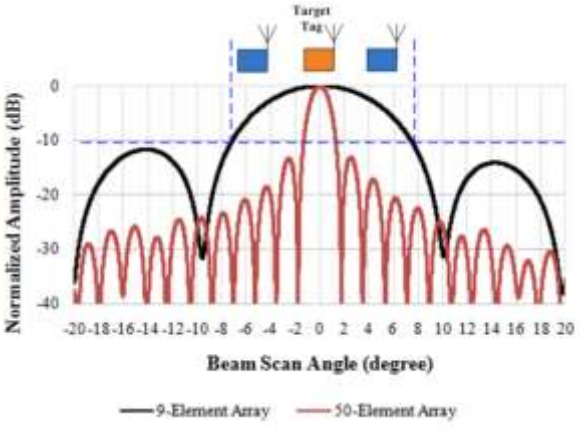


Figure 3. Radiation patterns with two different number of array elements

IV. Staircase Power Distribution of Array Elements

Array Factor (AF) of one-dimensional array antenna with staircase power distribution (SPD) can be expressed [11-12] by (4).

$$AF = \sum_{n=-(N-1)/2}^{(N-1)/2} \delta_1 e^{jn\psi} + \sum_{n=[-(N-1)/2]+N_{s1}}^{[(N-1)/2]-N_{s1}} (\delta_2 - \delta_1) e^{jn\psi} + \sum_{n=[-(N-1)/2]+N_{s1}+N_{s2}}^{[(N-1)/2]-N_{s1}-N_{s2}} (\delta_3 - \delta_2) e^{jn\psi} + \ldots + \sum_{n=[-(N-1)/2]+N_{s1}+N_{s2}\ldots+N_{sl}}^{[(N-1)/2]-N_{s1}-N_{s2}\ldots-N_{sl}} (\delta_l - \delta_{l-1}) e^{jn\psi} + \sum_{n=[-(N-N_S-1)/2]}^{[(N-N_S-1)/2]} (A - \delta_l) e^{jn\psi} \quad (4)$$

Following are the notations of (4),

N = Total number of antenna elements,

N_{s1}, N_{s2}, $N_{s3\ldots}$ N_{sl} etc. are no. antenna elements tapered from each side (starting from edge of the array) for 1st stage, 2nd stage, 3rd stage…….last stage.

TABLE I. ADVANTAGES OF MM-WAVE RFID OVER UHF BAND RFID SYSTEM.

Parameters	Advantages of mm-Wave band
Array antenna size and fabrication	Antenna size is smaller at mm-Wave. [For example: the array size for 100 elements of 900 MHz UHF band antenna is 16.66 meter. But the array size of 100 elements of 60 GHz band antenna is only 0.25 meter. In both cases the inter-element spacing is $\lambda/2$.] Fabrication is easier from the perspective of antenna size. Less costly from the perspective of number of antenna elements.
Number of antenna elements	Higher number of antenna elements can be used at mm-Wave. For UHF band array, antenna size becomes tremendously larger if the number of antenna elements is increased.
Beam shaping	Better beam shaping is possible at mm-Wave due to larger number of antenna elements which is shown in Figure 3. Tag separation becomes easier in mm-wave band due to comparatively very narrower beam. It can also be inferred from Figure 3.
Beam pointing angle and beam pointing error	Beam pointing error can be decreased by using increased number of antenna elements with mm-Wave band. A comparative study of beam pointing error is shown in Figure 2.
Beam Collection Efficiency (BCE)	BCE can be increased at mm-Wave due to: Less beam pointing error (BCE is more closely related to the beam pointing error than BE); Larger number of used elements; [The BCE will be higher for mm-wave band antenna, since with larger number of elements it is possible to make the main beam of the radiation pattern narrower. This way the RFID tag will receive more power through the main beam.]
Bit rate	Bit rate is higher due to higher bandwidth (according to Shannon channel capacity formula).
Interference	Interference is less due to narrower main beam and better spatial separation of RFID tag at mm-Wave band. [This scenario can also be inferred from Figure 3. For example the main beam width for 9 elements antenna is about 20°. It is the usual case for a UHF band antenna. On the other hand the main beam width for 50 elements antenna is 4° which can be a case for mm-wave band antenna.]
Frequency reuse	Frequency reuse is better due to higher attenuation at 60 GHz.
Multipath effect	Multipath effect would be less due to higher attenuation at 60 GHz.
Tag/Transponder size	Smaller at mm-Wave band.

Here last stage is defined as the stage before the middle antenna elements.

$N_S = N_{s1} + N_{s2} + N_{s3} + \ldots\ldots\ldots + N_{sl}$ = Number of elements tapered from each side,

$\psi = \beta d(\sin\theta - \sin\theta_0)$.

$\delta_1, \delta_2, \delta_3 \ldots\ldots\ldots\ldots \delta_l$ are the amplitudes of the antenna elements of 1st stage, 2nd stage, 3rd stage…….last stage.

d = spacing between elements (m).

$\beta = 2\pi/\lambda$ = phase constant.

A is the amplitude of middle antenna elements.

θ_0 = Direction of beam maximum along the broad side.

n = 0, 1, 2……N.

The concept of SPD is shown in Figure 4.

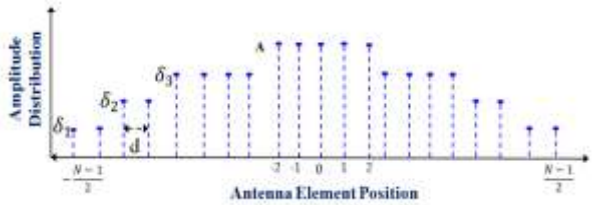


Figure 4. Staircase Power Distribution (SPD) for antenna elements.

BCE for two dimensional antenna with rectangular/square shape can be expressed as [6]:

$$BCE_{2D} = \int_{\theta_{ry}}\int_{\theta_{rx}} \left|P(\theta_x,\theta_y)\right|^2 d\theta_x d\theta_y \Big/ \int_{\theta_{ty}}\int_{\theta_{tx}} \left|P(\theta_x,\theta_y)\right|^2 d\theta_x d\theta_y \quad (5)$$

where,

θ_{tx} ; θ_{ty} ; are ± 90 degree angle sector;

θ_{rx} ; angle sector due to x dimension of receiving antenna;

θ_{ry} ; angle sector due to y dimension of receiving antenna;

$P(\theta_x,\theta_y)$ is the energy of the radiated electric field.

BCE for one dimensional case can be expressed as:

$$BCE = \int_{\theta_r} \left|P(\theta)\right|^2 d\theta \Big/ \int_{\theta_w} \left|P(\theta)\right|^2 d\theta \quad (6)$$

θ_r is the angle sector due to one dimensional receiving antenna and θ_w is the angle sector $\pm 90^\circ$.

$P(\theta)$ is the energy of the one dimensional radiated electric field.

Figure 5 shows the normalized BCE for two different beam pointing angles. Uniform power distribution of 200 array elements was used in this case. The BCE was calculated at a distance 10 meter from the reader by assuming 5 cm tag size. The power received can be improved further by implementing the SPD concept, since the BCE is higher with SPD than that of uniform power distribution and will be shown in the following section.

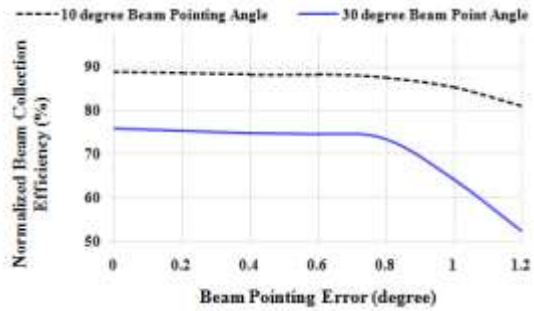


Figure 5. Beam collection efficiency vs. beam pointing error for different beam pointing angles

V. RADIATION PATTERNS WITH SPD AND GAUSSIAN POWER DISTRIBUTIONS

Radiation patterns, SLL and Beam Efficiency (BE) for different amplitude distributions (Gaussian and SPD) are compared in this section. BE for two dimensional radiation pattern can be expressed [16] by (7):

$$BE_{2D} = \iint_{main\_beam} |P(\theta,\varphi)|^2 \, d\Omega \Big/ \iint_{4\pi} |P(\theta,\varphi)|^2 \, d\Omega \quad (7)$$

where,

$P(\theta,\varphi)$ is the radiated electric field pattern;

BE for one dimensional array can be expressed [7] by (8):

$$BE_{1D} = \int_{\theta_m} |P(\theta)|^2 \, d\theta \Big/ \int_{\theta_w} |P(\theta)|^2 \, d\theta \quad (8)$$

where,

θ_m is the angle sector due to one dimensional main beam and θ_w is the observation angle sector of $\pm 90^\circ$.

$P(\theta)$ is the one dimensional radiated electric field pattern.

Figure 6 shows the amplitude distributions of 25 antenna elements for SPD (10 dB) and Gaussian (10 dB) power distribution. Radiation patterns, MSLL and BE by using 60 GHz signals were compared. Different beam pointing angles were also considered. Figure 7 shows the radiation pattern of 10 dB SPD with 35 degree beam pointing angle. The element spacing was 0.6λ. The performance of SPD can further be improved by considering larger number of antenna elements. In case of Gaussian edge tapering, the number of different power distributions becomes higher with larger number of elements. For example, the required number of different power distribution is 13 for 25 elements of Gaussian edge tapering. It is technically a very difficult task to achieve such a higher number of different power distributions. This also introduces more errors in power distribution. These problems become even worse with the increased number of elements. The number of different power distribution of SPD array (for the case shown in Figure 6) is 4.

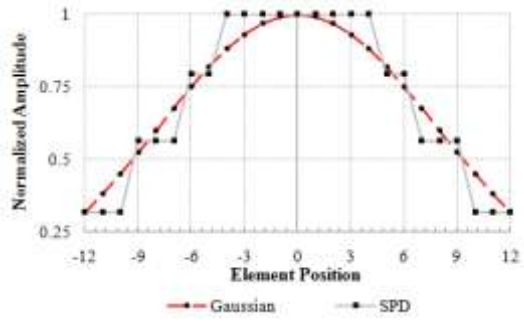


Figure 6. Amplitude distributions of 25 antenna elements for 10 dB Gaussian and 10 dB SPD

Technically it is much easier to implement 4 different power distributions than 13 different power distributions. Minimum error is introduced with SPD. Therefore SPD of array antenna elements is a good candidate for mm-wave RFID applications. MSLL as well as BE for four different beam steering angles and two different power distributions (Gaussian and SPD) are summarized in Table 2 and Table 3 respectively. Table 2 shows that the MSLL for SPD were minimum (-26 dB) for each of the beam steering angles (5°, 15°, 25°, and 35°). Table 3 shows that the BEs for SPD case are also comparable to those of Gaussian edge tapering and for different beam steering angle. The data shown in Table 2 and Table 3 asserts that larger number of SPD array will maximize the power reception and minimize the interference levels in mm-wave band RFID system.

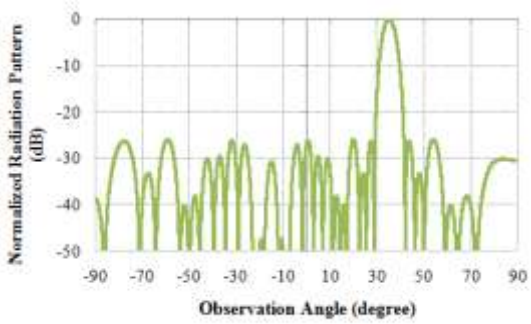


Figure 7. Radiation pattern of 25 antenna elements for 10 dB SPD at 35 degree beam pointing angle

TABLE II. MSLL FOR 10 DB GAUSSIAN AND 10 DB SPD EDGE TAPERING

Main Beam Pointing Angle (degree)		5	15	25	35
		MSLL			
Type of Power Distribution	Staircase Power Distribution (SPD)	-26	-26	-26	-26
	Gaussian	-23.69	-23.4	-23.25	-23.25

TABLE III. BEAM EFFICIENCY (BE) FOR 10 DB GAUSSIAN AND 10 DB SPD EDGE TAPERING

Main Beam Pointing Angle (degree)		5	15	25	35
		Beam Efficiency (BE)			
Type of Power Distribution	Staircase Power Distribution (SPD)	97.84	97.66	97.23	97.17
	Gaussian	98.67	98.65	98.31	97.14

VI. CONCLUSION

A little improvement in RFID-system performance, such as, antenna gain and directivity, can play a significant role in improving the bit error rate, collision mitigation, data rate, interference cancelation, localization of tag and reading range. Milli-meter wave and UHF band signals are analyzed and compared in this paper for Radio Frequency IDentication (RFID)-system. Two types of power distribution of array antenna are also analyzed and compared. The types are Gaussian edge tapering and Staircase Power Distribution (SPD). Maximum power will be transmitted through the main

beam and less power will be in the Side Lobe Level (SLL) in case of mm-wave band SPD system. SPD system is technically better; since in SPD less and stepwise uniform power distribution is required which will minimize amplitude and other technical errors. Milli-meter wave band array antenna with larger number of elements and SPD is easier to fabricate. Tag separation with SPD array antenna and mm-wave RFID-system will be easier than that of UHF band RFID-system. Exposure level to humans and all other living animals/things as well as interference to/from other communication systems outside the main beam will also be minimum in case of mm-wave band SPD system. Construction of UHF band RFID reader system with larger number of array elements is a difficult job since the array size becomes tremendously larger. This problem can be easily overcome by implementing mm-wave RFID system.

ACKNOWLEDGEMENT

The work is partly supported by Australian Research Council (ARC) Discovery Project (DP110105606: Electronically Controlled Phased Array Antenna for RFID applications).

REFERENCES

[1] Want, R. "The Magic of RFID," *ACMQueue,* vol. 2, (7), pp. 40-48, Oct. 2004.

[2] Klair, D. K. Chin, K. W. and Raad, R. "A Survey and Tutorial of RFID Anti-Collision Protocols," *IEEE Comm. Surveys & Tutorials,* vol. 12, no. 3, Third Quarter 2010, pp. 400 – 421.

[3] Pursula, Pekka; Karttaavi, T.; Kantanen, Mikko; Lamminen, Antti; Holmberg, Jan; Lahdes, Manu; Marttila, Ilkka; Lahti, Markku; Luukanen, Arttu; Vähä-Heikkilä, Tauno, *'60-GHz millimeter-wave identification reader on 90-nm CMOS and LTCC', IEEE Transactions on Microwave Theory and Techniques,* vol. 59(2011): 4, pp. 1166-1173, 2011.

[4] Nemai Chandra Karmakar, 'Recent Paradigm Shift in RFID and Smart Antenna', *Handbook of Smart Antennas for RFID Systems,* John Wiley & Sons, Inc. 2010, pp. 57~82.

[5] Carlowitz, C.; Strobel, A.; Schafer, T.; Ellinger, F.; Vossiek, M., "A mm-wave RFID system with locatable active backscatter tag," *Wireless Information Technology and Systems (ICWITS), 2012 IEEE International Conference on,* vol., no., pp. 1, 4, 11-16 Nov. 2012

[6] A. K. M. Baki, N. Shinohara, H. Matsumoto, K. Hashimoto, and T. Mitani, "Study of Isosceles Trapezoidal edge tapered phased array antenna for Solar Power Station/Satellite", *Ieice Trans. Commun.,* Vol. E90-B, No. 4, pp 968-977, APRIL 2007.

[7] A. K. M. Baki, Kozo HASHIMOTO, Naoki SHINOHARA, Tomohiko MITANI, and Hiroshi Matsumoto, "Isosceles-Trapezoidal-Distribution Edge Tapered Array Antenna with Unequal Element Spacing for Solar Power Satellite", *Ieice Trans. Commun.,* Vol. E91-B, No. 2 February 2008, pp 527-535.

[8] Arun Natarajan, Abbas Komijani, Xiang Guan, Aydin Babakhaniand Ali Hajimiri, 'A 77-GHz Phased-Array Transceiver With On-Chip Antennas in Silicon: Transmitter and Local LO-Path Phase Shifting', *IEEE Journal Of Solid-State Circuits, Vol. 41, No. 12, December* 2006, pp 2807-2819

[9] Ullrich R. Pfeiffer and David Goren, 'A 20 dBm Fully-Integrated 60 GHz SiGe Power Amplifier With Automatic Level Control, *IEEE Journal Of Solid-State Circuits',* Vol. 42, No. 7, July 2007 pp. 1455-1463

[10] Van-Hoang Do, Viswanathan Subramanian, Wilhelm Keusgen, and Georg Boeck, 'A 60 GHz SiGe-HBT Power Amplifier With 20% PAE at 15 dBm Output Power', *IEEE Microwave And Wireless Components Letters,* Vol. 18, No. 3, March 2008, pp. 209-211

[11] A. K. M. Baki, Nemai Chandra Karmakar, Uditha Bandara and Emran Md Amin, 'Beam Forming Algorithm with Different Power Distribution for RFID Reader, pages 64~95', *Book Title: Chipless and Conventional Radio Frequency Identification: Systems for Ubiquitous Tagging, IGI Global,* May, 2012, USA, ISB*N 978-1-4666-1616-5* (hardcover)

[12] A. K. M. Baki, Nemai Chandra Karmakar, '60 GHz Array Antenna with New Method of Beam Forming', 15th *International Conference on Computer and Information Technology,* December 2012, pp. 638-641.

[13] Karmakar, N. C. 'Smart Antennas for Automatic Radio Frequency Identification Readers', *Chapter XXI, in Handbook on Advancements in Smart Antenna Technologies for Wireless Networks, editior: Chen Sun, Jun Cheng & Takashi Ohira, IGI Global,* 2008 pp. 449-472.

[14] Pellerano, Stefano. Alvarado, Javier. and Palaskas, Yorgos. 'A mm-Wave Power-Harvesting RFID Tag in 90 nm CMOS', *IEEE Journal of Solid-State Circuits,* vol. 45, no. 8, August 2010, pp. 1627~1637.

[15] Keith, R Carver. Cooper, W. K. and Stutzman, W. L., "Beam-Pointing Errors of Planner-Phased Arrays", *IEEE Trans. On Antenna &Porp,* 1973, pp. 199-202.

[16] Warren L. Stutzman and Gary A. Thiele, "Antenna Theory and Design", *2nd edition, John Wiley & Sons,* Inc. pp. 29.

Keeping Desired QoS by a Partial Coverage Algorithm for Cluster-Based Wireless Sensor Networks

Lei Wang, Jui-Yu Yang, Yu-Yun Lin, and Wei-Jun Lin
Dept. Electrical Engineering, Feng-chia Univ., Taichung City 407, Taiwan
Email: leiwang@fcu.edu.tw; yjamy@yahoo.com; ful654@yahoo.com.tw; yume190@gmail.com

***Abstract*—Many studies were done on design algorithms to completely cover an area. We can call the issue as a complete coverage problem. Although there were many researches about proposing a partial coverage issue; almost all of the studies only focus on lengthening the lifespan of wireless sensor networks (WSNs) but ignore the truth that a wireless sensor network will inevitably lose its coverage because of exhausted energy during the operating time. Lifespan refers to wireless sensor network offering its service to meet the required coverage ratio. In this work, we propose a topology control algorithm for cluster-based wireless sensor networks to keep predefined Quality of Service (QoS) of coverage as long as the sensor nodes can stand. The algorithm forms a multi-hop cluster network with a required connectivity by using a novel cluster head competition scheme and proper transmission of power settings. It can organize sensor nodes into clusters actively to achieve required coverage ratio as long as possible. The algorithm is suitable for practical applications of large-scale or high-density wireless sensor networks due to its distributed processing and scalable cluster topology.**

***Index Terms*—Wireless Sensor Network; Coverage Intensity; Routing Protocol**

I. INTRODUCTION

Researches in wireless communications have led to the development of wireless sensor networks, which have shown their suitability to various kinds of applications [1]. Wireless sensor networks are composed of low-power, low-cost, small-sized and multifunctional sensor nodes. Each sensor node is capable of communication, data collection, and processing. The sensor nodes collaborate among each other to establish a sensor network for collecting critical information from the surrounding environment. These nodes are densely deployed either inside or very closed to the phenomenon that is being monitored, every node has the ability to sense, process and transmit data to a base station (BS). Due to the limitations of energy and cost of sensor nodes, it is crucial to minimize the energy consumption to prolong network lifespan [2]. Researches in wireless communications have led to the development of wireless sensor networks, which have shown their suitability to various kinds of applications [1]. Wireless sensor networks are composed of low-power, low-cost, small-sized and multifunctional sensor nodes. Each sensor node is capable of communication, data collection, and processing. The sensor nodes collaborate among each other to establish a sensor network for collecting critical information from the surrounding environment. These nodes are densely deployed either inside or very closed to the phenomenon that is being monitored, every node has the ability to sense, process and transmit data to a base station (BS). Due to the limitations of energy and cost of sensor nodes, it is crucial to minimize the energy consumption to prolong network lifespan [2].

Many studies were conducted on design algorithms to completely cover an area, such as [3] and [4], etc. We can call the issue as "complete coverage" problem. Most of the coverage-related works concern how to prolong network lifespan through different techniques. As a wireless sensor network consists of a large number of randomly distributed nodes, one of the most challenging issues is to detect events and send the corresponding data to a BS node successfully, to guarantee the required coverage and connectivity within the entire wireless sensor network's life cycle. The coverage rate reflects how well a sensor network is monitored or tracked by sensors. Besides the main viewpoint of the coverage issue which is to increase coverage rate of a wireless sensor network to achieve a most sensitive wireless sensor network, there is another viewpoint about coverage that is being proposed by recent studies: Can we limit the power consumption by guaranteeing an ideal coverage with less sensor nodes? One of the techniques which recently attract researchers' attention is to reduce the coverage quality to trade for network lifespan. For example, mudflows monitoring applications may only require part of the area to be covered in sunny days. Thus, to extend network lifespan, we can lower the coverage quality if it is acceptable. The problem of covering only a portion of an area is referred to as the "partial coverage" problem. The partial coverage problem is also referred to as α-coverage problem of which the objective is to cover only α-portion of the area.

Although there are many researches about partial coverage issue that have been proposed; almost all of the studies only focus on lengthening the lifespan of wireless sensor networks but ignore the truth that a wireless sensor network will inevitably lose its coverage because of

doi:10.4304/jnw.9.12.3221-3229

exhausted energy during the operating period. Lifespan refers to wireless sensor network being able to offer its service to meet the required coverage ratio. The truth leads the researches to develop some methods that overuse the energy of sensor nodes to achieve higher coverage ratio or to gain a longer lifespan by sacrificing the potential of graceful coverage degradation for future recovery. A realistic design for a wireless sensor network should consider the condition that a wireless sensor network need to keep working even though the desired coverage cannot be achieved until users can deploy new sensor nodes or recharge old nodes to recover its ideal coverage. A good design of wireless sensor networks, especially for partial coverage applications, should not only prolong the lifespan of a wireless sensor network, but also keep the wireless sensor network to offer an acceptable coverage ratio as long as possible.

In this work, we propose a topology control algorithm named as Keeping Desired Partial Coverage rate (KDPC) for cluster-based wireless sensor networks to keep predefined Quality of Service (QoS) of coverage as long as the sensor nodes can stand. There are several novel features that have been exploited: First, instead of using location information, KDPC forms a multi-hop cluster network with a required connectivity by using a novel cluster head competition scheme and proper transmission of power settings. Second, less redundant nodes are activated than the existing algorithms since the number of sensor nodes used to achieve the required coverage ratio will be determined and limited by the algorithm dynamically. Third, the algorithm can organize sensor nodes into clusters actively to achieve the required coverage ratio as long as possible. Finally, KDPC is suitable for practical applications of large-scale or high-density wireless sensor networks due to its distributed processing and scalable cluster topology.

This paper is organized as follows: Section 2 is a brief introduction about the issues of partial coverage problems. The related definitions about coverage estimation used in the paper are defined first as the basis of this research in Section 3. The idea and detail algorithm of KDPC is then introduced in the Section. By comparing the simulation results for KDPC with another similar algorithm, the goal of keeping QoS can be proved by the simulation described in Section 4. Finally, Section 5 is a conclusion of this study.

II. Related Works

The problem of partial coverage was recently analyzed in relevant literatures. For earlier studies, the work in [5] shows the upper bound of the network lifespan when only α-portion of the whole area is covered. It shows that the network lifespan may increase up to 15 percent for 99 percent coverage and 25 percent for 95 percent coverage. In [6], percentage coverage instead of complete coverage is selected as the design goal, and a location-based Percentage Coverage Configuration Protocol (PCCP) is developed to assure that the proportion of the area after configuration to the original area is no less than the desired percentage. Liu and Liang [7] presented a centralized algorithm which takes both coverage and connectivity into account. Their work is the first one to analyze partial coverage properties in order to prolong network lifespan. Initially, active sensors are randomly selected. Nodes on a chosen candidate path with the maximum gain are chosen in iterations.

For the α-coverage problem, to evaluate how uniformly the subregions are covered, the work in [8] uses sensing void distance (SVD) which is the distance from an uncovered point to the nearest covered point. The study claimed that their CDS-based distributed algorithm. The algorithm can provide a constant bounded SVD. However, coverage redundancy is high to guarantee a bounded SVD. The coverage redundancy is the price paid for a bounded coverage ratio. For transforming an existing complete coverage algorithm to a partial coverage one with any coverage ratio, a study proposed by Li, etc. [9] proposed a method by running a complete coverage algorithm to find full coverage sets with virtual radii and converting the coverage sets to partial coverage sets via adjusting sensing radii.

There are also many studies that focus on the wireless sensor network design for a dedicated application [10][11] by means of the issue of coverage. Although these researches restrict the property of the design by a dedicated application property, the studies can be provided as the proofs that the idea of coverage is very important for realistic applications.

Many algorithms were proposed to guarantee coverage and connectivity while a network forms in its initial stage [12-14]. These existing algorithms activate part of the nodes based on their locations and coverage requirements. Then, they establish the routes from the activated nodes to the BS and activate some extra nodes to guarantee the required connectivity if needed. However, location functionality is usually not available in sensor nodes due to the concern of cost, size, and battery-life of the nodes. Therefore, the location information based algorithms are not suitable for many practical applications.

Based on the characteristics of wireless sensor networks, Al-Karaki and Kamal categorized routing protocols into flat routing protocol, location-based routing protocol and hierarchical routing protocol [15]. Flat routing protocol [16] is a data-centric routing protocol. Initially, the base station (BS) broadcasts query packets; once the query packets reach a sensor node, the sensor nodes return data to the BS if the data is available. The advantage of a flat routing protocol is that each sensor node does not need to store much route information; the disadvantage is that if the required data is returned by several sensor nodes simultaneously, it may cause network congestion or a broadcast storm. Consequently, it is not applicable to large-scale networks. In the location-based routing protocol [17], each sensor node is equipped with a Global Positioning System (GPS) to distinguish its own geographical position from others and figure out the best transmission path for itself. The location-based routing protocol reduces transmitting unnecessary packets (compared to the broadcast type) and is best for network topology that changes frequently.

However, the cost is much higher than other protocols, too. In the hierarchical routing protocol [18][19], the geographical region of the internet is divided into several clusters, where each cluster selects a cluster head (CH) responsible for collecting the data from cluster members and transferring data to the BS via hierarchical routing. Utilizing clusters in hierarchical routing protocol has its advantages because it allows less power consumption in each node and the CH is capable of processing data aggregation. However, it imposes a larger load on the CH, as a CH must manage not only data collection but also data relay.

Most existing coverage and connectivity algorithms work to form tree networks when sensor nodes do not have location information of themselves. However, a tree topology network does not perform well in terms of energy efficiency and scalability if compared with a cluster network. A novel topology control algorithm called Adaptive Random Clustering (ARC) [20] is proposed to form a cluster network with required coverage and connectivity without location information. There are several novel features been exploited: First, instead of using location information, ARC forms a multi-hop cluster network with a required connectivity by using a novel cluster head competition scheme and proper transmission of power settings. Second, required coverage is achieved by cluster heads and activated nodes, and thus less redundant nodes are activated than the existing algorithms which employ a coverage-first and connectivity-second activation procedure. Third, the lifespan of a wireless sensor network is prolonged through balancing energy consumption by updating cluster heads periodically, reducing redundancy of activated nodes by adaptively adjusting activation threshold, and reducing energy consumption by collision avoidance mechanism. Finally, ARC is suitable for practical applications of large-scale or high-density wireless sensor networks due to its distributed processing, scalable cluster topology, and easy management. It uses a very limited number of transmission channels to support a large number of clusters.

III. PRELIMINARY DEFINITIONS

We dedicate this section to introduce some concepts and definitions that are adopted to be the basis of this research. For evaluating the coverage and connectivity of a wireless sensor network, the coverage intensity C is considered as below: if active nodes are independently and uniformly distributed in a deployment region, and each node can connect to the BS through a certain route, then network coverage ratio can be calculated from the number of active nodes n, the sensing area S, and the sensing radius R_s as shown in following equation:

$$C = 1-(1-q)^n, \qquad q = \frac{\pi R_S^2}{S} \tag{1}$$

In the equation, q is the probability that a point in the deployment region is covered by a single active node, and $(1 - q)^n$ is the probability that the point is not covered by any active nodes. The other is the probability of connectedness that gives the probability that for every active node in the network there is at least one route to the BS.

For the cluster-based wireless sensor networks, when a wireless sensor network periodically resets the network in order to reconstruct clusters for balancing energy consumption of nodes, each round of operation will organize a new structure of clusters at first. Because the CHN (Cluster Head Node) should be determined in a local range to organize a cluster and collect all sensed data for inter-cluster transmission. A CHN should be the nodes with relatively more residual energy. All deployed nodes will compete for being CHNs in CSMA/CA protocol. At first, a node has to wait a period of backoff time. If no broadcast packets are received from the other CHNs, it will declare itself as a CHN by broadcasting to its one-hop neighboring nodes.

Traditional cluster based protocols usually assume that CHNs could communicate with the BS directly. However, single-hop mode is not suitable for large-scale sensor networks due to packet collisions and high energy consumption. In our design, multi-hop routes among CHNs are established based on the minimum hop count and the band of each cluster for intra-cluster communication is determined so that the bands of any neighboring clusters are different from each other.

Based on the considerations described above, we summarize two conditions that should be considered for the determination of backoff time: First, the power of an executed node will be consumed no matter whether the node is a CHN or not. Although a CHN will consume more energy, a node that acts as a normal sensor node, say NCHN (Non-Cluster Head Node), many times should exhaust its energy, too. Second, two nodes may consume different power in the same round even though they both act as CHN. Different CHNs may consume different energy in the same round since the different amounts of up-stream packets are passed through the nodes. Based on the considerations, the equation to calculate the backoff time for Node i can be expressed as (2), and the symbols appearing in the equation are defined below:

$$T_{ci} = T_1 \times \frac{R_{execute\_i}}{R_{current}} + T_2 \times \frac{\sum_{k=1}^{Rcurrent} \left(\frac{N_{pass\_through(i,\,k\,-\,1)}}{N_{pass\_through(i,\,k\,-\,1)} + N_{cluster(k\,-\,1)}} \right)}{R_{execute\_i} + 1} + T_3 \times Rand[0,1] \tag{2}$$

$R_{execute\_i}$: The number of rounds that the node i has ever been activated, whether it is acting as a CN or a NCHN.

$R_{Current}$: The total number of rounds that has been executed.

$N_{pass\_through(i,\,k)}$: When node i acted as a CHN in the kth round, the number means the total number of CHNs that transmit packets through node i in the round; otherwise, the number is zero.

$N_{Cluster(k)}$: The number of NCHNs required for a cluster in k_{th} round.

There are three terms to make up the backoff time. The first term is weighed by the times that the node has been activated in the past rounds. The second term is weighed by the average amount of data that has been transmitted through the node. The third term is a random value introduced as an enhancement to the existing CSMA/CA

algorithm. The term can guarantee that each node has different random value and then different backoff times. This keeps the nodes close to each other from sending CHN packets at the same time, and avoids the collisions. T1, T2, and T3 are weights of these terms, respectively. Based on the equation, the differences among nodes will be more precisely determined by the status of actual energy consumption.

To achieve the required coverage ratio, each CHN will organize several sensor nodes as the members of the cluster controlled by the CHN. It is a critical part for an algorithm to determine the number of members included in a cluster. To the best of our knowledge, most proposed algorithms for the determination are centralized ones. It means that the most popular method is to complete the determination by the BS. BS must figure out the number of CHNs by receiving the message reported from CHNs, then broadcast the number of members in each cluster by calculating the expected number of sensor nodes for the expected coverage ratio. Although there are a few distributed algorithms such as proposed in [8], those algorithms work in a distributed manner but not in a parallel fashion, i.e., each sensor has to wait for the value of coverage ratio to be calculated by its neighbors to decide whether to be active or to sleep. So, the time complexity may be very high. In the worst case, the time complexity of a non-parallel algorithm may be of the order of the network size.

The number of members deployed in a cluster is usually redundant in order to take duty in turn and prolong the network lifespan. For each cluster, only a part of NCHNs are activated for each round. For the sake of energy saving, the number of active nodes should be minimized while still satisfying the required coverage ratio. For the research proposed in this paper, the number of members in a cluster is determined by expanding the estimation of the relationship between the coverage ratio and the number of nodes into every cluster. By modifying the equation (1) to fit the condition of a cluster, the number of members in a cluster can be calculated individually as (3).

$$N_{cluster} = \frac{\log(1-C_0)}{\log(1-\frac{\pi R_s^2}{\pi R_{c1}^2})} \quad (3)$$

In the equation, C_0 means the required coverage ratio provided via the message issued from BS. R_s and R_{C1} are the sensing radius of sensor node and the radius of intra-cluster communication range respectively. According to the number of members in a cluster calculated by every CHN individually, each CHN can deploy its NCHNs concurrently then reduce the time for constructing clusters.

Similar to many other cluster based topology control algorithms, it is assumed that there are several channels (bands) available, and different clusters use different channels to prevent collisions of data packets. Besides, there is a primary band assigned for transmitting all kinds of data packets in setup phase and inter-cluster data packets in working phase. Local synchronization within a cluster is assumed to apply the TDMA scheme. The packet transmission power between a CHN and an NCHN is denoted as P_1, corresponding to the intra-cluster communication radius R_{C1} [21], and the packet transmission power from a CHN to another CHN or to the BS is denoted as P_2, corresponding to the inter-cluster communication radius R_{C2}. P_1 is less than P_2 in order to reduce energy consumption and to inhibit mutual interference of data packets among different clusters.

IV. KDPC Algorithm

KDPC periodically resets the network in order to balance energy consumption of nodes and to achieve network robustness, each round of operation beginning with a setup phase to construct a new cluster topology for sensing in this round. The setup phase is primarily composed of two steps: Cluster assembling and Route setup. When clusters are assembled and route tables are established, then every active NCHN can send data packets to its cluster head using specified band and time slot in a TDMA manner. At the same time, every CHN sends data packets to its upstream CHN according to its route table as established in the stage of route setup. CHNs operate in a CSMA/CA protocol for inter-cluster communication.

A. Cluster Assembling

CHNs should be the nodes with relatively more residual energy. They should not be distributed too closely in order to prevent data collisions caused by redundant CHNs. The algorithm of the cluster assembly is shown in Algorithm (1): In this stage, all deployed nodes compete for being CHNs in CSMA/CA protocol. At first, a node has to wait a period of backoff time as defined in equation (2). If no broadcast packets are received from other CHNs, it will declare itself as a CHN by broadcasting a CHN declaration packet with transmission power P_1 to its one-hop neighboring nodes.

Algorithm (1)-Cluster Assembly
1. BS broadcasts a Round Beginning packet with the expected Coverage ratio to all nodes
2. For all nodes in the wireless sensor network
3. Calculate its backoff time for competing
4. Backoff time count down
5. While (Backoff time is not expired)
6. If (there is a CHN declaration packet received)
7. Save the CHN info into the Priority Queue using the signal strength
8. Endwhile
9. If (Backoff time expired AND there is no CHN declaration packet received)
10. Node announces itself as a CHN by broadcasting a CHN declaration packet with transmission power P1
11. Calculate the amount of NCHNs, say N, needed for the coverage ratio
12. while $N \neq 0$ {
13. If (there is a JOIN message sent from a Node, say $Node_i$, received)
14. Assign a time slot for the new NCHN
15. Reply with a PERMISSION message with the slot number to the node $Node_i$
16. N -1
17. Endif
18. If (Route setup message sent from the BS received)
19. Break this routine

```
20.  Endif
21.  If (there is a CANCEL message sent from a NCHN)
22.   Remove the slot number to delete the NCHN
23.   N +1
24.  Endif
25. }
26. Broadcast a COMPLETION message to declare the cluster is assembled
27. Else
28.  While (Priority Queue is not empty)
29.   Dequeue to get the info of CHN
30.   Send a JOIN message to the node
31.   Waiting time count down
32.   While (Waiting time is not expired)
33.    If (PERMISSION message is received)
34.     Receive and record the time slot assigned
35.     Break this routine
36.    Endif
37.    If (Time Out message sent from the BS received)
38.     Sleep in this round
39.    Endif
40.    If (there is a COMPLETION message received)
41.     Remove the CHN info from the priority queue
42.    Endif
43.   Endwhile
44.   If (there is no PERMISSION message been received)
45.     Send a CANCEL message to the CHN to abandon the join request
46.   Endif
47.  Endwhile
48.  Sleep in this round
49. Endif
50. End_Algorithm
```

If a node received CHN declaration packet from other CHNs during the backoff time, it becomes a NCHN candidate in the current round. However, the node will keep its timer going until its backoff time is expired. A NCHN candidate may receive several CHN declaration packets during the backoff time. It will store the messages into a Queue according to the strength of message signal received. When the backoff time is expired, the NCHN candidate will request to join a cluster by sending a JOIN message to the CHN with the strongest signal for registering as a NCHN of this cluster.

On the other hand, the selection of NCHNs of a cluster begins by the sending of CHN declaration packet. The CHN will calculate the amount of NCHNs needed to achieve the required coverage at first as defined in equation (3). When the backoff time of other nodes has expired, they will send JOIN message to a CHN to request for joining the cluster. Since every node is assigned different backoff times basing on their remaining energy, the CHN can receive the JOIN messages in the order of the energy remaining in the nodes. The decision as to whether a node can be a CHN's member is then very simple and efficient: When a CHN does not collect enough NCHN for the required coverage, the CHN will reply an ACCEPT message immediately when it receives a new JOIN message. When the required number of NCHNs is achieved, the CHN will stop the collection process and broadcast COMPLETION message to notify other nodes that are still stuck in backoff time to abandon the CHN. Of course, a node receiving a COMPLETION message does not mean that the node cannot be a NCHN in the current round. It can still request to join other clusters when it backoff time expires. This method will guarantee that the members of a cluster are all recruited with the NCHNs with more energy that the range can provide. The number of nodes deployed in a deployment region is usually redundant in order to take duty in turn and prolong the network lifespan. For each cluster, only a part of NCHNs are activated for each round. For the sake of energy saving, the number of active nodes should be minimized while still satisfying the required coverage ratio.

B. Route Setup

The task of this step is to establish multi-hop route from every CHN to the BS so as to ensure network connectivity. In KDPC, multi-hop routes among CHNs are established based on the minimum hop count as shown in Fig. 1, and the band of each cluster for intra-cluster communication in the working phase is determined so that the bands of any neighboring clusters are different from each other. Here, neighboring clusters are defined as the clusters that their CHNs can communicate directly with transmission power P_2.

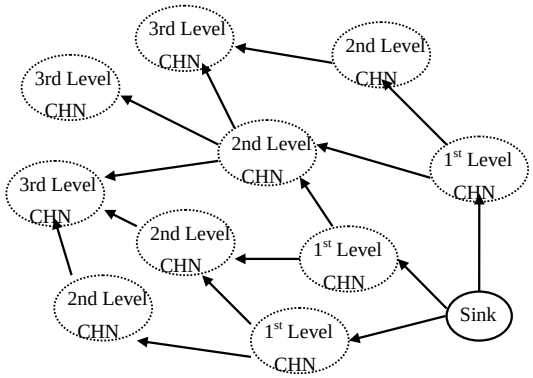


Figure 1. Multi-hop routing

The process of route setup is described as follows: The BS broadcasts a HOP packet with transmission power P2. The neighboring CHNs receive the HOP packet, which consists of the serial number of the CHN, the minimum hop count to the BS, the total number of nodes in the cluster, and the band for intra-cluster communication in the working phase. Each CHN waits a period of time Tb after it receives the HOP packet [9]. CHN may receive several HOP packets during the time Tb. It will record the minimum value of hop count as its own hop stages to BS. When the time Tb is expired, the CHN rebroadcasts the HOP packet by adding one to hop count value to downstream CHNs for following hop connections.

The band chosen by a CHN is ensured to be different from the bands of its neighboring clusters, because neighboring CHNs broadcast their HOP packets in a CSMA/CA protocol and later a CHN is forbidden to choose the same bands as those chosen by the former CHNs. A CHN would drop the HOP packet pending in the sending queue and reselect its band if it receives another HOP packet at the backoff time of CSMA/CA, to deal with the situation that the selected band happens to be the same as that in the received HOP packet. According to hop count, each CHN will choose the

neighboring CHNs with the less minimum hop count as the candidates of the upstream CHN. The candidate from which the HOP packet arrives first is chosen as the upstream. Finally, every CHN will be able to determine its minimum hop count to the BS, its upstream CHN and its unique cluster band among its neighboring CHNs.

In the working phase, every active NCHN sends data packets to its cluster head using specified band and time slot in a TDMA manner, and sleeps in other time slots. Every CHN sends data packets to its upstream CHN according to its route table established in the stage of route setup. CHNs operate in a CSMA/CA protocol for inter-cluster communication.

V. SIMULATIONS

To verify the practicality of our proposed KDPC algorithm, we conduct many extensive simulations with different numbers of nodes randomly scattered over various different sensing areas. The simulation results reported in the study are all deduced by simulating each scenario 5 times to get the average values as the results. All simulations are designed by JAVA language with Eclipse development environment.

Many wireless sensor network topology control algorithms proposed do not complete a comprehensive simulation for their methods. By examining related studies about topology control algorithms with the feature of partial coverage, we found the method named ARC [20] is an algorithm that is similar to our method with comprehensive simulation results. Thus we choose ARC as a basis for performance comparison for KDPC. We evaluate the coverage ratio achieved in each round for the two algorithms.

The major differences between KDPC and ARC algorithms include: The rule used for determining a node to active as a NCHN or just sleep in this round is different. The amounts of NCHN for each CHN will be different from ARC since the equations for calculating the amounts of NCHN are different. Furthermore, the equations that determine backoff time of each node are different, too.

A. Coverage Ratio Comparison with ARC

The related simulation parameters are listed below:

There are N nodes uniformly and independently distributed in a deployment range. The BS node is located at the corner with coordinates (0,0). The sensing range is set as a circle with a radius of R_s. The communication ranges for intra-cluster and inter-cluster are circles with radius of R_{c1} and R_{c2}, respectively. It is noted that the value of R_{c2} is three times bigger than R_{c1} in the simulation.

For the calculation of backoff time in simulation, the parameters of ARC are set as: the weighted ratio of T1:T2 is 7:3 that is the same as the original design of ARC. For KDPC, the three weighted values, T1, T2, and T3 are 1:6:3 that are observed by the study to offer best energy balance in most of the simulations.

Energy consumption of a sensor node can be divided into two parts: energy consumed by the sensing module, and energy consumed by the transceiver. The former depends on the type of sensing module, while the latter consists of the energy costs for necessary data transmission, overhearing, and retransmissions due to collisions, respectively. Traffic load in our simulations is set very light such that there is almost no collision. As a result, the energy consumed by the transceiver is mainly for data transmission and overhearing. We adopt the energy model in [21] and assume that the energy cost of overhearing a packet equals to that of receiving a packet.

The simulation parameters are set the same as the ARC made in [9]. For a coverage emulated as (1), and the nodes that cannot connect to the BS are omitted for coverage. By setting the parameters as listed below:

Deployment range: 100*100 m^2

Number of Nodes: 1000

QoS (Expected Coverage Ratio): 90%

R_s: 5m R_{c1}: 20m, R_{c2}: 60m

Power initiated: 5J

Number of rounds: 2000

Working time per round: 1000 seconds

Transmission rate: 5 seconds/packet

Packet size: 32 Bits

Fig. 2. is the average coverage ratio achieved in the first 2000 rounds. We can observe from the figure that the coverage ratio of ARC begins to drop down around 1500 rounds. For the last round, the coverage ratio is dropped below 0.7. On the contrary, KDPC can prolong the required sensing quality until the last 100 rounds. The dropped ratio achieved is about 0.75 in the last round that is still higher than ARC.

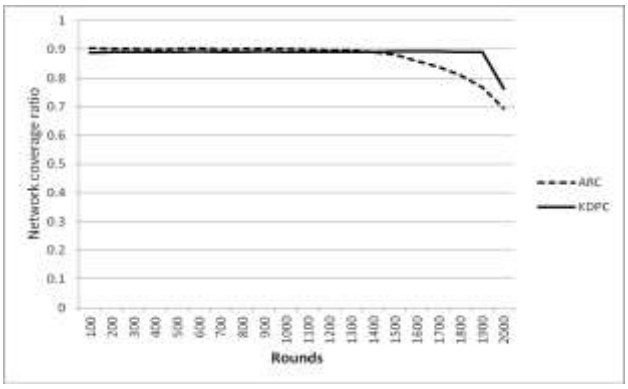


Figure 2. Average coverage ratio for KDPC and ARC

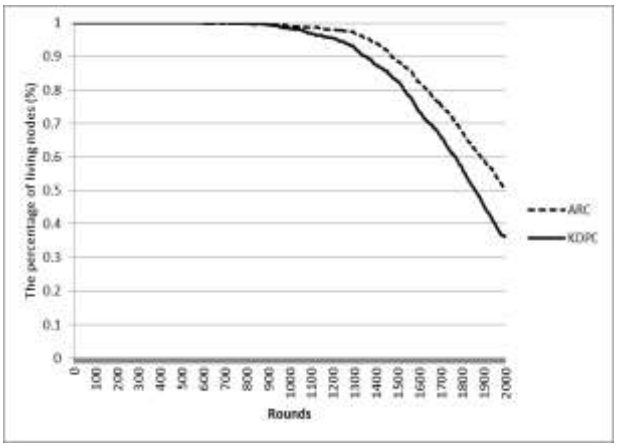


Figure 3. The number of living nodes

The average number of living nodes for the testing rounds are shown in Fig. 3. The curves show that the number begins to drop down from around 1000 rounds. Because of the higher coverage ratio achieved by KDPC, the energy that has been consumed is inevitably more than ARC. The truth leads the remaining living nodes of KDPC to be less than ARC. It is interesting that by comparing the coverage ratio shown in Fig. 2 and the number of living nodes in Fig. 3, we can find that KDPC can always achieve a higher QoS by means of fewer living nodes than ARC.

B. Performance Improved by Uneven Deployment

By examining the status of each round in simulations, we found that the degradation of coverage ratio always induced by the exhausting of energy of innermost nodes, where the nodes in the innermost layer refers to the nodes that are located in the circle of the BS' communication scope. It is reasonable since the nodes in the innermost layer will spend more energy to transmit the packets that came from the outer ranges because of multi-hop transmission. The truth leads the research to simulate the conditions that the wireless sensor network deploys more nodes in the innermost layer to find a better strategy for physical node deployment. We first define a QoS threshold for the simulations. QoS threshold means the lower bond of the coverage ratio that a normal wireless sensor network can offer. If the coverage ratio achieved is lower than the threshold, the wireless sensor network is treated as dead. In the simulations, we define 90% of the expected coverage ratio as the threshold. It means that the wireless sensor network will be claimed to be dead when the coverage ratio achieved is lower than 81% since the expected ratio is 90%.

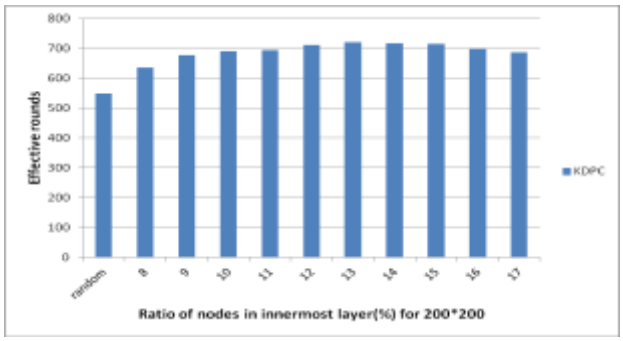


Figure 4. Rounds offered for 200*200 deployment range

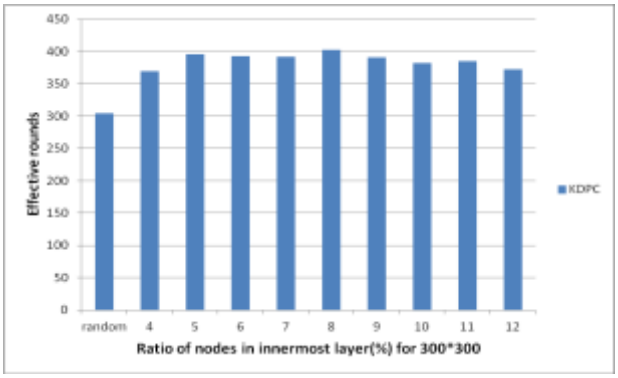


Figure 5. Rounds offered for 300*300 deployment range

The simulations are made by different deployment ranges with same node density to observe the characters of density effects for the innermost layer under different multi-hop overhead. The range size and numbers of nodes to be simulated are 200*200 with 4000 nodes, 300*300 with 9000 nodes, and 400*400 with 16000 nodes. In the simulations, we first determine the number of nodes that should be located in the inner-most layer according to the ratio of expected density, deploy the nodes randomly in the range. The rest of the nodes are then distributed onto the outer range normally for simulation. Fig. 4 to Fig. 6 show the simulation results for various ranges. The y-axis of the figures is the rounds that KDPC can offer to meet the QoS lower bound, and the x-axis is the density of the innermost range in simulations. It is noted that the word, Random, appeared in x-axis is the simulation with normal distribution. The values for the Random conditions are 7.1%, 3.1%, and 1.8% for the three deployment ranges.

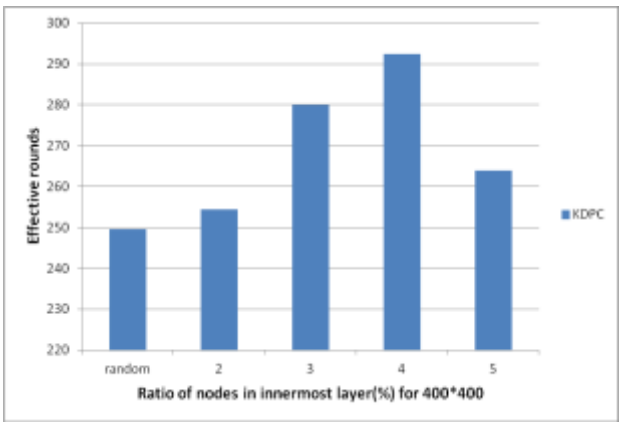


Figure 6. Rounds offered for 400*400 deployment range

From the results shown in the figures, we can find that when the distribution density of nodes in the innermost layer has been increased to twice than the normal distribution, the number of rounds that has been achieved for the QoS requirement can be increased for 17% to 32%. The energy consumption used for the required QoS can also be raised. In 200*200 deployment range, increasing the density of the innermost layer to double can use 67% energy for the service that is higher than 53% which has been used for normal distribution. For the cases of 300*300 and 400*400 deployment ranges, the energy consumption can also been raised from 42% to 58%, and 43% to 49%.

It is worthy to point out that by observing the status of the last rounds in these simulations, we find that the cause of the coverage degradation is changed from the lack of nodes in the innermost layer to the lack of nodes in the second layer of the wireless sensor network. It is reasonable because the transmission overhead is increased from outside to inside nodes, when the number of nodes in the inner layer is enough for transmission, the exhausting condition will happen in the outside layer in a multi-hop transmission. The feature shows us another interesting topic for further research: How to distribute sensor nodes for a cluster-based multi-hop wireless sensor network to prolong the lifespan. The distribution

function should not be a normal distribution but a function determined by various parameters such as range size, number of nodes, transmission cost, etc.

VI. CONCLUSION

This research proposes a topology control algorithm for large-scale wireless sensor networks with randomly deployed nodes. The study is done under the considerations for the real world. For example, a wireless sensor network may reduce its QoS to save the nodes' energy for longer usage. As a matter of fact, it is difficult and time consuming to recharge sensor nodes or relocate new sensor nodes. A realistic wireless sensor network should keep a required sensing quality by graceful degradation to leave enough time for the user to rebuild the wireless sensor network. The assumption that all nodes can transmit data to BS directly is not realistic, either. Since the cost, size and power limitation, a sensor node is always been built without GPS support. A cluster based multi-hop wireless sensor network can resolve the connectivity problem by the techniques of wireless communication. Based on the considerations, the algorithm proposed is designed with several novel features: First, KDPC forms a multi-hop cluster network with a required connectivity by using a novel cluster head competition scheme. Second, less redundant nodes are activated than the existing algorithms since the number of sensor nodes used to achieve the required coverage ratio will be determined and limited by the algorithm. Third, the algorithm can organize sensor nodes into clusters actively to achieve required coverage ratio as long as possible. Finally, KDPC is suitable for practical applications of large-scale or high-density wireless sensor networks due to its distributed processing and scalable cluster topology.

There are many issues worthy of investigation. For example, an interesting condition is found from the simulation that KDPC wireless sensor networks are always dead when all of the nodes nearby the BS node are dead. It is reasonable because these nodes must transfer the messages that come from the outer range when they act as a CHN. The condition prompts us that if there are more sensor nodes located in the innermost range, the lifespan of the scheme will be extended efficiently. As another example, the messages passed through CHNs to BS are transmitted by a data-centric routing paradigm, an energy-efficient routing protocol that is worth proposing for multi-source transmission scenarios. An efficient routing protocol can significantly reduce network traffic, and thus promote energy efficiency.

REFERENCES

[1] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Net-works," *IEEE Comm. Magazine*, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] D. J. Cook and S. K. Das, Smart Environments Technologies, Protocols, and Applications, *1st ed. John Wiley, New Jersey*, 2005, ch. 2, pp. 13-46.

[3] Zhen Jiang, Jie Wu, Kline, R. and Krantz, J, "Mobility Control for Complete Coverage in Wireless Sensor Networks", *ICDCS*, pp. 291-296, June. 2008.

[4] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "application-specific protocol architecture for wireless micro sensor networks," *IEEE Trans. On Wireless Communications*, vol. 1, no. 4, PP. 660–670, Oct. 2002.

[5] H. Zhang and J. Hou, "On Deriving the Upper Bound of α-Lifetime for Large Sensor Networks," *in Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, Tokyo, May 2004, pp. 121-132.

[6] H. Bai, X. Chen, Y. Ho, and X. Guan, "Percentage Coverage Configuration in Wireless Sensor Networks," *Lecture Notes in Computer Science*, vol. 3758, pp. 780-791, 2005.

[7] Y. Liu and W. Liang, "Approximate Coverage in Wireless Sensor Networks," *in IEEE Conf. Local Computer Networks 30th Anniversary* (LCN '05), Sydney, Nov. 2005, pp. 68-75.

[8] Y. Wu, C. Ai, S. Gao, and Y. Li, "p-Percent Coverage in Wireless Sensor Networks," *Lecture Notes in Computer Science*, vol. 5258, pp. 200-211, 2008.

[9] Y. Li, C. Vu, C. Ai, G. Chen, and Y. Zhao, "Transforming complete coverage algorithms to partial coverage algorithms for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, Issue 4, pp. 695-703, Apr. 2011.

[10] L. Yu, N. Wang, and X. Meng, "Real-Time Forest Fire Detection with Wireless Sensor Networks," *Wireless Comm. Networking and Mobile Computing*, vol. 2, nos. 23-26, pp. 1214-1217, Sept. 2005.

[11] L Liu, and H. Ma, "On Coverage of Wireless Sensor Networks for Rolling Terrains," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, Issue 1, pp. 118-125, Jan. 2012.

[12] F. P. Quintao, F. G. Nakamura, and G. R. Mateus, "A hybrid approach to solve the coverage and connectivity problem in wireless sensor networks," *in Workshop on Meta-heuristics: Design and Evaluation of Advanced Hybrid Meta-heuristics*, United Kingdom, Nov. 2004.

[13] Y. H. Wang, C. Y. Yu, and P. F. Fu, "A coverage and connectivity method to cluster topology in wireless sensor networks," *in 21st International Conference on Advanced Information Networking and Applications Work-shops*, Niagara Falls, Ont., May 2007, pp. 97–102.

[14] M. A. Habib, and K. D. Sajal, " Clustering-based minimum energy wireless m-connected k-covered sensor networks," *Lecture Notes in Computer Science(LNCS)*, vol. 4913, pp. 1–16., 2008.

[15] J. N. Al-Karaki, A. E. Kamal, "Routing Techniques in Sensor Networks: A Survey," *IEEE Wireless Communications*, vol. 11, issue 6, pp. 6- 28, Dec. 2004.

[16] K. L. Pang, and Y. Qin, "The Comparison Study of Flat Routing and Hierarchical Routing in Ad Hoc Wireless Networks, " *in 14th IEEE International Conference on Networks*(ICON '06), Singapore, Sep. 2006, PP. 1-6.

[17] K. Zheng, L. B. Tong, and W. J. Lu, "Location-Based Routing Algorithms for Wireless Sensor Network," *ZTE Communications*, No. 1, 2009.

[18] A. Joshi, L. Priya, "A Survey of Hierarchical Routing Protocols in Wireless Sensor Network," i*n 2010 2nd International Conference on Computer Engineering and Tech-nology (ICCET)*, Chengdu 2010, pp. V3-650 - V3-654.

[19] K. Iwanicki, M. van Steen, "On Hierarchical Routing in Wireless Sensor Networks," *in IPSN '09 Proceedings of*

the 2009 International Conference on Information Processing in Sensor Networks, San Francisco, April 2009, pp. 133 – 144.
[20] N. Xu, A. Huang, T. W. Hou, and H. H. Chen, "Coverage and connectivity guaranteed topology control algorithm for cluster-based wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 12, issue 1, pp. 23-32, Jan. 2010.
[21] B. Q. Kan, L. Cai, H. S. Zhu, and Y. J. Xu, "Accurate Energy Model for WSN Node and Its Optimal Design," *Journal of Systems Engineering and Electronics*, vol. 19, issue 3, pp. 427–433, June 2008.

Lei Wang received the PH. D. degree in Computer Science and Information Engineering from Feng-Chia University in 2000. He is the director of Embedded System Development and Research Center in Feng-Chia University. His research interests include micro-processor architectures, embedded systems, network, and image processing

Jui-Yu Yang is an undergraduate student in the Department of Electrical Engineering at Feng-Chia University. His interest includes sensor network, system software, and object oriented programming.

Yu-Yun Lin is an undergraduate student in the Department of Electrical Engineering at Feng-Chia University. Her interest includes sensor network, system modeling, and theoretical analysis.

Wei-Jun Lin received the bachelor degree in Electrical Engineering from Feng-Chia University in 2013. He is an research assistant in the Embedded System Development and Research Center in Feng-Chia University.. His research interests include Object Oriented programming, embedded system, and network applications design.

Achieving VoIP Guarantee in Wireless Local Area Networks

Wen-Li Li
Department of Computer Science and Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan
Department of Computer Science and Information Engineering, Tajen University, Pingtung, Taiwan
Email: lwl@tajen.edu.tw

Chun-Hung Richard Lin
Department of Computer Science and Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan
Corresponding author, Email: lin@cse.nsysu.edu.tw

Chih-Heng Ke
Department of Computer Science and Information Engineering, National Quemoy University, Kinmen, Taiwan
Email: smallko@gmail.com

***Abstract*—Recently, voice over Internet Protocol (VoIP) has gained much attention in wireless local area networks (WLANs). Although IEEE 802.11e enhanced distributed channel access (EDCA) has been standardized to provide voice traffic with quality of service (QoS) support, the voice quality could still be severely degraded by the traffic transmitted from low-priority stations (LP-STAs). Like 802.11b, the 802.11e EDCA also has the performance anomaly problem. Therefore, the voice quality of the high-rate stations (HR-STAs) could be severely degraded by the traffic transmitted from low-rate stations (LR-STAs). In fact, the LP-STAs and LR-STAs can be present simultaneously in practical WLAN environments. In this paper, we consider the effects of LP-STAs and/or LR-STAs on voice traffic and propose an extended EDCA scheme called voice differentiation-EDCA (VD-EDCA) to protect voice traffic from LP-STAs and/or LR-STAs. With VD-EDCA, the voice AC in a HR-STA has an absolute priority over LP-STAs and LR-STAs when they are notified that the wireless delay of a voice frame at the QoS access point (QAP) is larger than or equal to the predefined maximal delay threshold. We evaluate the performance of the proposed VD-EDCA scheme through extensive simulations. The simulation results show that, with appropriate maximal delay threshold settings, the proposed scheme well protects all of the VoIP calls transmitted by HR-STAs from LP-STAs and/or LR-STAs.**

***Index Terms*—VoIP; WLAN; IEEE 802.11e; EDCA; QoS; Performance Anomaly**

I. INTRODUCTION

Voice over Internet Protocol (VoIP) is a telephony technology which delivers voice packets over IP-based packet-switched networks. Recently, VoIP has become an attractive and popular application because it provides the cheaper calls than those through the traditional public switched telephone network (PSTN). Furthermore, with the widespread deployments of IEEE 802.11 wireless local area networks (WLANs) [1], VoIP over WLAN (VoWLAN) has become one of the most interesting research topics in recent years.

VoIP is a real-time application that requires very strict quality of service (QoS) requirements on delay and packet lose. The main challenge in VoWLAN is the QoS provisioning capabilities of WLANs since currently the QoS supporting capabilities of the most commonly used WLAN schemes are insufficient to achieve QoS guarantee for voice traffic.

The distributed coordination function (DCF), the mandatory MAC scheme in IEEE 802.11 standard, cannot provide any QoS support since it treats all frames types equally. Therefore, the IEEE 802.11e enhanced distributed channel access (EDCA) [2] was proposed to provide QoS support for real-time applications by the IEEE 802.11 working group.

As an extension of DCF, the 802.11e EDCA is a priority-based access control scheme that provides service differentiation among voice, video, best effort and background traffic by defining four prioritized access categories (ACs) respectively, i.e., *AC_VO*, *AC_VI*, *AC_BE*, and *AC_BK*. As a result, the voice traffic has a much better chance of gaining the medium than other types of traffic. However, since EDCA provides only a relatively higher priority for *AC_VO*, the voice quality could still be severely degraded by the traffic from low-priority stations (LP-STAs), including DCF stations and non-voice ACs, particularly in a highly congested environment.

On the other hand, IEEE 802.11 provides multi-rate capability. For example, IEEE 802.11b supports rates of 1, 2, 5.5, and 11 Mbps, while IEEE 802.11g supports eight different transmission rates ranging from 6 to 54 Mbps. However, the standards face a fundamental performance anomaly problem [13] in a multi-rate environment, which is the phenomenon that the throughput of high-rate stations (HR-STAs) is down-equalized to that of the lowest-rate stations due to the fair channel contention

doi:10.4304/jnw.9.12.3230-3236

between low-rate stations (LR-STAs) and HR-STAs. Similar to the above standards, the IEEE 802.11e EDCA also has a performance anomaly problem. Therefore, the voice quality of HR-STAs could be severely degraded by the traffic transmitted from LR-STAs.

In fact, the LP-STAs and LR-STAs can be present simultaneously in a WLAN. In this paper, we consider the effects of LP-STAs and/or LR-STAs on voice traffic and propose an extended EDCA scheme called voice differentiation-EDCA (VD-EDCA) to protect VoIP calls transmitted by HR-STAs from LP-STAs and/or LR-STAs by using adaptively appropriate interframe space (*IFS*) values.

The primary contributions of this paper are the follows:

We identify two factors of degrading the QoS of voice traffic, namely LP-STAs and LR-STAs. By considering the two negative factors, our novel MAC scheme can provide QoS guarantee for the *AC_VO* in HR-STAs to well protect all of the VoIP calls transmitted by HR-STAs from LP-STAs and/or LR-STAs, whereas most previous schemes only consider one of the two factors, but not both.

Our scheme is capable of guaranteeing the *AC_VO* in a HR-STA the absolute priority over LP-STAs and LR-STAs with appropriate maximal delay threshold settings. The smart control mechanism that adaptively adjusts the IFS values of LP-STAs and LR-STAs after each data/ACK transmission exchange is designed so that the channel access priorities among stations can be changed immediately.

We conduct extensive simulations to evaluate the performance of the proposed scheme, and compare it with that of three well-known schemes. The results show that our scheme outperforms those schemes.

The rest of this paper is organized as follows. In Section II, the background and related work are reviewed. In Section III, the proposed VD-EDCA mechanism is described in detail. Simulation results are presented in Section IV and we conclude this paper in Section V.

II. Background and Related Work

A. IEEE 802.11 DCF

The DCF is a channel access scheme based on the carrier sense multiple access with collision avoidance (CSMA/CA) protocol. Two mechanisms defined for packet transmission in DCF are, namely, the basic access mechanism and the optional request to send/clear to send (RTS/CTS) mechanism. Under the basic access mechanism, a station desiring to transmit first senses the medium. If the medium is determined to be idle for a distributed interframe space (*DIFS*) period, the station transmits immediately. Otherwise, the station will enter the backoff procedure to avoid collisions among stations.

The backoff procedure works as follows. The station sets its backoff timer to a random backoff time which is an integer uniformly chosen in the range of [0, *CW*], where *CW* is the contention window. Initially, *CW* is set to CW_{min}. After each failed transmission, *CW* is doubled until it reaches the maximum contention window size, CW_{max}. When the packet is transmitted successfully or it is discarded caused by failed transmissions, *CW* will be reset to the CW_{min}. Backoff timer is decreased by *aSlotTime* whenever the channel is sensed idle for the duration of *aSlotTime* following a *DIFS* period. If the channel is determined to be busy during *aSlotTime* period, then the backoff procedure is suspended. Backoff procedure will be resumed when the medium becomes idle again for the duration of a *DIFS* period. Transmission shall commence whenever the backoff timer reaches zero. Consequently, the station with the lowest backoff timer will gain the contention for the medium.

In addition, DCF uses a well-known stop-and-wait automatic repeat-request (ARQ) mechanism as an error control scheme. After transmitting a unicast frame that requires an acknowledgement to response, the sender does not send any further frames until it receives a positive ACK frame from the receiver. After receiving an error-free frame, the receiver will send an ACK frame back to the sender. If the sender does not receive the ACK frame during the *ACKtimeout* interval, retransmission will be scheduled by the sender.

B. IEEE 802.11e EDCA

The 802.11e EDCA, an extension of 802.11 DCF, provides services differentiation among different types of traffic. In EDCA, four ACs are defined to support eight different user priorities. The four ACs are: *AC_VO*, *AC_VI*, *AC_BE*, and *AC_BK*. Each corresponds to its prioritized queue for voice, video, best effort, and background traffic, respectively. When a packet arrives at MAC, it will be mapped into an appropriate *AC* according to its priority. In addition, each *AC* is associated with a set of AC-specific parameters called the EDCA parameter set consisting of arbitrary interframe space number (*AIFSN*[*AC*]), minimum contention window (CW_{min}[*AC*]), and maximum contention window (CW_{max}[*AC*]). A higher priority *AC* is assigned with smaller parameter values to have a much better chance of gaining the medium. As a result, the four ACs are differentiated by distinct EDCA parameter sets.

On the whole, each *AC* behaves like an independent DCF station. Each *AC* starts transmitting or resuming the backoff procedure whenever the channel is sensed idle for the arbitrary interframe space (*AIFS*) time, which is determined by the *AIFSN*[*AC*] according to the following equation:

$$AIFS[AC] = SIFS + AIFSN[AC] \times aSlotTime . \quad (1)$$

C. Related Work

To provide strict QoS for voice traffic, studies have been massively present in the literature. In [3], voice traffic in the access point (AP) was given strict priority over data traffic by using zero backoff time and prioritized queuing policy for downlink voice traffic. In [4], RT and NRT queues were implemented inside the AP for real-time and non-real-time packets, respectively. The AP did not serve the NRT queue whenever the RT queue was not empty. In [5], the rate control mechanism was proposed to control the impact of best-effort traffic on

voice traffic by regulating the packet sending rate at which the best-effort packets were delivered to the MAC-layer. In [6], the ACK skipping technique was proposed to reduce the impact of legacy DCF stations on voice traffic. Lee et al. [7] proposed the differentiated service-EDCA (DS-EDCA) scheme guaranteeing voice traffic the most stringent priority by carefully assigning the *AIFS* value of the lower priority traffic. That *AIFS* was set to a value larger than *AIFS* of the higher priority AC plus its *CWmax* size. In [8], the non-zero ACK (NZ-ACK) scheme was proposed to mitigate the effects of DCF users on voice traffic by introducing a new NZ-ACK frame. Upon receiving a NZ-ACK frame, each DCF station inherently deferred its channel access according to the non-zero duration value included in the received NZ-ACK frame. Wu et al. [9] showed that the dropping rates for voice packets could be significantly reduced by using a larger *AIFSN* for *AC_BE* (i.e., *AIFSN*[*AC_BE*]) to differentiate the priorities of voice and best-effort packets. In [10], the specific EDCA parameter values for QoS access point (QAP) and wireless stations were recommended. In [11], the DB-ACK scheme was proposed to protect voice traffic from best-effort traffic by using adaptive DIFS and AIFS values to DCF and EDCA stations respectively. In [12], the optimal configuration of the EDCA parameters in ad-hoc mode was computed. Among the schemes, only the DS-EDCA and DB-ACK schemes can guarantee *AC_VO* to have an absolute priority over other ACs; however, in the DS-EDCA scheme, the throughput of best-effort traffic would be severely degraded due to a fixed and larger *AIFS* value for *AC_BE* (i.e., *AIFS*[*AC_BE*]).

As for the solutions of the performance anomaly, at present two basic methods exist, namely contention window differentiation (CWD) [14] and packet size differentiation (PSD) [15], [16]. In the CWD method, the initial contention window size for each transmission rate is set inversely proportional to the transmission rate. In the PSD approach, the HR-STAs transmit longer packets, while the LR-STAs transmit shorter packets. Research shows that the CWD method outperforms the PSD method in terms of throughput and delay [17], [18].

III. VOICE DIFFERENTIATION-EDCA (VD-EDCA)

In this section, the VD-EDCA scheme is proposed. We assume that the transmission rate of the QAP is fixed and is at its highest rate. If the transmission rate of a wireless station is lower than the one adopted in the QAP, the station is regarded as a LR-STA. Otherwise, it is regarded as a HR-STA.

To fulfill the requirements of high voice quality, the QAP keeps track of the wireless delay for each voice frame. Initially, the IFS factor (*IFSF*) value is determined, which is used to regulate IFS values of LP-STAs and LR-STAs. When the QAP is ready to send an ACK frame after the successful receipt of a packet, it checks whether there is any voice frame in MAC. If there is no voice frame in MAC, the QAP resets the *IFSF* value to zero and sends a normal ACK frame back to the sender. Otherwise, the QAP converts the experienced wireless delay of the voice frame being transmitted in MAC to an appropriate *IFSF* according to the following equation:

$$IFSF = IFSF(D_c) = \begin{cases} 0 & D_c < D_{min} \\ \left\lceil CW_{max}[AC\_VO] \times \dfrac{D_c - D_{min}}{D_{max} - D_{min}} \right\rceil & D_{min} \le D_c < D_{max} \\ CW_{max}[AC\_VO] + 1 & D_c \ge D_{max} \end{cases} \quad (2)$$

where D_c denotes current wireless delay of the voice frame being transmitted in MAC, $CW_{max}[AC\_VO]$ is the maximal contention window value for *AC_VO*, and the two predefined parameters D_{min} and D_{max}, in milliseconds, are the minimal and maximal delay thresholds, respectively. If D_c is below D_{min}, the *IFSF* value is set to zero. If D_c varies from D_{min} to D_{max}, the *IFSF* is an integer value varying from zero to $CW_{max}[AC\_VO]$. Otherwise, the *IFSF* value is set to $CW_{max}[AC\_VO] + 1$.

To inform both LP-STAs and LR-STAs of the delay information (i.e., the *IFSF* value), the QAP piggybacks the *IFSF* value into the Duration/ID field of the ACK frame by utilizing the reserved values of the Duration/ID field in the interval [32769, 32770 + $CW_{max}[AC\_VO]$]. Therefore, the content value of the Duration/ID field of the ACK frame is set to be equal to the sum of 32769 and the *IFSF* value when the QAP has voice frames to be transmitted.

On the other hand, when a wireless station overhears an ACK frame from the QAP, the Duration/ID field is checked. If a normal ACK is received, the *DIFS* and *AIFS* values are reset to their default values as specified in the standards. Otherwise, if the value of the Duration/ID field is in the interval [32769, 32770 + $CW_{max}[AC\_VO]$], the IFS values of LP-STAs and LR-STAs are regulated as follows:

$$DIFS = DIFS_{802.11} + (Duration - 32769) \times aSlotTime . \quad (3)$$

$$AIFS[AC] = AIFS_{802.11e}[AC] + (Duration - 32769) \times aSlotTime . \quad (4)$$

where the *Duration* is the value of the Duration/ID field in the MAC header of the ACK frame, the $DIFS_{802.11}$ is the default *DIFS* value as specified in the IEEE 802.11, the $AIFS_{802.11e}[AC]$ is the default *AIFS*[*AC*] value as specified in the IEEE 802.11e.

In addition, to regulate the internal contention among the ACs at the QAP, the non-voice *AIFS* values at the QAP are adjusted as follows:

$$AIFS[AC] = AIFS_{802.11e}[AC] + IFSF \times aSlotTime . \quad (5)$$

Obviously, the longer a voice frame waits, the larger the *IFSF* value becomes and consequently the longer the LP-STAs and LR-STAs must defer. Note that, as shown in Fig. 1, our VD-EDCA scheme guarantees the *AC_VO* in a HR-STA the absolute priority over LP-STAs and LR-STAs when they are notified that the wireless delay of a voice frame at QAP is larger than or equal to the predefined maximal delay threshold.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the three representative EDCA-based schemes, i.e., the standard EDCA scheme, the DS-EDCA scheme, and the proposed VD-EDCA scheme. In addition, we apply the CWD mechanism to the wireless stations in the IEEE 802.11e EDCA network, denoted by CWD$^+$, to study its capability of protecting VoIP calls especially when the LR-STAs are present. The schemes are implemented by extending the NS-2 simulator [19].

TABLE I. BASIC PARAMETERS USED IN SIMULATIONS

Parameter	Value
aSlotTime	20 us
SIFS	10 us
CW_{min}	31
CW_{max}	1023
AIFSN[*AC_VO*]	2
AIFSN[*AC_VI*]	2
AIFSN[*AC_BE*]	3
CW_{min}[*AC_VO*]	7
CW_{min}[*AC_VI*]	15
CW_{min}[*AC_BE*]	31
CW_{max}[*AC_VO*]	15
CW_{max}[*AC_VI*]	31
CW_{max}[*AC_BE*]	1023

TABLE II. THE INITIAL CONTENTION WINDOW SIZE USED IN CWD$^+$ FOR DIFFERENT TRANSMISSION RATES

Transmission rate (Mbps)	CW_{min}	CW_{min}[*AC_VO*]	CW_{min}[*AC_BE*]
11	31	7	31
5.5	62	14	62
2	171	39	171
1	341	77	341

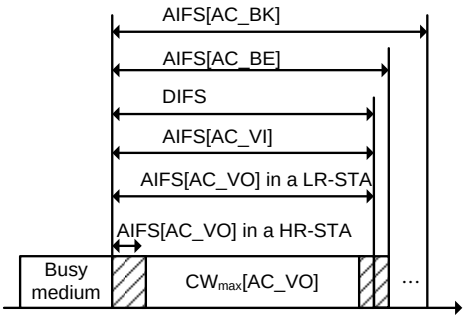


Figure 1. The VD-EDCA channel access when wireless stations are notified that D_c is larger than or equal to D_{max}

The simulation network is composed of a wired and a wireless network. The wireless network consists of several wireless stations that connect to the wired network through a QAP. The transmission rate of the QAP is fixed and is set to 11 Mbps. The transmission rate of a wireless station is adaptively set to 1, 2, 5.5 or 11 Mbps according to the channel condition. Unless otherwise stated, it is set to 11 Mbps. Two types of data traffic are considered: voice traffic and best-effort traffic. Packets of each voice flow are generated by a CBR/UDP source at a rate of 64 Kbps with a fixed payload size of 160 bytes, as generated by G.711 voice coder. Packets of each best-effort flow are generated by a CBR/UDP source at a rate of 1 Mbps with a fixed payload size of 1000 bytes. We assume that each wireless station can generate one flow at most. Since the EDCA-based schemes allow legacy DCF stations to coexist with them, in this paper we consider two scenarios for best-effort traffic. The first scenario is the Scenario AC_BE where the best-effort traffic is transmitted from *AC_BE* stations, and the second scenario is the Scenario DCF where the best-effort traffic is transmitted from DCF stations. Table I shows the basic parameters used in our simulations, which are used as recommended in [1] or [2]. The initial contention window size for each transmission rate used in the CWD$^+$ scheme is summarized in Table II. In order to maintain acceptable voice quality, an upper bound end-to-end one-way delay of 150 ms for a voice packet and a maximum tolerable packet loss rate of 5% for a voice flow are recommended by ITU-T [20] and ETSI [21], respectively. Thus, the wireless delay experienced by a voice packet should be small so that the overall end-to-end delay of a voice packet can meet the delay requirement; the packet loss rate of a voice flow in WLANs should be low so as to meet the packet loss rate requirement. On the basis of the above considerations, in our studies, the wireless delay of 70 ms is considered to be the maximal acceptable delay and the packet loss of each voice flow at wireless link should be below 1%. Note that the delayed packets are handled as lost if they exceed the delay bound. Accordingly, provided that there is no coexisting background data traffic, there can be up to nine calls with acceptable voice quality in the EDCA scheme, which is in conformance with the simulation results in [10].

TABLE III. THE MAXIMUM NUMBER OF VOIP CALLS PROTECTED BY DIFFERENT SCHEMES WHEN THERE EXIST 60 BEST-EFFORT STATIONS

Scenario	EDCA	CWD$^+$	DS-EDCA	VD-EDCA^1	VD-EDCA^2
AC_BE	1	1	9	9	9
DCF	1	1	1	9	9

* VD-EDCA^1 : the VD-EDCA scheme with D_{min} = 0 (ms) and D_{max} = 0.1 (ms)
* VD-EDCA^2 : the VD-EDCA scheme with D_{min} = 10 (ms) and D_{max} = 20 (ms)

A. Effects of LP-STAs

To understand the impact of LP-STAs on voice quality and identify how well our proposed scheme can protect VoIP traffic from LP-STAs, we consider the case where there are only LP-STAs in WLANs. Fig. 2 shows the average wireless delay when there exist 60 best-effort flows. As can be seen from Fig. 2(a) which is in Scenario AC_BE, we observe that both VD-EDCA and DS-EDCA schemes well protect voice traffic from best-effort traffic because the average wireless delay on the uplink and downlink remains very small. However, both EDCA and CWD$^+$ schemes cannot effectively protect voice traffic from best-effort traffic because the average wireless delay on the downlink far exceeds the delay bound when the number of VoIP calls is more than one. Fig. 2(b) shows the average wireless delay in Scenario DCF. The proposed VD-EDCA scheme well protects voice traffic from best-effort traffic because the average wireless delay on the uplink and downlink remains fairly small. However, the EDCA, CWD$^+$, and DS-EDCA schemes

cannot effectively protect voice traffic from best-effort traffic since the average wireless delay on the downlink is on a timescale of seconds when the number of VoIP calls exceeds one. We summarize the maximal number of VoIP calls protected by the schemes in Table III. Note that only the proposed VD-EDCA scheme well protects voice traffic from LP-STAs in both scenarios.

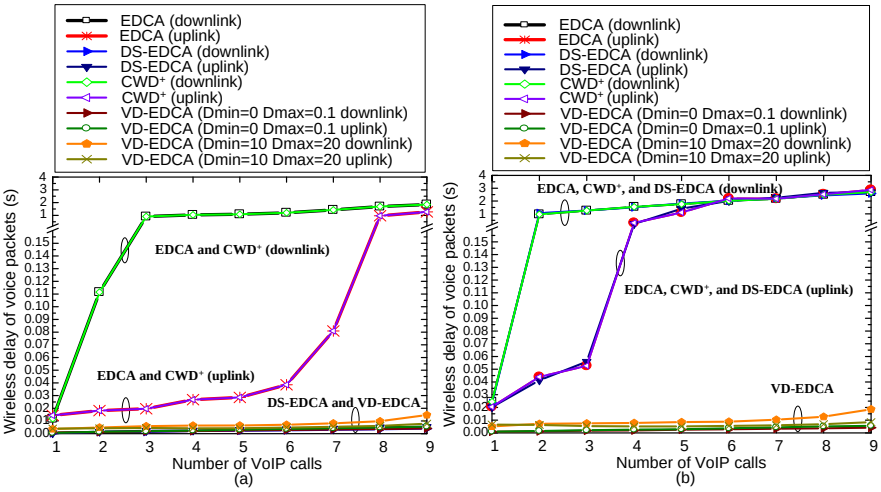


Figure 2. Average wireless delay for VoIP calls when there are 60 best-effort flows. (a) Scenario AC_BE (b) Scenario DCF

TABLE IV. THE NUMBER OF VOIP CALLS PROTECTED BY DIFFERENT SCHEMES IN A MULTI-RATE ENVIRONMENT

N1	N2	N3	N4	N5	N6	EDCA	CWD+	DS-EDCA	VD-EDCA[1]	VD-EDCA[2]
9	0	0	0	0	0	9	9	9	9	9
8	1	0	0	0	0	0	9	0	9	8
7	2	0	0	0	0	0	7	0	9	7
6	3	0	0	0	0	0	6	0	6	6
5	4	0	0	0	0	0	5	0	5	5
4	5	0	0	0	0	0	4	0	4	4
3	6	0	0	0	0	0	3	0	3	3
2	7	0	0	0	0	0	2	0	2	2
1	8	0	0	0	0	0	1	0	1	1
9	0	0	1	0	0	0	4	9	9	9
9	0	0	2	0	0	0	0	9	9	9
9	0	0	0	0	1	0	4	0	9	9
9	0	0	0	0	2	0	0	0	9	9
9	0	60	60	0	0	0	0	9	9	9
9	0	0	0	60	60	0	0	0	9	9

* N1: the number of *AC_VO* stations with a transmission rate of 11 Mbps
* N2: the number of *AC_VO* stations with a transmission rate of 1 Mbps
* N3: the number of *AC_BE* stations with a transmission rate of 11 Mbps
* N4: the number of *AC_BE* stations with a transmission rate of 1 Mbps
* N5: the number of DCF stations with a transmission rate of 11 Mbps
* N6: the number of DCF stations with a transmission rate of 1 Mbps
*VD-EDCA[1] : the VD-EDCA scheme with D_{min} = 0 (ms) and D_{max} = 0.1 (ms)
*VD-EDCA[2] : the VD-EDCA scheme with D_{min} = 10 (ms) and D_{max} = 20 (ms)

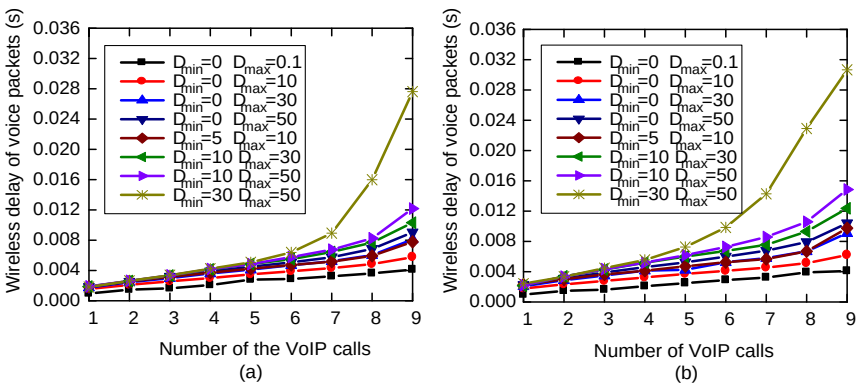


Figure 3. The effects of delay thresholds on average wireless delay. (a) The number of best-effort flows is 5 (b) The number of best-effort flows is 10

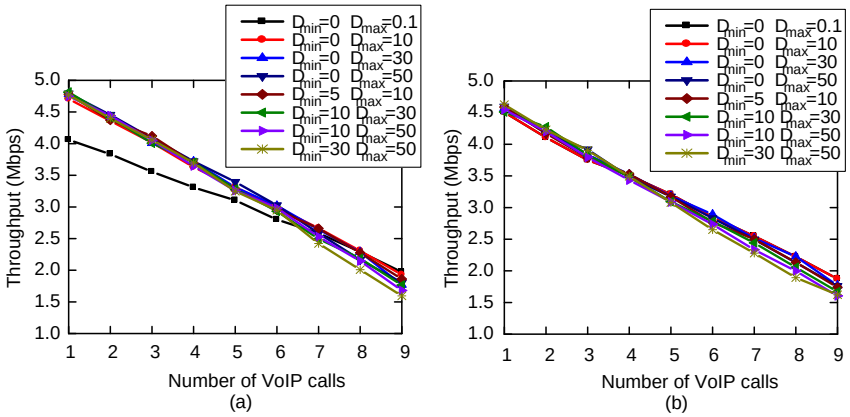


Figure 4. The effects of delay thresholds on average throughput. (a) The number of best-effort flows is 5 (b) The number of best-effort flows is 10

B. Effects of LR-STAs

We next study the capability of these comparing schemes of protecting voice traffic from LR-STAs. Table IV shows the number of VoIP calls protected by different schemes in a multi-rate environment; the first data row in the table indicates that all of the comparing schemes can support up to nine voice calls when there are only voice HR-STAs in WLANs. In our VD-EDCA scheme, all of the VoIP calls transmitted by HR-STAs are protected. In particular, with the settings of D_{min} = 0 and D_{max} = 0.1, all of the VoIP calls transmitted by the HR-STAs and LR-STAs are protected when the number of voice LR-STAs is equal to one or two. In the CWD$^+$ scheme, all of the VoIP calls transmitted by HR-STAs are protected from voice LR-STAs, but the scheme does not protect any VoIP call when the number of best-effort LR-STAs exceeds one. In the DS-EDCA scheme, no VoIP call is protected whenever voice or DCF LR-STAs exist in the WLAN. In the EDCA scheme, no VoIP call is protected whenever there exist LR-STAs in the WLAN. Therefore, our VD-EDCA scheme outperforms the others since it protects more VoIP calls.

C. Effects of LP-STAs and LR-STAs

Finally, we study the capability of these comparing schemes of protecting voice traffic from the LP-STAs and LR-STAs. As shown in the last two rows of Table IV, even in a highly congested environment, only our VD-EDCA scheme well protects all of the VoIP calls transmitted by the HR-STAs.

D. Effects of Delay Thresholds

In order to understand the effects of the two thresholds, we conduct a set of simulations by varying the threshold settings. Without loss of generality, in what follows, we only consider the scenario where VoIP traffic coexists with *AC_BE* LP-STAs. Fig. 3 and Fig. 4 show the average downlink delay of voice packets and the average throughput of all packets with the variances of delay thresholds, respectively. From Fig. 3, we can observe that the downlink delay increases as the value of D_{min} or D_{max} increases. As a result, the settings of D_{min} = 0 and D_{max} = 0.1 lead to the best delay performance. However, the settings of D_{min} = 0 and D_{max} = 0.1 do not necessarily achieve better throughput than other settings. For example, in Fig. 4(a) which is at a relatively light traffic load, the settings of D_{min} = 0 and D_{max} = 0.1 can result in the worst throughput when the number of VoIP calls is below seven. On the other hand, in Fig. 4(b) which is at a relatively heavy traffic load, the settings of D_{min} = 0 and D_{max} = 0.1 can achieve higher throughput than some settings when the number of VoIP calls exceeds five.

V. CONCLUSION AND FUTURE WORK

In this paper, we identify two factors of degrading the QoS of VoIP, namely LP-STAs and LR-STAs. We consider the two factors together and propose an extended EDCA scheme called VD-EDCA to protect voice traffic from the two factors solely by the adaptive IFS. Simulation results reveal that, with appropriate maximal delay threshold settings, the proposed scheme well protects all of the VoIP calls transmitted by HR-STAs from LP-STAs and/or LR-STAs.

To investigate the accuracy of the proposed scheme, it is helpful for us to have a mathematical model. In the future, we will develop an analytical model so that the wireless delay of voice frames can be estimated by closed-form formulas.

REFERENCES

[1] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, *IEEE Std.* 802.11-1999.

[2] Wireless LAN media access control (MAC) and physical layer (PHY) specifications: medium access control (MAC) quality of service enhancements, *IEEE Std.* 802.11e-2005.

[3] F. Anjum, M. Elaoud, D. Famolari, A. Ghosh, R. Vaidyannthan, A. Dutta, P. Ageawal, T. Kodama, and Y. Katsube, "Voice Performance in WLAN Networks - An Experimental Study," *in IEEE Globecom*, pp. 3504-3508, 2003.

[4] J. Yu, S. Choi, and J. Lee, "Enhancement of VoIP over IEEE 802.11 WLAN via Dual Queue Strategy," *in IEEE ICC*, pp. 3706-3711, 2004.

[5] H. Zhai, J. Wang, and Y. Fang, "Providing statistical QoS guarantee for voice over IP in the IEEE 802.11 wireless LANs," *IEEE Wireless Communications*, vol. 13, no. 1, pp. 36-43, 2006.

[6] A. Banchs, P. Serrano, and L. Vollero, "Reducing the impact of legacy stations on voice traffic in 802.11e EDCA

WLANs," *IEEE Communications Letters*, vol. 11, no. 4, pp. 331-333, 2007.
[7] J. F. Lee, W. Liao, and M. C. Chen, "A differentiated service model for enhanced distributed channel access (EDCA) of IEEE 802.11e WLANs," *ACM/Springer Mobile Net. Applications*, vol. 12, no. 1, pp. 69-77, 2007.
[8] H. Al-Mefleh and J. M. Chang, "A new ACK policy to mitigate the effects of coexisting IEEE 802.11/802.11e devices," *in Proc. IEEE INFOCOM*, pp. 131-135, 2008.
[9] P. Y. Wu, J. J. Chen, Y. C. Tseng, and H. W. Lee, "Design of QoS and admission control for VoIP services over IEEE 802.11e WLANs," *Journal of Information Science and Engineering*, vol. 24, no. 4, pp. 1003-1022, 2008.
[10] J. F. Lee, W. Liao, J. M. Chen, and H. H. Lee, "A Practical QoS Solution to Voice over IP in IEEE 802.11 WLANs," *IEEE Communications Magazine*, vol. 47, no. 4, pp. 111-117, 2009.
[11] W. L. Li, C. R. Lin, C. H. Ke, and K. Y. Tung, "A delay-based ACK scheme for VoIP services in an IEEE 802.11e infrastructure network," *in ChinaCom*, pp. 858-862, 2009.
[12] P. Serrano, A. Banchs, P. Patras, and A. Azcorra, "Optimal Configuration of 802.11e EDCA for Real-Time and Data Traffic," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2511-2528, 2010.
[13] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance Anomaly of 802.11b," *in Proc. IEEE INFOCOM*, pp. 836-843, 2003.
[14] H. Kim, S. Yun, I. Kang, and S. Bahk, "Resolving 802.11 performance anomalies through QoS differentiation," *IEEE Communications Letters*, vol. 9, no. 7, pp. 655-657, 2005.
[15] O. Abu-Sharkh and A. H. Twefik, "Throughput Evaluation and Enhancement in 802.11 WLANs with Access Point," *in Vehicular Technology Conference*, pp. 1338-1341, 2005.
[16] M. Ergen and P. Varaiya, "Formulation of distributed coordination function of IEEE 802.11 for asynchronous networks: Mixed data rate and packet size," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 1, pp. 436-447, 2008.
[17] P. C. Lin, W. I. Chou, and T. N. Lin, "Achieving Airtime Fairness of Delay-Sensitive Applications in Multirate IEEE 802.11 Wireless LANs," *IEEE Communications Magazine*, vol. 49, no. 9, pp. 169-175, 2011.
[18] C. H. Ke, C. C. Wei, and K. W. Lin, "A Dynamic and Adaptive Transmission Scheme for Both Solving Uplink/Downlink Unfairness and Performance Anomaly Problems in a Multi-Rate WLAN," *Applied Mathematics & Information Sciences*, vol. 6, pp. 531S-537S, 2012.
[19] Network simulator version 2, Available: http://www.isi.edu/nsnam/ns.
[20] One-way Transmission Time, ITU-T Rec. G.114-1996.
[21] Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 6: Actual measurements of network and terminal characteristics and performance parameters in TIPHON networks and their influence on voice quality, ETSI TR 101 329-6 V2.1.1-2002.

Wen-Li Li received the B.S. and M.S. degrees from the Department of Computer Science and Information Engineering from Tamkang University, Taiwan, in 1993 and 1996, respectively. Currently he is working toward the Ph.D. degree in the Department of Computer Science and Engineering, National Sun Yat-Sen University. His research interests include QoS control and wireless networks.

Chun-Hung Richard Lin received the B.S. and M.S. degrees from the Department of Computer Science and Information Engineering from National Taiwan University, Taipei, Taiwan, in 1987 and 1989, respectively, and the Ph.D. degree from Computer Science Department, University of California, Los Angeles (UCLA), in 1996. Dr. Lin joined National Chung Cheng University in Taiwan in 1996. Since August 2000, he has been with the Department of Computer Science and Engineering, National Sun Yat-Sen University, Taiwan. His research interests include QoS control, wireless networks, and embedded systems.

Chih-Heng Ke received his B.S., M.S., and Ph.D. degrees from Electrical Engineering Department of National Cheng Kung University, Taiwan in 1999, 2000 and 2007, respectively. Since 2007, he has been with the Department of Computer Science and Information Engineering, National Quemoy University, Taiwan. His current research interests include QoS control, multimedia communications, and wireless networks.

DOA Estimation for Coherent Sources in Impulsive Noise Environments

Baobao Liu [1], Junying Zhang [1]*, and Cong Xu [2]
1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China
2. HopeRun Technology Corporation, Xi'an 710065, China
*Corresponding author, Email: liubaobao1222@163.com, jyzhang@mail.xidian.edu.cn, xucong0623@126.com

***Abstract*—Direction-of-arrival (DOA) estimation of coherent sources is a significant problem in impulsive noise environments. In this paper, a robust estimation algorithm which combines the ideas of spatial smoothing (SS) and infinity-norm normalization (INF) is presented, referred to as INF-SSR. The proposed algorithm exploits the Root–MUSIC technique to computer the DOA estimates, thus avoiding the peak searching and can be applied to seriously impulsive noise environments compared with the fractional lower order moment spatial smoothing MUSIC algorithm (FLOM-SS). Simulation results demonstrate effectiveness of the proposed algorithm.**

***Index Terms*—Coherent Sources; Direction of Arrival (DOA); Impulsive Noise; Fractional Lower Order Statistics**

I. INTRODUCTION

In recent years, there has been drawing the increasing attention of high-resolution techniques for estimating the direction of arrival (DOA), which are widely applied in radar, radio astronomy, medical imaging, and wireless and mobile communication [1, 2], using multiple sensors. Many high resolution algorithms such as the multiple signal classification (MUSIC) [3] and estimation method of signal parameters via rotational invariance techniques (ESPRIT) [4] algorithms have been proposed and have good performances based on the Gaussian noise assumption, where second-order statistics is assumed to be finite. Unfortunately, the assumption cannot be satisfied in some scenarios such as sea clutter noise, atmospheric noise, wireless channel noise, acoustic radar echo, low-frequency atmospheric noise and artificial signal. They in practice often demonstrate non-Gaussian properties, primarily due to impulsive characteristics [5, 6] and thus the performance of most existing DOA algorithms may severely degrade in impulsive noise environments.

A recent research suggests [5, 6] that stationary symmetric alpha stable processes are better models for impulsive noise than Gaussian processes. For tackling impulsive noises, a class of subspace based DOA estimation algorithms employs the fractional lower-order statistics such as the robust covariation in ROC-MUSIC [7], fractional lower-order statistics in FLOM-MUSIC [8], instead of the second-order sample covariance. However, the fractional lower-order statistics based algorithms need prior knowledge of the impulsive noise's statistics and large sample sizes for a satisfactory performance. On the other hand, they have a heavy computational load for peak searching and cannot be applicable to the exponential parameter case of $\alpha < 1$ in impulsive noise environments. Fortunately, Ref. [9] presents IN-MUSIC method, which does not require any prior knowledge of the impulsive noise's statistics and can be applicable to the exponential parameter case of $\alpha < 1$. However, the algorithm is based on MUSIC method, which also has a heavy computational load for peak searching. It is wroth noting that all the algorithms mentioned above have an assumption that signals are incoherent and thus existing algorithms cannot effectively distinguish the DOA of coherent sources. Although fractional lower order moment spatial smoothing MUSIC algorithm (FLOM-SS) is presented in Ref. [10] for the direction of arrival estimation of coherent sources in impulsive noise environments, it cannot be applicable to the exponential parameter case of $\alpha < 1$ and has a heavy computational load.

In this paper, we have proposed INF-SSR algorithm which does not require peak searching for direction of arrival (DOA) estimation of coherent sources in the presence of impulsive noise. It outperforms FLOM-SS with the following advantages: (a) requiring no prior knowledge of the impulsive-noise's statistics; (b) offering better estimation accuracy and resolution; (c) light computational cost; (d) applicable to the exponential parameter case of $\alpha < 1$.

II. DATA MODEL

Without loss of generality, supposing that there are K $(K < M)$ uncorrelated with narrowband far-field signals at directions θ_k $(k = 1, 2, \ldots, K)$ impinging on an M element uniform linear array (ULA), and the elements are separated by a distance d. The array output vector $\mathbf{x}(t)$ is then given by [11, 12, 22]

$$\mathbf{y}(t) = \mathbf{A}(\theta)\mathbf{s}(t) + \mathbf{n}(t) \tag{1}$$

where $\mathbf{A}(\theta) = [a(\theta_1), a(\theta_2), \ldots, a(\theta_K)]$ Array manifold;

$a(\theta_k) = [1, e^{-j\frac{2\pi d}{\lambda}\sin\theta_k}, \ldots, e^{-j\frac{2\pi d(M-1)}{\lambda}\sin\theta_k}]^T$ Steering vector;

doi:10.4304/jnw.9.12.3237-3241

$\mathbf{s}(t) = [s_1(t), s_2(t), \ldots, s_K(t)]^T$ Signal vector;

$\mathbf{n}(t) = [n_1(t), n_2(t), \ldots, n_M(t)]^T$ Noise vector;

when the sources are coherent, which means they differ from a complex scalar [13]

$$s_i(t) = \alpha_i s_0(t),\ i = 1, 2, \ldots, K \tag{2}$$

Then the array output vector is given by

$$\begin{aligned} \mathbf{x}(t) &= \mathbf{A}(\theta)[s_1(t), s_2(t), \ldots, s_K(t)]^T + \mathbf{n}(t) \\ &= \mathbf{A}(\theta)\rho s_0(t) + \mathbf{n}(t) \end{aligned} \tag{3}$$

where $\rho = [\alpha_1, \alpha_2, \ldots, \alpha_K]^T$ is $K \times 1$ vector. In this letter, the noise is assumed to be impulsive.

III. Alpha Stable Distribution

Alpha stable distribution is a wide class of distributions and Gaussian family is a special situation of it. Since it does not have a closed form of probability density function (pdf), it is defined [5, 14] by its characteristics function as follows

$$\varphi(u) = \exp\{jau - \gamma|u|^{\alpha}[1 + j\beta\,\mathrm{sgn}(u)(u, \alpha)]\} \tag{4}$$

where

$$\omega(u, \alpha) = \begin{cases} \tan(\pi\alpha/2), & \alpha \neq 1 \\ (2/\pi)\log|u|, & \alpha = 1 \end{cases}$$

and sgn(•) is a sign function. α is a characteristic exponent restricted in $0 < \alpha \leq 2$ controlling thickness of the tail of the distribution. β $(-1 \leq \beta \leq 1)$ is a symmetry parameter. When $\beta = 0$ and $\alpha = 2$, the distribution becomes Gaussian distribution. γ $(\gamma \geq 0)$ is a dispersion parameter that is similar to the variance for Gaussian process. a $(-\infty < a < +\infty)$ is a location parameter. If $\beta = 0$, the distribution is called as symmetry α stable $(S\alpha S)$ distribution. In this paper, noise is assumed to be impulsive and modelled by a $S\alpha S$ distribution.

IV. Infinity-Norm Normalization

A. Infinity-Norm Normalization

When the noise is impulsive, the second-order moment does not exist. Thereby, the second-order moment based many DOA estimation algorithms cannot be applied in impulsive noise environments. In order to overcome the difficulty, we use infinity-norm normalization for array output vector [9, 15, 16].

The infinity-norm normalized array data is $\mathbf{z}(t)$ simply described by the received data $\mathbf{y}(t)$ as

$$\mathbf{z}(t) = w(t)\mathbf{y}(t) \tag{5}$$

$$w(t) = \frac{1}{\|\mathbf{y}(t)\|_{\infty}} = 1/\max\{|y_1(t)|, \ldots, |y_M(t)|\} \tag{6}$$

$$\mathbf{z}(t) = \mathbf{A}\mathbf{g}(t) + \mathbf{m}(t) \tag{7}$$

where $\mathbf{g}(t) = [w(t)s_1(t), \ldots, w(t)s_K(t)]^T$ is weighted signal vector, $\mathbf{m}(t) = [w(t)n_1(t), \ldots, w(t)n_M(t)]^T$ is weighted noise vector. Then an estimated $\hat{\mathbf{R}}$ of the covariance matrix of the normalized data is given by

$$\hat{\mathbf{R}} = \frac{1}{N}\sum_{t=1}^{N}\mathbf{z}(t)\mathbf{z}^H(t) \tag{8}$$

Theorem [9, 15, 16]: The covariance matrix defined from the weighted array data (5) is bounded and can be expressed as

$$\begin{aligned} \mathbf{R} &= \mathbf{E}[\mathbf{z}(t)\mathbf{z}^H(t)] = \mathbf{E}[w(t)\mathbf{y}(t)\mathbf{y}(t)w^*(t)] \\ &= \mathbf{A}\boldsymbol{\Gamma}_s\mathbf{A}^H + \boldsymbol{\eta}^2\mathbf{I} \end{aligned} \tag{9}$$

where $\boldsymbol{\Gamma}_s = \mathbf{E}[\mathbf{g}(t)\mathbf{g}^H(t)] = \mathrm{diag}[\eta_1^2, \eta_2^2, \ldots, \eta_K^2]$ and $\boldsymbol{\eta}^2$ is the weighted noise power at each sensor. The mathematical proof of the infinity-norm normalization is given in References [9, 15, 16].

V. INF Spatial Smoothing Root Music Algorithm

A. Spatial Smoothing

In the following sections, we will introduce the infinity-norm normalization spatial smoothing Root MUSIC algorithm (INF-SSR) for DOA estimation of coherent sources in impulsive noise environments. The spatial smoothing is a useful method for the DOA estimation of coherent signals. The main idea under spatial smoothing [17-19] is to divide the main array into a number of overlapping subarrays, and then the subarray covariance matrices are averaged.

In this section, we describe how to apply infinity-norm normalization in the forward/backward spatial smoothing MUSIC [17-19] and compute its signal and noise subspaces in impulsive noise environments, respectively.

Let us divide a uniform linear array composed of M identical sensors spaced d half-wave lengths apart, into overlapping subarrays of size m.

With sensors $[1, \ldots, m]$ consisting the first subarray, sensors $[2, \ldots, m+1]$ consisting the second subarray, etc. Thus, the vector of received signals at the kth subarray is given by

$$\mathbf{x}_k(t) = [x_k, x_{k+1}, \ldots, x_{k+m-1}] = \mathbf{A}\mathbf{D}^{(k-1)}\mathbf{s}(t) + \mathbf{n}_k(t) \tag{10}$$

where $\mathbf{D} = \mathrm{diag}[e^{j\beta_1}, \ldots, e^{j\beta_K}]$ and $\beta_i = 2\pi d \sin\theta_i / \lambda$, $i = 1, 2, \ldots, K$. Then, using (5) and (6) for $\mathbf{x}_k(t)$, we can rewrite (10) as

$$\mathbf{z}_k(t) = w_k(t)\mathbf{x}_k(t) \tag{11}$$

Thus, the covariance matrix of the *kth* subarray is therefore given by

$$\mathbf{R}_k = \mathbf{A}\mathbf{D}^{(k-1)}\boldsymbol{\Gamma}_s(\mathbf{D}^{(k-1)})^H\mathbf{A}^H + \boldsymbol{\eta}^2\mathbf{I} \tag{12}$$

The forward spatially smoothed covariance matrix is denoted as the average of the subarray covariance

$$\begin{aligned}\mathbf{R}^f &= \frac{1}{p}\sum_{i=1}^{p}\mathbf{R}_i = \mathbf{A}(\frac{1}{p}\sum_{i=1}^{p}\mathbf{D}^{(i-1)}\mathbf{\Gamma}_s(\mathbf{D}^{(i-1)})\mathbf{A}^H + \boldsymbol{\eta}^2\mathbf{I} \\ &= \mathbf{A}\mathbf{\Gamma}_s^f\mathbf{A}^H + \boldsymbol{\eta}^2\mathbf{I}\end{aligned} \tag{13}$$

where

$$\mathbf{\Gamma}_s^f = \frac{1}{p}\sum_{i=1}^{p}\mathbf{D}^{(i-1)}\mathbf{\Gamma}_s(\mathbf{D}^{(i-1)})^H$$

and $p = M - m + 1$ is the number of subarrays. Similarly, the back spatially smoothed covariance $\mathbf{R}^b$ is given by

$$\begin{aligned}\mathbf{R}^b &= \frac{1}{p}\sum_{i=1}^{p}\mathbf{R}_{p-i+1}^b \\ &= \mathbf{A}(\frac{1}{p}\sum_{i=1}^{p}\mathbf{D}^{-(m+i-2)}\mathbf{\Gamma}_s^*\mathbf{D}^{(m+i-2)})\mathbf{A}^H + \boldsymbol{\eta}^2\mathbf{I}\end{aligned} \tag{14}$$

where $\mathbf{\Gamma}_s^b = \frac{1}{p}\sum_{i=1}^{p}\mathbf{D}^{-(m+i-2)}\mathbf{\Gamma}_s^*\mathbf{D}^{(m+i-2)}$. Using $\mathbf{R}^f$ and $\mathbf{R}^b$, we obtain the backward/forward spatially smoothed covariance matrix in case of impulsive noise as follows

$$\mathbf{R}^{fb} = \frac{1}{2}(\mathbf{R}^f + \mathbf{R}^b) \tag{15}$$

Performing eigenvalue decomposition to the matrix $\mathbf{R}^{fb}$, one can obtain signal subspace matrix $\mathbf{U}_s$ which is spanned by the eigenvectors corresponding to the K largest eigenvalues of $\mathbf{R}^{fb}$ and the noise subspace matrix $\mathbf{U}_n$ is the eigenvectors corresponding to the smallest eigenvalues of $\mathbf{R}^{fb}$, respectively.

B. DOA Estimation Using Polynomial Rooting

To obtain high DOA accuracy, conventional spatial smoothing-MUSIC method generally requires searching peaks, thus, resulting into great computational burden. To reduce the computational complexity, the polynomial rooting technique [20, 21] is applied in the proposed algorithm. Defined a polynomial as the equation (16)

$$p_l(z) = u_l^H p(z),\ l = K+1, K+2, \ldots, m \tag{16}$$

where u_l is the *lth* eigenvectors corresponding to the smallest eigenvalues of covariance matrix $\mathbf{R}^{fb}$, and $p(z) = [1, z, \ldots, z^{(m-1)}]^T$. Then, the Root-MUSIC polynomial is given by

$$p(z) = z^{(m-1)}p(z^{-1})\mathbf{U}_n\mathbf{U}_n^H p(z) \tag{17}$$

The direction of arrivals of all coherent sources in the impulsive environments can be obtained from the phase of the largest K roots

$$\hat{\theta} = \arcsin[\frac{\lambda}{2\pi d}\arg(\hat{z}_i)],\ i = 1, \ldots, K \tag{18}$$

C. Basic Steps of the INF-SSR Algorithm

The Steps of INF-SSR algorithm is summarized as follows:

Step1 Obtain the processing snapshot data $\mathbf{z}_k(t)$ using the equation (11).

Step2 Construct forward spatially smoothed covariance matrix $\hat{\mathbf{R}}^f$ and backward spatially smoothed covariance matrix $\hat{\mathbf{R}}^b$, respectively.

Step4 Construct backward/forward spatially smoothed covariance matrix $\hat{\mathbf{R}}^{fb}$.

Step5 Perform the eigenvalue decomposition for $\hat{\mathbf{R}}^{fb}$ and obtain the noise subspace $\hat{\mathbf{U}}_n$.

Step6 Solve the equation (17) and find K roots which are closet to the unit circle.

Step7 Obtain the DOA estimation according to equation (18) in impulsive noise environments.

VI. Simulation Results

The INF-SSR and FLOM-SS algorithms are compared in their DOA estimation precision for simulated sensor array system. Other algorithms for tackling impulsive noises are not compared here since they just think about noncoherent sources and cannot resolve the DOA estimation of coherent sources in impulsive noise environments. Assume that there exist $K = 2$ coherent signals, which are located at angles $\theta_1 = 10^\circ$ and $\theta_2 = 18^\circ$, and the number of snapshots is $N = 200$ for a uniform linear array (ULA) with $M = 10$ sensors. The array is divided into 3 subarrays, each of them with $m = 8$ sensors. Two quantities are used to evaluate the performance: root mean squared error (RMSE) and probability of resolution. RMSE is defined in Ref. [9] and 500 MC trials are used. For each Monte Carlo (MC) trial, two estimated signals are considered being successfully estimated if they satisfy $9^\circ < \hat{\theta}_1 < 11^\circ$ and $17 < \hat{\theta}_2 < 19^\circ$, respectively.

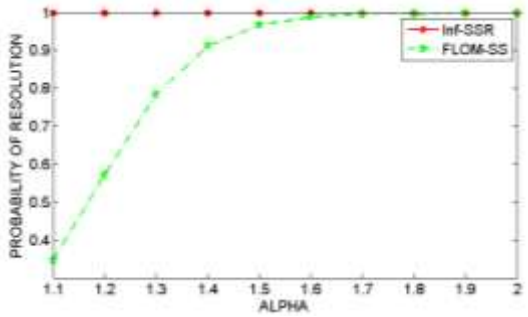
Because alpha stable distribution has no second order moment and infinite variance, a generalized signal-to-noise ratio (GSNR) [1, 2] is defined as GSNR which is a direct generalization from SNR. When the alpha-stable noise degenerates to the Gaussian noise, the GSNR is the ratio of signal variance to noise variance.

$$GSNR = 10\log\left(\frac{\sum_{t=1}^{N}|s(t)|^2}{\gamma N}\right) \tag{19}$$

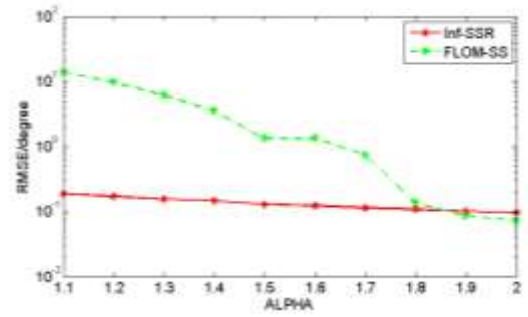
The probability of resolution is the ratio, in percentage, of the number of successful MC iterations to the total number of MC iterations.

Fig. 1(a) and Fig. 2(a) show probability of resolution for the INF-SSR and FLOM-SS algorithms on different impulsiveness situations of noises, respectively. From the two subfigures we observe that the INF-SSR algorithm has higher probability of resolution than the FLOM-SS algorithm especially in low GSNR case and seriously impulsive noise environments, respectively and the GSNR is lower, the better the estimation performance of the proposed INF-SSR algorithm compared to that of the FLOM-SS algorithm. This indicates that the proposed INF-SSR algorithm is especially suitable to seriously

impulsive noise situation. This characteristic of the proposed algorithm can also be seen from Fig.1(b) and Fig.2(b) where RMSE is presented and it can be shown that the proposed method has better angle performance than the FLOM-SS algorithm. Fig.3(a) and (b) show that the proposed algorithm has the better angle estimation performance when the FLOM-SS algorithm [6] is inapplicable to the $\alpha < 1$ case. Therefore, the proposed algorithm is robust especially to seriously impulsive noises environments.

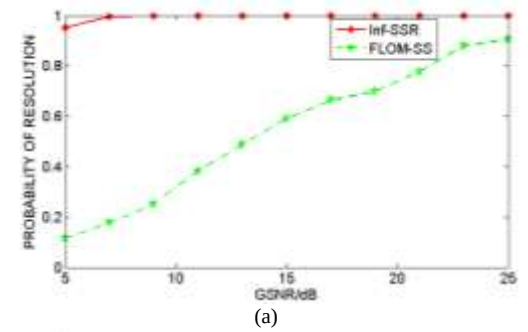


(a)

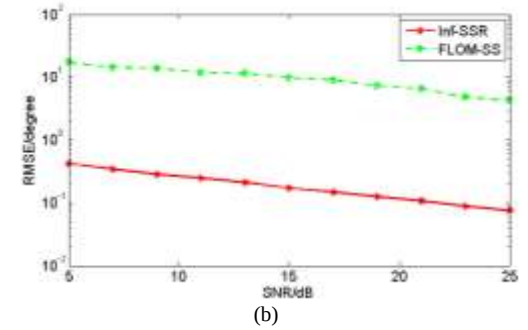


(b)

Figure 1. (a) Probability of resolution versus α with GSNR=15dB and RMSE of DOA estimation versus α with GSNR=15dB

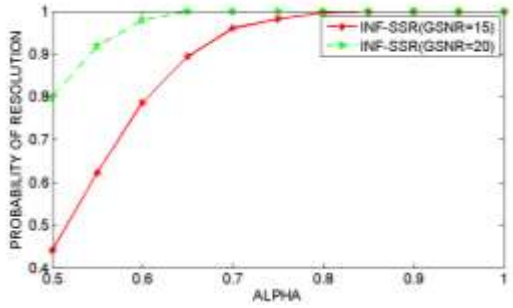


(a)

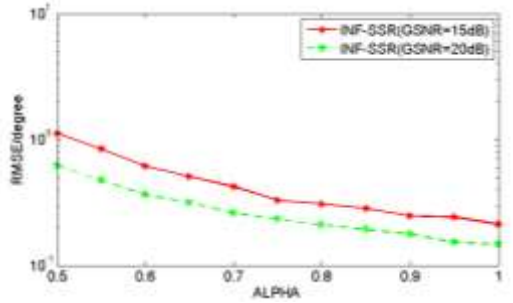


(b)

Figure 2. (a) Probability of resolution versus GSNR and (b) RMSE of DOA estimation versus GSNR. (a)-(b): $\alpha = 1.2$

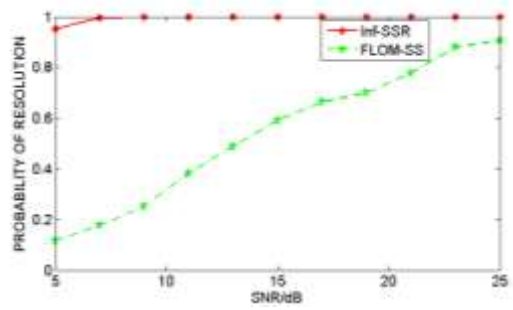


(a)

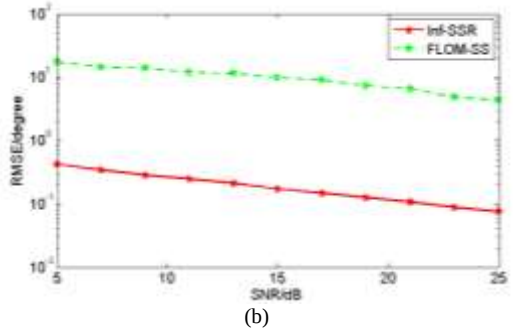


(b)

Figure 3. (a) Probability of resolution versus α and (b) RMSE of DOA estimation versus α



(a)



(b)

Figure 4. (a) Probability of resolution versus SNR and (b) RMSE of DOA estimation versus SNR

From the figure 4, we can find that the proposed algorithm is also applicable for estimation of coherent sources' DOA under Gaussian noise but its angle estimation performance is inferior to the SS-MUSIC algorithm [18] especially at low SNR.

VII. CONCLUSION

In this paper, we have proposed a robust INF-SSR algorithm based on infinity-norm normalization for DOA of coherent sources in impulsive noise environments. The

proposed algorithm has much better performance for DOA estimation in contrast to the FLOM-SS algorithm in impulsive noise environments. In addition, it dose not need any prior knowledge of the impulsive noise's statistics. Furthermore, it avoids high computational cost and reduces runtime compared to traditional peak searching based FLOM-SS algorithm. But its performance of angle estimation is inferior to the SS-MUSIC algorithm [18] in the presence of Gaussian noise. The limitation inspires us to continue working to improve the angle estimation performance of INF-SSR algorithm in the future.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China under Grants 61070137 (91130006 and 61201312), Research Fund for the Doctoral Program of Higher Education of China (No. 20130203110017), and the Fundamental Research Funds for the Central Universities of China (Nos. BDY171416 and JB140306).

REFERENCES

[1] Mouhamadou, M,. P. Vaudo, and M. Rammal, "Smart antenna array patterns synthesis: Null steering and multi-user bearmforming by phase control," Progress In Electromagnetics Research, PIER 60, pp. 95-106, 2006.

[2] Mukhopadhyay, M., B. K. Sarkar, and A. Chakrabarty, "Augmentation of anti-jam GPS system using smart antenna with a simple DOA estimation algorithm," Progress In Electromagnetics Research, PIER 59, pp. 251-265, 2006

[3] Schmidt, R. O., "Multiple emitter location and signal parameter estimation," IEEE Trans. on Antennas and Propagation, vol. 34, pp. 276-280, 1986.

[4] Roy, R. and T. Kailath, "ESPRIT-estimaiton of signal parameters via rotational invariance techniques," IEEE Trans. on Acoustics, Speech and Signal Processing, vol. 37, pp. 984-995, 1989.

[5] T. H. Liu and Mendel J M, "A subspace-based direction finding algorithm using fractional lower order statistics," IEEE Trans. on SP, vol. 49, pp. 1605-1613, 2001.

[6] M. Shao and C. L. Nikias, Signal Processing With Alpha-stable Distributions and Applications. New York: Wiley, 1995.

[7] Tsakalides P and Nikias C. L, "The robust covariation-based MUSIC (ROC-MUSIC) algorithm for bearing estimation in impulsive noise Environments," IEEE Trans. On SP, vol. 44, pp. 1623-1633, 1996.

[8] Liu T H and Mendel J M, "A subspace-based direction finding algorithm using fractional lower order stasistics," IEEE Trans. on SP, vol. 49, pp. 1605-1613, 2001.

[9] J. He, Z. Liu and K. T. Wong, "Snapshot-Instantaneous $\|\bullet\|_\infty$ Normalization against heavy-tail Noise," IEEE Trans. on Aerospace and Electronic Systems, vol. 44, pp. 1221-1227, 2008.

[10] H. S. Li, R. J. Yang, Y. He and J. Guan "Research on DOA estimation methods of coherent sources in the presence of impulsive noise," Journal of microwaves, vol. 24. pp. 82-86, 2008.

[11] S. N. Shahi, M. E. maid, and K. Sadeghi, "High resolution DOA estimation in fully coherent environments," Progress In Electromagnetics Research C, vol. 5, pp. 135-148, 2008.

[12] Q. C. Zhou, H. T. Gao, and F. Wang, "A high resolution DOA estimating method without estimating the number of sources," Progress In Electromagnetics Research C, vol. 25, pp. 233-247, 2012.

[13] C. Y. Qi, Z. J, Chen, Y. L. Wang and Y. S, Zhang, "DOA estimation for coherent sources in unknown nonuniform noise fields," IEEE Trans. on Aerospace and Electronic Systems, vol. 43, pp. 1195-1204, 2007.

[14] W. Qin. Guo, T. S, Qiu, and H. Tong, W. R. Zhang, "Performance of RBF neural networks for array processing in impulsive noise environment," Digital Signal Processing, vol. 18, pp. 168-178, 2008.

[15] He J, and Liu Z, "Linearly constrained minimum-'normalised variance' beamforming against heavy-tailed impulsive noise of unknown statistic," IET Radar, Sonar Navigation, Vol. 2, pp. 449-457, 2008.

[16] J. He and Z. Liu., "WARD: A weighted array data scheme for subspace processing in impulsive noise acoustics," Speech and Signal Processing, IEEE International Conference on, vol. 4, 2006.

[17] Shan, T. J., Wax, M and Kailath, T, "On spatial smoothing of estimation of coherent signals, "IEEE Tans on Acoustics Speech, and Signal processing, Vol. 33, pp. 806-811, 1985.

[18] Pillal, S. U., and Kwon, B. H, "Forward/Backward spatial smoothing techniques for coherent signal identification," IEEE Trans on Acoustics Speech and SP, Vol. 37, pp. 8-15, 1989.

[19] Friedlander. B and J. Weiss. A, "Direction finding using spatial smoothing with interpolated arrays," IEEE Trans on aerospace and electronic systems, Vol. 28, pp. 574-587, 1992.

[20] Q. S. Ren and A. J. Willis, "Fast root MUSIC algorithm," Electronics letters, vol. 33, pp. 450-451, 1997

[21] Barabell, AJ., "Improving the resolution performance of eigenstructure based direction finding algorithms," In Proceedings of the International Conference on Acoustics Speech and Signal Processing, Boston, MA, pp. 336-339, 1983.

[22] X. J. Mao and H. H. Pan, "An Improved DOA Estimation Algorithm Based on Wavelet Operator," Journal of Communications Vol. 8, No. 12, December 2013.

Baobao Liu received his M.S degree in Computer Science and Technology from An Hui University of Technology, An Hui, China in 2011. He is currently working toward the Ph.D.degree at the Xidian University. His research interest lies in array signal processing, machine learning and MIMO array radar signal processing.

Junying Zhang received her Ph.D. degree in Signal and Information Processing from Xidian University, Xi'an, China, in 1998. From 2001 to 2002, she was a visiting scholar at the Department of Electrical Engineering and Computer Science. The Catholic University of America Washington, DC, USA, and in 2007, she was a visiting professor at the Department of Electrical Engineering and Computer Science,Virginia Polytechnic institute and State University, USA. She is currently a professor in the school of Computer Science and Technology, Xidian University. Her research interests focus on intelligent information processing, including machine learning and its application to bioinformatics.

Cong Xu received her M.S. degree in circuit and system from Xidian University, Xi'an, China, in 2013. Her research interests focus on intelligent information processing.

Research on Structure Ontology Characteristic of Blogosphere

Xue Li
International Business School of Shaanxi Normal of University, Xi'an, China
Email: lixue@snnu.edu.cn

Yingan Cui [1, 2*] and Xia Hui [2]
1. School of Electronic and Information Engineering, Xi'an JiaoTong University, Xi'an, China
2. School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China
*Corresponding author, Email: cuiyan@xaut.edu.cn; xia_hui@xaut.edu.cn

***Abstract*—Structure ontology characteristic of blogosphere is one of the hot topics in social computing. It has an important research value for blog dissemination, blog community discovery, blog mining etc. From the empirical research on a number of blogospheres in the real world, we find that the blogosphere is characterized by local centralized large-scale complex social network, whose characteristic is closely related to blog channel, and composed of multiple discrete small social networks. The previous methods by using structure reductionism or functional reductionism cannot fully explain the evolution and development of the blogosphere. Based on the structure ontological viewpoint, This paper presents the blogosphere is composed of belief space, group space and content space. The content space is a information network, the group space is a network of relationships, the belief space is a cultural network, among of which, each one has endogenous rules of evolution, and also interacts with each other, under the common actions of the downward causal relationship and the upward causal relationship, it shows a wealth of structural features.**

***Index Terms*—Blogosphere; Social Tie; Data Sampling Scheme; Structural Ontology Characteristic**

I. INTRODUCTION

A blog is a user-generated website where the entries are made and displayed in a reverse chronological order. Blog often provide commentaries or news on a particular subject such as music, politics, or local news, and other functions are more personal online diaries. Most blogs are interactive, allowing visitors to leave comments and even message each other via widgets on the blog [1-2]. Due to the growing influence of this specialized publishing infrastructure of blogs, this subset of the web sphere is popularly known as blogosphere [3-5]. Today the blogosphere serves as a social medium and plays a very important role in people's life, according to the criterion in the reports provide by CNNIC (China Internet Network Information Center) in 2013, blog users are approximately 436 million, 70.7% of which often update blogs. More and more people exchange messages, build relationships, express their viewpoints in blog, it has already become the primary channel to spread public opinions [6-7].

Several studies had analyzed the blogosphere due to its strong affects on social opinions.C. Marlow collected citations and blogrolls on weblog entries in the Blogdex project and applied social network analysis to reveal the social structure of weblogs [8]. N. Glance discussed the topics of political bloggers by studying link patterns [9], the result of study shown there were some differences in the behaviors of politically liberal and conservative blogs, with conservative blogs linking to each other more frequently. Lento et al. conducted data analyses about the Wallop System and compared users who remained active to those who did not [10]. Those studies extracted some relations among blogs and generated a social network for analysis. For community detection, Y. Lin et al. seeked interesting aspects of social relations [11]. They presented a computational model for mutual awareness that incorporated specific action types including commenting and changing blogrolls. The mutual awareness feature was not only used for community extraction but also for blog classification. Several studies had investigated weblog relationships and real-world relationships. J. Cummings et al. discussed online and offline social interactions [12]. R. Kumar et al. investigated abundant profiles of more than one million livejournal.com bloggers in 2004, and analyzed the demographic and geographic characteristics of users [3]. L. Adamic found interesting characteristics of bloggers' online and real-life relationships [13].They investigated three blog communities using an online survey, which revealed that many online relationships were formed through blogging and few blogging interactions reflect close online relationships. Where after, C. Marlow seeked to understand the social implications of hypertext links within the community. using a large corpus of weblogs collected over a one-month period, characterized structural properties of the weblog readership network [14]. C. Woo-young exmimined Koreans' protests against U.S. beef imports by deconstructing online dynamics of news diffusion, using a qualitative examination of bloggers' profile [15]. M. Klaus used social network

doi:10.4304/jnw.9.12.3242-3250

analysis to uncover the blog structure. They introduced quantitative assessments of the revealed structure and highlight the relevance for direct marketing communication [16]. T. Nguyen examined the use of the blogosphere as a framework to study user psychological behaviors, using their sentiment responses as a form of 'sensor' to infer real-world events of importance automatically [17].

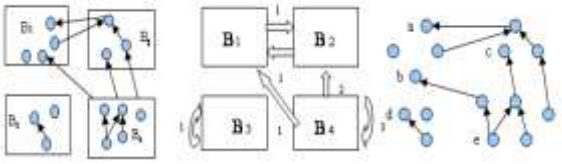
To sum up previous studies, we can find that the system theory was selected as a research paradigm to emphasize the system environment's effect on blogosphere, behavior science was selected as a research paradigm to emphasize the blogger's behavior characteristics' effect on blogosphere, and group dynamics was selected as a research paradigm to emphasize the blogger cognitive approaches' effect on blogosphere. The results of previous research indicated some explanations on the structure ontology characteristics of the blogosphere, but there are still two prominent issues: first of all, there are shortcomings in research methods, although the above-mentioned methods are different, they have such a common feature that the "function" is studied to illustrate the changes in the "structure", and the scale expansion is falsely deemed as the first impetus for the evolution of the blogosphere, which is trapped into the functional reductionism. This paper outlines the data sampling scheme of comprehensive blogosphere and the technical framework for crawling social network information from four well known blog websites in China. Secondly, the combination of social network analysis ("structure") and behavior analysis ("function") were used to do empirical research from three perspectives include global centrality, hierarchy and interactivity. By empirical research, we find that the blogosphere is characterized by local centralized large-scale complex social network, whose characteristic closely related to blog channel, and composed of multiple discrete small social networks. From the perspective of ontological, blogosphere is a complex system composed of belief space, group space, content space, among of which, each one has endogenous rules of evolution, and also interact with each other, with the common influence of the downward causal relationship and the upward causal relationship, it shows a wealth of structural features.

The rest of the paper is organized as follows: section II proposes the data sampling scheme from four well known blog websites in China, section III analyze the structure characteristic of blogosphere from three perspectives (including global centrality, hierarchy and interaction characteristic), section IV provides the structure ontology characteristics of blogosphere.

II. BLOGOSPHERE OVERVIEW

A. Blog Network and Post Network

The blogosphere consists of two main graph structures – a blog network and a post network. A post network is formed by considering the links between blog posts, and ignoring the blogs which they belong to. In a post network, the nodes represent individual blog posts, and edges represent the links between them. A post network gives a microscopic view of the blogosphere and helps in discerning "high-resolution" details like blog post level interaction, communication patterns in blog post interactions, authoritative blog post based on links, etc. A blog network is formed by collapsing those individual nodes in the post network that belong to a single blog. By doing so links between the blog posts that belong to a single blog disappear and links between blog posts of different blogs are agglomerated and weighted accordingly. A blog network gives a macroscopic view of the blogosphere and observes the "low-resolution" details like blog level interactions, communication patterns in blog-blog interactions, authoritative blogs based on links, etc. Both post and blog networks are directed graph(see Fig. 1) [18].



(a) blogosphere (b) blog network (c) post network

Figure 1. Compositions of Blogosphere [18]

B. Blog Social Ties

Link is the social currency of this interaction, allowing bloggers to be aware of who is reading and commenting on their writings. A number of distinct subtypes of links have emerged within the medium, each one conveying a slightly different kind of social information [8, 19].

(1) Blogrolls. Nearly every blog contains a list of other weblogs that the author reads regularly, termed the blogroll. This form evolved early in the development of the medium both as a type of social acknowledgement and as a navigational tool for readers to find other authors with similar interests. A link within a blogroll often indicates a general social awareness on behalf of the author. In most of blog hosted services, the blogroll is a core part of the interaction, allowing users to be notified when their friends make a post or even to create a group dialog represented by the sum of the group's individual weblogs.

(2) Permalinks. A permalink (portmanteau of permanent link) is a URL that points to a specific blog or forum entry after it has passed from the front page to the archives. Because a permalink remains unchanged indefinitely, it is less susceptible to link rot. Most modern weblogging and content-syndication software systems support such links. Other types of websites use the term permanent links, but the term permalink is most common within the blogosphere. Permalinks are often simply stated so as to be human-readable.

(3) Comments. The most basic form of blog social interaction is the comment. Comment systems are usually implemented as a chronologically ordered set of responses, much like BBS. Depending on the amount of traffic that a particular blog might entertain, comments serve a range of usefulness; on extremely popular sites, the amount of response a post receives can render the

comments long and unreadable, while on smaller sites a lack of any responses can give the author and readers the sense that the site is generally unread. Between these two extremes, the comment serves as a simple and effective way for bloggers to interact with their readership.

(4) Trackbacks. A recent feature of weblog tools is the trackback, an automatic communication that occurs when one weblog references another. If both weblogs are enabled with trackback functionality, a reference from a post on weblog A to another post on weblog B will update the post on B to contain a back-reference to the post on A. This automated referencing system gives authors and readers an awareness of whom is discussing their content outside the comments on their site.

III. DATA SAMPLING SCHEME

A. Data Sampling Design

The sampling process include the following steps:

(1) Sampling design. According to the BSP (blog service providers) business operating strategies, social influence, comprehensiveness of blog channel, we selected blog. sina.com, blog.sohu.com, blog.qq.com and blog.netease.com as the research objects in this paper. "Population" means all blogs contained by these four blog systems, "sample" refers to the blogs acquired actually by data acquisition program. Combining cluster sampling with snowball sampling was adopted for sample selection.

(2) Determining clusters. In order to attract different types of bloggers to visit the website, BSP set various channels in the blog systems, such as blog.sina.com, is divided into the culture, emotions, sports, music and other channels, etc. This study made a parent directory of each channel corresponding to a sample cluster. The data acquisition program start with a separate thread for each sample cluster to extract data automatically (isolated blogs do not belong to any blogosphere, thus, they are not within the scope of sampling).

(3) Collect samples. Information collectors randomly selected a certain amount of blogs within each sample clusters, and then started from the selected blogs by snowball way, with a combination of random walk and depth-first search method to analyze the social networks of the blogs. In the process of sampling, it was necessary to control the time and scope of snowball to prevent the social network analysis from being trapped into infinite loop.

(4) Fetch blog page.Load the url of initial blog, use Java URLConnection class to establish http session with the target blog, further more, use Java URL class to read the content information of the specified blog, and then return the web page in the form of Java InputStream. The crawled information will be analyzed according to the page structural features of each blog system. At first, those hyperlinks unrelated to the blogosphere should be filtered. And then the JavaScript codes in the web page should be resolved. Finally, XMLHttpRequest should be run in accordance with the invoking relationships in JavaScript codes to send AJAX requests so as to obtain the dynamic data in the blog page (shown in Fig.2).

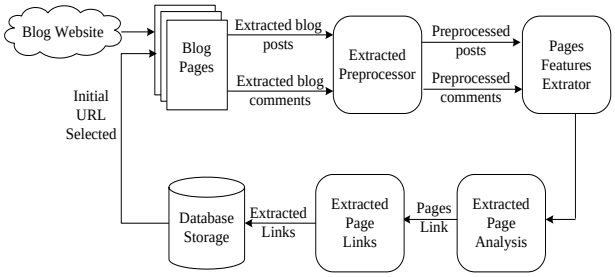


Figure 2. The process of extract social network information in blogosphere

B. Sample Statistics

Blog sampling data were analyze by social network analytic method, detailed information shown in Table I and Table II.

TABLE I. KEY PERFORMANCE INDICATORS OF BLOG NETWORK

Properties of blog network				
property	blog.sina	blog.sohu	blog.qq	blog.netease
Number of blogs	40,915	107,198	130,207	65,132
blog links	874,763	1,970,299	4,460,891	1,839,328
Average number of links	21.38	18.45	34.26	28.24
In-degree law exponent	-1.542	-1.709	-0.682	-1.633
Out-degree law exponent	-1.629	-1.885	-0.723	-1.687
Degree CC	0.058	0.077	0.219	0.137
Average path length	19.13	17.62	9.87	14.29
Largest SCC size	55,631	33,408	73,608	65,365

TABLE II. KEY PERFORMANCE INDICATORS OF POST NETWORK

Properties of post network				
property	blog.sina	blog.sohu	blog.qq	Blog.netease
Number of posts	44,179	124,695	122,057	91,911
post links	678,147	1,732,021	1,982,220	1,770,212
Average number of links	15.35	13.89	16,24	19.26
In-degree law exponent	-2.202	-1.891	-2.033	-2.232
Out-degree law exponent	-2.325	-1.969	-2.145	-2.357
Degree CC	0.163	0.074	0.189	0.147
Average path length	24.66	21.23	19.98	17.82
Largest SCC size	62,399	48,767	93,238	81,658

IV. STRUCTURE CHARACTERISTICS OF THE BLOGOSPHERE

We discuses the structure characteristics of the blogosphere from three perspectives: global centrality analyze, hierarchy analyze and interaction analyze.

A. Global Centrality Analyze

1) Degree Distribution

Degree distribution is the number of connections or edges the node has to other nodes. If a network is directed, means that edges point in one direction from one node to another node, then nodes have two different degrees, the in-degree, which is the number of incoming edges, and the out-degree, which is the number of out-going edges. The degree distribution $p(k)$ of a network is then defined to be the fraction of nodes in the network with degree k. We have $p(k_i) = k_i \Big/ \sum_j k_j$, Fig. 3 show the out-degree and in-degree complementary cumulative distribution function for each blogosphere. All of the networks show behavior consistent with a power-law network whether for the blog network or post network, the majority of the nodes have small degree, a few nodes have significantly higher degree. This phenomenon indicates that the opinion leaders have already formed after a long period of interaction, meanwhile, the reading and writing behaviors of bloggers have already tend to stable. The new users will find the target blog based on the principle of preferential attachment. Thus, these objects of study selected as samples have higher reliability and better validity.

2) Densely Connected Core

We loosely define a core of a network as any set of nodes that satisfies two properties: First, the core must be necessary for the connectivity of the network (i.e., removing the core breaks the remainder of the nodes into many small, disconnected clusters). Second, the core must be strongly connected with a relatively small diameter. Thus, a "core" is a small group of well-connected group of nodes that is necessary to keep the remainder of the network connected.

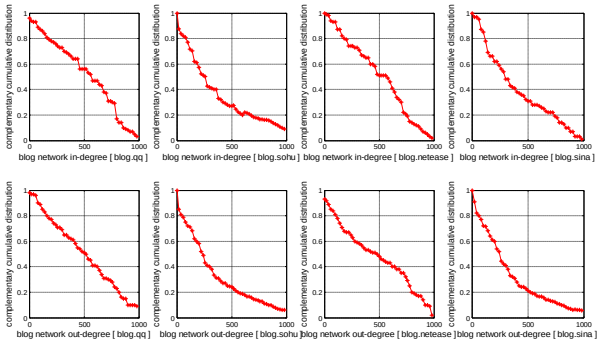


Figure 3. The degree distribution of blog network

To more closely explore whether there is a core group exist in blogosphere on the global level, we remove increasing numbers of the largest-SCC (Strongly Connected Component) and analyze the degree of the remaining in the blogosphere. Fig. 4 shows the composition of the splits as we remove between 0.1% and 10% of the largest-SCC in blog.netease. Although we remove 10% of the largest SCC, the low degree nodes (<120) of the blogosphere is not changed obviously. This phenomenon indicates that there really exists cluster phenomenon in the blogosphere, but rather than form a highly centralized core group via cluster, a number of discrete small social networks are formed in its internal. Meanwhile, Table Ⅱ and Table Ⅲ show larger average path length, indicates that there is no obvious aggregation feature within the blogosphere, or the average path distance would be relatively small. Through further study on opinion leaders (high in-degree bloggers), it was found that the average path length among these "opinion leaders" is relatively high, indicating no direct linking among of them. Therefore, there is no highly concentrated core group exists within the blog.netease, the corresponding graphs for the other blogospheres look similar, and we omit them for lack of space.

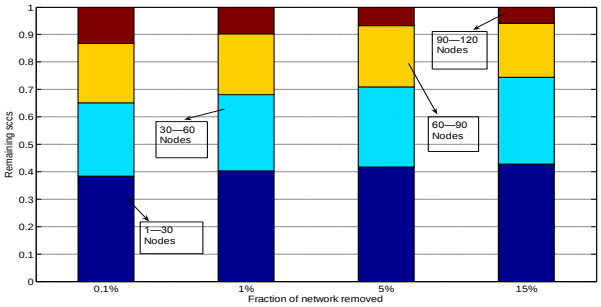


Figure 4. The correlation between SCC and degree in blogosphere

3) Cross-channel Distribution of High In-degree Nodes

High in-degree nodes refer to those bloggers with higher reputation. Under normal circumstances, they have more followers to form a social network with themselves as the core. The present study analyzes the cross-channel distribution phenomenon of these high in-degree bloggers. The result of this investigation is shown in Table Ⅲ: only a few high in-degree bloggers cross 2-4 channels, and then the proportion of cross-channel rapidly decays with the increase of channels, indicating that a large number of high in-degree bloggers just belong to a specific channel and have a certain influence on the bloggers within the channel.There is no bloggers group with great influence on the whole blogosphere.

TABLE III. THE PROPORTION OF HIGH IN-DEGREE NODES CROSS DIFFERENT CHANNEL

Behaviour properties of blogger				
Cross num	blog.sina	blog.sohu	blog.qq	Blog.netease
c-2	8.732%	9.379%	13.249%	13.816%
c-4	7.297%	12.937%	10.773%	12.305%
c-6	6.915%	7.598%	7.632%	8.365%
c-8	1.238%	0.937%	1.499%	1.735%
c-10	0.023%	0.015%	0.018%	0.027%

Through the study on the global centrality, it was found that high in-degree nodes have indeed formed by

preferential attachment within the blogosphere after long-term business operation. But with the lack of connection among these nodes, there is no core group on the macro scope and these high in-degree nodes are dispersedly distributed in different channels. Thus it can be seen that the real blogosphere is a large-scale social network composed of multiple discrete small social networks, with its bloggers closely related to the blog channels, as well as the local centrality feature (local preferential attachment). There is no highly concentration core group inside the blogosphere, so it has not such a structure feature of "core- periphery" on the macro level.

B. Hierarchy Analyze

The hierarchy is the hierarchical order in status and role manifested by various differences of internal nodes in the blogosphere, which reflects the differences and orders in the structure, the dendrogram is adopted in the research on the hierarchies of the blogosphere. Empirical studies indicated that all blogospheres have obvious hierarchy, which demonstrate that the phenomenon of "hierarchy" has universality in the blogosphere (shown in the Fig. 5). Through further study, it was found that the hierarchy of blogosphere is most closely related to the "user preference", "user level", "total amount of posts", "total amount of visits", "total amount of social ties", "total amount of cites" and "total amount of shares".

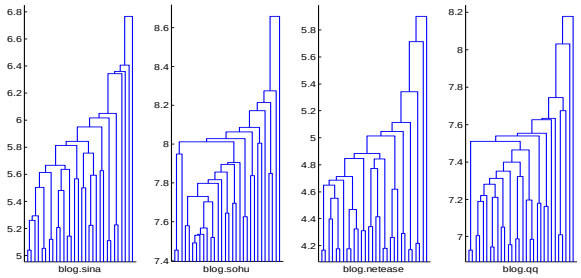


Figure 5. The dendrogram of blogosphere

1) The Relationship Between Hierarchy and User Preference.

Empirical studies indicated that the primary reason for the formation of hierarchical clustering in the blogosphere is user preference. The so-called "user preference" refers to the content that bloggers are interested, with corresponding to the "channel" of the blog system, which is the entry for bloggers access to the blog system. Each BSP provides various types of channels, but most of bloggers only read and write around the channels they are interested (cross-channel statistics shown in Table IV), therefore, the hierarchical clustering within the blogosphere is the result of long-term self-selection of bloggers. Meanwhile, Tab-5 can prove relevant conclusions on global centrality of the blogosphere in the former part of this paper, although the social network within the blogosphere evolves in accordance with the rules of the "preferential attachment", preferred behavior primarily place within each blog channel, therefore, comprehensive blogosphere is difficult to form a core group with global influence, the diversity of user preference determines the diversity of the social network, which are the major reasons to generate hierarchical clustering in the blogosphere.

Within the same channel, further analysis was made on the hierarchy. Empirical studies showed that there are still very distinct "cluster" and "hierarchy" features within the same channel, but still with the lack of the "core" having global influence within the channel. By research, it was found that the "cluster" within the channel is still based on the subdivision of user preferences. For example, in the sports channel of blog.sina, different groups are formed according to different variations of the sports game, and then different sports games are subdivided into different clubs or sports star, thus, rich hierarchy is formed within the same channel.

TABLE IV. THE PROPORTION OF READING BEHAVIOUR ACROSS DIFFERENT CHANNEL

Behaviour properties of blogger				
channel	blog.sina	blog.sohu	blog.qq	blog.netease
Min ADC	3.824%	4.243%	4.082%	5.471%
Min ADC Channel	automobile	art	financial	sports
Max ADC	12.277%	11.149%	12.125%	12.751%
Behaviour properties of blogger				
channel	blog.sina	blog.sohu	blog.qq	blog.netease
Max ADC Channel	sports	livelihood	Emotion	Society
Avg ADC	6.626%	7.371%	6.084%	6.242%

2) Relationship Between the Hierarchy Position and the "User Level" in the Blogosphere.

"User level" is an evaluation indicator used to reflect the authority of bloggers, and this function is provided by blog.sina and blog.netease. Integer from 1 to 100 is used to specify the user level, the higher their level is, the more authoritative the user is. Empirical studies have shown that the "user level" has positive correlation with the hierarchy position in the blogosphere, and the user with higher level is more closely in the core position in the blogosphere, and vice versa in the "periphery" position. It was also found that the "user level" in Fig-4 has obvious segment feature, and when doing further research on the law of "segment", it was found that the reason of segmentation has a clear correlation with the blogger's information literacy, it will be discussed in more detail in the latter part of this paper.

3) Relationship Between the Hierarchy Position and the "Total Amount of Visits"

"Total amount of visits" is an evaluation indicator used to reflect the social influence of bloggers, it is the summation of a blog visited by other users, and this function is provided in all four sample objects of study. Empirical studies have shown a positive correlation between the "total amount of visits" with the hierarchy position in the blogosphere, and large "total amount of visits" means that blog is more closely in the "core" position in the blogosphere, and vice versa in a "periphery" position. Meanwhile, it is also found that the larger difference of "total amount of visits" is, the more obvious the hierarchy change is, with a positive correlation, or else the change is relatively smooth, which

demonstrates that "amount of visits" is an important indicator to reflect hierarchy.

4) Relationship Between the Hierarchy Position and the "Total Amount of Posts"

"Total amount of posts" is an evaluation indicator used to reflect the activity level of bloggers, it is the summation of posts belong to a blogger his or her own, this function is provided in all four sample objects of study. Empirical studies have shown a positive correlation between the "total amount of posts" with the hierarchy position in the blogosphere. The larger "total amount of posts" means that blog is more closely in the "core" position in the blogosphere, and vice versa in a "periphery" position. For the bloggers at the "periphery", four curves have shown the trend of rapid decay, it means that bloggers at the periphery of blogosphere have the weaker information creative abilities.

5) Relationship Between the Hierarchy Position and the "Total Amount of Social Ties"

"Total amount of social ties" is an evaluation indicator used to reflect the interact ability of bloggers. It is the summation of various social hyperlinks within a blog, and this type of function is provided in three sample objects of study (social tie function in blog.qq is imperfect). Empirical studies have shown a positive correlation between the "total amount of social ties" with the hierarchy position in the blogosphere, and the blogs with the more "social ties" are, the more closely in the "core" position in the blogosphere, and vice versa in the "periphery" position. Further research showed that: comments as the widely used social tie have the most prominent impact on the hierarchy position, and the blogs with more comments are often those blogger that with strong original content creation capabilities, who are the basis for the existence of the blogosphere. The influence of blogroll on the hierarchy in blogosphere presents different characteristics in different sample objects of study, which can not indicate that it has determined law. Trackback is rarely used in blogs, thus, with no prominent influence on hierarchy, the overall trend shows a linear trajectory under the action of comments.

6) Relationship between the Position in Blogosphere and the "Total Amount of Cites"

"Total amount of cites" is an evaluation indicator used to reflect the ability to acquire information of bloggers. It is the summation of posts cited by an individual blogger, and this function is provided in all four sample objects of study. Empirical studies have shown that the "total amount of cites" indicate the irregular distribution of the middle high and low on both sides. Relatively less "total amount of cites" in the core position and the periphery position in the blogosphere, especially for the nodes at the "periphery" position, which shows a very clear decay trend.This phenomenon indicates the ability and the subjective desire of bloggers acquiring information is weaker.

7) Relationship between the Hierarchy Position and the "Total Amount of Shares"

"Total amount of cites" is an evaluation indicator used to reflect the ability to dispersal information in the blogosphere, it is the summation of posts shared by a blogger to his friends. Empirical studies have shown that the "total amount of shares" indicate the distribution of the center-left high and low on both sides, relatively less "total amount of shares" in the core position and the periphery position of the blogosphere, and sharing behavior mostly focused to the middle part of hierarchy in the blogosphere. By further study on the "total amount of shares" and "total amount of cites", it was found that there is a certain relationship between the both indicators. Bloggers with more "cites" usually have more "shares", which indicates that there is a special type of bloggers whose behavior character is keen on reading about the posts of those bloggers in the "core" position and then share to his friend, with no strong ability to create information, but strong ability to diffuse information.

Fig. 6 shows the main reason to generate the hierarchical clustering phenomenon in the blogosphere, the horizontal axis indicates the hierarchy in the blogosphere, and the vertical axis indicates various influencing factors. The primary reason for the formation of hierarchical clustering in the comprehensive blogosphere is the interaction of subdivided blog channels and user preference, the second is the natural hierarchy as a result of differences in blogger's information literacy (the ability of posts sharing and posts citing). Based on the information literacy, bloggers were divided into three categories, leaders (active, well-respected posters), participants (active to occasional posters), and lurkers (readers only). Leaders are the "opinion ones" at the core in the network, also the original content providers within the blogosphere, various types of leaders are surrounded by participants who create very limited but enthusiastic contents about the content "sharing " and "reproduction", as the transfers of leaders and lurkers . Lurkers are at the edge of hierarchy, although they have a small amount of original posts, in more cases, they read the contents shared by participants, which means that differences in information using abilities makes some inevitability in blogosphere hierarchy.

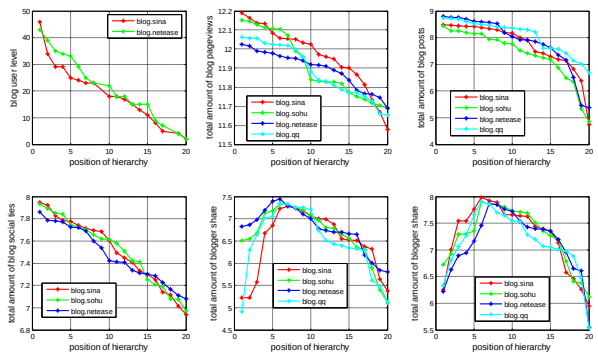


Figure 6. Influence factors of blogosphere hierarchy

C. Interaction Characteristic

1) Degree Correlations Coefficient

The correlation coefficient is a measure of the strength of the linear relationship between two variables that is

defined in terms of the sample covariance of the variables divided by their sample standard deviations. It is a number between 0 and 1, if there is no relationship between the predicted values and the actual values the correlation coefficient is 0 or very low. As the strength of the relationship between the predicted values and actual values increases, So does the correlation coefficient. $r = \sum(X-\bar{X})(Y-\bar{Y}) \Big/ \sqrt{\sum(X-\bar{X})^2 \sum(Y-\bar{Y})^2}$. A perfect fit gives a coefficient of 1.0. Fig. 8, and Fig. 9 show the in-degree and out-degree correlations coefficient in the blogosphere. Empirical studies have shown that the high out-degree nodes do not have a positive correlation with the high in-degree nodes both in blog network and post network. To explore the reasons, compare analysis was made on bloggers with high degree (they were divided into two categories: successful people in the real society and influential grass-roots users in the blogosphere), the results have shown that successful people in the real society have higher in-degree, but lower out-degree, even some successful people have 0 out-degree. In contrast, the grass-roots bloggers with high influence show a positive correlation in out-degree and in-degree distributions, but the summation of influential grass-roots bloggers are much less than the successful people bloggers. This means that the status difference in realistic social is still difficult to be bridged in the blogosphere, and the interpersonal relation is not reciprocal, thus, leading to the asymmetrical relationship in the global performance. In Fig. 7, the in-degree and out-degree of blog.qq have higher positive correlations, mainly because its blog relationship is based on the instant communication (Tencent QQ), whose blog relationship is enhanced by the real social network.

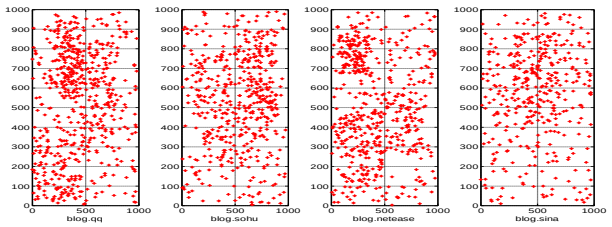


Figure 7. Blog network correlations coefficient

2) Average Path Length

Average path length is a concept in network topology that is defined as the average number of steps along the shortest paths for all possible pairs of network nodes. It is a measure of the efficiency of information or mass transport on a network. By letting N be the number of nodes, the average distance l of a network is defined as $l = 2 \Big/ (N(N+1) \sum_{1}^{n} \sum_{i \neq j}^{n-1} d_{ij})$, where d_{ij} is the shortest path length from node v_a to node v_b. Table V show the average path length, diameter, and radius in the blogosphere.

Empirical studies have shown that either blog network or post network has higher average path length and diameter, this phenomenon illustrates that the relationship is alienation and without small world effect. Compared with the law of average distance in different channels within the blogosphere, it was found that the larger number of members, the richer the connotations of channels, the more alienated their relationships will be, thus, for the comprehensive blogosphere, its membership inevitably shows the feature of weak link on the whole.

TABLE V. AVERAGE PATH LENGTH IN BLOG NETWORK

Properties of blog network				
property	blog.sina	blog.sohu	blog.qq	Blog.netease
Avg path length	18	20	13	17
radius	29	28	18	22
diameter	36	39	29	34

3) Clustering Coefficient.

Clustering coefficient is a measure of degree to which nodes in a network tend to cluster together. The clustering coefficient of a network is defined as $C = \frac{1}{N} \sum_{i=1}^{n} C_i$, where C_i is the clustering coefficient of node i , which is defined as: $C = 2E_i / k_i(k_i - 1)$,In the above equation, k_i is the degree of node i , and E_i is the total number of triangular cycles, which start from and return to node i . Fig. 8 shows the clustering coefficient for the blogosphere.

Empirical studies have shown that the four sample objects have relatively low average clustering coefficients, indicating that the blogosphere does not have a higher degree of clustering characteristic, which is consistent with the research result above that the blogosphere has no highly centralized “core” on the macro level. And then the study was made on the relationships between “user level”, “total amount of posts”, “total amount of social ties” with the clustering coefficient. The results of empirical studies have shown that the three elements mentioned above have no positive correlations with the blogosphere’s clustering coefficient, indicating that although the user authority, level of activity and influence can promote the formation of vertical hierarchy of the blogosphere, but can not effectively promote the horizontal interaction of bloggers. Thus, it can be seen that belief(culture) can be deemed as a means to make scattered individuals come together to form a loose group, but it is difficult to condense the loose group into a higher centralized organization. Lack of enthusiastic organizers and organizational resources within the blogosphere, therefore, the clustering level is relatively low, and its relationship does not have obvious transitivity.

The interaction characteristic intuitively indicates that the social behavior of bloggers is inactivity, with the relation alienated and non-transitivity. Since the nature of the primary cause of the relationship is lack of such organizer who can guide the grass-roots bloggers, and short of organizational resources that can make various bloggers highly gathered. As a consequenc, even after a long period of business operation, it is still difficult to change its relationship characteristic of weak link in blogosphere.

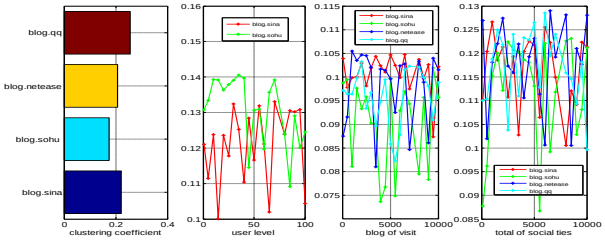


Figure 8. Clustering coefficient in blogosphere

V. Analysis of Structural Ontology Characteristics of the Blogosphere

The philosopher Karl Popper divides all the phenomena of human society into three worlds according to the coexistence way: the physical world (world I), spiritual world (world II) and objective knowledge world (world III). Three worlds contact and interact with each other. The effect from world I to world II, and then to world III is known as the "upward causal relationship", and the reverse feedback effect is known as the "downward causal relationship". Our research shows that the blogosphere is a typical system having characteristics of "three worlds", composed of belief (cultural) space, group space, and content space (shown in Fig. 9), three types of spaces form a complex social system under the combined action of the upward causal relationship and the downward causal relationship.

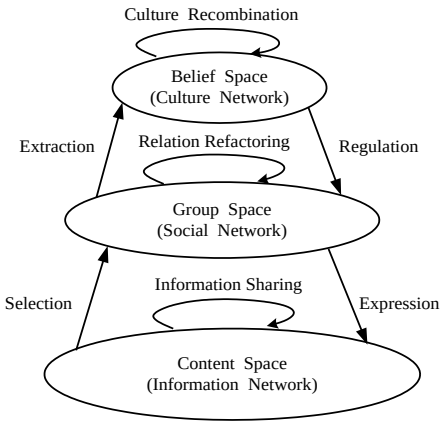


Figure 9. The relation of the three space

Content space is composed of posts, photos, comments and other elements inside the blog, these elements are organized by social ties together to form content networks contacting with each other. In addition to the relativity of information itself, the evolution inside the content space is also affected by "total amount of visits", "total amount of posts", and other factors. Therefore, the evolution rules of internal elements in the content space is the most complex, showing more distinct randomness and uncertainty. The group space is a community of information owners (bloggers), with their relationships were established on the basis of information linkages, as a social network understood in the conventional sense, with obvious characteristics of hierarchical clustering in structure. In group space, the evolution of interactive subject is not only affected by the user preference, but also closely related to the blogger's information literacy, "information creator→Information diffuser→information recipient" is the main vertical hierarchy structure mode in the group space. The belief space is a high-degree extraction of specific information, and from the sociological perspective, it can be understood as culture (belief), specifically, blog channel is a kind of meta-belief. In belief space, more complex cultural networks may be formed through the inheritance and evolution of meta-belief, thus, cultural network has priori characteristics.

Three worlds not only have series of endogenous rules of evolution, but also have some interactions among each other. In the evolution of the content space, various types of contents (posts) are generated continuously, these contents are passed from the content space through the "selection" behavior to the group space, and the social networks composed of bloggers are gradually formed by complex cognitive mechanisms. During the interactive process in the group space, "extraction" behavior is used to pass on the people's cognitions into the belief space to form the abstract meta-belief, then the meta-belief interact with other meta-beliefs to evolve a rich cultural network. At the meanwhile, those priori meta-believes in belief space are sent to the group space through the "regulation" behavior, and then members inside the group space continuously adjust their social network by making this as the guideline of personal action. The ever-changing social network within the group space pass the specific contents (posts) into the content space by the "expression" behavior that impact on the reading and writing behaviour of other bloggers to form content network in accordance with the correlations of contents themselves.

In conclusion, it is believed that the blogosphere is composed of three types of spaces, namely the belief space, group space and content space. Content space is an information network, group space is a network of relationships and belief space is a cultural network, each of which has its endogenous orders of evolution, and also interacts with each other, thus constituting a complex system having both heter-organization ability and self-organizing ability. The fundamental cause for the structural ontology characteristics of the blogosphere is the co-evolution of the three spaces, and at the horizontal level. Each space shows the synergy of multiple endogenous rules, and at the vertical level, different spaces indicate the interactive feature of "deduction-induction", therefore, any simple structural reductionism or functional reductionism cannot comprehensively describe the structure ontology characteristics of the blogosphere.

Acknowledgment

This work was supported in part by a grant from the Ministry of Education, Humanities and Social Sciences Research on the West and the Border Area (Grant No.14XJC910002), the National Natural Science Foundation (Grant No.71401092), the Fundamental Research Funds for the Central Universities (Grant No.13SZYB01), and the Scientific Research Program

Funded by Shaanxi Provincial Education Department (Program No.14JK1545).

REFERENCES

[1] E. Adar, L. Zhang and R. Lukose. "Implicit structure and the dynamics of blogspace, "*Proc of the 16th International World Wide Web Conference*, pp. 937-945, 2006.

[2] N. Agarwal, M. Galan, Huan Liu and S. Subramanya. "Clustering blogs with collective wisdom, "*Proc of the International Conference on Web Engineering*, *IEEE*, pp. 739-742, 2008.

[3] R. Kumar, J. Novak, P. Raghavan, and A. Tomkins. "Structure and evolution of blogspace, "*Communicationsof the ACM*, vol. 47, no. 12, pp. 35-39, 2004.

[4] Chen Yu, Zong Xiao, Hao Jie, XU yan, "Chinese blog burst in people's life, "*Journal of news commuciation*, vol. 34, no. 10, pp. 234-239, 2008.

[5] N. Agarwal, M. Galan, Huan Liu and S. Subramanya, "Clustering blogs with collective wisdom," *Proc of the International Conference on Web Engineering*, pp. 336-339, 2008.

[6] Yang G. B, "The Power of the Internet in China: Citizen Activism, "*Columbia University Press*, 2009.

[7] CNNIC, "33th Statistical Report on Internet Development in China," *http: //www. cnnic. cn/hlwfzyj/hlwxzbg/hlwtjbg /201403/t20140305_46240. htm*, 2014.

[8] C. Marlow and N. Glance, "Audience structure and authority in the weblog," *Proc of the International Communication Association Conference*, vol. 27, pp. 43-51. 2004.

[9] L. Adamic, and N. Glance, "The political blogosphere and the 2004 US election: divided they blog," *Proceedings of the 3rd international workshop on Link discovery. ACM*, pp. 36-43, 2005.

[10] T. Lento, H. Welser, L. Gu, and M. Smith. "The tiesthat blog: Examining the relathionship between social ties and continued participation in the wallop weblogging system," *In 3rd Annual Workshop on the Weblogging Ecosystem*, vol. 12, 2006.

[11] Y. Lin, H. Sundaram, Y. Chi, J. Tatemura, and B. Tseng. "Discovery of blog communities based on mutual awareness," *In WWW2006 Workshop on Weblogging Ecosystem*, 2006.

[12] J. Cummings, B. Butler, and R. Kraut. "The quality of online social relationships," *Communications of the ACM*, vol. 45, no. 7, pp. 103-108, 2002.

[13] N. ALi-Hasan and L. Adamic. "Expressing social relationships on the blog through links and comments," *Ann Arbor*, 1001: 48109, 2007.

[14] C. Marlow. "Investment and attention in the weblog community," *In, AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs*, pp. 128-135, 2006.

[15] C. Woo‐young and H. W. Park, "The network structure of the Korean blogosphere". *Journal of Computer - Mediated Communication*, vol. 17, No. 2, pp. 216-230, 2012.

[16] M. Klaus and R. Wagner, "Exploring the Interaction Structure of Weblogs, "*Advances in Data Analysis, Data Handling and Business Intelligence*, Springer Berlin Heidelberg, 545-552, 2010.

[17] T. Nguyen, D. Phung, B. Adams and S. Venkatesh. "Event extraction using behaviors of sentiment signals and burst structure in social media," Knowledge and information systems, vol. 37, No. 2, pp. 279-304, 2013.

[18] J. Leskovec, M. McGlohon, C. Faloutsos, N. S. Glance and M. Hurst. "Patterns of Cascading behavior in large blog graphs," *SDM*. Vol. 7, pp. 551-556, 2007.

[19] A. J. Kim and R. E. Tarja, "Community Building on the Web: Secret Strategies for Successful Online Communities," *Peachpit Press*, pp. 289-293, 2002.

Xue Li was born in ShaanXi, China, in 1974. She received the M.S. degree and Ph.D degree from Xi'an University of technology in 2004 and 2013 respectively. She is currently a postdoctor in ShaanXi Normal University. Her research interests include electric commerce, social commerce, social computing, and complex network.

Ying'an Cui was born in ShaanXi, China, in 1975. He received the M.S. degree in communication engineering in 2005. He is currently working towards the Ph.D. degree in network technology from Xi'an jiaotong University, Xi'an China. He is corresponding author. His research interests include social computing, cloud computing, web2.0 and complex network.

Hui Xia was born in ShaanXi, China, in 1978.He received the M.S. degree in computer technology and application from Xi'an university of technology in 2005.He is currently study for Ph.D. degree in computer science from Northwest university, Xi'an, China. His research interests include Social computing, cloud computing and computer system design.

Source-Directed Path Diversity in the Interdomain Routing

Miao Xue, Gang Fu, Ruitao Ma, and Longshe Huo
Network Technology Research Institute of China Unicom, Beijing, China
Email: {xuemiao9, fugang16, mart7, huols}@chinaunicom.cn

***Abstract*—The Internet has abundant path redundancy, especially in the interdomain routing. However, current routing system can not exploit the Internet path diversity and utilize the disjoint end-to-end paths efficiently. The unawareness of sources to the path selection and the best paths advertisement mechanism in the interdomain routing make it difficult to use disjoint end-to-end paths. In this paper, we present the Source-Directed Path Diversity (SDPD), leveraging which sources can specify the alternate paths to forward the traffic besides the default path. In SDPD, the packets carry the Source-Directed Tag (SDT) in the packet headers to hint the BGP routers the preference of the sources on the path selection, while the BGP routers forward the packets independently based on the sources' indication. Moreover, we propose the multipath advertisement of the BGP route reflectors in SDPD to reduce the filtration of the redundant paths in the interdomain routing. We evaluate the SDPD through simulations over a synthetic Internet-like topology. The simulation results show that the SDPD can exploit alternate paths with low similarity and stretch efficiently.**

***Index Terms*—Source-Directed; Path Diversity; Multipath Routing; Interdomain Routing**

I. INTRODUCTION

In recent years, path diversity in the Internet has received significant attention. Many previous studies have shown that path diversity has the ability to improve the end-to-end throughput and reliability [1-3]. Driven by the benefits of path diversity, lots of network technologies are deployed in the Internet to improve the path diversity at both the infrastructure level and the protocol level. For example, multihomed stub networks are capable to access multiple ISPs, and multi-interface mobile terminals, such as Laptops and tablet PCs, can access heterogeneous networks simultaneously. While the multipath routing based Enhanced Interior Gateway Protocol (EIGRP) [4] and Open Shortest Path First (OSPF) [5] and the end-to-end multipath transfer[6-8] try to exploit the path diversity at the protocol level.

Although the evolving network infrastructure provides abundant path redundancy, the path diversity in the Internet is still not exploited sufficiently. A measurement study of a large ISP found that almost 90% of Point-of-Presence (PoP) pairs have at least four link-disjoint paths between them [9]. Savage [10] found that although Internet traffic traverses a single path, 30% to 80% of the time, an alternate path with lower loss or smaller delay exists. However in [11], Han shows that a significant portion of the paths from a multihomed site overlaps near the endhosts and in the core of the Internet, and concludes that simply having a stub network connected to multiple ISPs does not necessarily guarantee high levels of path diversity.

The existing multipath routing protocols are mainly used in the intradomain routing, such as, OSPF and EIGRP. Though the interdomain routing has the most abundant path redundancy, the Border Gateway Protocol (BGP) does not support multipath routing, which leads to poor path diversity, at both Autonomous System (AS)-level and route-level. Furthermore, for scaling and ease of management purposes, many ISPs have moved their iBGP architecture from a full mesh of iBGP sessions to route reflection [12]. But the Route Reflector (RR) only advertises its best paths to other RRs as well as to its clients, which hides most of the redundant routes.

Even if there are multiple routing entries for each prefix at the control plane of the BGP routers [18-19], how to utilize the multiple routing entries at the forwarding plane is still a problem. In the routing system using traditional destination-based forwarding, the end system has little knowledge about which path it utilizes. Loose coupling between the data flow and the forwarding path produces a mass of packets reordering, which degrades the throughput of the reliable transport layer protocols drastically [13]. Source routing, which carries routing information in the packet headers, could specify partially or fully the paths taken by the packets. However, it faces the scalability and security problems since each end-system needs a map of the overall network to formulate the end-to-end paths.

Since the path redundancy provided by network infrastructure cannot guarantee the end-to-end path diversity always, it is necessary to study how to exploit the path diversity in the Internet at different levels. To achieve end-to-end path diversity, two issues need to be addressed: 1) setting up multiple independent paths between the end-nodes (multipath routing); 2) utilizing the given independent paths based on the network and/or terminal. Based the principals above, we propose the SDPD. At the control plane, the SDPD improves the RR to advertise multiple routes toward the same prefix over the iBGP sessions, thus the BGP routers have more consistent and comprehensive routing view to provide a

doi:10.4304/jnw.9.12.3251-3262

diverse set of paths. Besides, the BGP routers in SDPD are allowed to install multiple routing entries towards the same IP prefix in the Forwarding Information Base (FIB). At the forwarding plane, the SDPD makes use of the source-directed multipath forwarding. Leveraging the SDPD, the source could specify the end-to-end paths for the data flow, but it is not necessary to strictly restrict which routes to take for the end-system. In SDPD, the source only provides an indication, the SDT, which includes the Connection Identifier (CID) and Path Index (PI), to the BGP routers to hint which path is preferred. The BGP routers in the path choose the next-hops based on the source indication and their own routing policy. The forwarding rules are similar to the mechanisms in [14-15], but the SDPD could recognize the data flow and assign it to a specific path in its lifetime. The source can measure the path characters based on the SDT and specify the paths with better performance.

We evaluate the SDPD in the simulations with a synthetic Internet-like topology. The simulation results show that the SDPD provides more abundant paths at the control plane of the interdomain routing without increasing the update messages overhead and the convergence time significantly. Leveraging the SDPD, the end-systems could exploit more end-to-end paths with low path similarity and stretch. In the simulations, with different PIs, at least 70% of the alternate paths are totally edge disjoint with the best path, and 99% of the alternate paths have the same length as the best path.

The rest of this paper is organized as follows. Related works are reviewed in Section II. In Section III, we present the design of multipath BGP based the multipath advertisement of RR. Section IV details the source-directed multipath forwarding rules. In section V, we evaluate the source-directed path diversity. Section VI discusses some open issues when deploying the SDPD. Finally, the conclusions are given in section VII.

II. Related Works

This section provides an overview of existing solutions to exploit the path diversity for the interdomain routing.

Multipath routing, which provides nodes access to multiple paths for each destination, can increase the reliability and improve the capacity by increasing the number of paths utilized. OSPF explicitly allows equal cost multi-path routing, while the EIRGP provides more aggressive multipath routing by utilizing unequal cost multiple paths. OSPF is also capable to obtain path diversity by doing multi-topology routing [16]. Besides, new intradomain routing architecture [32] is proposed to introduce hierarchical network model and source routing. Since in a specific domain, all the routing devices are under a single management entity, the multipath routing based intradomain routing protocols could be easy to deploy.

The interdomain routing has the most abundant path redundancy, as the ISPs usually design their networks with resiliency in mind, and tend to be multihomed and multiconnected. In order to exploit the path diversity of BGP, many proposals are put forward. MIRO [17] uses BGP by default and can negotiate the use of additional paths between arbitrary pairs of ASes. But it requires establishing additional state at BGP routers for each alternate path and additional out-of-band control-plane signaling. Wang [18] proposes the D-BGP, a path diversity aware routing protocol. The D-BGP extends BGP to allow each BGP router to advertise a most disjoint alternative path along with the best path. But when choosing the alternative path, the D-BGP considers mainly the AS-path length property but less the other properties like Loc_Pref and MED. Add-Paths [19] allows the BGP routers to advertise multiple paths to the same prefix over the iBGP sessions and keeps the eBGP sessions unchanged. However the Add-Paths does not limit the number of the routings to the same prefix in the FIB, which increases the consumption of the routers' memory significantly. YAMR [21] presents the YPC which constructs a set of policy-complaint interdomain routing paths to tolerate any single interdomain link failure. Besides, the YAMR also puts forward a mechanism to reduce control message overhead imposed by alternative path advertisement by localizing routing updates. BGP-XM [31] allows routers to use multiple paths across different ASes. BGP-XM defines a router architecture tailored to accommodate the information of multiple paths to the same network prefix into a single BGP update message to guarantee path diversity, and proposes an optimal path selection algorithm.

Some novel routing architectures have been proposed to exploit the path diversity in the interdomain routing. Yang presents the NIRA [20], a new interdomain routing system that supports user choice. NIRA allows networks to offer any valley-free path and a user can specify a path using both the source and destination address. The work in [22] proposes the pathlet routing to construct the multipath routing. In pathlet routing, networks advertise fragments of end-to-end paths from which a source can assemble an end-to-end route. Pathlet routing could be a simple generalization of both path vector routing and source routing, depending on the length of each pathlet. However, it needs a significant change to the current Internet to implement the proposed architectures in practice. Reference [33] proposes to establish a logically centralized multi-AS routing control platform leveraging the control plane and forwarding plane separating of SDN(Software Defined Network), for taking efficient routing decisions, detecting policy conflicts, troubleshooting routing problems in a global view.

On the other hand, source-controlled routing reserves some choice of routes for the sources to select on a per-packet basis, which provides more flexible path diversity and more direct control on the path selection. Source routing could specify partially or fully the paths taken by the packets, however, it faces the scalability and security problems. Yang [14] puts forward a tag-based source routing architecture that uses routing deflections to provide path diversity. End-systems tag packets with hints, rather than explicit source routes, and routers use these hints to select among alternate paths. Similar to [14], path splicing [15] makes use of the splicing bits in the

TABLE I. MULTIPATH INTER-DOMAIN ROUTING PROTOCOLS COMPARISON

Protocols		Path Diversity	Control Plane Overhead	Data Plane Overhead		Loop-free	Scalability	Source-Directed
				Packet Overhead	Forward Table (FT)			
BGP based	MIRO	High	Low	Tunnel ID	Tunnel ID based FT	Yes	Yes	No
	Add-Paths	High	High	Local Path ID	Destination and Path ID based forwarding	---	---	---
	D-BGP	Medium	Medium	No	BGP FT	No	Yes	No
	YAMR	High	High	Path ID	Destination and Path ID based forwarding	No	Yes	No
	BGP-XM	High	Medium	No	BGP FT	Yes	Yes	No
New routing architecture based	NIRA	High	Medium	No	Multiple FT	Yes	Yes	Yes
	Pathlet	Medium	High	Forwarding ID	Forwarding ID based	Yes	Yes	Yes
	SDN based	High	Medium	No	Multiple FT	Yes	Yes	No
Source directed based	Path deflect	Low	Low	Deflect tag	Multiple next-hop	Yes	Yes	Yes
	Path slicing	Low	Low	Splicing bits	Multiple FT	No	Yes	Yes
	Slick packet	Medium	Low	FS bits	Multiple next-hop	Yes	No	Yes

packet header to switch the traffic among multiple routing trees ("slices") along a single path. By setting different splicing bits, the end-systems can obtain diverse paths both at the AS-level and the route-level. Slick Packets [23] allows the source to embed the routing information within the packet header in the form of a forwarding subgraph. Based on the routing information in the packet header, Slick Packets could quickly switch the packets from a primary path to the alternate paths. Since it is necessary to recognize the source tag or source encode, the routers in [14-15, 23] need to modify the forwarding plane.

Table I shows the comparison of the multipath inter-domain routing protocols mentioned above.

III. MULTI-PATH BGP

A. Path Hiding in Route Reflector

The BGP is the interdomain routing protocol used in the Internet. In order to maintain a consistent routing state, the routers running the BGP instance need to establish sessions to their neighbors to exchange the BGP paths. External BGP (eBGP) sessions are used among adjacent routers belonging to different ASes to exchange paths, while internal BGP (iBGP) sessions are used among the routers belonging to the same AS to exchange the paths learned at the border of their own AS. To guarantee each router in an AS receiving all the usable paths, classical iBGP architecture initially adopted the Full Mesh [24] of iBGP sessions. However, for scaling and ease of management purposes, many ISPs have moved their iBGP architecture from a full mesh of iBGP sessions to route reflection [12]. The RR collects paths received from its neighbors over both the iBGP sessions and eBGP sessions. Based on its own routing view, the RR advertises its best paths to other RRs as well as to its clients and non-client BGP neighbors. Though the utilization of the route reflection improves the scalability of the iBGP and reduces the advertisement of the update messages, it also filters the paths that some routers suppose to receive and leads to the path hiding.

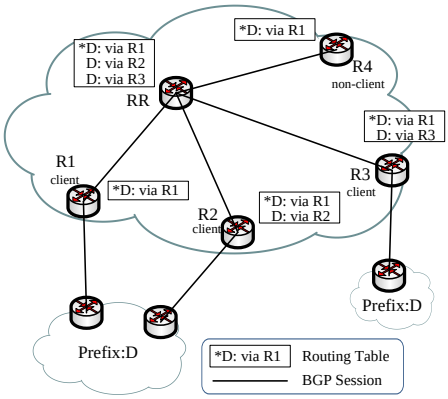


Figure 1. Path hiding in route reflector

Fig. 1 shows a simple scenario to explain how the RR hides the paths. In this scenario, there are three paths to the prefix D separately via R1, R2 and R3. Providing the path via R1 has higher local preference, thus the RR chooses the path to the prefix D via R1 as the best path and advertises to its clients R2 and R3 and non-client peer R4. As a result, the R4 knows only one path to the prefix D. And the clients of RR also only know the best path and the paths collected by their own, though there exist other paths, the clients are not aware of. For example, the R2 has no knowledge of the path via R3, and vice versa. Although all the routers could receive the best paths and eventually converge, the path diversity is lost seriously comparing to using the full mesh of iBGP sessions. Such a lack of router-local path diversity causes BGP route oscillations, prevents fast recovery and restricts the load balancing on multiple BGP nexthops [19].

B. Multipath Advertisement of RR

In order to recover the path diversity in an AS, we convert the RR as a routing relay and allow the RR to disseminate multiple BGP nexthop-disjoint paths towards the same IP prefix. Advertising multiple paths increases the overhead of the update messages, thus it is necessary to select the paths advertised carefully to guarantee the path diversity as well as to reduce the control plane overhead.

The RR plays two roles in SDPD. The first one is to reduce the number of BGP sessions, as the role it plays normally. The second one is to collect the paths from its clients and non-client peers and forward the paths to other clients and non-client peers. Leveraging the multipath advertisement, the RR disseminates not only the best paths, but also other nexthop-disjoint paths. Actually, by utilizing the full mesh of iBGP sessions, though the iBGP router knows all the paths of the other iBGP routers in the same AS and has high path redundancy, many paths are worthless. For example, assuming there are multiple nexthop-disjoint paths with relatively higher local preference, the paths with low local preference do not need to be disseminated over the iBGP sessions, as these paths with little chance are chosen to forward packets for the factors of routing policies and economic relationship. Therefore, the RR in SDPD only selects the nexthop-disjoint paths with better condition to advertise.

BGP uses incremental updates. After having exchanged all their routing entries among the BGP speakers, BGP routers only need to send BGP Updates to each other if a path changes. The new BGP Update implicitly replaces the previous BGP message for the same prefix. Herein, we modify the BGP routers to recognize a path not only based on the destination prefix but also the Next-hop in the path. If a path in the Adj-Rib-Ins has the same destination prefix and Next-hop as the Network Layer Reachability Information (NLRI) in the Update messages, the path is replaced by the new path. Since the Withdrawn routes have no Next-hop information in the Update messages, we extend the Withdrawn routes encodings to <length, prefix, Next-hop> to avoid withdrawing one prefix but multiple paths.

To support the multipath BGP, the FIB needs to store multiple nexthop-disjoint paths for each destination prefix. In [19], the BGP routers import all the paths in the Routing Information Base (RIB) to FIB, while in [25], the FIB only reserves 4 best paths for each destination prefix. In order to reduce the consumption of the FIB memory, we take a similar method as in [25] to keep 4 paths for each destination prefix, one best path and three alternate paths. It is worthwhile to note that the paths installed in the FIB should be nexthop-disjoint, which provides the path diversity at the best effort.

The multipath advertisement is only implemented over the iBGP sessions, between the RRs and the clients or the RRs and non-client peers. The eBGP sessions still follow the standard BGP and only advertise the best path towards a prefix. Providing a best path to a prefix in one of the eBGP peers becomes unfeasible, the border router does not need to propagate the Withdrawn route over the eBGP session, as long as there is an alternative path to that prefix existing in the FIB of the border router.

The multipath advertisement of RR increases the path diversity, at the cost of reflecting Update messages and re-triggering the BGP decision process more often. The additional Update messages impact the control plane convergence, but since the FIB has multiple paths to the same prefix, it is not necessary for the BGP routers to forward packets after the convergence of the control plane, as long as there is at least one path left in the FIB.

C. Path Selection of Multipath Advertisement

To reduce the control plane overhead, the RR only advertises the nexthop-disjoint paths towards the same destination prefix, which provides path diversity as well as the capability for load balancing. The other BGP routers still disseminate the best paths. We propose four modes in this section to select the paths for advertising.

BGP-RR-all-Paths: The RR advertises all the nexthop-disjoint paths in the RIB to its clients and non-client peers. Intuitionally, this mode brings the most path diversity and also the most Update messages. As no path is filtered, this mode has nearly the equivalent effect as using the full mesh of iBGP sessions on supplying the path diversity.

BGP-RR-Highest-Locpref-Paths: The RR only advertises the nexthop-disjoint paths with the highest local preference. This mode takes the routing policy and economic relationship of the ISPs into consideration. Since the paths with low local preference are unlikely to be selected by the BGP path decision process to install in the FIB, it is not necessary to disseminate these paths. Thus, this mode filters a fraction of paths useless.

BGP-RR-Shortest-ASlen-Paths: The RR disseminates the paths with the shortest AS length after the selection of the BGP-RR-Highest-Locpref-Paths mode. This mode considers the path condition and filters out more paths than using BGP-RR-Highest-Locpref-Paths.

BGP-RR-Lowest-MED-Paths: After using the BGP-RR-Shortest-ASlen-Paths mode, the RR selects the paths with the lowest MED and advertises them. If there are multiple paths to the same prefix via the same nexthop AS, only the paths with the lowest MED are chosen.

Here it needs to note that the selection modes are only implemented on the paths having the same destination prefix. The path selection of the multipath advertisement also follows the best path decision process of BGP, but the process may break before reaching the end in order to get multiple candidate paths. In addition, the path selection of the multipath advertisement in the RR strictly complies the export policies and import policies as the standard BGP. The computational cost to run the selection modes still remains low, as comparing to standard BGP, the selection modes do not go through the whole sequence of the decision rules. The multipath advertisement introduces additional control plane overhead, but also provides more path diversity in the RIB of the BGP routers. Therefore, it needs a tradeoff between the control plane overhead and the path diversity.

IV. SOURCE-DIRECTED MULTIPATH FORWARDING IN SDPD

Previous multipath routing selects the forwarding path based on the local decisions of the router, for example, the OSPF makes use of the Round-Robin algorithm to send data packets over the multiple paths. Although the utilization of the multipath routing improves the path diversity, the sources can not tell which paths they are

using. The source only knows the endpoint interfaces of the end-to-end path, but is unaware how the paths go through the network. SDPD reserves some routes choice for the sources on per-packet basis. For example, sources can perceive the link failure in the end-to-end path and switch to a working path within a few Round-Trip Times (RTTs), also the sources can pick better paths based on the observed performance. Thus, SDPD is a promising approach to improve the utilization of path diversity.

In order to make the source have a more comprehensive knowledge about the end-to-end path it utilizes, we propose the Connection Identifier (CID) which is used to identify a data flow in the network, and Path Index (PI) which indicates the path preference of the source. The CID and PI both are encoded into the Source-Directed Tag (SDT), and we detail the generation of the SDT in the next section. The BGP routers need to refer the indications of the CID and PI to forward packets. The forwarding goal of the SDPD is twofold, the fast failure reaction by switching the path to alternate one, and the flexibility of routes chosen by sources at the edge of the network.

A. Source-Directed Tag Generation

We design the Source-Directed Tag to be an IP option in the IP header. But it is important to note that the location of the SDT should not be limited by our design, it also may be at a shim header between the IP and MAC layer, or in the header of a next-generation Internet protocol. There are two principles in designing the encoding format of SDT. Firstly, the size of the encoding format should be minimized; secondly, the processing at forwarding plane should be simple.

The CID is used to identify a data flow in the network. When an end system begins to communicate with a peer, <source IP, destination IP, source port, destination port> is utilized to generate the CID. Here we apply the hash algorithm, CRC16, which is considered having more computational efficiency[28], to calculate the CID.

$$CID = CRC16(srcIP, dstIP, srcport, dstport)$$

The source could get the 4-tuple from the application service or the negotiation signals for initiating the connection, for example, the TCP SYN. Although there are transport protocols using multiple addresses in the communication, such as the Stream Control Transfer Protocol (SCTP) and Datagram Congestion Control Protocol (DCCP), the CID is generated by utilizing the 4-tuple which is carried in the packet header in the initialization of the connection. Since the data flow is unidirectional, the CIDs may be different in the peers of the same communication connection. The length of the CID is 2 bytes. When the packet with CID going through a BGP router, the router records the CID in its flow list. If there is no packet with the CID passing the router in a specific period, the router removes the CID from the flow list. We set the specific period to 2s, as the default timeout of TCP and SCTP is 1s. Even if the packets with the CIDs removed reach the router again and are deflected along alternative path, there is little chance to cause packet reordering. We detail the flow list and the packet forwarding rules in the next section.

The PI is the index of the path the source selects. In this paper, the length of the PI is 1 byte, that is, the source could specify 256 paths at most. The PI does not need to specify exactly each hop's selection as in [14-15, 22-23], since it is difficult to predict how many hops the path goes through and it is also insecure to provide the network map to the source. The PI only gives the routers a hint on which path is preferred, however it does not require the routers to forward the packets strictly following the source's indication. The routers have completely independent forwarding decision, they could take the PI as a forward option, but they may also ignore the PI if necessary, for example, the source indication conflicts with the router's local policy. The Fig. 2 shows the encoding format of the SDT option.

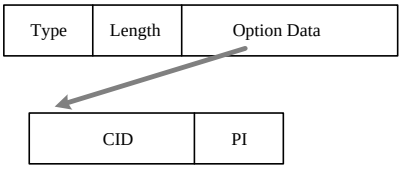


Figure 2. Encoding format of SDT

B. Forwarding Principles

In this section, we elaborate the forwarding principles of the packets with SDT. When sending packets, the source embeds the SDT in the IP headers. Upon receiving a packet, the BGP router checks the IP option. If there is no IP option of SDT in the packet header, for the backward compatibility, the router forwards the packet along the best path. Otherwise, the router checks the value of CID in SDT. If the CID is not in the router's flow list, which means the data flow did not pass through this router, the router adds the SDT.CID to its flow list, forwards the packets over the best path and records the SDT.PI going through the best path. If the router records a CID which equals to the SDT.CID, which means the flow has passed through the router, the router chooses the forwarding path based the SDT.PI. If the SDT.PI equals the CID:PI in the flow list, the packet is forwarded along the best path. If the SDT.PI is 0, but the CID:PI in the router's flow list does not equal to 0, set the CID:PI to CID:0. When the SDT.CID is in the router's flow list and SDT.PI does not equal to 0 and in the flow list the CID:PI is 0, the forwarding path index is calculated by FPI=PI%MAXPI, where the FPI is the index of the forwarding path, MAXPI is the number of the paths towards the same destination as the received packet. And the packet is forwarded along the FPIth path in the router. The forwarding algorithm is described in the Algorithm 1.

Fig. 3 demonstrates a simple forwarding example using SDT. In the Fig. 3, the Router A has two disjoint iBGP nexthops, Router B and Router C, and the path passing Router C is the best to reach the prefix D. There are four packets with SDT option reaching the Router A. The SDT of the first packet is $CID_1:1$. Since the Router A does not record the CID_1, it adds the CID_1 to its flow

list, forwards the packet along the best path, and records the PI using the best path in the flow list, here the PI is 1. Then the second packet arrives with SDT $CID_1:3$. Checking the flow list of Router A, there exists CID_1. As the PI using the best path does not equal to 0, and the SDT.PI is 3, following the Algorithm 1 the Router A get the *FPI* 1 for the second packet. Thus, the second packet is sent over the alternative path via Router B. The flow list of Router A has no CID_2, therefore the third packet is transmitted along the best path. As the fourth packet's SDT.PI is 1, we obtain the *FPI* is 1, thus the Router A propagates the packet along the alternative path.

Algorithm 1: BGP Router Forwarding Algorithm

```
Forwarding Procedure:
if SDT.CID not in the Router.flow_list then
    add SCT.CID to Router.flow_list
    Router.flow_list[SDT.CID] = SDT.PI
    forwarding packet along the best path
else
    if Router.flow_list[SDT.CID]! = 0 then
       if Router.flow_list[SDT.CID] == SDT.PI and
          SDT.PI! = 0 then
          forwarding packets along the best path
       else if SDT.PI == 0 then
          forwarding packet along the best path
          Router.flow_list[SDT.CID] = 0
       else
          FPI = SDT.PI%MAXPI
          forwarding packet along the FPIth path
       end if
    else
       FPI = SDT.PI%MAXPI
       forwarding packet along the FPIth path
    end if
end if
```

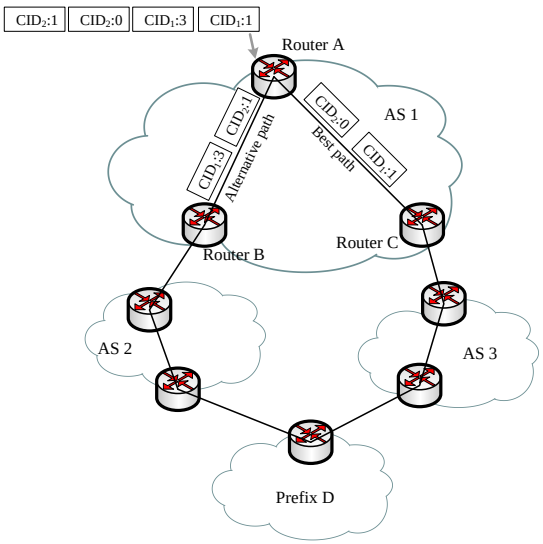


Figure 3. A simple forwarding scenario using SDT

The forwarding algorithm is designed with two principles in mind. Firstly, the forwarding algorithm should exploit the path diversity at the best effort. Secondly, when exploiting the path diversity, the best path has the highest priority to be selected to forward packets, as the best path in BGP is usually considered as the shortest path to the destination and the most consistent path in policy.

C. Loop-free Alternate Paths

The multipath BGP improves the path redundancy and installs multiple nexthops in the FIB for the same prefix. According to the standard BGP, the packets are forwarded along the best path in each router, which can guarantee the end-to-end path is loop-free. While the SDT could make the BGP routers deflect the packets over different BGP routing trees and change the AS egress point (and hence next ingress point) comparing to the best routes, which may cause loops in the end-to-end forwarding paths.

Fig. 4 shows an example of routing loop caused by SDPD. In Fig. 4, suppose that AS 1 receives three path advertisements to prefix D from its neighbors. Following the design in Section 3, all the three paths are installed in the routers' FIB in AS 1. And the AS 2 also has three paths to the prefix D in the routers' FIB. Here we assume the network has converged. If a packet whose destination is prefix D reaches the AS 1, the standard BGP forwards the packet along the best path (1 3 5). However, the multipath BGP may introduce paths not the best, which may violate the "prefer-customer" routing policy. For example by using SDMF, the AS 1 forwards a packet with SDT.PI =3 along the path (1 2 4 5) to the peer AS 2. When the AS 2 receiving the packet with SDT.PI=3, it may also select the path (2 1 3 5) to send the packet back to AS 1. Thus, the packet is forwarded back and forth between the AS 1 and AS 2 and falls into a loop.

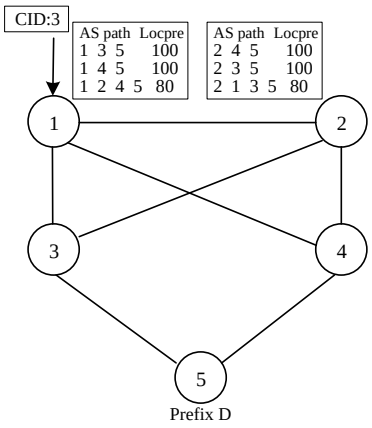


Figure 4. An example of routing loop caused by SDPD. The AS paths around a node represent the available paths in the nodes routing table, which are ordered in the descending order of local preference

The Local Preference Attribute represents the AS's preference in forwarding the traffic. Furthermore, the Local Preference Attribute plays an important role in implementing the "prefer-customer" and "valley-free" routing policies and avoiding the routing loop. When ASes use "prefer-customer" and "valley-free" routing policies, it means that any router of the AS will only choose an egress point that advertises the most preferred path, barring inter-AS loops as long as there are no

customer-provider loops[14]. In the multipath BGP, the multipath advertisement is only implemented in the iBGP, while the eBGP still disseminates the most preferred path. That is, the relationship of the ASes in the multipath BGP is just as in the standard BGP. Therefore, though the routers running multipath BGP receive multiple paths, if they follow the "prefer-customer" and "valley-free" routing policies, the loop can be avoided. Formally, we have the following theorem.

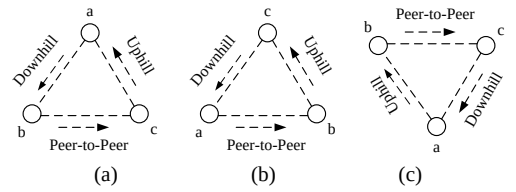


Figure 5. Assuming scenarios of the AS path loop in SDPD

Theorem 4.1: If all the AS paths follow the "prefer-customer" and "valley-free" routing policies, the end-to-end path using SDPD is loop-free.

Proof: Suppose the forwarding path is $\{s,\ldots,u_i,\{u_{i+1,1},u_{i+1,2},\ldots,u_{i+1,m}\},\ldots,d\}$ $m\le 4, i<n$, where $\{u_i,\{u_{i+1,1},u_{i+1,2},\ldots,u_{i+1,m}\}\}$ $m\le 4, i<n$ means the multiple forwarding edges in the FIB of the BGP routers, s is the source and d is the destination. We prove the theorem 4.1 using the proof by contradiction. Assuming the AS path (a,b,c,a), a portion of the SDPD forwarding path, is a loop. There are 3 loop scenarios as shown in Fig. 5.

In Fig. 5 (a), the loop $a\to b\to c\to a$ corresponds to Downhill path, Peer-to-Peer edge, Uphill path. According the "valley-free" principles, node c can be followed by only provider-to-customer edge. While the provider-to-customer edge can not appear in an Uphill path. Thus the AS path loop shown in Fig. 5 (a) is untenable.

In Fig. 5 (b), the loop $a\to b\to c\to a$ corresponds to Peer-to-Peer edge, Uphill path, Downhill path. According the "valley-free" principles, node b can only export paths of itself and paths learned from its customers to node a. Therefore, node b should be followed by a provider-to-customer edge. However in Fig. 5 (b), node b is followed by a customer-to-provider edge, which apparently violates the "valley-free" principle. Thus the AS path loop shown in Fig. 5 (b) is untenable.

In Fig. 5 (c), the loop $a\to b\to c\to a$ corresponds to Uphill path, Peer-to-Peer edge, Downhill path. Apparently, (a,b,c,a) is a "provider-customer" loop. Following the "valley-free" principles, node a should not export the paths learned from its provider b to its another provider c. Therefore the AS path loop shown in Fig. 5 (c) is also untenable.

In order to avoid the routing loop, we improve the path decision process by only allowing the paths with the highest Local Preference to be installed in the FIB. Thus, the routers no longer violate the "prefer-customer" and "valley-free" routing policies as they are in the single path case. For example in Fig. 4, the routers in AS 1 only select the paths with the highest Local Preference, (1 3 5) and (1 4 5), to install in the FIB. The path (1 2 4 5) is not allowed to install in the FIB, as the AS 1 and AS 2 are "Peer-to-Peer" relationship and have relatively low preference. However, the maximum number of the paths towards each prefix in the FIB is still 4.

D. Path Diversity Metrics

Since the SDT could hint the BGP routers to forward the packets along the alternate paths, it is necessary to measure how much these paths differ from the best path. Here we propose two metrics to evaluate the alternate paths.

Suppose $P_b=\{A,N_1,N_2,\cdots N_n,B\}$ is the best path between node A and B, $P_a=\{A,M_1,M_2,\cdots M_m,B\}$ is an alternative path between node A and B. If the edge (M_i,M_{i+1}) in P_a does not appear in P_b, we consider it as an edge difference. In this paper, we mainly measure the edge difference of the multiple paths towards the same destination.

1) Path Similarity: Given the same (source, destination) pair, the path similarity is denoted

$$\text{Path Similarity}=\frac{|P_a\bigcap P_b|}{|P_b|} \tag{1}$$

where $|P|$ denote s the edge length of path P.

Path similarity provides a diversity metric of P_a and P_b between the same source-destination pair. From the definition of the path similarity, we can see that the path similarity decreases as the increasing of the disjointness of P_a and P_b. And two paths that are completely edge-disjoint have path similarity 0.

2) Path Stretch: Given the same (source, destination) pair, the path stretch is defined as the edge length ratio of P_a and P_b. The path stretch is denoted

$$\text{Path Stretch}=\frac{|P_a|}{|P_b|} \tag{2}$$

When the SDT.FI is not 0, the forwarding path is not the best path between the (source, destination) pair, and it is necessary to quantify the additional length that is incurred by the alternate paths. There are different metrics, such as, the actual end-to-end latency of the alternate paths [15] and the number of hops that the paths traverse [14], while here we count the edges that the alternative paths go through.

The path similarity and the path stretch are somewhat conflict goals in quantifying the path diversity. On one hand, the path diversity prefers small path similarity, thus the paths could be more disjoint. While on the other hand, the small path similarity implies the alternative path deflects the default shortest path substantially, which may result a large path stretch. Therefore, the well-designed forwarding principles which can select the paths with low path similarity and acceptable path stretch are very important.

E. SDPD Analysis

SDPD not only provides path diversity in the control plane but also guarantees the end host using the disjoint end-to-end paths in the forwarding plane. On the one hand, through the multipath advertisement of RR, the control plane of the interdomain routing could have multiple paths to the same destination. On the other hand, the source leverages CID and PI to hint the path selection, that is, the sources can exploit the diverse paths usage when the BGP router support the forwarding based the CID and PI. Therefore, the SDPD exploits the path diversity both the control plane and the forwarding plane.

V. SIMULATION AND EVALUATION

This section performs a set of simulations to evaluate the SDPD. We first evaluate the impact of multipath advertisement with different modes to the BGP convergence time, the control plane overhead and the path redundancy in the RIB and the FIB. Then we measure the path similarity and the path stretch of different source-destination pairs in the whole network when using SDPD forwarding.

A. Simulation Configuration

In this paper, we use the SimBGP [26], a BGP simulator written in Python, to simulate the multipath advertisement of BGP RR and measure SDPD. SimBGP is well suited for dynamic BGP simulations, as it takes the propagation and processing delays of the messages into consideration. In addition, it is an event-driven simulator that relies on an ordered queue to successively process simulation events. The original SimBGP supports the classical BGP. We extended it to support the multipath advertisement of the RRs, the receipt of multiple paths for the same prefix and installing multiple paths to the same destination in the FIB.

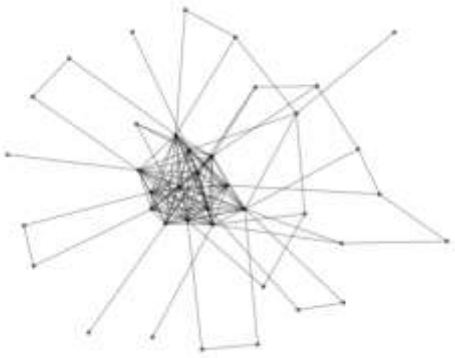


Figure 6. AS-level simulation topology

Following the [19], we get an Internet-like synthetic topology to provide an indicative evaluation of the SDPD. At the AS-level, the topology includes simple business relationships between ASes. In the AS, we choose a cluster size of 10 routers as in [19]. Two routers in each cluster are chosen as the RR and the backup RR. The other routers in the cluster connect with both the RR and backup RR. All the RRs are connected in a full-mesh way in the AS. To put more focus on the impact of multipath advertisement to the Tier-1 AS, the topology includes only a few Tier-2 ASes and stub ASes using to trigger the routing update event. In our simulation topology, we set that the Tier-1 ASes include 100-130 routers, the Tier-2 ASes include 30-50 routers, and the stub ASes include 10-20 routers. The Fig. 6 shows the AS-level simulation topology.

In the simulations, each router has a random processing delay with uniform distribution between 1 and 10 milliseconds. The bandwidth of each link is set to 100MB, and a queuing delay is uniformly distributed between 10 and 100 milliseconds. In addition, the Minimum Route Advertisement Interval (MRAI) timer for the iBGP sessions is set to 15 seconds and for eBGP sessions 30 seconds.

B. Control Plane Overhead of Multipath Advertisement

In this section, we simulate to have an Update advertising in a Tier-1 AS and measure the Update messages overhead and control plane convergence time. In order to compare with the standard BGP intuitively, we compute the ratio between the values of each advertisement mode and the standard BGP. Thus, the ratio value for the standard BGP is always 1. We take 10 Tier-1 ASes in the topology to measure and compare the average BGP Update message overhead and convergence time in this simulation.

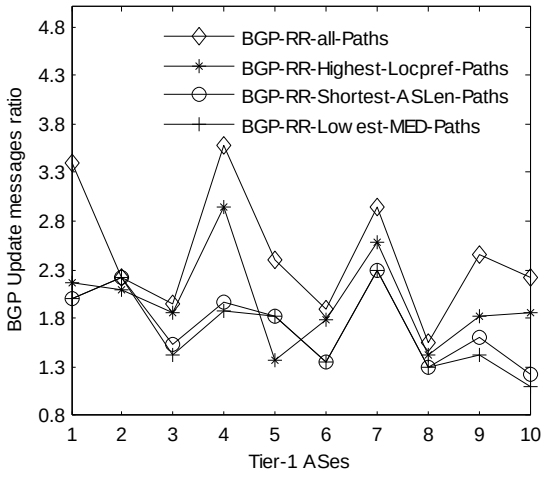


Figure 7. BGP Update messages ratio in the Tier-1 ASes

Since the RRs disseminate the redundant paths towards the same prefix to their clients and non-client peers, the proposed four advertisement modes introduce more Update messages overhead intuitionally. Fig. 7 shows the ratio of the BGP Update messages in the selected Tier-1 ASes. From the Fig. 7, we can see that the BGP-RR-All-Paths mode produces the most Update messages. As the path selection of the other three modes is progressively strict, the advertised backup paths keep decreasing. Though the 10 Tier-1 ASes chosen have different internal topologies, the trend that the Update message ratio decreases as the progressively strict of the path selection modes is the same. In the simulation, we observe that, the BGP-RR-Shortest-ASLen-Paths and BGP-RR-Lowest-MED-Paths have approximately the same ratio. And we

consider that there are little paths with different MEDs but equivalent AS length.

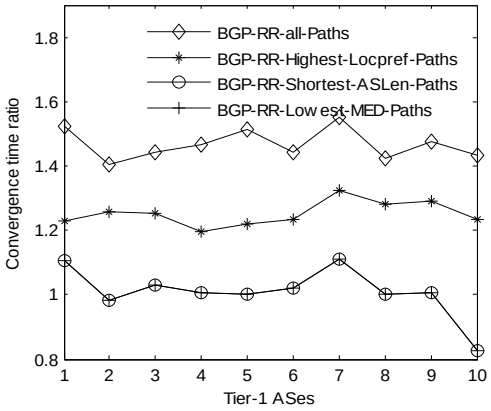


Figure 8. BGP control plane convergence time ratio in the Tier-1 ASes

Once there is no Update message about the advertising prefix in an AS, we start to compute the convergence time in this AS. The Fig. 8 demonstrates the control plane convergence time ratio. The modes of BGP-RR-All-Paths and BGP-RR-Highest-Locpref-Paths have larger convergence time ratio. While the convergence time of the other two modes is very close to the standard BGP, though the Update message overhead of this two modes is higher comparing to the standard BGP. Besides, the BGP-RR-Shortest-ASLen-Paths and BGP-RR-Lowest-MED-Paths have an overlapped convergence time ratio, though there is a little disparity in the Update messages ratio between the two modes. The Fig. 8 shows that filtering the advertised paths carefully do have effect to reduce the control plane convergence time. Besides, when backup paths in the FIB are available, the BGP forwarding plane convergence time could be cut down to nearly 0, as the data forwarding could continue by using an alternative path and it is not necessary to wait the control plane convergence.

C. Path Redundancy in RIB

We evaluate the path redundancy caused by the multipath advertisement of RRs in this section. We take 10 Tier-1 ASes and 10 Stub ASes in the synthetic topology, and calculate the average number of the routing entries towards the advertised prefix in each BGP router.

Fig. 9 demonstrates the path redundancy of RIBs in the routers of the Tier-1 ASes. The results show that the BGP-RR-All-Paths mode produces the most path redundancy, the average number of the paths in the RIB is nearly 12 times of the standard BGP. Too much path redundancy is not the goal we pursue, as the larger the number of the paths in the RIB is, the more memory is needed. Here, we seek to exploit the path redundancy with the most diversity. The other three advertisement modes also improve the path redundancy, though not so good as the BGP-RR-All-Paths. In the Fig. 10 we can observe the average number of the paths in the RIBs in the routers of the Stub ASes. The path redundancy in the Stub ASes is relatively scarce comparing to that in the Tier-1 ASes.

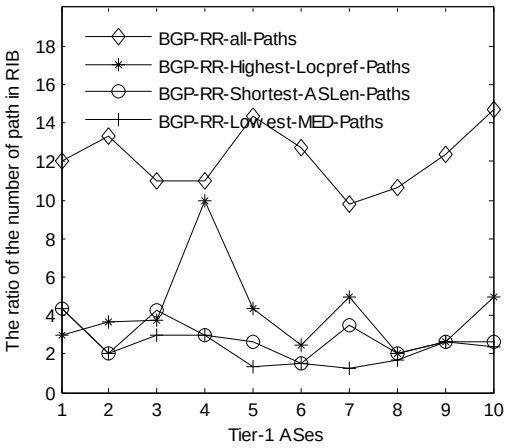


Figure 9. Path redundancy in RIB in the Tier-1 ASes

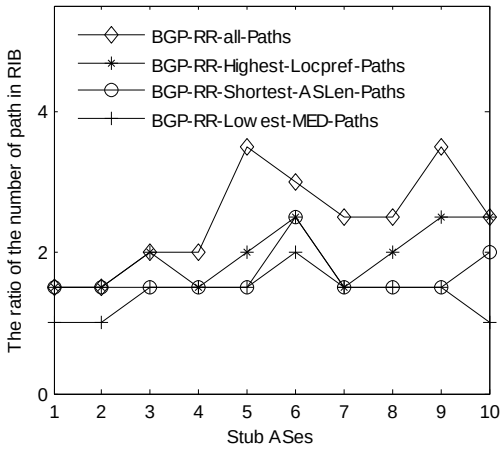


Figure 10. Path redundancy in RIB in the Stub ASes

Roughly, the increase in terms of path redundancy is proportional to the number of paths advertised. In additional, the number of available paths to the same prefix also depends on the level of the AS. Generally, the large and highly connected ASes have more path redundancy than the ASes with a few peering/provider links. In our observation, the BGP-RR-Lowest-MED-Paths mode introduces about average 2-3 times of routing entries in RIB comparing to the standard BGP, in both the Tier-1 ASes and the Stub ASes. We consider that the BGP-RR-Lowest-MED-Paths mode can provide sufficient path redundancy and the additional memory requirement is acceptable. Such a result may encourage the operators to configure the RR with the BGP-RR-Lowest-MED-Paths as the default multipath advertisement mode.

D. Path Redundancy in FIB

The number of the paths in the RIB has a directly impact on the path diversity in the FIB, as the BGP path decision process selects the best paths from the paths in the RIB. In this section, we measure the average number of paths in the FIB using the same Tier-1 ASes and Stub ASes above. Table II and Table III separately show the average number of paths in the FIB.

TABLE II. AVERAGE PATH NUMBER OF THE FIB IN TIER-1 ASES

Modes \ AS	1	2	3	4	5	6	7	8	9	10
Standard BGP	1	1	1	1	1	1	1	1	1	1
All	4	4	4	4	4	4	4	4	4	4
Highest-Locpref	3	4	4	2	3	4	3	4	4	4
Shortest-ASlen	3	4	3	4	4	4	4	3	4	4
Lowest-MED	3	4	3	3	3	3	4	4	4	4

TABLE III. AVERAGE PATH NUMBER OF THE FIB IN STUB ASES

Modes \ AS	1	2	3	4	5	6	7	8	9	10
Standard BGP	1	1	1	1	1	1	1	1	1	1
All	2	2	2	2	4	4	2	3	4	3
Highest-Locpref	2	2	2	2	4	4	2	2	4	3
Shortest-ASlen	2	2	2	2	2	4	2	3	2	3
Lowest-MED	2	2	2	2	2	3	2	3	2	2

From the tables we can observe that the Tier-1 ASes have more path diversity in the FIB than the Stub ASes. Nevertheless, the Stub ASes still have average 2 paths in the FIB at least, which could guarantee the fast convergence of the forwarding plane. Besides, since the maximum path number that is allowed to install in the FIB is 4, many ASes reach that limit value, which implies more candidate paths existing.

E. Path Similarity and Stretch in SDPD

In this section, we evaluate the path similarity and path stretch of SDPD. Each end host in the synthetic topology starts a traceroute to the new advertised prefix with different PIs. Thus, there are totally 2456 source-destination pairs and 2456*(maximum PI) traceroutes in each simulation. The BGP-RR-Lowest-MED-Paths mode is utilized in RRs to collect the paths at the control plane. We compare each alternative path with the best path between the same source and destination and calculate the path similarity and path stretch. We set diverse maximum PIs in the simulations and set the PI from 1 to the maximum PI in each traceroute.

Fig. 11 shows the path similarity with different maximum FIs. From the Fig. 11 we can see that, approximately 70% of the paths are totally edge disjoint. There are two reasons for the low path similarity: firstly, the control plane has the path redundancy, which provides the alternative choice for the packet forwarding; and secondly the FI indicates the routers to forward the packets along the diverse path at the best effort. As the increasing of the used maximum FI, the fraction of the total edge-disjoint paths is cut down.

Fig. 12 demonstrates the path stretch with different maximum FIs. As the SDPD forwarding algorithm prefers the best path when forwarding packets, thus even deflected from the best path, the packets are still sent along the best paths in alternative BGP routing trees. Therefore, though the packets may be deviated from the best path repeatedly, the path stretch is still low and the length of most paths is very close to the best path. In the Fig. 12, 99% of the paths have a path stretch 1. Furthermore, the maximum path stretch in our simulation is only 1.6.

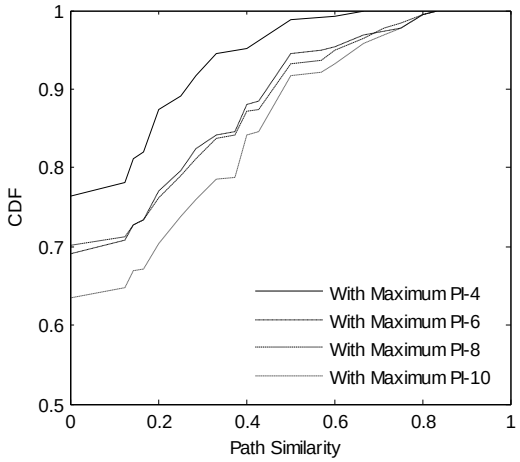


Figure 11. Path similarity in SDPD with different maximum PIs

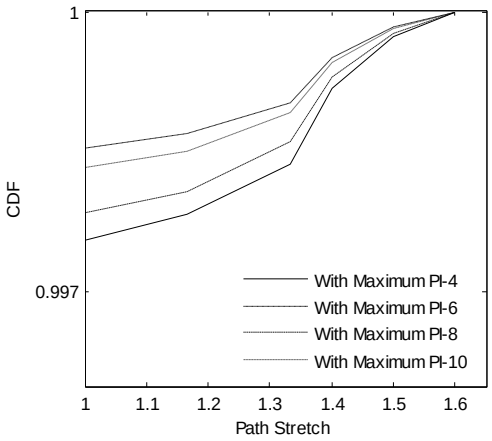


Figure 12. Path stretch in SDPD with different maximum PIs

VI. DISCUSSIONS

This section investigates the challenges to deploy the SDPD in practice and discusses the open issues on the implementation.

Changes to end systems. To support the source-directed path diversity, the end systems are required to have the ability to generate and process the SDT option. Though the SDPD provides multiple choices for the forwarding path, the end systems still need to be compatible backward. If the end systems just want the packets to be forwarded along the best path, they do not insert the SDT option to the packet header. The SDT option also could be generated on the gateways of the edge networks, such as the Ingress Tunnel Routers of the LISP [27].

Changes to BGP routers. The multipath advertisement requires changes to the control plane of the BGP routers in order to support receiving multiple routings towards the same destination. In addition, since the RR is considered as a routing relay between the iBGP peers, it is required to have the ability to advertise multiple routings towards the same destination. To reduce the Update message overhead, the RR has to implement methods to filter the paths for advertising, for example, the four modes proposed in section 3.3. Moreover, the

routers need to improve the forwarding plane to recognize the CIDs and forward packets depending on the PIs. Note that the changes in the forwarding plane do not introduce implementing burden to the route system, as the design is similar to the hash-based multipath routing[28] which has deployed in the Internet[29].

Routing scalability. As the BGP routing table increases rapidly in recent years, the BGP routing scalability is a major concern of the Internet routing system. The multipath advertisement disseminates multiple paths with the same destination prefix, which does not produce new prefix. Therefore, the total number of the reachable prefix in the multipath BGP is the same with the standard BGP. The multipath advertisement does not bring new routing scalability problem.

Memory consumption. The RIB of BGP routers will contain more paths and thus consume more memory because of the multipath advertisement. It is important to note that the actual memory increase due to the reception of multiple paths towards the same IP prefix is rendered sub-linear with the number of paths thanks to attribute-sharing [30]. Thus, to a certain extent, data structure optimization counteracts the increment of the memory consumption caused by the multiple path advertisement. Besides, the RIB is part of the control plane, the speed of memory access to the RIB does not need to be as high as the FIB, therefore the RIB memory can be extended easily by adding RAM to the routers. To reduce the memory consumption of the FIB, we set that the maximum number of the paths allowed to install in the FIB is 4. The operator can adjust the maximum value based on each router.

CID space. In this paper we set the length of CID to be 16 bits in the IP option. It is noted that, the CID space is about 10^5 , which is not enough to identify all flows in the Internet, but the CIDs are mainly used to identify the flows in a BGP router, and 10^5 is enough to identify the flows in most of the routers[28]. Even if there are CID conflicts in BGP router, the router still can forward the packets over the right paths based on the destination prefix. The SDPD just aims to exploit the path diversity at the best effort, the CID conflicts could be tolerated.

Transport layer performance. Different SDT.FIs cause the packets transmitting along edge-disjoint paths. Provided a path has good quality, such as low delay or high available bandwidth, the end systems could guide the application data to that path by specifying the CID and FI. Utilizing the SDPD in conjunction with the end-to-end multipath transfer, such as CMP-SCTP[6] and MPTCP[7], in the end systems with multiple network access interfaces, it is promising to achieve better throughput performance as well as reliability.

VII. CONCLUSIONS

This paper has presented the design of SDPD to exploit the path diversity in the interdomain routing. The main contributions are as below: firstly, we have proposed the multipath advertisement of RR in BGP to exploit the path diversity in the control plane. Secondly, a source-directed multipath forwarding scheme in SDPD, which leverages the SDT to allow the end systems to find alternate paths, has been proposed. The end systems tag packets with CIDs and PIs, and the BGP routers use the CIDs and PIs to select alternate paths. Lastly, we performed simulations over an Internet-like topology to evaluate the proposed SDPD. The simulation results have demonstrated that the multipath advertisement of RR increases the path redundancy at the control plane significantly. Furthermore, the results have also shown that even with a random PI in the SDT, the source could exploit alternative paths with low similarity and small stretch. Since the source have the ability to impact the forwarding operation of the BGP routers, the SDPD is promising to be applied with end-to-end multiple paths transfer and source-based traffic engineering.

As this paper mainly focuses on the interdomain path diversity exploited by the sources, the efficiency of the forwarding plane needs to be further investigated, and we plan to systematically study on the CID lookup and fast forwarding of the packets of SDPD in our next step work.

ACKNOWLEDGMENT

This work was supported by the National Key Technology R&D Program of China, under grant No.2012BAH06B01.

REFERENCES

[1] D. Wischik, M. Handley and M. B. Braun, “The resource pooling principle”, *ACM CCR*, Vol. 38, No. 5, 2008, pp. 47–52.

[2] L. Muscariello, D. Perino and D. Rossi, “Do next generation networks need path diversity”, *proc. IEEE ICC*, Dresden, Germany, 2009, pp. 1-6.

[3] S. Fashandi, S. O. Gharan and A. K. Khandani, “Path diversity over packet switched networks: performance analysis and rate allocation”, *IEEE/ACM Transactions on Networking*, Vol. 18, No. 5, 2010, pp. 1373-1386.

[4] B. Albrightson, J. J. Garcia-Luna-Aceves and J. Boyle, “EIGRP-A fast routing protocol based on distance vectors”, *proc. Networld Interop*, Las Vegas, 1994, pp. 136-147.

[5] J. Moy, OSPF Version 2, 1998, RFC2328.

[6] J. R. Iyengar, P. D. Amer and R. Stewart, “Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths”, *IEEE/ACM Transactions on Networking*, Vol. 14, No. 5, 2006, pp. 951-964.

[7] A. Ford, C. Raiciu, M. Handley, S. Barre and J. Iyengar, Architectural guidelines for multipath TCP development, 2011, RFC6182.

[8] J. X. Liao, J. Y. Wang and X. M. Zhu, “A multi-path mechanism for reliable VoIP transmission over wireless networks”, *Computer Networks*, Vol. 52, No. 13, 2008, pp. 2450-2460.

[9] R. Teixeira, K. Marzullo, S. Savage and G. M. Voelker, “Characterizing and measuring path diversity of Internet topologies”, *proc. ACM SIGMETRICS*, San Diego, USA, 2003, pp. 304-305.

[10] S. Savage, A. Collins, E. Hoffman, J. Snell and T. Anderson, “The end-to-end effects of Internet path selection”, *proc. ACM SIGCOMM*, Massachusetts, USA, 1999, pp. 289-299.

[11] J. Han, D. Watson and F. Jahanian, “An experimental study of Internet path diversity”, *IEEE Transactions on*

Dependable and Secure Computing, Vol. 3, No. 4, 2006, pp. 273-288.
[12] T. Bates, R. Chandra and E. Chen, BGP route reflection - an alternative to full mesh iBGP, 2000, RFC 2796.
[13] K. Leung, V. O. K. Li and D. Yang, "An overview of packet reordering in transmission control protocol (TCP): problems, solutions, and challenges", *IEEE Transactions on Parallel and Distributed System*, Vol. 18, No. 4, 2007, pp. 522-535.
[14] X. W. Yang and D. Wetherall, "Source selectable path diversity via routing deflections", *proc. ACM SIGCOMM*, Pisa, Italy, 2006, pp. 159-170.
[15] M. Motiwala, M. Elmore, N. Feamster and S. Vempala, "Path splicing", *proc. ACM SIGCOMM*, Seattle, USA, 2008, pp. 27-38.
[16] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen and P. Pillay-Esnaul, Multi-Topology (MT) Routing in OSPF, 2007, RFC4915.
[17] W. Xu and J. Rexford, "MIRO: Multi-path interdomain routing", *proc. ACM SIGCOMM*, Pisa, Italy, 2006, pp. 171-182.
[18] F. Wang and L. X. Gao, "Path diversity aware interdomain routing", *proc. IEEE INFOCOM*, Rio de Janeiro, 2009, pp. 307-315.
[19] V. V. Schrieck, P. Francois and O. Bonaventure, "BGP Add-Paths: the scaling/performance tradeoffs", *IEEE Journal on Selected Areas in Communications*, Vol. 28, No. 8, 2010, pp. 1299 – 1307.
[20] X. W. Yang, D. Clark and A. W. Berger, "NIRA: a new inter-domain routing architecture", *IEEE/ACM Transactions on Networking*, Vol. 15, No. 4, 2007, pp. 775–788.
[21] I. Ganichev, B. Dai, P. Brighten Godfrey and S. Shenker, "YAMR: Yet another multipath routing protocol", *ACM CCR*, Vol. 40, No. 5, 2010, pp. 14-19.
[22] P. B. Godfrey, I. Ganichev, S. Shenker and I. Stoica, "Pathlet routing", *proc. ACM SIGCOMM*, Barcelona, Spain, 2009, pp. 111-122.
[23] G. T. K. Nguyen, R. Agarwal, J. Liu, M. Caesar, P. B. Godfrey and S. Shenker, "Slick packets", *ACM SIGMETRICS Performance Evaluation Review*, Vol. 39, No. 1, 2011, pp. 205-216.
[24] Y. Rekhter, T. Li, and S. Hares, A border gateway protocol 4 (BGP-4), 2006, RFC 4271.
[25] BGP Multipath. Cisco online documention. Avaiable: http://www. cisco. com/en/US/tech/tk365/ technologies_tech_note09186a0080094431. shtml#bgpmpath
[26] J. Qiu. SimBGP: Python event-driven BGP simulator. Available: http://www. bgpvista. com/simbgp. php
[27] D. Farinacci, V. Fuller, D. Meyer, D. Lewis, Locator/ID Separation Protocol (LISP), 2011, IETF draft.
[28] Z. Cao, Z. Wang and E. Zegura, "Performance of hashing-based schemes for internet load balancing", *proc. IEEE INFOCOM*, 2000, pp. 332-341.
[29] Juniper. Configuring per-flow load balancing based on hash Values. https://www. juniper. net/techpubs/en_US/junos11. 1/topics/usage-guidelines/policy-configuring-per-flow-load-balancing-based-on-hash-values. html
[30] R. Zhang and M. Bartell, "BGP design and implementation: practical guidelines for designing and deploying a scalable BGP routing architecture", 2003, CISCO Press.
[31] J. M. Camacho, A. Garcia-Martinez, M. Bagnulo and F. Valera, "BGP-XM: BGP eXtended Multipath for transit Autonomous Systems", Computer Networks, Vol. 57, No. 4, 2013, pp. 954-975.
[32] M. Chiesa, G. Lospoto, M. Rimondini, G. D. Battista, "Intra-domain routing with pathlets", Computer Communications, Vol. 46, No. 6, 2014, pp. 76-86.
[33] V. Kotronis, X. Dimitropoulos and B. Ager, "Outsourcing the Routing Control Logic: Better Internet Routing Based on SDN Principles", *Proc Hotnets '12*, Seattle, USA, 2012, pp. 55-60.

Miao Xue is a researcher at Network Technology Research Institute of China Unicom. He received B.S. and Ph.D. in communication engineering from Beijing Jiaotong University in 2007 and 2012, respectively. His research interests include routing architecture, multipath routing, and future network architecture theory.

Gang Fu is a senior researcher at Network Technology Research Institute of China Unicom. He received His M.S. in Xidian University in 2004. His research interests include Mobile Core Network, routing theory and future network architecture theory.

Ruitao Ma is a senior researcher at Network Technology Research Institute of China Unicom. He received His M.S. in Beijing University of Posts and Telecommunications in 2006. His research interests include Mobile Core Network, IMS and future network architecture theory.

Longshe Huo is a researcher at Network Technology Research Institute of China Unicom. He received the B.S. and M.S. degrees in computer science from Xi'an Jiaotong University, Xi'an, China, in 1990 and 1993, respectively, and received the Ph.D. degree in computer science from the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China, in 2006. From 2006 to 2008, he worked in Peking University as a post-doctor researcher. His main research interests include broadband and mobile networks, multimedia communications, etc.

Markov Chain Based Trust Management Scheme for Wireless Sensor Networks

Xiaolong Li and Donglei Feng
Guilin University of Electronic Technology, School of Computer Science and Engineering, Guilin, China
Email: xlli@guet.edu.cn, fengdonglei1333@foxmail.com

***Abstract*—As the effective supplement to traditional cryptography security, trust management plays a key role for detecting malicious behaviors in wireless sensor networks. In this paper, we consider a sensor network wherein nodes have fixed number of states and probabilities of state transitions can be specified. We introduce Markov chain model and Fokker-Planck equation for evaluating the short-term trust value of nodes. In order to avoid the drawbacks of existing long-term trust evaluation models, we propose a new evaluation model with adaptive forgetting factors, where step functions are introduced to calculate the current forgetting factor. Simulation results show that the proposed trust management scheme can effectively detect malicious nodes in wireless sensor networks, and significantly improve the packet delivery ratio compared to the counterparts.**

***Index Terms*—Markov Chain; Trust Management; Sensor Networks; Forgetting Factor**

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of many resource-constrained sensor nodes. Due to low cost, sensor nodes have poor reliability and are prone to node compromise and node failures. Traditional security mechanisms, such as authentication and cryptography, can not secure the network against internal attacks launched by captured nodes. E.g, an adversary can place several intruder nodes or compromise sensor nodes in the network to disrupt the network's normal operation by sending false sensing data or falsifying delivered results. The false messages can mislead users to make a wrong decision. If malicious nodes injecting these false data into the network have been authenticated as legal nodes, conventional security mechanisms have no ability to differentiate those from legal nodes. Trust management, which has been proved as an effective approach to assessing trustworthiness of sensor nodes [1], becomes essential to the robust operation of sensor networks. Trust management techniques have been widely used in various fields, from Internet, P2P networks to ad−hoc networks, such as eBay [2], RFSN [3], TEFDN [4], etc.

In the past decade, a large number of trust management schemes in WSNs have been proposed to identify malicious nodes. Although trust management of sensor networks has made a lot of progress, existing Trust Management Systems (TMSs) are difficult to distinguishing between normal and malicious nodes effectively because of sensor nodes being cheap, unreliable, and easily impacted by environmental noise. When sensor nodes were deployed in complicated environment, normal nodes were usually judged to be malicious nodes since packet loss and packet forwarding failure often occurred in the complicated environments. If too many normal nodes were judged to be malicious nodes, it will eventually lead to network paralysis.

How to improve the success ratio of distinguishing malicious nodes in complex environments, has become an urgent problem in the trust management field of WSNs. This paper considers that trust value should be an estimate for the current state of nodes, and proposes a TMS scheme under the motivation of reducing the impact of complicated environments on node status evaluation.

The rest of this paper is organized as follows. Some related works are reviewed in Section II. The proposed markov chain based trust model for short-term trust value estimation of nodes is presented in Section III. Section IV describes a model to compute the long-term trust value. Section V compares the proposed TMS with counterparts, and shows simulation results. The paper ends with conclusion in section VI.

II. RELATED WORK

In the WSN environment, due to the feature that sensor nodes are very vulnerable to security threats or attacks, and are prone to be captured by attackers, many researchers began to pay their attention to TM (Trust Management) model [3]–[13]. Using Bayesian model, [3] proposed a reputation-based framework for sensor networks (RFSN) where each sensor node maintains reputation metrics which reflect past behaviors of other nodes and are used as an inherent aspect in predicting their future behavior, and put forward a general trust management system. In [4], a framework to quantitatively measure trust and model trust propagation against malicious attacks was proposed. In [5], a reputation-based framework was proposed. Ref. [9] also presented a trust model to evaluate the trustworthiness of nodes. In order to reduce the high computation, communication and storage overheads caused by the trust management, Shaikh [6] proposed a lightweight TMS based on grouping. Ho [7] proposed a new TMS based on regional block. Ref. [8] presented a systematic analysis of the relationship between trust metrics and trust-based routing protocols. The authors in [10] proposed a distributed

doi:10.4304/jnw.9.12.3263-3267

trust-based framework and a mechanism for the election of trustworthy cluster headers. Each node stored a trust table for all surrounding nodes and these values were reported to the cluster header. Tanachaiwiwat [11] proposed a method to distinguish untrusted locations and area based on TM, which guarded the security routing between base station and nodes. Krasniewski [12] proposed a protocol called TIBFIT to use the trust management on security data fusion. In [13], by utilizing a highly scalable hierarchical trust management protocol, the authors proposed a trust-based intrusion detection (TBID) scheme for clustered wireless sensor networks. TBID presented a trust metric considering both quality of service (QoS) trust and social trust for detecting malicious nodes. Each cluster header applied trust-based intrusion detection to assess the trustworthiness and maliciousness of sensor nodes in its cluster. Cluster headers themselves are evaluated by the base station.

III. Markov Chain Based Trust Model

In this section, we will describe the markov chain based trust model, which can forecast the short-term trust value of nodes through current behaviors. The predicted trust value only can reflect the trust level of the short time period. We use this trust model to determine nodes' current state, and to identify whether the node is malicious.

We suppose that the nodes state transition process in our model follows a Markov chain. Thus, the trust value estimation of nodes can be modeled mathematically as a five-tuple markov model

$$\Omega = (R, V, Q, \Lambda, \Pi)$$

Among them, $R = \{r_1, r_2, \cdots, r_N\}$ is the set of normal state; $V = \{v_1, v_2, \cdots, v_M\}$ is the set of malicious state; $Q = \{q_{ij}\}$ is a $K * K$ state transition matrix, where $K=M+N$ and q_{ij} represents the transfer rate from i to j, $i, j \in R \cup V$; $\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ is the system parameters, Where λ_i represent the index distribution parameter that node's state change between R and V. $\Pi = \{\pi_1, \pi_2, \cdots, \pi_{N+M},\}$ is the node's initial(current) trust distribution, where $\pi_i = P_0\{X(t) = r_i\}$, $1 \le i \le N$, $\pi_j = P_0\{X(t) = r_j\}$, $N+1 \le j \le N+M$ and $\sum_{i=1}^{N+M} \pi_i = 1$.

We define $X(t)$ as the state of moment t. λ_1 is the index distribution parameter from state R to state R, T_1 is the node's work time. In the same way, λ_2 is from R to V, λ_3 is from V to V, λ_4 is from V to R. T_2, T_3 and T_4 are their work time. $\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ will change along with the transform of node state.

A. Assumptions

For the sake of formulate the mathematical expressions of the markov chain based trust value, we must make some assumptions as follows:

1. In all of the $N+M$ states, transition probabilities of every node are belonging to them. Each node's state can not beyond these $N+M$ states.

2. The markov chain is time-homogeneous, ergodic, irreducible and aperiodic.

B. Formula Derivation

In order to calculate the final trust value, we should get the matrix Q at first. Firstly, take a positive number τ which is sufficiently small. Then, calculate the transition probability within the time interval $[t, t+\tau]$. The transition probability is given by

$$P_{ij}(\tau) = P\{X(t+\tau) = j \mid X(t) = i\}$$
$$= \begin{cases} P\{T_1 \le \tau\} = \int_0^\tau \lambda e^{-\lambda_1 t} dt = 1 - e^{-\lambda_1 \tau} = \lambda_1 \tau + O(\tau) \\ \text{when } i, j \in R, \text{and } i \ne j. \\ P\{T_2 \le \tau\} = \int_0^\tau \lambda e^{-\lambda_2 t} dt = 1 - e^{-\lambda_2 \tau} = \lambda_2 \tau + O(\tau) \\ \text{when } i \in R, j \in V. \\ P\{T_3 \le \tau\} = \int_0^\tau \lambda e^{-\lambda_3 t} dt = 1 - e^{-\lambda_3 \tau} = \lambda_3 \tau + O(\tau) \\ \text{when } i, j \in V, \text{and } i \ne j. \\ P\{T_4 \le \tau\} = \int_0^\tau \lambda e^{-\lambda_4 t} dt = 1 - e^{-\lambda_4 \tau} = \lambda_4 \tau + O(\tau) \\ \text{when } i \in V, j \in R. \\ 1 - (N-1)\lambda_1 \tau - M\lambda_2 \tau + O(\tau) \\ \text{when } i, j \in R, \text{and } i = j. \\ 1 - (M-1)\lambda_3 \tau - M\lambda_4 \tau + O(\tau) \\ \text{when } i, j \in V, \text{and } i = j. \end{cases} \quad (1)$$

Then, we can calculate each state transition's transfer rate q_{ij} , and obtain matrix Q in the end. The transfer rate q_{ij} is formulated by

$$q_{ij} = \lim_{\tau \to 0^+} \frac{P_{ij}(\tau) - P_{ij}(0)}{\tau} \quad (2)$$

If $i = j$, $Pij(0) = 1$, else $Pij(0) = 0$ .According to (1) and (2), we can get the $K*K$ transition matrix. The matrix is given by

$$Q = \begin{pmatrix} q_{r1r1} & \cdots & q_{r1v1} & \cdots & q_{r1vM} \\ q_{r2r1} & \cdots & q_{r2v1} & \cdots & q_{r2vM} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ q_{vM-1r1} & \cdots & q_{vM-1v1} & \cdots & q_{vM-1vM} \\ q_{vMr1} & \cdots & q_{vMv1} & \cdots & q_{vMvM} \end{pmatrix} \quad (3)$$

Furthermore, we can use Fokker-Planck equation and the current probability distribution to forecast the absolute probability of node state at the next phase. The solve process is as follows.

$$\begin{cases} (P'_{r1}(t) \cdots P'_{vM}(t)) = (P_{r1}(t) \cdots P_{vM}(t)) \cdot Q \\ (P_{r1}(0) \cdots P_{vM}(0)) = \Pi \end{cases} \quad (4)$$

where $\pi_i = 1$, and $1 \le i \le N+M$. From the above requirements, we can derive the absolute probability of every state. Moreover, the node's trust value also can be worked out. The result is as follow.

$$T = \sum_{i=1}^{N} P_{ri}(t) = \frac{N\lambda_4}{M\lambda_2 + N\lambda_4}[1 - e^{-(M\lambda_2 + N\lambda_4)t}] \quad (5)$$

where T is the prediction of trust value, and it only means the possible trust level of next state. In this paper, we define T as the short-term trust value, and node's real trust level as the long-term trust value. In next section, we will talk about the long-term trust determination approach.

IV. Node Trust Determination Approach

In this section, we will describe the long-term trust determination approach for wireless sensor networks. The new approach can identify malicious and normal nodes more correctly, and improve the security of WSNs.

A. Node Status Evaluation

In different network environments, the probability that malicious acts occur to a node in the normal state is not a fixed value, but a fluid value. We assume a node only has two states: normal state and malicious state. Nodes in different state of different environment have distinguishing performance. In this paper, we evaluate node's real state through four elements: current state, real state, short-term trust value and long-term trust value.

For example, we forecast a normal node's short-term trust value is T_1, and a malicious behavior happened to the node in the next time slot. This paper considers that it is still a normal node, but its long-term trust value will reduce because of the bad behavior. Through this approach, we can finally ensure every node's real state and trust value.

B. Long-term Trust Value Determination

Ref. [4] put forward one method to evaluate a node long-term trust value based on adaptive memory factor. In order to derive our new model, we will introduce the formula at first. The formula is shown as follow:

$$trust\_l^{new} = \beta_1 trust\_l^{t} + \beta_2 trust\_s \quad (6)$$

where $trust\_l^t$ is the long-term trust value of time t, $trust\_s$ is the short-term trust value from time t to t+1, and $trust\_l^{new}$ is the long-term trust value of time t+1. β_1 and β_2 are the unfixed memory factors. We can adjust the two factors dynamically.

Form the formula (6), we can easily find out the disadvantage of this approach. If a nodes long-term trust value is low, the long-term trust value that node behaves badly in the current time is better than node behaves well. It can not identify malicious node accurately.

Because of this reason, we propose a new method to identify malicious nodes and evaluate long-term trust value. The new formula is given by

$$trust\_l^{new} = \begin{cases} \beta_1 trust\_l^n + \beta_2 trust\_f, \text{when } i, j \in R \\ \text{and } trust\_l^n \geq trust\_f \\ \beta_2 trust\_l^n + \beta_1 trust\_f, \text{when } i, j \in R \\ \text{and } trust\_l^n < trust\_f \\ \beta_1 trust\_l^n + \beta_2 trust\_f, \text{when } i \in R \\ , j \in V \text{ and } trust\_l^n \geq trust\_f \\ \beta_2 trust\_l^n + \beta_1 trust\_f, \text{when } i \in R \\ , j \in V \text{ and } trust\_l^n < trust\_f \\ \beta_1 trust\_l^n + \beta_2 trust\_f, \text{when } i \in V \\ , j \in R \text{ and } trust\_l^n \geq trust\_f \\ \beta_2 trust\_l^n + \beta_1 trust\_f, \text{when } i \in V \\ , j \in R \text{ and } trust\_l^n < trust\_f \end{cases} \quad (7)$$

In the formula, $trust\_l^n$ is the long-term trust value of current time, $trust\_f$ is the prediction of trust value from current time to next time slot, i is node's current state and j is its next state. From above equation, we can get the new long-term trust value. For example, at a given time t, if the current state of the node belongs to the normal state set and the next state of the node is judged as being in malicious state, then we have $i \in R$, $j \in V$. For the purpose of explanation, we assume $trust\_l^n$=0.85, $trust\_f$ =0.45, and $\beta_1 = 0.35, \beta_2 = 0.65$. According to formula (7), we can get that $trust\_l^{new} = \beta_1 trust\_l^n + \beta_2 trust\_f$ =0.35*0.85 +0.65*0.45=0.59.

Through analysis, we can obtain that the new method not only can overcome the above shortcoming effectively but also can overcome the environmental influence.

Algorithm 1 MCTM algorithm

Initialize the trust value of every node, and their currently state.
Set the initialize parameters $\lambda_1, \lambda_2, \lambda_3, \lambda_4$.
Repeat {Main Loop}
Figure out every nodes state transfer rate q_{ij} with formula (1) and (2)
Obtain the short-term trust value through formula (3), (4) and (5).
Get the value of $trust\_f$ and $trust\_l^n$
After a period of time, each node monitors other nodes within its coverage area and get the current state of every node.
Figure out the new long-term trust value $trust\_l^{new}$ with formula (7).
If environment change, reset the parameters $\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$
10: $trust\_l^n = trust\_l^{new}$
11: Return $trust\_l^n$
12: Begin a new loop.

V. Performance Evaluation

To evaluate the performance of markov chain based trust model, we realized MCTM (Markov Chain based Trust Model in Wireless Sensor Networks) with MATLAB. We compare our model MCTM with RFSN [3] and TBID [13] in the experiment.

In order to display the performance of MCTM, we run the network in different kinds of condition. All of the conditions are deployed in a complicated environment. In the process of simulation, we compare normal nodes trust value and success transaction ratio in different situations.

In this way, can we get the real performance of MCTM, TBID and RFSN.

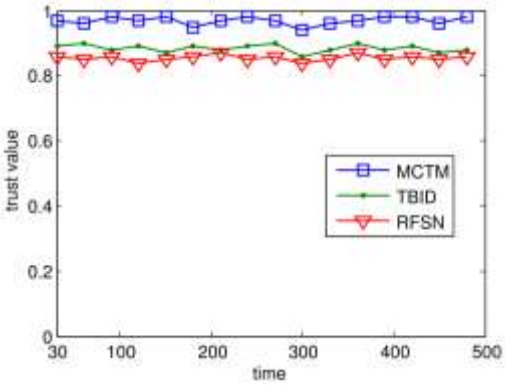


Figure 1. Time vs. trust value of normal node

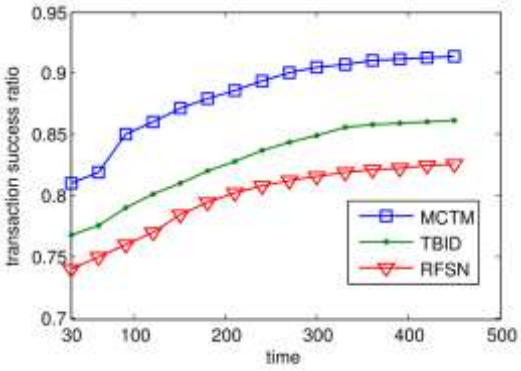


Figure 2. Time vs. the transaction success ratio suffering bad mouthing attack

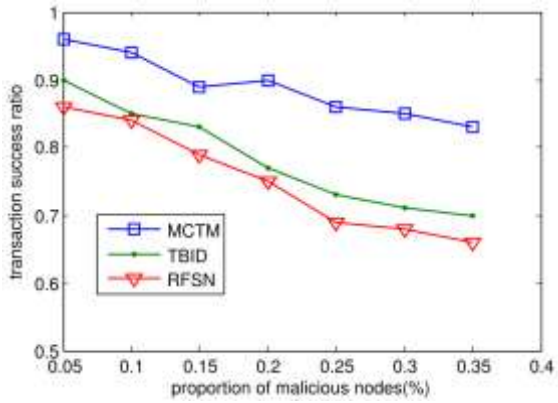


Figure 3. Proportion of malicious nodes vs. transaction success ratio

Fig. 1 is the simulation results of trust value of normal node as time grows. In order to improve the new model MCTM is feasible and effective, we compare it with the classical model RFSN and a recent model TBID. We can observe that in TBID and RFSN, the trust value maintains fluctuation near 0.85, but our MCTM maintains more than 0.95. This means MCTM can identify normal node more accurately. This is because the new model use markov chain to forecast the trust and to correct the trust value based on many elements.

Fig. 2 shows the ratio of successful dealing when the network suffering bad mouthing attack. The bad mouthing attacks reduce the good node's trust value, or increase the credibility of malicious nodes by providing false information. As the time changes, the success deals also change. Compared with TBID and RFSN, MCTM has a better transaction success ratio when suffering attack. In MCTM, the new trust value can track node's behaviors and current state carefully, and give punishment for the phenomenon of increasing of false dealing cause by malicious nodes. Hence, the success transaction rate will increase obviously with dealing going on. From fig. 2, we can observe the success ratio of MCTM can easily reach 90%. Although the success rate will increase along with time change, TBID and RFSN can not exceed 86%. This means our model is more stable than the existing model.

Fig. 3 presents the relationship between success process rate and the number of malicious nodes. We analyze the success rate when the proportion of malicious nodes increases from 5% to 35%. From the figure, we can observe that MCTM performs better than TBID and RFSN in terms of success process rate. It is because the markov chain base trust model can distinguish malicious more correctly.

VI. Conclusions

In this paper, we proposed a new trust management model based on Markov chain to evaluate node state, which reduced the impact of environments on evaluating node state. Simulation results show that MCTM can achieve higher network security and is more effective to identify malicious and malfunctioning nodes in complex environments. In this paper, we built the scheme upon the strong assumption that the number of node state is fixed. In the following days, we will further proceed with trust management studies for the cases where sensor nodes may have changeable states.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61462021, 61162008), Opening Project of Guangxi Key Laboratory of Trusted Software (Grant No. kx201305).

References

[1] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management." *IEEE Security and Privacy*, Oakland, CA, May. 1996.

[2] P. Resnick, R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system," *Emerald Group*, vol. 11, no. 1, pp. 127-157, Apr. 2002.

[3] S. Ganeriwal, M. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM S Network*, New York, USA, 2004.

[4] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks," *IEEE Infocom*, vol. 6, pp. 1-13, 2006.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM T Network*, vol. 4, no. 3, pp. 1-37, 2008.

[6] R. A. Shaikh, H. Jameel, and B. J. Auriol, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE T Systems*, vol. 20, no. 11, pp. 1698-1712, 2009.
[7] J. W. Ho, "Zone-based trust management in sensor networks," *IEEE PerCom, Galveston, TX*, March. 2009.
[8] X. Y. Zhu, Y. Song, and Y. G. Fang, "A formal study of trust-based routingin wireless Ad Hoc networks," *IEEE INFOCOM, San Diego, CA*, March. 2010.
[9] G. X. Zhao, W. S. Shi, and J. L. Deng, "Sensortrust: a resilient trust model for WSNs," *ACM CONF E SYSTEMS, New York*, USA, 2009.
[10] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," *IEEE DSSNS. Columbia*, MD, april. 2006.
[11] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks," *ACM SenSys, New York, USA*, 2003.
[12] M. D. Krasniewski, P. Varadharajan, B. Rabeler, S. Bagchi, and Y. C. Hu, "TIBFIT: Trust index based fault tolerance for ability data faults in sensor," *IEEE DSN, Yokohama*, Japan, July. 2005.
[13] F. Bao, R. Chen, and M. J. Chang, "Trust-based intrusion detection in wireless sensor networks," *IEEE COMMUN, Kyoto, Japan*, June. 2011.

Fast Finite-Time Consensus Tracking of Second-Order Multi-Agent Systems with a Virtual Leader

Qiuyun Xiao, Zhihai Wu*, and Li Peng
Key Laboratory for Advanced Process Control of Light Industry of the Ministry of Education, School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, China
*Corresponding author. Email: xiaoqy1007@163.com; wuzhihai@jiangnan.edu.cn; pengli@jiangnan.edu.cn

***Abstract*—This paper proposes a new finite-time consensus tracking protocol for reaching the fast finite-time consensus tracking. The Lyapunov function method, algebra graph theory, and homogeneity with dilation are employed to obtain the convergence criteria. Numerical simulations show that compared with the traditional finite-time consensus tracking protocols, the proposed protocol can accelerate the convergence speed of achieving the finite-time consensus tracking.**

***Index Terms*—Second-Order Multi-Agent Systems; A Virtual Leader; Fast Finite-Time Consensus Tracking; Convergence Speed**

I. INTRODUCTION

During the past decade, distributed coordinated control of multi-agent systems due to its broad applications has received considerable attention in various fields such as physics, biology, computer science and control engineering. In the distributed coordinated control of multi-agent systems, a critical problem is to find proper control protocols to enable all agents to reach an agreement on certain quantities of interest, which is usually called the consensus problem. For most of the existing consensus protocols [1-5], the final common value to be achieved is a function of initial states of all agents and is inherently a prior unknown constant. This is the so-called χ-consensus [6].

However, in many practical applications, it is required that all agents communicating with their neighbors eventually converge to a desired reference state. This is the so-called leader-follower consensus or consensus tracking.

In leader-follower multi-agent networks, the leaders are usually independent of their followers, but have influence on the followers' behaviors. Hence, by controlling only the leaders, the control objective of the networks can be realized easily. This not only simplifies the design and implementation of the controls but also saves the control energy and cost [7]. Up to now a lot of attention has been paid to consensus tracking of leader-follower multi-agent systems [8-22].

However, most of the above references are mainly about finding convergence conditions of achieving the consensus or consensus tracking rather than improving the convergence performance, one of which is the convergence speed. However, the convergence speed is really an important performance index, which affects the real-time performance. In recent years, significant attentions have been paid to how to enhance the convergence speed of multi-agent systems or networks [23-26]. Li and Fang designed the optimal weights associated with edges of undirected graph to make the states of the multi-agent systems converge to consensus with a fast speed as well as the maximum communication time-delay can be tolerated [23]. Zhou and Wang proposed the asymptotic and per-step convergence factors as measures of the convergence speed, and derived the exact value for the per-step convergence factor [24]. Wu and Fang proposed the consensus protocol with delayed-state-derivative feedback, demonstrating that choosing the proper gain of delayed-state-derivative feedback can accelerate the convergence speed [25]. Fang et al. [26] proposed the consensus protocol with weighted average prediction, and proved that choosing the proper length of weighted average prediction can enhance the convergence speed.

Although using the methods in Refs. [23-26] can accelerate the convergence speed of achieving the consensus, the achievement of consensus is asymptotical, which means that the consensus can never be reached in finite time. However, in many situations, it is often required that the consensus be reached in finite time, such as when the control accuracy is crucial. Besides faster convergence, other advantages of finite-time consensus include better disturbance rejection and robustness against uncertainties [27]. Therefore, it is necessary to investigate the finite-time consensus of multi-agent systems. Now, there are a lot of results about finite-time consensus. [28-31] In Ref. [28], Cortes considered the finite-time consensus based on the discontinuous protocol. In Ref. [29] Xiao and Wang gave two continuous consensus protocols to solve the finite-time consensus problems of first-order multi-agent systems. Sun and Guan investigated the finite-time consensus problems of leader-follower second-order multi-agent systems under fixed and switching networks [30]. In Ref. [31], Zhu and Guan investigated the finite-time consensus problems for

doi:10.4304/jnw.9.12.3268-3274

heterogeneous multi-agent systems, where the virtual leader can be a first-order or a second-order integrator agent.

Compared with the existing consensus protocols with asymptotical convergence in Refs. [23-26], the protocols in Refs. [28-31] can guarantee the finite-time consensus. However, in some practical applications such as braking systems of multiple autonomous vehicles, the faster finite-time consensus, i.e., the consensus with a shorter setting time, is needed. Therefore, it is significant to study how to accelerate the convergence speed of finite-time consensus. Therefore, the main motivation of this paper is to explore the finite-time distributed tracking control protocol based on the traditional finite-time consensus idea and to acquire a fast convergence speed. To this end, in this paper we propose a novel finite-time consensus tracking protocol to solve the fast finite-time consensus tracking problems of the second-order multi-agent systems.

An outline of the paper is as follows. Some preliminaries are provided and the problem is stated in section II. Convergence analysis of the fast finite-time consensus protocol is given in section III. In section IV numerical simulations illustrate the theoretical results, and in section V conclusions are drawn.

II. PRELIMINARIES AND PROBLEM STATEMENT

A. Algebra Graph Theory

Let $G=(V, E, A)$ be a weighted undirected graph with a set of nodes $V=\{v_1, v_2, ..., v_n\}$, a set of edges $E \subseteq V \times V$, and the weighted adjacency matrix $A=[a_{ij}]$ with nonnegative adjacency elements a_{ij}. The node indexes of G belong to a finite index set $I=\{1, 2, ..., n\}$. An edge of G is denoted by $e_{ij}=(v_i, v_j)$. The adjacency elements associated with the edges are positive, i.e., $e_{ij} \in E \Leftrightarrow a_{ij}>0$. Moreover, we assume $a_{ii}=0$ for all $i \in I$. For the undirected graph G, the adjacency matrix A is symmetric, i.e., $a_{ij}=a_{ji}$. The set of neighbors of node v_i is denoted by $N_i=\{v_j \in V: e_{ij} \in E\}$. The degree of node v_i is defined as $d_i=\sum_{j \in N_i} a_{ij}$. The Laplacian matrix of G is defined as $L=D-A$, where $D=Diag\{d_1, d_2, ..., d_n\}$ is the degree matrix of G with diagonal elements d_i and zero off-diagonal elements. An important fact of L is that all row sums are zero and thus L has a right eigenvector 1_n associated with the zero eigenvalue, where 1_n denotes the n-dimensional column vector with all elements being equal to 1. A path between two distinct nodes v_i and v_j means a sequence of distinct edges of the form $(v_i, v_{k_1}), (v_{k_1}, v_{k_2}), \ldots, (v_{k_i}, v_j)$. A graph is called connected if there is a path between any two distinct nodes of the graph. For the leader-follower consensus problem, we consider graph G associated with the system consisting of n agents (which are called followers) and one virtual leader denoted by agent 0. Let a_{i0} be the adjacency weight between agent i and the virtual leader. Assume that $a_{i0}=1$, if the virtual leader is a neighbor of agent i, and otherwise $a_{i0}=0$.

B. Problem Statement

In a multi-agent system with n agents, an agent and an available information flow between two agents are considered as a node and an edge in an undirected graph, respectively.

Consider the system of first-order dynamic agents described by

$$\dot{x}_i(t)=v_i(t), \quad i \in I, \tag{1}$$

where $x_i(t) \in R$ is the position state of agent i, and $u_i(t) \in R$ is the control input. The dynamics of the virtual leader is

$$\dot{x}_0(t)=0 \tag{2}$$

Consider the second-order system of dynamic agents described by

$$\begin{cases} \dot{x}_i(t)=v_i(t), \\ \dot{v}_i(t)=u_i(t), \end{cases} i \in I, \tag{3}$$

where $x_i(t) \in R$ and $v_i(t) \in R$ are the position state and the velocity state of agent i, respectively, and $u_i(t) \in R$ is the control input. The dynamics of the virtual leader is

$$\begin{cases} \dot{x}_0(t)=v_0(t), \\ \dot{v}_0(t)=0, \end{cases} \tag{4}$$

In Ref. [32], the finite-time consensus tracking protocol for a first-order multi-agent system with n agents and a virtual leader is described by

$$u_i(t)=\sum_{j \in N_i} a_{ij} sig(x_j-x_i)^{\alpha_{ij}} - p_i sig(x_i-x_0)^{\alpha_{i0}}, \tag{5}$$

where $i=1, 2, ..., N$, $0<\alpha_{ij}<1$, $|\cdot|$ denotes the absolute value, p_i is the adjacency weight between the virtual leader and agent i, and $sign(\cdot)$ is the sign function. Under the condition that network graph $G(A)$ is balanced and the leader is globally reachable, the finite-time consensus tracking of the first-order multi-agent system was investigated.

Moreover, in Ref. [30] Sun et al. proposed the following finite-time consensus tracking protocol for a second-order multi-agent system with n follower-agents and a virtual leader

$$\begin{aligned} u_i(t)=&\sum_{j \in N_i} a_{ij} sig(x_j-x_i)^{\alpha_1} + \sum_{j \in N_i} a_{ij} sig(v_j-v_i)^{\alpha_2} \\ &+ a_{i0} sig(x_0-x_i)^{\alpha_1} + a_{i0} sig(v_0-v_i)^{\alpha_2}. \end{aligned} \tag{6}$$

Different from the protocol (6), in this paper we develop a new finite-time consensus tracking protocol for the second-order multi-agent system:

$$\begin{aligned} u_i(t) &= \sum_{j\in N_i} a_{ij} sig(x_j - x_i)^{\alpha_1} + \sum_{j\in N_i} a_{ij} sig(v_j - v_i)^{\alpha_2} \\ &+ a_{i0} sig(x_0 - x_i)^{\alpha_1} + a_{i0} sig(v_0 - v_i)^{\alpha_2} \\ &+ \gamma \sum_{j\in N_i} a_{ij}(x_j - x_i + v_j - v_i) \\ &+ \gamma a_{i0}(x_0 - x_i + v_0 - v_i), \end{aligned} \tag{7}$$

where $0 < \alpha_1 < 1, \alpha_2 = 2\alpha_1/\alpha_1 + 1, \gamma \geq 0$.

Definition 1 Leader-follower finite-time consensus is said to be achieved, if there is a setting time $T_0 \in [0, +\infty)$ such that for any initial states, the solution of system (3) satisfies:

$$\lim_{t\to T_0} \|x_i(t) - x_0(t)\| = 0, \quad \lim_{t\to T_0} \|v_i(t) - v_0(t)\| = 0,$$

and $x_i(t) = x_0(t), v_i(t) = v_0(t), \quad \forall t \geq T_0, i \in I$.

III. Convergence Analysis

In this section, employing the Lyapunov function method, algebra graph theory, homogeneity with dilation, and some other techniques, we prove that multi-agent system (3) applying the protocol (7) can reach the finite-time consensus tracking.

Before moving on, we need the following assumption and lemmas.

Assumption 1 The communication network topology G composed of n agents is fixed, undirected and connected, and at least one agent has access to the leader.

Remark 1 Analogous to the analysis in Ref. [30], it is easy to prove that the multi-agent system (3) applying the protocol (6) can achieve consensus in finite time, if the systems (3) and (4) with $(x_1, ..., x_n, v_1, ...v_n)$ are homogeneous of degree $\kappa = \alpha_1 - 1 < 0$ with dilation $(\underbrace{r_1, ..., r_1}_{n}, \underbrace{r_2, ...r_2}_{n})$ and can achieve consensus asymptotically.

Lemma 1 [31] Suppose that the function $\varphi: R^2 \to R$ satisfies $\varphi(x_i, x_j) = -\varphi(x_j, x_i), i, j \in \Gamma, i \neq j$. Then for any undirected graph G and a set of numbers $y_1, y_2, \ldots, y_n$,

$$\sum_{i=1}^{N} \sum_{j\in N_i} a_{ij} y_i \varphi(x_j, x_i) = -\frac{1}{2} \sum_{(v_i, v_j)\in E} a_{ij}(y_j - y_i)\varphi(x_j, x_i).$$

Lemma 2 [33] (Lasalle's Invariance Principle) Let $x(t)$ be a solution of $\dot{x} = f(x)$, $x(0) = x_0 \in R^n$, where $f: U \to R^n$ is continuous with an open subset U of R^n, and $V: U \to R^n$ is a locally Lipschitz function such that $D^+V(x(t)) \leq 0$, where D^+ denotes the upper Dini derivative. Then $\Theta^+(x_0) \cap U$ is contained in the union of all solutions that remain in $S = \{x \in U : D^+V(x) = 0\}$, where $\Theta^+(x_0)$ denotes the positive limit set.

Next, the homogeneity with dilation (Rosier 1992 [34]) is given for the finite-time convergence analysis. For the n-dimensional system

$$\dot{x} = f(x), x = (x_1, x_2, \ldots, x_n) \in R^n, \tag{8}$$

a continuous vector field $f(x) = (f_1(x), f_2(x), \ldots, f_n(x))^T$ is homogeneous of degree $\kappa \in R$ with dilation $r = (r_1, r_2, \ldots, r_n)$, if for any $\varepsilon > 0$,

$$f_i(\varepsilon^{r_1} x_1, \varepsilon^{r_2} x_2, \ldots, \varepsilon^{r_n} x_n) = \varepsilon^{\kappa + r_i} f_i(x), i = 1, 2, ..., n.$$

Definition 2 System (8) is called homogeneous if its vector field is homogeneous. Moreover,

$$\dot{x} = f(x) + \tilde{f}(x), \tilde{f}(0) = 0, \quad x \in R^n, \tag{9}$$

is said to be locally homogeneous of degree $\kappa \in R$ with respect to the dilation $(r_1, r_2, \ldots, r_n)$, if $f(x)$ is homogeneous of degree $\kappa \in R$ with respect to the dilation $(r_1, r_2, \ldots, r_n)$ and $\tilde{f}$ is a continuous vector field satisfying

$$\lim_{\varepsilon\to 0} \frac{\tilde{f}_i(\varepsilon^{r_1} x_1, \varepsilon^{r_2} x_2, \ldots, \varepsilon^{r_n} x_n)}{\varepsilon^{\kappa + r_i}} = 0, \quad \forall x \neq 0, \quad i = 1, 2, ..., n. \tag{10}$$

For convenience, let $sig(x)^\alpha = |x|^\alpha sign(x)$, where $sign(\cdot)$ denotes the sign function and $|x|$ denotes the absolute value of the real number x.

Lemma 3 [35] Suppose that system (8) is homogeneous of degree $\kappa \in R$ with dilation $(r_1, r_2, \ldots, r_n)$, the function $f(x)$ is continuous, and $x = 0$ is its asymptotically stable equilibrium. Then the equilibrium of system (8) is finite-time stable if the homogeneity degree $\kappa < 0$. Moreover, the equilibrium of system (9) is locally finite-time stable if (10) holds.

Now, we give the main results.

Theorem 1 Under Assumption 1, the multi-agent system (3), applying the consensus tracking protocol (7), achieves the finite-time consensus tracking.

Proof Define the error vector

$$\bar{x}_i(t) = x_i(t) - x_0(t), \ \bar{v}_i(t) = v_i(t) - v_0(t), \ \forall i \in I. \tag{11}$$

According to Eqs. (3), (4), (7), and (11), we have

$$\begin{cases} \dot{\bar{x}}_i(t) = \bar{v}_i(t), \\ \dot{\bar{v}}_i(t) = u_i(t) \\ \quad = \sum_{j\in N_i} a_{ij} sig(\bar{x}_j - \bar{x}_i)^{\alpha_1} + \sum_{j\in N_i} a_{ij} sig(\bar{v}_j - \bar{v}_i)^{\alpha_2} \\ \quad - a_{i0} sig(\bar{x}_i)^{\alpha_1} - a_{i0} sig(\bar{v}_i)^{\alpha_2} \\ \quad + \gamma \sum_{j\in N_i} a_{ij}(\bar{x}_j - \bar{x}_i + \bar{v}_j - \bar{v}_i) \\ \quad - \gamma a_{i0}(\bar{x}_i + \bar{v}_i). \end{cases} \tag{12}$$

Take the following candidate Lyapunov function $V = V_1 + V_2 + V_3 + V_4 + V_5$ with

$$V_1 = \frac{1}{2}\sum_{i=1}^{n}\bar{v}_i^2,$$

$$V_2 = \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\int_0^{\bar{x}_i-\bar{x}_j} a_{ij}sig(s)^{\alpha_1}ds,$$

$$V_3 = \sum_{i=1}^{n}\int_0^{\bar{x}_i} a_{i0}sig(s)^{\alpha_1}ds,$$

$$V_4 = \frac{\gamma}{2}\sum_{i=1}^{n}a_{i0}\bar{x}_i^2$$

and

$$V_5 = \frac{\gamma}{4}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)^2.$$

Consider the derivative of $V_i(i=1, 2, 3, 4, 5)$ along the trajectories of system (12),

$$\begin{aligned}\dot{V}_1 &= \sum_{i=1}^{n}\bar{v}_i\dot{\bar{v}}_i\\ &= \sum_{i=1}^{n}\bar{v}_i[\sum_{j=1}^{n}a_{ij}sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}+\sum_{j=1}^{n}a_{ij}sig(\bar{v}_j-\bar{v}_i)^{\alpha_2}\\ &\quad -a_{i0}sig(\bar{x}_i)^{\alpha_1}-a_{i0}sig(\bar{v}_i)^{\alpha_2}\\ &\quad +\gamma\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i+\bar{v}_j-\bar{v}_i)-\gamma a_{i0}(\bar{x}_i+\bar{v}_i)],\end{aligned}$$

$$\dot{V}_2 = \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{v}_j-\bar{v}_i)sig(\bar{x}_j-\bar{x}_i)^{\alpha_1},$$

$$\dot{V}_3 = \sum_{i=1}^{n}a_{i0}\bar{v}_i sig(\bar{x}_i)^{\alpha_1},$$

$$\dot{V}_4 = \gamma\sum_{i=1}^{n}a_{i0}\bar{x}_i\bar{v}_i$$

and

$$\dot{V}_5 = \frac{\gamma}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)(\bar{v}_j-\bar{v}_i).$$

Then

$$\begin{aligned}\dot{V} &= \dot{V}_1+\dot{V}_2+\dot{V}_3+\dot{V}_4+\dot{V}_5\\ &= \sum_{i=1}^{n}\bar{v}_i[\sum_{j=1}^{n}a_{ij}sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}+\sum_{j=1}^{n}a_{ij}sig(\bar{v}_j-\bar{v}_i)^{\alpha_2}\\ &\quad -a_{i0}sig(\bar{x}_i)^{\alpha_1}-a_{i0}sig(\bar{v}_i)^{\alpha_2}\\ &\quad +\gamma\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i+\bar{v}_j-\bar{v}_i)-\gamma a_{i0}(\bar{x}_i+\bar{v}_i)]\\ &\quad +\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{v}_j-\bar{v}_i)sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}\\ &\quad +\sum_{i=1}^{n}a_{i0}\bar{v}_i sig(\bar{x}_i)^{\alpha_1}+\gamma\sum_{i=1}^{n}a_{i0}\bar{x}_i\bar{v}_i\\ &\quad +\frac{\gamma}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)(\bar{v}_j-\bar{v}_i)\\ &= \sum_{i=1}^{n}\bar{v}_i\sum_{j=1}^{n}a_{ij}sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}+\sum_{i=1}^{n}\bar{v}_i\sum_{j=1}^{n}a_{ij}sig(\bar{v}_j-\bar{v}_i)^{\alpha_2}\\ &\quad -\sum_{i=1}^{n}a_{i0}\bar{v}_i sig(\bar{x}_i)^{\alpha_1}-\sum_{i=1}^{n}a_{i0}\bar{v}_i sig(\bar{v}_i)^{\alpha_2}\\ &\quad +\gamma\sum_{i=1}^{n}\bar{v}_i\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)+\gamma\sum_{i=1}^{n}\bar{v}_i\sum_{j=1}^{n}a_{ij}(\bar{v}_j-\bar{v}_i)\\ &\quad -\gamma\sum_{i=1}^{n}a_{i0}\bar{x}_i\bar{v}_i-\gamma\sum_{i=1}^{n}a_{i0}\bar{v}_i^2\\ &\quad +\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{v}_j-\bar{v}_i)sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}\\ &\quad +\sum_{i=1}^{n}a_{i0}\bar{v}_i sig(\bar{x}_i)^{\alpha_1}+\gamma\sum_{i=1}^{n}a_{i0}\bar{x}_i\bar{v}_i\\ &\quad +\frac{\gamma}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)(\bar{v}_j-\bar{v}_i)\\ &= \sum_{i=1}^{n}\bar{v}_i\sum a_{ij}sig(\bar{v}_j-\bar{v}_i)^{\alpha_2}-\sum_{i=1}^{n}a_{i0}\bar{v}_i sig(\bar{v}_i)^{\alpha_2}\\ &\quad +\gamma\sum_{i=1}^{n}\bar{v}_i\sum_{i=1}^{n}a_{ij}(\bar{v}_j-\bar{v}_i)-\gamma\sum_{i=1}^{n}a_{i0}\bar{v}_i^2\\ &= \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{v}_i-\bar{v}_j)sig(\bar{v}_j-\bar{v}_i)^{\alpha_1}-\sum_{i=1}^{n}a_{i0}\bar{v}_i sig(\bar{v}_i)^{\alpha_2}\\ &\quad -\frac{\gamma}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{v}_i-\bar{v}_j)^2-\gamma\sum_{i=1}^{n}a_{i0}\bar{v}_i^2\le 0.\end{aligned}$$

Note that $\dot{V}=0$ if and only if $\bar{v}_j=\bar{v}_i=0$, then $\dot{\bar{v}}_i=0, \forall i\in I$, that is

$$\begin{aligned}\dot{\bar{v}}_i &= \sum_{j\in N_i}a_{ij}sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}+\sum_{j\in N_i}a_{ij}sig(\bar{v}_j-\bar{v}_i)^{\alpha_2}\\ &\quad -a_{i0}sig(\bar{x}_i)^{\alpha_1}-a_{i0}sig(\bar{v}_i)^{\alpha_2}\\ &\quad +\gamma\sum_{j\in N_i}a_{ij}(\bar{x}_j-\bar{x}_i+\bar{v}_j-\bar{v}_i)-\gamma a_{i0}(\bar{x}_i+\bar{v}_i)\\ &= \sum_{j\in N_i}a_{ij}sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}-a_{i0}sig(\bar{x}_i)^{\alpha_1}\\ &\quad +\gamma\sum_{j\in N_i}a_{ij}(\bar{x}_j-\bar{x}_i)-\gamma a_{i0}(\bar{x}_i)=0.\end{aligned}$$

Thus,

$$\begin{aligned}&\sum_{i=1}^{n}\bar{x}_i[\sum_{j=1}^{n}a_{ij}sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}-a_{i0}sig(\bar{x}_i)^{\alpha_1}\\ &+\gamma\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)-\gamma a_{i0}(\bar{x}_i)]\\ &=-\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}-\sum_{i=1}^{n}a_{i0}x_i a_{i0}sig(\bar{x}_i)^{\alpha_1}\\ &\quad -\frac{\gamma}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)^2-\gamma a_{i0}(\bar{x}_i)^2=0.\end{aligned}\tag{13}$$

At the same time, from Assumption 1, one can get

$$\begin{aligned}&\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)sig(\bar{x}_j-\bar{x}_i)^{\alpha_1}+\sum_{i=1}^{n}a_{i0}x_i sig(\bar{x}_i)^{\alpha_1}\\ &+\frac{\gamma}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}(\bar{x}_j-\bar{x}_i)^2+\gamma a_{i0}(\bar{x}_i)^2\ge 0.\end{aligned}\tag{14}$$

The inequality (14) together with (13) gives $\bar{x}_j = \bar{x}_i = 0$, $\forall i \neq j, i, j \in I$. From Lemma 3, we have $x_i - x_0 \to 0, v_i - v_0 \to 0, \forall i \in I$, as $t \to \infty$.

Next, from Remark 1, we know that the systems (3) and (4) under protocol (7) are homogeneous of degree $\kappa = \alpha_1 - 1 < 0$ with dilation $(\underbrace{2, 2..., 2}_{n}, \underbrace{\alpha_1 + 1, \alpha_1 + 1, ...\alpha_1 + 1}_{n})$. Therefore, it follows from Lemma 3 that the multi-agent systems (3) and (4) under protocol (7) reach consensus in finite time. The proof is completed.

Remark 2 It is obvious that if $\gamma = 0$, the protocol (7) degenerates into the protocol (6). With the non-zero parameter γ, the convergence speed of the multi-agent systems (3) and (4) under the protocol (7) is faster than that under the protocol (6). This improvement of convergence speed will be illustrated by the following comparison simulations.

IV. SIMULATIONS

In this section, numerical simulations are provided to illustrate the effectiveness of the above theoretical results. Consider a multi-agent system composed of three agents and one virtual leader labeled as agent 0 with the network topology shown in Fig. 1.

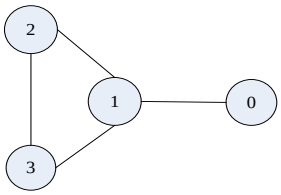


Figure 1. Network topology composed of three agents and one virtual leader.

Without loss of generality, all weights of edges are assumed to be 1 if $e_{ij} \in E$, and the initial states are chosen as $x(0) = (2, 5, 8)^T$ and $v(0) = (10, 4, 1)^T$. Suppose $\alpha_1 = 0.8$, $\alpha_2 = 2\alpha_1/\alpha_1 + 1 = 0.8889$, $x_0 = 2t$ and $v_0 = 2$. The numerical results are shown in Figs. 2 and 3, respectively. It can be seen from Fig. 2 that the system (3), applying the consensus tracking protocol (6), achieves the finite-time consensus tracking with $T_0 \approx 30s$. From Fig. 3, we find that the system (3), applying the consensus tracking protocol (7) with $\gamma = 3$, achieves the finite-time consensus tracking with $T_0 \approx 10s$. This numerically shows that the proposed finite-time consensus tracking protocol (7) has the faster convergence speed than the finite-time consensus tracking protocol (6).

V. CONCLUSIONS

In this paper, we have investigated the fast finite-time consensus tracking problems of second-order multi-agent systems. Applying the Lyapunov function method, algebra graph theory, homogeneity with dilation, and some other techniques, we have proved that second-order multi-agent systems applying the proposed consensus tracking protocol can reach the finite-time consensus tracking. Last, comparison simulations verified the effectiveness of the proposed protocol on improving the convergence speed. One of future research directions is to consider the case with time delays.

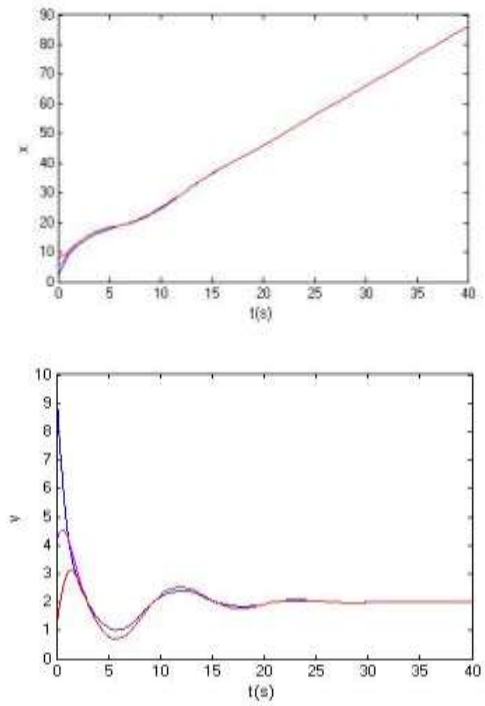


Figure 2. States of the system (3) using the protocol (6)

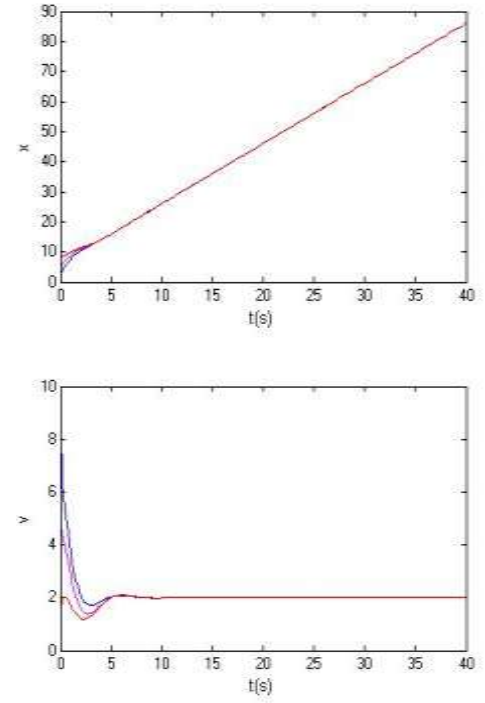


Figure 3. **S**tates of the system (3) using protocol (7) with $\gamma = 3$

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61203147 and 6120312) and the Humanities and Social Sciences Youth Funds of the Ministry of Education, China (Grant No. 12YJCZH218).

REFERENCES

[1] Yuping Tian, Chenglin Liu, Consensus of multi-agent systems with diverse input and communication delays, *IEEE Transactions on Automatic Control*, vol. 53, no. 10, pp. 2122-2128, 2008.

[2] Abdelkader Abdessameud, Abdelhamid Tayebi, On consensus algorithms design for double integrator dynamics, *Automatica*, vol. 49, no. 1, pp. 253-260, 2013.

[3] Long Cheng, Zengguang Hou, Min Tan and Xu Wang, Necessary and sufficient conditions for consensus of double-integrator multi-agent systems with measurement noises, *IEEE Transactions on Automatic Control*, vol. 56, no. 8, pp. 1958-1963, 2011.

[4] Jia Wei, Huajing Fang. State feedback consensus for multi-agent system with multiple time-delays, *Journal of Networks*, vol. 8, no. 9, pp: 1960-1966, 2013.

[5] Jing Yan, Xinping Guan and Xiaoyuan Luo, Consensus pursuit of heterogeneous multi-agent systems under a directed acyclic graph, *Chinese Physics B*, vol. 20, no. 4, pp. 48901, 2011.

[6] Jorge Cortés, Distributed algorithms for reaching consensus on general functions, *Automatica*, vol. 44, no. 3, pp. 726-737, 2008.

[7] Ren, W. and Beard, R. W. and Mclain, T. W. Coordination variables and consensus building in multiple v ehicle systems, *Lecture Notes in Control and Information Science*, vol. 309, pp. 171-188, 2004.

[8] Housheng Su, Xiaofan Wang and Guanrong Chen, A connectivity-preserving flocking algorithm for multi-agent systems based only on position measurements, *International Journal of Control*, vol. 82, no. 7, pp. 1334-1343, 2009.

[9] Housheng Su, Xiaofan Wang and Zongli Lin, Flocking of multi-Agents with a virtual leader, *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 293-307, 2009.

[10] Shihua Li, Haibo Du and Xiangze Lin, Finite-time consensus algorithm for multi-agent systems with double-integrator dynamics, *Automatica*, vol. 47, no. 8, pp. 1706-1712, 2011.

[11] Yongcan Cao, Wei Ren and Ziyang Meng, Decentralized finite-time sliding mode estimators and their applications in decentralized finite-time formation tracking, *Systems and Control Letters*, vol. 59, no. 9, pp. 522-529, 2010.

[12] Dimos V. Dimarogonas, Panagiotis Tsiotras and Kostas J. Kyriakopoulos, Leader-follower cooperative attitude control of multiple rigid bodies, *Systems and Control Letters*, vol. 58, no. 6, pp. 429-435, 2009.

[13] Qiang Song, Jinde Cao and Wenwu Yu, Second-order leader-following consensus of nonlinear multi-agent systems via pinning control, *Systems and Control Letters*, vol. 59, no. 9, pp. 553-562. 2010.

[14] Housheng Su, Guanrong Chen, Xiaofan Wang and Zongli Lin, Adaptive second-order consensus of networked mobile agents with nonlinear dynamics, *Automatica*, vol. 47, no. 2, pp. 368-375, 2011.

[15] Wei Zhu, Daizhan Cheng, Leader-following consensus of second-order agents with multiple time-varying delays, *Automatica*, vol. 46, no. 12, pp. 1994-1999, 2010.

[16] Ziyang Meng, Wei Ren, Leaderless and leader-following consensus with communication and input delays under a directed network topology. *IEEE Transactions on Systems Man and Cybernetics Part B-cybernetics*, vol. 41, no. 1, pp. 74-88, 2011.

[17] Ke Peng, Yupu Yang, Leader-following consensus problem with a varying-velocity leader and time-varying delays, *Physica A*, vol. 388, no. 2-3, pp. 193-208, 2009.

[18] Guanghui Wen, Guoqiang Hu, Wenwu Yu, Jinde Cao and Guanrong Chen, Consensus tracking for higher-order multi-agent systems with switching directed topologies and occasionally missing control inputs, *Systems and Control Letters*, vol. 62, no. 12, pp. 1151-1158, 2013.

[19] Xiaole Xu, Shengyong Chen, Wei Huang and Lixin Gao, Leader-following consensus of discrete-time multi-agent systems with observer-based protocols, *Neurocomputing*, vol. 118, no. 2-3, pp. 334-341, 2013.

[20] Zhihai Wu, Li Peng, Linbo Xie and Jiwei Wen, Stochastic bounded consensus tracking of second-order multi-agent systems with measurement noises and sampled-data, *Journal of Intelligent & Robotic Systems*, vol. 68, no. 3-4, pp. 261-273, 2012.

[21] Zhihai Wu, Li Peng, Linbo Xie and Jiwei Wen, Stochastic bounded consensus tracking of leader-follower multi-agent systems with measurement noises based on sampled-data with small sampling delay, *Physica A*, vol. 392, no. 4, pp. 918-928, 2013.

[22] Zhihai Wu, Huajing Fang and Yingying She, Weighted average prediction for improving consensus performance of second-order delayed multi-agent systems, *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 42, no. 5, pp. 1501-1508, 2012.

[23] Xiangshun Li, Huajing Fang. Optimal weights for consensus of networked multi-agent systems. *Information Technology Journal*, vol. 8, no. 1, pp. 77-82, 2009.

[24] Jing Zhou, Qian Wang, Convergence speed in distributed consensus over dynamically switching random networks, *Automatica*, vol. 45, no. 6, pp. 1455-1461, 2009.

[25] Zhihai Wu, Huajing Fang. Improvement for consensus performance of multi-agent systems based on delayed-state-derivative feedback, *Journal of Systems Engineering and Electronics*, vol. 23, no. 1, pp. 137-144, 2012.

[26] Huajing Fang, Zhihai Wu and Jia Wei, Improvement for consensus performance of multi-agent systems based on weighted average prediction, *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 249-254, 2012.

[27] Sanjay P. Bhat, Dennis S. Bernstein, Finite-time stability of continuous autonomous systems, *SIAM Journal on Control and Optimization*, vol. 38, no. 3, pp. 16, 2000.

[28] Jorge Cortés, Finite-time convergent gradient flows with applications to network consensus, *Automatica*, vol. 42, no. 11, pp. 1993-2000, 2006.

[29] Feng Xiao, Long Wang and Jie Chen, General distributed protocols for finite-time consensus of multi-agent systems, *Joint 48th IEEE Conference on Decision and Control and 28th Chinese Control Conference Shanghai, P. R. China*, December 16-18, 2009

[30] Fenglan Sun and Zhihong Guan, Finite-time consensus for leader-following second-order multi-agent system, *International Journal of Systems Science*, vol. 44, no. 4, pp. 727-738, 2013.

[31] Yakun Zhu, Xinping Guan and Xiaoyuan Luo, Finite-time consensus of heterogeneous multi-agent systems, *Chinese Physics B*, vol. 22, no. 3, pp. 038901, 2013.

[32] Fenglan Sun, Wei Zhu, Finite-time consensus for leader-following multi-agent systems over switching

network topologies, *Chinese Physics B*, vol. 22, no. 11, pp. 110204, 2013.
[33] N. Rouche, P. Habets and M. Laloy, Stability theory by liapunov's direct method, *New York: Springer-Verlag*, 1977.
[34] Lionel Rosier, Homogeneous lyapunov function for homogeneous continuous vector field, *Systems and Control Letters*, vol. 9, no. 6, pp. 467-473, 1992.
[35] Yiguang Hong, Finite-time stabilization and stabilizability of a class of controllable systems, *Systems and Control Letters*, vol. 46, no. 4, pp. 231-236, 2002.

Qiuyun Xiao received the BS degree in automation from Jiangnan University, Wuxi, China, in June 2012. She is currently working towards the MS degree in control science and engineering at Jiangnan University. Her interests include finite-time consensus of networked multi-agent systems (xiaoqy1007@163.com).

Zhihai Wu received the Ph.D degree in control theory and control engineering from Huazhong University of Science and Technology, Wuhan, China, in March 2011. He is currently with the Key Laboratory for Advanced Process Control of Light Industry of the Ministry of Education, the School of Internet of Things Engineering, Jiangnan University, Wuxi, China, where he is an associate professor. His interests include cascading failures of complex networks and robust consensus of multi-agent systems (wuzhihai@jiangnan.edu.cn).

Li Peng received the Ph.D degree in control theory and control engineering from University of Science & Technology Beijing, Beijing, China, in June 2002. He is currently with the School of Internet of Things Engineering, Jiangnan University, Wuxi, China, where he is a professor. His interests include information fusion of wireless sensor networks and theory and applications of Internet of Things (pengli@jiangnan.edu.cn).

A Hybrid Classifier Using Reduced Signatures for Automated Soft-Failure Diagnosis in Network End-User Devices

C. Widanapathirana X. Ang J. C. Li M. V. Ivanovich P. G. Fitzpatrick Y. A. Şekercioğlu
Department of Electrical and Computer Systems Engineering, Monash University, Australia
{chathuranga.widanapathirana, xavier.ang, jonathan.li, milosh.ivanovich, paul.fitzpatrick, ahmet.sekercioglu}@monash.edu

***Abstract*— We present an automated system for the diagnosis of both known and unknown soft-failures in end-user devices (UDs). Known faults that cause network performance degradation are used to train the classifier-based system in a supervised manner while unknown faults are automatically detected and clustered to identify the existence of new categories of soft-failures. The supervised classifier used in the system can be retrained by including the newly detected faults to enhance its performance.**

The system uses 460 features to construct Normalized Statistical Signatures (NSSs) for fault characterization. Due to the high dimensionality of NSSs, EigenNSS was proposed to reduce the complexity without losing important information. Because of the natural network inconsistencies that exist in communication links, we propose FisherNSS, a reduced signature that provides improved linear separability between classes to further enhance classification performance.

The system is evaluated over a live campus network using 17 emulated UD faults. The results show that the best overall classification accuracy of up to 97% was achieved by using FisherNSS with a dimensionality reduction of 96.74%. In comparison, both EigenNSS and FisherNSS have faster training and diagnosis time compared to NSS, which makes them suitable for on-demand as well as real time diagnostic applications. Furthermore, FisherNSS compared to EigenNSS has a higher diagnostic accuracy and quicker diagnosis time (order of microseconds).

I. Introduction

Network performance problems affect many end-users, ranging from everyday internet users to large corporations. Studies have shown that these problems are caused by service provider servers, backbone networks, access networks, or the end-user devices (UDs) themselves [1]. The performance of a network is usually defined by two main categories [2]: *hard-failures* and *soft-failures*. Hard failures correspond to the inability to transfer any data between users and the network, which can be easily identified and resolved due to immediately noticeable loss in connectivity. Soft-failures are characterized by degraded performance, which are more difficult to diagnose and are usually assisted by Network Monitoring Systems (NMS) to collect signs from the network. However, interpreting such signs to diagnose the root causes of the problem still require expensive resources which include intervention by skilled personnel.

Possible root causes of soft-failures in UDs are

- misconfiguration of parameters in the protocol layers, generally due to the conservative default values in operating systems [3],
- Hardware problems such as new application installations, NIC driver issues,
- kernel level software problems,
- mismatch between system settings and the link [4], or
- protocol implementation errors [5].

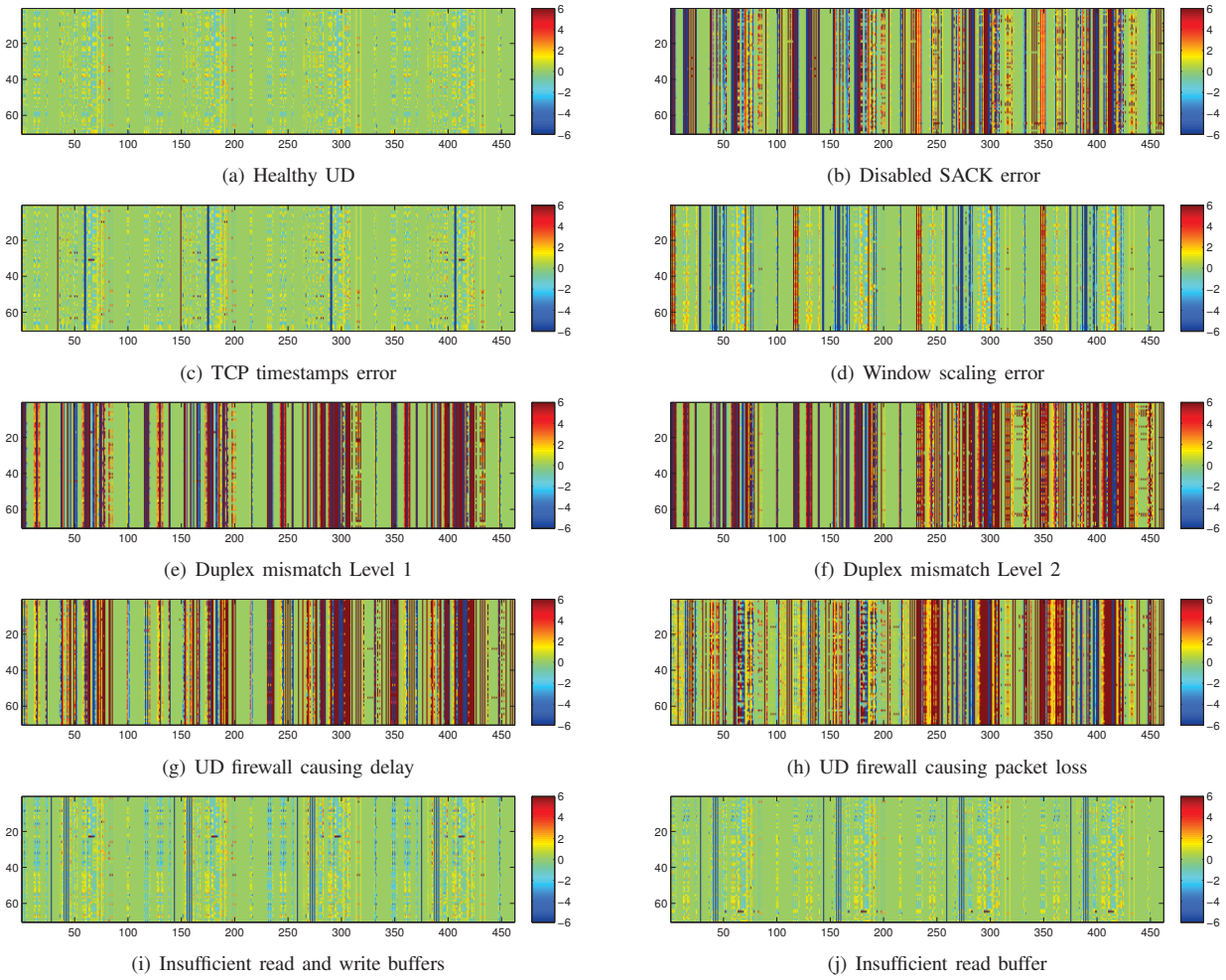
Recently, researchers have proposed an automated diagnosis solution especially focused on core networks, access networks and servers [6] but there is not much development taking place in automated solutions for UDs. Diagnosis methods based on collected packet traces over a TCP (Transmission Control Protocol) connection have been shown to be effective for finding the root causes of network performance problems [7]. Collected packet traces contain artifacts that represent behavioural characteristics of the network. These characteristics can be utilized by skilled investigators to identify the root causes of the faults. Another advantage of trace analysis-based diagnosis approach is that the traces can be collected very easily without the requirement of any special equipment.

A. Motivation

Our search on the research literature has revealed the lack of a fully automated solution for identifying the root causes of network soft-failures using TCP traces. To fill this gap, we previously proposed an automated diagnostic system based on supervised Machine Learning (ML) algorithms and network fault signatures[1] created using aggregated TCP statistics [8], [9]. In our system, the ML algorithms are first trained using signatures that we call as *Normalized Statistical Signatures (NSS)*, which are generated from collected packet traces. However, the diagnostic capability of the system is limited by the number of fault classes present in the training set. In the

[1] A *signature* is often defined as a collection of features, where each of these features represents a single aspect of behavioural characteristics in the network.

doi:10.4304/jnw.9.12.3275-3289



(a) Healthy UD

(b) Disabled SACK error

(c) TCP timestamps error

(d) Window scaling error

(e) Duplex mismatch Level 1

(f) Duplex mismatch Level 2

(g) UD firewall causing delay

(h) UD firewall causing packet loss

(i) Insufficient read and write buffers

(j) Insufficient read buffer

Figure 1. Visualization of NSSs for a healthy UD and nine common UD soft-failures. Here, the columns of each figure represent 460 features of the 70 NSSs. Each NSS occupies a row. Features have been normalized and scaled to $[-6, 6] \subset \mathbb{R}$ and their values are represented by colored pixels to project the scaled feature values to RGB space. This representation offers easy visualization and comparison. The images demonstrate that the combination of features uniquely represents each fault and can be used as a "fingerprint" for diagnosis.

case of diagnosing an unknown fault, this often leads to a false positive error. We have also found that the NSSs contain large numbers of features, which could cause over fitting of the classifier models, a problem known as the "curse of dimensionality" [10].

As a step to compensate for the limitations encountered, we present a new hybrid classifier architecture that extends the diagnosis capability of the system to both previously known faults as well as new types of faults. The hybrid classifier system combines unsupervised clustering algorithms[11], [12] to analyze previously unknown signatures to detect new faults and iterative training of a supervised ML classifier for root-cause diagnosis.

We also present two new signatures called *EigenNSS* and *FisherNSS*, both motivated by techniques used in facial recognition applications. The new signatures transform the NSSs to lower dimensions without sacrificing useful information. In addition, FisherNSS strives to maximize the ratio of the between-class scatter to the within-class scatter for better classification results. We perform a detailed comparison of performance between both EigenNSS and FisherNSS with data gathered from real-world networks. Preliminary results of the work have been published in a conference paper [13]. Whilst the published work only offer a limited discussion focused just on EigenNSS, this publication significantly extends the concept to introduce the FisherNSS. Additionally, this publication offer much detailed discussion and performance evaluation on both types of transformed signatures as well the hybrid classifier system.

II. System Overview

A. Normalized Statistical Signature (NSS)

In our work, we use a self-initiated controlled connection between the diagnostic server and UD to collect TCP packet traces. The collected traces are sent through a feature extraction module. In this paper, we use 230 extracted features from each trace, which totals to 460 when both upload and download traces are combined. Features extracted include cumulative totals of packet types, payload characteristics, observation frequencies of specific events, initial and final state parameters, delay

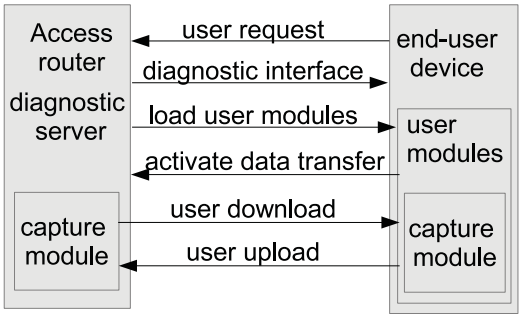


Figure 2. Deployment of the diagnostic system over the access network and operational overview.

based statistics, and TCP Boolean parameters. Various other extracted features that was included can be found in [14].

To standardize all the signatures, each of the 'faulty' raw signatures are normalized against the healthy baseline signature, which is obtained using a UD with optimal system settings. The resultant feature vector is called the Normalized Statistical Signature (NSS). Figure 1 shows NSSs collected from UDs exhibiting 9 types (classes) of faults and one 'healthy'[2] UD. Throughout all 70 samples for each type of fault, unique feature patterns are observed, providing the distinction needed for an effective and reliable diagnosis.

Since an NSS contains a large feature set (460 features), it theoretically enables a range of faults to be characterized through a single representation. However, as evident from the Figure 1, not all features contribute equally for the separability of the classes and even features within the same class show variations due to the inconsistent nature of the connection link. Having a large feature set can also lead to over fitting of the data when training a ML-based system; this consequently will lead to poor generalization and classification accuracy. Therefore, the dimensionality of the NSSs should be reduced while preserving the important information to build an effective diagnostic system.

In this study, we include two techniques to achieve dimensionality reduction in NSSs. Principal Component Analysis (PCA) is used to transform the NSS into a new signature called EigenNSS whereas Fisher's Linear Discriminant Analysis (FLDA) is used to generate another signature type called FisherNSS [15].

B. Operational Details of the Diagnostic System

1) Deployment: The diagnostic server is deployed as an application on the access router as shown in Figure 2. The complexities that can affect the uniformity of the captured packet traces can be eliminated by narrowing down the path to the UD into an access link. Firstly, upon initiation from the user, the modules needed for file transfers and packet captures are loaded. Two TCP-based data transfers of a fixed size of 20 MB file (an upload and download) are conducted serially between the UD and server. A file size of 20 MB was found, empirically, to provide the best balance between signature accuracy and collection time. A self-contained, portable packet-capturing mechanism that does not require kernel manipulations or installations is used to capture the packets. To satisfy the privacy concerns, we limit the amount of traffic captured and also control the content to be captured. Finally, the captured TCP packet traces are sent to the feature extraction modules where they are analysed and extracted to obtain statistical attributes (features), known as 'raw' signatures.

[2]In this work, we define a 'healthy' UD as a device that receives the maximum network performance level reasonably expected by a user.

D	Selected number of eigenvectors that account for the highest variation
p	Number of samples in signature set
m	Number of features in each NSS (m = 460)
$\mathbf{x}$	m-dimensional feature vector of the training NSS set
Φ	Mean of the training NSS set
Δ	Mean centered training NSS set
Ψ_{PCA}	Eigen matrix formed using a pre-determined D number of eigenvectors, v
Θ_{PCA}	EigenNSS is generated by projecting the mean centered NSS onto the Eigen matrix (Θ_{PCA} = $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_p\}$)
Φ_{PCA}	Mean of the entire EigenNSS set
Φ_i	Mean of the EigenNSS for the i^{th}
S_B	Between-class scatter
S_W	Within-class scatter
Ψ_{FLD}	Eigen matrix formed using a pre-determined D number of eigenvectors, w
Θ_{FLD}	FisherNSS is generated by projecting EigenNSS onto the Fisher matrix (Θ_{FLD} = $\{\mathbf{f}_1, \mathbf{f}2, \ldots, \mathbf{f}_p\}$)
$\epsilon_{f,\text{PCA}}$, $\epsilon_{f,\text{FLD}}$	Pattern vectors of each class
$\sigma_{f,\text{PCA}}$, $\sigma_{f,\text{FLD}}$	Euclidean distance between the test sample with each of the class pattern vectors
μ	Squared distance between the test NSS feature vector sample and the mean of the training NSS set

TABLE I.
MATHEMATICAL NOTATION

2) Operation: Figure 3 shows the operational stages of the diagnostic system. There are three main stages that the system operates in

1) Training stage
2) Diagnosis stage which also includes the
3) New class recognition stage.

During the training phase, the packet traces are colu-vjlected from UDs with known faults induced. Statistical attributes of these traces are extracted to form the *raw signature* and given a class label. The raw signatures are then normalized against the healthy performance baseline to create the NSSs. The NSSs generated from multiple classes are stored in a database and are used to calculate the *transformation matrices* of the database. The NSSs are projected onto either one of the transformation matrices to create the transformed signatures, EigenNSS and FisherNSS respectively. The transformed signatures of each class are used to calculate the pattern vector (ϵ_f) (Table I can be referred for the descriptions of the mathematical symbols used throughout the paper) of that

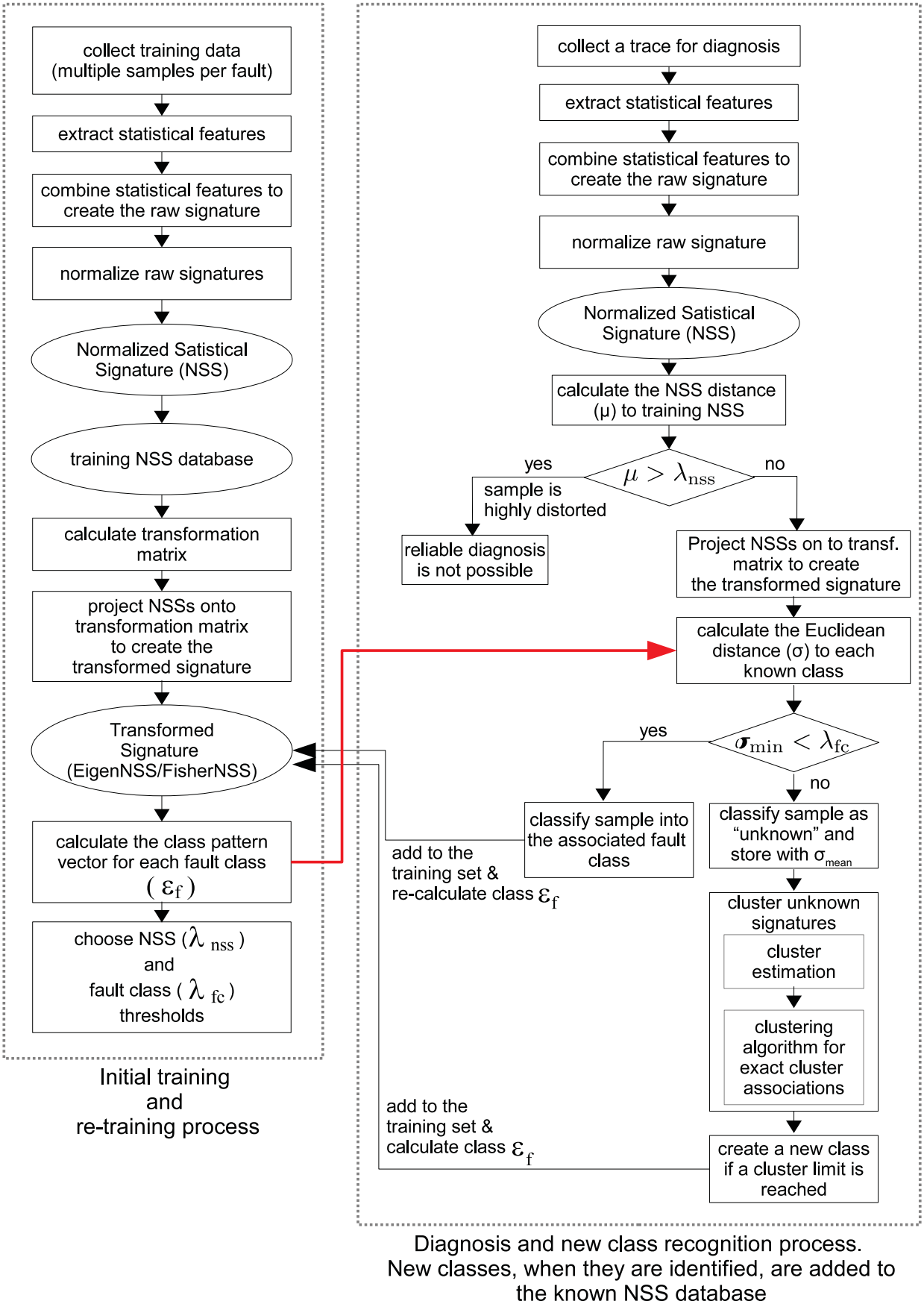


Figure 3. Operational overview of the classifier system.

particular class. Finally, two thresholds are chosen for the system:

1) λ_{nss} for determining if a particular signature is valid, and
2) λ_{fc} for determining class associations.

Once the system is trained, UDs that are suspected to be faulty can be diagnosed by collecting packet traces and sending them through the same feature extraction and NSS generation process. Then, EigenNSS and FisherNSS can be generated by projecting the NSSs onto either one of the transformation matrices created during the training stage. These transformed signatures are then used to calculate the pattern vector (ϵ) and Euclidean distance (σ) of the pattern vector from each known class. The NSS can also be used to calculate the square distance (μ) from the training NSS data set. Finally, depending on the minimum Euclidean distance ($\sigma_{\min}$) and square distance (μ), one of the three possible outcomes is decided by the system as follows

if $\mu > \lambda_{\text{nss}}$ **then**
  The sample is highly distorted.
  Reliable diagnosis is not possible.
else
  if $\sigma_{\min} < \lambda_{\text{fc}}$ **then**
    The sample is classified to the class associated with the minimum distance. The sample then is added to the training NSS database and the ϵ_f of the class is recalculated to include the new sample.
  else
    The sample contains a valid signature, but it does not belong to any of the known classes. Hence, the sample is classified as an unknown class.
  end if
end if

When the system detects a predetermined number of unknown signatures, new class recognition phase begins. This predetermined number is usually defined to be twice the minimum threshold size that a given cluster is accepted as a new class. These unknown signatures are first stored in a separate database with their pattern vectors. Then, these signatures are sent through a cluster estimation algorithm [11] which determines (i) if the data set has samples that can be clustered within the λ_{fc} bound, and (ii) the number of clusters that can be created. These clusters will be matched with their exact cluster memberships with the assistance of a clustering algorithm, which uses a fuzzy C-means clustering technique with iterative optimization [12]. If any of the clusters reach the minimum threshold size, they will be considered as a new class and will be added into the training database. The transformed signatures of the new class are sent to the class pattern vector calculation while its NSSs are sent to the classifier training database. Although new classes can be added by calculating the class pattern vectors, the system can be re-trained in a short time when it isn't performing any diagnostics if the training database is updated with the new NSSs. Re-training includes the new class and improves the final accuracy of the system. The system also prompts administrators that a new fault class has been detected, and after investigative analysis of its actual root cause, a class label can be created.

The rest of the paper is organized as follows. Section III recaps some of the related work done by other researchers. Section IV presents how the NSSs are transformed to generate EigenNSS and in Section V, the creation of the new signature, FisherNSS is discussed elaborately. Section VI includes the training and diagnosis process of the system. Finally, Section VII contains detailed performance analyses of the systems comparing both types of signatures used followed by the conclusion in Section VIII.

III. Related Work

Characterizing the behaviour of the network to model a signature is an approach found mainly in network applications with detection tasks. A signature is defined as a collection of features (or attributes), each representing a single aspect of the network's behaviour. In a detection process, signatures provide the key to differentiate "healthy" behaviours from the abnormal or faulty ones. However, depending on a particular application, the generation process of a signature may vary to account for the requirements and constraints. In order to find a suitable network signature, investigations about several available types of network signatures are carried out to maximize the capability of our diagnostic system. In addition to that, various existing dimensionality reduction techniques are reviewed, weighing between their pros and cons.

A. Network signatures

This subsection shows a summary of the different types of network signatures and their limitations in the context of UD, soft-failure characterization. Firstly, network signatures generated from flow-based characteristics have been commonly used in online traffic classification as in Roughan *et al.* [16] and IDSs as in Zhang *et al.* [17]. Kihara et al. [18], Hajji [19] and Thotta and Ji [6] have used signatures created using the behavioral changes in traffic flows for network fault detection. These applications focus on detecting abnormalities in the overall traffic flow pattern of the network when compared with the normal traffic flow. However, these flow-based signatures are not suitable for UD diagnosis applications due to their passive and continuous monitoring nature. Our application requires diagnosis to be run on-demand when a user experiences a network performance problem.

Another common approach is to use system logs from devices or 'reports' compiled by the user. Aggarwal *et al.* [20] and Reidemeister *et al.* [21] incorporated internal system logs whereas Lee and Kim [22] used user-reports to create their respective fault signatures. The usage of the system logs not only brings up privacy concerns in public networks but is also inconvenient for network operators as

they have to gain privileged access to the UDs. Reports generated by users may be unreliable if users have no specific network knowledge. Although system logs and user-reports can provide valuable information when generating a fault signature, we believe the challenges far outweigh the benefits.

Communication protocols are another common source of information to create network signatures. Popular protocols such as IP, TCP, UDP, and HTTP have often been used because they are usually supported by most devices. Dahmouni *et al.* [23], Manikopoulos and Papavassiliou [24], and Wolfgang [25] extracted features from multiple protocols, whereas other studies such as Gomes *et al.* [26] and Chen *et al.* [27] have limited feature collection to a single protocol. However, these proposed signatures have been created to detect a very specific network problem which doesn't provide us with much flexibility for our application. In the case of UD soft-failure detection, the requirements are to be able to effectively characterize not only a large number of faults, but also any new types that are unknown to our system. Hence, these proposed signatures with limited features can limit the ability to capture valuable information needed to generalize the signatures.

Our literature review has revealed that the existing network signatures are unsuitable for our application as they do not offer satisfactory solutions to characterize UD soft-failures. Therefore, we propose a more comprehensive signature to characterize UD soft-failures and analyse how uniquely different the signatures are on different network properties.

B. Complexity reduction

This subsection shows a summary of the different types of dimensionality reduction techniques used by other researchers and their limitations. Network signatures generated from flow-based characteristics for traffic classification such as the one illustrated by Zhang *et. al.* [17] contain large amounts of data as they are collected from one of China's seven major backbone networks. The complexity of their dataset was reduced by only capturing packet headers, which surprisingly still contain excessive amount of data for a whole day. For further complexity reduction, each day is divided into 24 hours where data is only captured in the first minute for each hour. Due to the on-demand requirement, this reduction method is deemed unsuitable for our application.

Clustering algorithms are commonly used in reducing the complexity of a large data set. Vaarandi proposed a density-based approach clustering [28] to reduce the amount of data (signatures from system log files) required by a support person to evaluate the behaviour of the system. In a density-based clustering, clusters are usually defined as areas of higher density than the remaining data set. The algorithm consist of three steps which include (i) data summarization, (ii) building cluster candidates, using the summary information collected and finally, (iii) cluster selection based on the candidates. This method not only clusters data into regions based on frequent patterns from the log files but also extracts the static parameters that are unique to the system.

In other domains, Fisher's Linear Discriminant (FLD) [15] is used to reduce the dimensionality of image data sets. This method is also very versatile in overcoming inconsistencies and variances in an image (eg. lighting variations in facial recognition). FLD provides linear class separation in huge data sets which helps simplify classification process.

Our complexity reduction method was greatly motivated by how well facial recognition methods have performed in their respective fields and we were inspired to try these methods on our generated signatures.

IV. EigenNSS: NSS Transformation Using Principal Components

To overcome the challenges with having high dimensionality in NSSs, we searched for a way to emphasize on significant global features that contain a maximum amount of information. Dimensionality reduction can be achieved by firstly finding the principle components (i.e eigenvectors of the covariance matrix) of the distribution of NSSs. Then, these eigenvectors can be ordered according to the amount of variation among the NSSs. Finally, the NSSs are projected onto a selected number (D) of eigenvectors that accounts for the highest variation. These projections are called "EigenNSS" which represent most of the information from the original samples in a D-dimensional space.

A. Generating EigenNSS

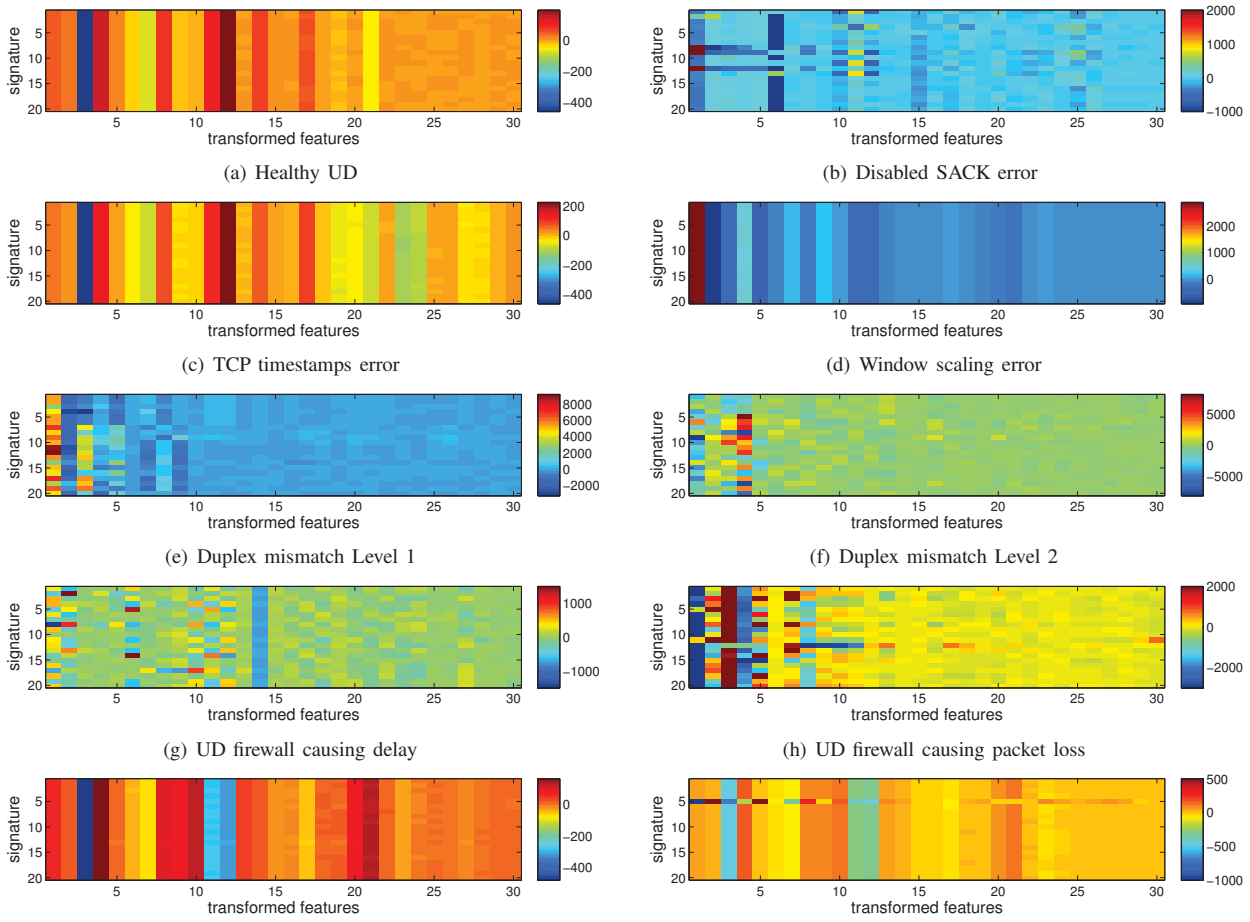
The following subsection provides details of the EigenNSS generation and calculation process. Consider a training NSS set of $\mathbf{x}_1$, $\mathbf{x}_2$, ..., $\mathbf{x}_p$ where x is a m-dimensional feature vector. For example, the set of NSS shown in Figure 1 has 70 samples for each of the 10 classes (p = 70 x 10 = 700), in which each of them has 460 feature vector (m = 460). Principal Component Analysis (PCA) can be performed either on co-variance matrix or on correlated matrix and the choice usually depends on the variance of features. Correlation matrix is preferred when the scales of the features are significantly different from one another. When the scales of the features are similar, the covariance matrix is preferred, as the correlation matrix will lose information when standardizing the variance. We have chosen to perform PCA on covariance matrix since features in NSSs are already normalized and approximately have similar scales.

The mean of the NSSs can be found by

$$\Phi = \frac{1}{p}\sum_{k=1}^{p}\mathbf{x}_k$$

The training NSSs are then mean centered by

$$\bar{\mathbf{x}}_i = \mathbf{x}_i - \Phi$$



(a) Healthy UD (b) Disabled SACK error

(c) TCP timestamps error (d) Window scaling error

(e) Duplex mismatch Level 1 (f) Duplex mismatch Level 2

(g) UD firewall causing delay (h) UD firewall causing packet loss

(i) Simultaneous insufficient read-write buffer (j) Insufficient read buffer

Figure 4. Comparison of EigenNSSs for common UD soft-failures.

where $\bar{\mathbf{x}}_i$ is the mean centered m-dimensional feature vector of the i^{th} instance. The resultant matrix $\Delta = \{\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2, ..., \bar{\mathbf{x}}_p\}$ has the dimensions of m x n and used to calculate covariance matrix Δ_{cov}. Δ_{cov} is then subjected to PCA where eigenvectors, $\mathbf{v}_i$ and the corresponding eigenvalues n_i are determined by solving a well-known singular value decomposition (SVD) problem. Then, a pre-determined D number of eigenvectors, v that are arranged from the highest eigenvalue, n are selected to create the Eigen matrix which has the dimensions of m x D. Finally, EigenNSSs are created by projecting the mean centered NSS matrix, Δ onto the Eigen matrix, Ψ_{PCA} as

$$\Theta_{\text{PCA}} = {\Psi_{\text{PCA}}}^T \Delta$$

where $\Theta_{\text{PCA}} = \{\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_p\}$ and $\mathbf{e}$ is a D-dimensional EigenNSS.

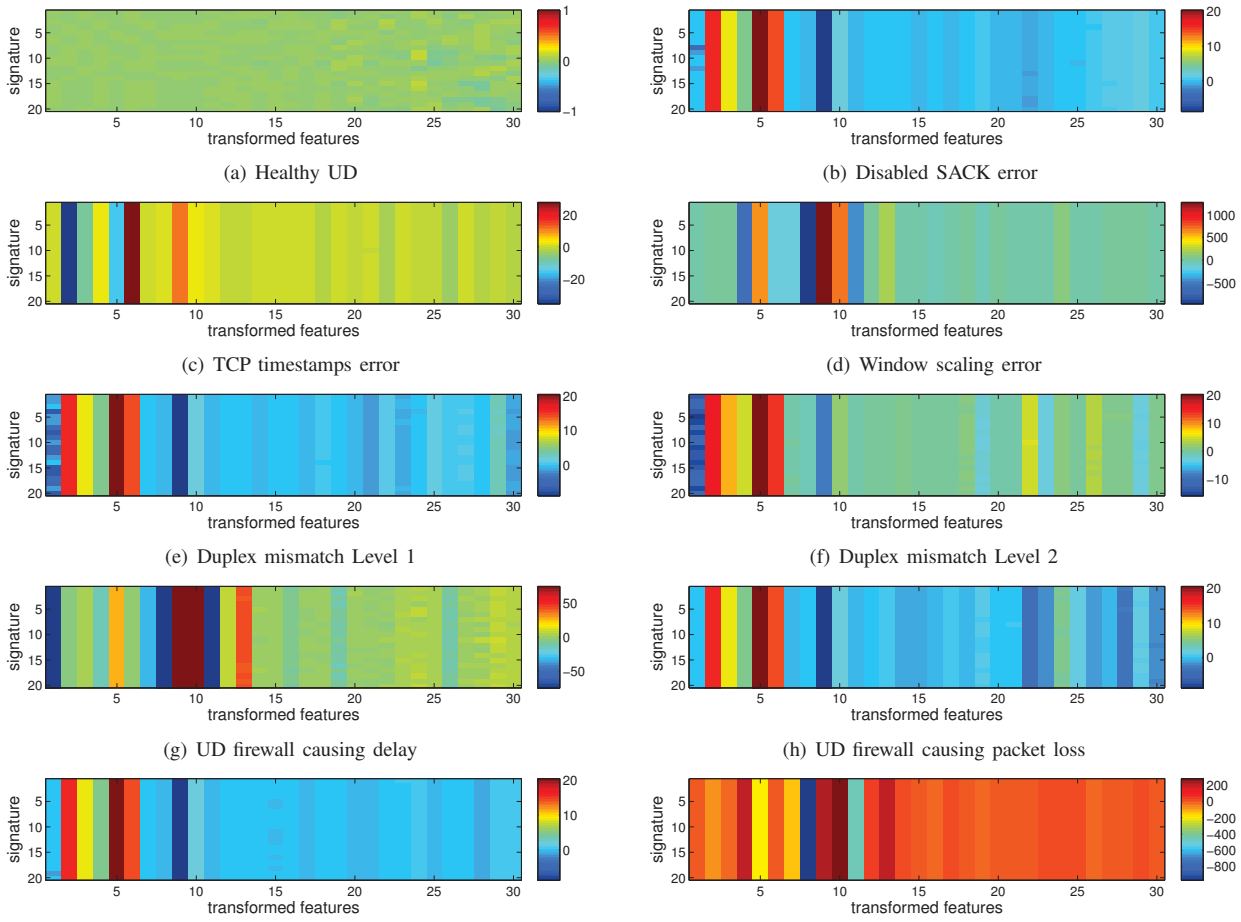
Figure 4 shows the comparison of EigenNSSs for various types of common UD faults with D=30. Note that the figure only shows 25 signature samples per class for clarity. As shown in the figure, the dimensionality of NSSs has been reduced while preserving the most important information for class separation. This is clearly visible as the EigenNSS shows significant differences between classes compared to the NSSs. However, it can be seen that the EigenNSS samples within the same classes can vary due to the inconsistent nature of the network links.

V. FisherNSS: NSS Transformation Using Fisher's Linear Discriminant Analysis

As shown in the previous section, EigenNSS reduced the dimensionality of NSS. However, to account for the errors in data collection and the inconsistent nature of the networks, separation between these unwanted information is needed for a better classification outcome. This section shows the motivation and generation process of FisherNSS, a new transformed signature.

A. Fisher's Linear Discriminant

The inconsistent nature of the network affects the extracted features and may lead to a poor fault detection. These inconsistencies (noise terms) are embedded inside the data which makes it difficult to distinguish from the actual information. PCA used in EigenNSS calculates the eigenvalues that explain most of the variation across the data; in this case it would operate per feature vector and does not take account of class labels. As previously mentioned, Fisher's Linear Discriminant (FLD) aims to maximize Fishers discriminant ratio, i.e. it maximizes the



(a) Healthy UD

(b) Disabled SACK error

(c) TCP timestamps error

(d) Window scaling error

(e) Duplex mismatch Level 1

(f) Duplex mismatch Level 2

(g) UD firewall causing delay

(h) UD firewall causing packet loss

(i) Simultaneous insufficient read-write buffer

(j) Insufficient read buffer

Figure 5. Comparison of FisherNSSs for common UD soft-failures.

distance between classes and provides linear separability between classes, to facilitate correct fault diagnosis. However, to guarantee within class scatter matrix in FLD not to become singular, we require at least $x + c$ samples (x=number of dimensions, c=classes) and in the case of NSS, at least 475 samples per class. This requirement reduces the usability of FishersNSS to more mature systems with large data sets. To reduce the minimum sample requirement, we use a well-established two-phase framework of PCA plus FLD where PCA first reduces the dimensions of the feature space, and then apply Fisher's Linear Discriminant Analysis (FLD) for further reduction and between class separation [29], [30].

FLD is an example of a *class specific method*, that attempts to "shape" the scatter of feature values to facilitate reliable classification. To illustrate the benefits of a class specific linear projection, we construct a set of 10 2-dimensional (n=2) sample points. In Figure 6, a comparison of both PCA and FLD for a two-class problem is shown by projecting the constructed sample points from 2D down to 1D respectively. Comparing the projections, PCA smears the classes together so that they are no longer linearly separable in the projected space. Although the total scatter of FLD is smaller than of

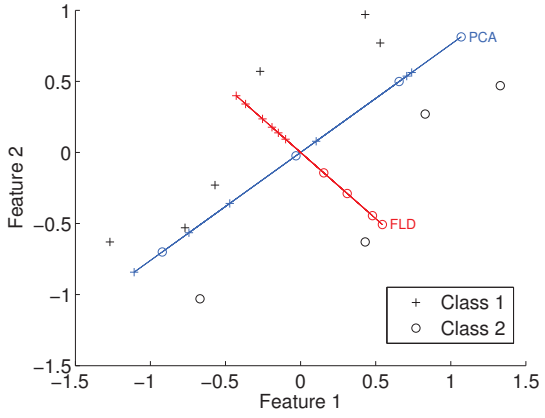


Figure 6. A comparison of principal component analysis (PCA) and Fisher's Linear Discriminant (FLD) for a two class problem.

PCA, FLD achieves greater between-class scatter, and consequently results in better classification.

B. Generating FisherNSS

The following subsection illustrates how the FisherNSS is generated including the calculation process. Assuming we have a training EigenNSS set, Θ_{PCA} of $\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_p$

, where **e** is a D-dimensional transformed feature vector. For example, the set of EigenNSS shown in Figure 4 has N=25 samples for each of the 10 classes (p = 25 x 10 = 250), in which each of them has D=30 features. The mean of the entire EigenNSS set can be found by

$$\Phi_{\text{PCA}} = \frac{1}{p}\sum_{k=1}^{p}\mathbf{e}_k$$

The mean of the EigenNSS for the i^{th} class can be found by

$$\Phi_i = \frac{1}{N_i}\sum_{\mathbf{e}_k \in E_i}\mathbf{e}_k$$

where Φ_i is the mean EigenNSS of class E_i and N_i is the number of samples in class E_i. The between-class scatter matrix can then be computed by

$$S_B = \sum_{i=1}^{c}(\Phi_i - \Phi_{\text{PCA}})(\Phi_i - \Phi_{\text{PCA}})^T$$

and the within-class scatter matrix by

$$S_W = \sum_{i=1}^{c}\sum_{\mathbf{e}_k \in E_i}(\mathbf{e}_k - \Phi_i)(\mathbf{e}_k - \Phi_i)^T$$

The optimal projection W_{opt} is chosen as the matrix with orthonormal columns (eg. eigenvectors, w) which maximizes the ratio of the determinant of the between-class scatter matrix to the determinant of the within-class scatter matrix, i.e.,

$$W_{\text{opt}} = \arg\max\frac{|W^T S_B W|}{|W^T S_W W|}$$

However, only a pre-determined D number of eigenvectors that are arranged from the highest eigenvalue, are selected to create the Fisher matrix which has the dimensions of D x D. Finally, FisherNSS are created by projecting the EigenNSS matrix, Θ_{PCA} onto the Fisher matrix, Ψ_{FLD} as

$$\Theta_{\text{FLD}} = {\Psi_{\text{FLD}}}^T\Theta_{\text{PCA}}$$

where $\Theta_{\text{FLD}} = \{\mathbf{f}_1, \mathbf{f}_2, ..., \mathbf{f}_p\}$ and **f** is an D-dimensional FisherNSS.

Figure 5 shows the FisherNSSs for various types of common UD faults with D=30. Similarly, only 25 signature samples per class are shown for clarity. As evident from the figure, the signature samples in each class exhibit very little variation and appear to reduce the effects of network inconsistencies on the extracted signatures.

VI. Training and Diagnosis of Reduced Signatures

A. Training

The following subsection shows the diagnostic system training process using EigenNSS and FisherNSS respectively, where the pattern vectors (ϵ_f) of each class are calculated. We assume the EigenNSS matrix, Θ_{PCA} and FisherNSS matrix, Θ_{FLD} contains n signature samples from multiple classes (faults, f). The D-dimensional class pattern vector, ϵ_f is calculated by averaging the reduced signatures as

$$\epsilon_{f,\text{PCA}} = \frac{1}{n}\sum_{k=1}^{n}\mathbf{e}_k$$

$$\epsilon_{f,\text{FLD}} = \frac{1}{n}\sum_{k=1}^{n}\mathbf{f}_k$$

where these pattern vectors, ϵ_f are used during the diagnosis stage to calculate the distance between any given unknown (test) signatures. These distances are used to determine the best class fit of the unknown signatures.

B. Diagnosis

1) Known Faults: In this subsection, the classification criteria required for the diagnosis of known faults are shown. The simplest method of determining the class association of a test sample is to calculate the Euclidean distance, σ between **e** and **f** respectively with each of the class pattern vectors as

$$\sigma_{f,\text{PCA}} = ||\mathbf{e} - \epsilon_{f,\text{PCA}}||^2$$

$$\sigma_{f,\text{FLD}} = ||\mathbf{f} - \epsilon_{f,\text{FLD}}||^2$$

Euclidean distance assumes the data to be isotropically Gaussian. Euclidean distance was used over more computationally expensive measures such as Mahalanobis distance because our previous analysis of NSSs have shown that features are largely uncorrelated and clearly follow a Gaussian distribution[31]. The test sample is classified and associated with a class, f when its respective minimum Euclidean distance, σ_{min} is below the chosen fault class threshold, λ_{fc}.

Due to errors in data collection and the inconsistent nature of networks, some of the collected packet traces can be distorted. This may lead to a false detection, where the erroneous NSSs generated from these distorted packet traces are wrongly classified. Hence, we introduced another term for a more reliable outcome which is the squared distance, μ between the NSS feature vector of the test sample, y and the mean of the training NSSs, Φ.

$$\mu = ||y - \Phi||^2$$

The test sample is considered valid only if the minimum squared distance is less than the chosen NSS threshold, λ_{nss}.

Depending on the minimum values of σ_f and μ, the outcome of the diagnosis process is determined following the criteria previously mentioned in Section I.

2) Unknown faults: Here, we present the new class recognition process for the diagnosis of unknown faults. A test signature samples is classified as "unknown" if it contains a valid signature but does not belong to any of the known classes. These unknown samples are sent through a cluster estimation algorithm to determine the number of clusters that can be created and whether or not, the samples can be clustered within the λ_{fc} bound.

Assume that we have a set of n unknown signature samples $\{x_1, x_2, ..., x_n\}$ in the database. We consider

each of the unknown samples as a potential cluster center and its respective measured potential, P_i as a function of its distances to all the other unknown samples. The measure of potential for the i^{th} unknown samples are given as

$$P_i = \sum_{j=1}^{n} \mathbf{e}^{-\alpha||x_i - x_j||^2}$$

where

$$\alpha = \frac{4}{r_a^2}$$

and r_a is a positive constant, corresponding to the radius defining a neighbourhood, where unknown samples outside this radius have limited influence on the potential. After the potential of every unknown sample has been computed, we choose the unknown sample with the highest measured potential as the first cluster center.

Let x_1^* be the location of the first cluster center and P_1^* be its measured potential value. The potential of each unknown sample x_i is then revised by subtracting an amount of potential as a function of its distance from the first cluster center. The revised potential of the i^{th} unknown sample can be calculated as

$$P_i = P_i - P_1^* \mathbf{e}^{-\beta||x_i - x_1^*||^2}$$

where

$$\beta = \frac{4}{r_b^2}$$

and r_b is a positive constant, corresponding to the radius defining the neighbourhood that will have measureable reductions in potential. The constant r_b is set to be somewhat greater than r_a, to avoid cluster centers being too closely spaced together. A good choice of values is $r_b = 1.5r_a$. The unknown samples near the first cluster center will have greatly reduced potential, and are unlikely to be the source of the next cluster center. Therefore, the unknown sample with the highest remaining potential is selected to be the second cluster center.

In general, the process of acquiring new cluster centers, x_k^* is repeated using the general formula for revising potentials as

$$P_i = P_i - P_k^* \mathbf{e}^{-||x_i - x_k^*||^2}$$

following these criteria:

if $P_k^* > \overline{\epsilon} P_1^*$ **then**
  Accept x_k^* as a cluster center and continue.
else if $P_k^* < \underline{\epsilon} P_1^*$ **then**
  Reject x_k^* and end process.
else
  Let $d_{\text{min}} \leftarrow$ shortest distances between x_k^* and all previously found cluster centers.
  if $\frac{d_{\text{min}}}{r_a} + \frac{P_k^*}{P_1^*} \geq 1$ **then**
    Accept x_k^* as a cluster center and continue.
  else
    Reject x_k^* and set the potential at x_k^* to 0.
    Select the unknown sample with the next highest potential as the new x_k^* and re-test.
  end if
end if

Here $\overline{\epsilon}$ represents the threshold for the potential above which we will definitely accept the unknown samples as a cluster centers. Whereas $\underline{\epsilon}$ represents a threshold below which we will definitely reject the unknown samples.

Once the cluster data are obtained, they are sent to a clustering algorithm to determine the exact cluster membership. This algorithm uses Fuzzy C-Means (FCM) clustering with iterative optimization that minimizes the cost function

$$J = \sum_{k=1}^{n} \sum_{i=1}^{c} \mu_{ik}^m ||x_k - v_i||^2$$

where n is the number of unknown test samples, c is the number of clusters (obtained from cluster estimation), x_k is the k^{th} unknown sample, c_i is the i^{th} cluster center, μ_{ik} is the degree of membership of the k^{th} sample in the i^{th} cluster, and m is a constant greater than 1 (typically m = 2). The degree of membership, μ_{ik} is defined by

$$\mu_{ik} = \frac{1}{\sum_{j=1}^{c} \left(\frac{||x_k - v_i||}{||x_k - v_j||}\right)^{2/(m-1)}}$$

FCM will converge to a solution for v_i, that is either a local minimum or a saddle point of the cost function, J. The performance of the FCM solution depends strongly on the choice of the initial values used (eg. the number of clusters, c and the initial cluster centers, v_i), which are taken from the cluster estimation algorithm. Finally, the exact cluster membership can be computed by using the final iteration value of v_i.

VII. Performance Analysis

In this section, we evaluate the performance of the system and analyse its diagnostic capability.

A. Data Set

Collecting data from actual user complaints is challenging considering the amount of time required to collect a sufficient number of samples, and resources needed to manually identify the issues. In order to recreate a realistic fault detection scenario, we designed a fault emulator module to reproduce commonly found problems in UDs. The fault emulator is installed in test computers connected to the live university network in multiple locations. This allows us to demonstrate the viability of the system in real computing environments, where cross traffic and congestion is present. This method of emulating faults offered an efficient way of collecting accurate data with minimal resources.

A total of 16 common UD faults that can affect network performance are emulated as listed in Table II. By including the "Healthy" UD case, a total of 17 classes are formed and used in this evaluation. Over the entire evaluation period, we collected 12685 traces from UDs emulating these 17 fault cases, each having approximately

Fault	Description
CF1	Healthy
CF2	Disabled SACK error
CF3	Insufficient write buffer
CF4	Insufficient read buffer
CF5	Simultaneously insufficient read & write buffer
CF6	TCP timestamps are not working/in error
CF7	Window scaling error
CF8	Limited reordering threshold
CF9	Link-UD speed mismatch level 1
CF10	Link-UD speed mismatch level 1 & duplex mismatch
CF11	Link-UD speed mismatch level 2
CF12	Link-UD speed mismatch level 2 & duplex mismatch
CF13	UD firewall causing packet loss
CF14	UD firewall causing packet delay
CF15	Overloaded UD CPU
CF16	Overloaded UD memory
CF17	UD HDD i/o overloaded - faulty

TABLE II.
KEY: LIST OF FAULTS

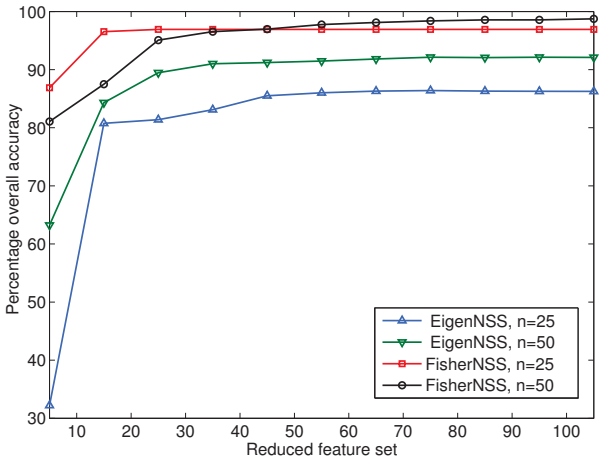


Figure 7. Overall accuracy of the system against dimensionality (D) of the reduced signatures. Each graph represents a different per-class training dataset size.

equal amounts (750) of samples. Data was also collected from UDs that operates with 8 different flavours of TCP, as they contribute to a variation in connection behaviour.

B. System Performance

The system is initially trained using only 13 classes as our evaluation needed to consider unknown faults. The faults CF2, CF8, CF10, and CF17 are kept as the unknown faults (refer to Table II), and are introduced at random intervals into the system during the testing stage. The data sets of the 13 classes are randomly divided into training and testing groups. We conducted the experiment over 8 iterative sessions and averaged the results in order to achieve statistical robustness.

The cluster threshold to add an unknown fault as a known fault are set to be equal to the number of per-class training samples used to initiate the system (e.g. if the system is initially trained with 50 samples per class, an unknown class is added as a known fault when its cluster membership reaches 50). This cluster membership minimum threshold is a design choice and will dictate the confidence level in detecting the existence of a new fault. Having a large cluster membership before categorizing them as a new fault improves the reliability of the system and yet, increases the time taken to offer users with a valid diagnosis.

Figure 7 shows the overall accuracy of the system in recognizing the testing samples which were previously unseen. Figure 8 shows the overall confusion rate of the system, which indicates the ratio between wrongly classified samples to the total samples. For both figures, n represents the number of samples used for each class during training, and the x-axis shows the dimensionality (D) of the EigenNSS and FisherNSS respectively. From Figure 7 and 8, we see that the system using FisherNSS managed to achieve a higher overall accuracy compared to the EigenNSS for any D transformed signature features and n-values. Any additional features used to construct the transformed signature only add a marginal performance gain. Noting that the original NSS contained 460 features, these results show a successful dimensionality reduction of 96.74%. Figure 7 shows that as the number of samples used for training increases, the system performance improves to a saturation limit. The overall accuracy gap between both EigenNSS-ED and FisherNSS-ED systems become closer as the number of training samples increases. Most importantly, the FisherNSS-ED system performs better than the EigenNSS-ED system when lesser numbers of training samples are used. This improvement is explained by adding to the system, and retraining with, correctly classified test samples. An overall accuracy of 80% and 20% confusion rate was achieved using EigenNSS with n=25 samples per class and D=15 reduced features for the 17 class system. Using FisherNSS, an overall accuracy of 97% and 3% confusion rate was achieved. FisherNSS is deemed to be the better system due to the fact that it requires lesser number of training samples to obtain a higher overall accuracy.

Table III summarizes the performance of the 17 classes used in our system. Metrics used in the table are as follows:

1) True-Positive Rate (TPR): Members of class X correctly classified as belonging to class X.
2) False-Positive Rate (FPR): Members of other classes incorrectly classified as belonging to class X.
3) True-Negative Rate (TNR): Members of class X incorrectly classified as belonging to other classes.
4) False-Negative Rate (FNR): Members of class X incorrectly classified as not belonging to class X.

Table III also shows that, all different types of faults can be uniquely identified independently with high-level of accuracy as suggested by high TPR and TNR. For example, faults CF6, CF7, CF12, CF13, CF14, and CF15 using both EigenNSS and FisherNSS have high TPR of about 90% and above. Most of the faults show a low FPR and FNR which indicates that the classifier has a low false detection rate.

Faults that were kept unknown to the system such as CF2, CF8, CF10, and CF17 only have a slightly smaller

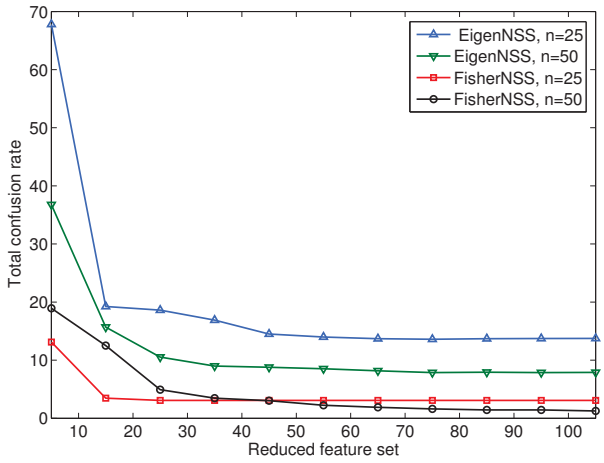


Figure 8. Overall confusion rate of the diagnostic system against dimensionality (D) of the reduced signatures for different per-class training dataset size (n).

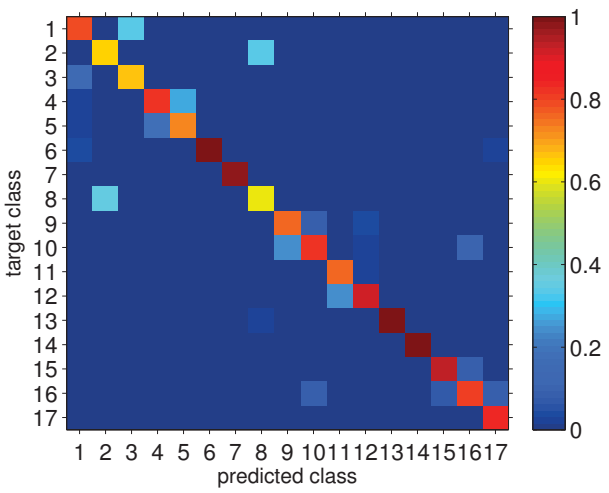


Figure 9. Confusion matrix for the 17 classes in EigenNSS-based diagnostic system.

TPR compared to other faults. This shows that the system has a high detection accuracy of unknown faults.

When EigenNSS are used, some of the faults such as CF1, CF2, CF3, CF5, CF8, CF9, and CF11 have relatively low TPR which makes them less likely to be correctly classified belonging to its respective class. However in some fault cases such as CF6, CF7, CF13, and CF15, EigenNSS has a better TPR than FisherNSS.

Figures 9 and 10 show the confusion matrix of the EigenNSS-based and FisherNSS-based system respectively. A confusion matrix is a typical form of visualization to observe the performance of an algorithm, in this case, the multiclass classifiers. The rows represent target or expected (actual) classes and the columns represent the predicted classes. The diagonal elements of the matrix represent the correct classifications whereas the other indices represent the incorrect instances. The ratio of each instance is color coded for better visualization. In Figure 10, the FisherNSS-based system manages to successfully avoid large misclassifications, satisfying a primary requirement of the system. However, Figure 9 shows a poorer performance due to the greater chance of misclassifications between classes for the EigenNSS-based system.

The proposed FisherNSS-based Euclidean distance classifier system (FisherNSS-ED) and the previously introduced systems (EigenNSS-ED and NSS-ED) are tested against a Naive Bayes multiclass classifier that used the original NSS data set (NSS-NB). The system is trained with all 17 classes at the beginning using similar training and testing sets of data. Figure 11 compares the overall system accuracy between the 4 systems, where the x-axis represents the number of training samples used. For any given number of training samples used, the figure shows that both EigenNSS-ED and FisherNSS-ED systems perform much better than the NSS-ED and NSS-NB systems. This is due to "over fitting" of classifiers used in the 460 feature NSSs, leading to degraded performance.

Fault	TPR		FPR		TNR		FNR	
	EigenNSS	FisherNSS	EigenNSS	FisherNSS	EigenNSS	FisherNSS	EigenNSS	FisherNSS
CF1	78.3	90.6	21.7	9.4	96.6	99.3	3.4	0.7
CF2	65.0	92.3	35.0	7.7	97.8	99.9	2.2	0.1
CF3	66.5	89.1	33.5	10.9	99.1	99.2	0.9	0.8
CF4	82.1	99.0	17.9	1.0	97.5	99.3	2.5	0.7
CF5	72.8	91.9	27.2	8.1	98.7	99.9	1.3	0.1
CF6	100	99.7	0	0.3	99.7	99.9	0.3	0.1
CF7	97.1	95.5	2.9	4.5	99.9	100.0	0.1	0.0
CF8	60.9	98.5	39.1	1.5	97.6	99.4	2.4	0.6
CF9	75.4	97.1	24.6	2.9	99.3	100.0	0.7	0.0
CF10	82.0	100	18.0	0	97.8	99.9	2.2	0.1
CF11	75.4	100	24.6	0	99.9	99.8	0.1	0.2
CF12	92.0	95.1	8.0	4.9	98.1	99.9	1.9	0.1
CF13	99.1	98.9	0.9	1.1	99.9	99.8	0.1	0.2
CF14	100	100	0	0	100	100.0	0	0.0
CF15	93.5	90.8	6.5	9.2	99.5	99.8	0.50	0.2
CF16	80.8	91.9	19.2	8.1	98.9	99.6	1.1	0.4
CF17	83.6	99.4	16.4	0.6	99.9	99.7	0.1	0.3

TABLE III.
PER-CLASS ESTIMATION PERFORMANCE OF THE EIGENNSS AND FISHERNSS BASED DIAGNOSTIC SYSTEMS AT $D = 15$ AND $n = 25$

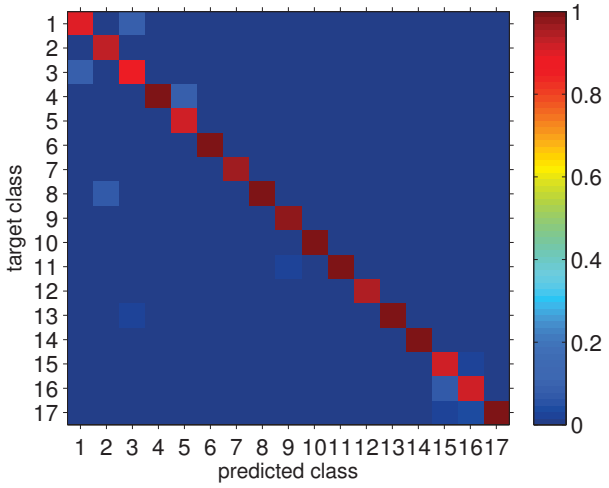


Figure 10. Confusion matrix for the 17 classes in FisherNSS-based diagnostic system.

Another important performance criteria for a system with iterative training process is the time taken to train the system and evaluate a new sample (diagnosis). We included this into the experiment to compare how both the total training time and a single diagnosis time vary with training samples per class for the previously mentioned classifiers. The NSS-NB classifier requires a much longer training time compared to the other classifiers as justified in Figure 12. The training time for the EigenNSS-ED classifier (24 ms-435 ms) is faster than the FisherNSS-ED classifier (33 ms-365 ms) when $n = 10 - 200$. Since both the training times are in the order of milliseconds, this suggests that iterative training does not impact the practical usability of either the EigenNSS-ED and FisherNSS-ED systems. The diagnosis time for a FisherNSS sample is in the order of microseconds (4 μs-59 μs), which is significantly faster than the other types of signatures, despite the fact that FisherNSS calculation involves more steps. This is followed by the EigenNSS-ED system which have a diagnosis time of about 4 μs-66 μs. This shows that both systems are not limited to an on-demand diagnosis, but could also be considered for "real-time" diagnosis applications. Real-time applications are often required to provide guaranteed response within a strict time constraint, usually in the order of milliseconds and sometimes even microseconds.

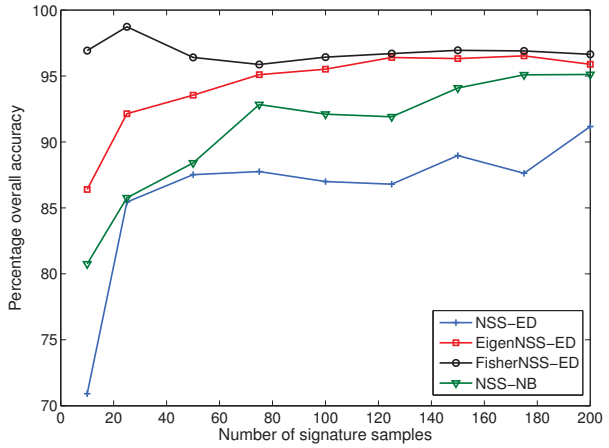


Figure 11. Comparison of overall accuracies of diagnostic systems.

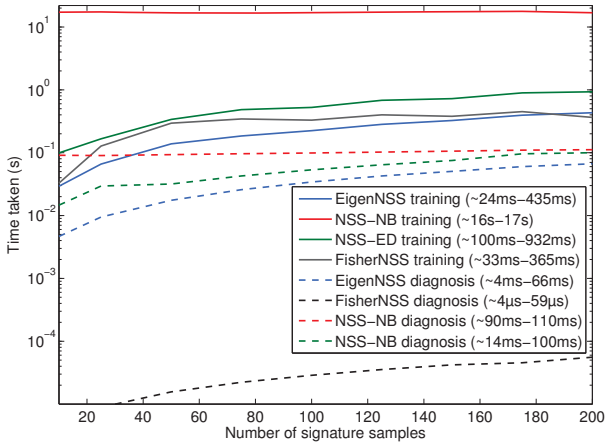


Figure 12. Training and single sample diagnosis time variations against increasing training dataset size for classifiers.

VIII. Conclusions

We have proposed and evaluated an automated UD soft-failure diagnostic system based on a single multi-class classifier design. The system is capable of diagnosing known and unknown faults by combining both supervised and unsupervised machine learning (ML) techniques. We have also presented another signature transformation technique to reduce the dimensionality of NSSs and also to remove network inconsistencies (unwanted information) from EigenNSS. This new transformed signature, FisherNSS aims to maximize the ratio of the between-class scatter matrix to the within-class scatter matrix to improve the classification process.

The system was evaluated by diagnosing 17 UD faults collected over a live campus network, achieving an overall accuracy of up to 97% using FisherNSS. When using FisherNSS, faults such as CF4, CF6, CF7, CF8, CF9, CF10, CF11, CF12, CF13, CF14, and CF17 have a high True Positive Rate of about 95% and above. We have also achieved a dimensionality reduction of 96.74% and low confusion rate between classes. Although the EigenNSS classifier have the shortest training time of about 24 ms-435 ms, the FisherNSS classifier is only marginally slower at about 33 ms-365 ms. Most importantly, FisherNSS samples have the shortest diagnosis time, in the order of microseconds of about 4 μs-66 μs compared to all the other types of samples.

This work provides the foundation to extend the system to a more sophisticated network environment with thousands of users, diverse client platforms and complex traffic patterns.

References

[1] S. Sundaresan, W. de Donato, and N. Feamster, "Broadband Internet Performance: A View From the Gateway,"

SIGCOMM Comput. Commun. Rev., vol. 41, no. 4, pp. 134–145, Aug. 2011.

[2] R. Maxion and F. Feather, "A Case Study of Ethernet Anomalies in a Distributed Computing Environment," *IEEE Trans. Rel.*, vol. 39, no. 4, pp. 433 –443, Oct. 1990.

[3] M. Mathis, J. Heffner, and R. Reddy, "Web100: Extended TCP Instrumentation for Research, Education and Diagnosis," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 3, pp. 69–79, 2003.

[4] S. Shalunov and R. Carlson, "Detecting Duplex Mismatch on Ethernet," in *Proceedings of PAM 05*. Boston, MA: Springer-Verlag, Berlin, Oct. 2005, pp. 135–148.

[5] C. Callegari, S. Giordano, M. Pagano, and T. Pepe, "Behavior Analysis of TCP Linux Variants," *Comput. Netw.*, vol. 56, no. 1, pp. 462–476, Jan. 2012.

[6] M. Thottan and C. Ji, "Anomaly Detection in IP Networks," *IEEE Trans. Signal Process.*, vol. 51, no. 8, pp. 2191–2204, 2003.

[7] T. J. Hacker, B. D. Athey, and J. Sommerfield, "Experiences Using Web100 for End-to-end Network Performance Tuning," in *Proceedings of the 4th Visible Human Project Conference*, Nov. 2002.

[8] C. Widanapathirana, Y. A. Şekercioğlu, M. Ivanovich, P. Fitzpatrick, and J. Li, "Automated Inference System for End-To-End Diagnosis of Network Performance Issues in Client-Terminal Devices," *Int. Jour. of Comput. Netw. & Comm. (IJCNC)*, vol. 4, no. 3, pp. 37–56, 2012.

[9] C. Widanapathirana, J. Li, Y. A. Şekercioğlu, M. Ivanovich, and P. Fitzpatrick, "Intelligent Automated Diagnosis of Client Device Bottlenecks in Private Clouds," in *Proceedings of IEEE UCC 11*. Melbourne, Australia: IEEE, New York, Dec. 2011, pp. 261 –266.

[10] P. Sterlin, "Overfitting Prevention with Cross-Validation," Master's thesis, University Pierre and Marie Curie (Paris VI), Paris, France, 2007.

[11] S. L. Chiu, "Fuzzy model identification based on cluster estimation," *Journal of intelligent and Fuzzy systems*, vol. 2, no. 3, pp. 267–278, 1994.

[12] J. C. Bezdek, "Fuzzy mathematics in pattern classification," *PhD Dissertion, Applied mathematics center, Cornell University*, 1973.

[13] C. Widanapathirana, J. Li, M. Ivanovich, P. Fitzpatrick, and A. Sekercioglu, "Automated diagnosis of known and unknown Soft-Failure in user devices using transformed signatures and single classifier architecture," in *38th Annual IEEE Conference on Local Computer Networks (LCN 2013)*, Sydney, Australia, Oct. 2013.

[14] C. Widanapathirana, J. C. Li, M. V. Ivanovich, P. G. Fitzpatrick, and Y. A. Şekercioğlu, "Adaptive Statistical Signatures of Network Soft-Failures in User Devices," *The Computer Journal*, p. bxt079, 2013.

[15] P. Belhumeur, J. Hespanha, and D. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 711–720, 1997.

[16] M. Roughan, S. Sen, O. Spatscheck, and N. Duffield, "Class-of-Service Mapping for QoS: A Statistical Signature-based Approach to IP Traffic Classification," in *Proceedings of SIGCOMM IMC 04*. Taormina, Italy: ACM, New York, Oct. 2004, pp. 135–148.

[17] B. Zhang, J. Yang, J. Wu, and Z. Wang, "MBST: Detecting Packet-Level Traffic Anomalies by Feature Stability," Comp. J., Advance Access, published January 5, 2012, Oxford, UK, 2012.

[18] T. Kihara, N. Tateishi, and S. Seto, "Evaluation of Network Fault-detection Method Based on Anomaly Detection With Matrix Eigenvector," in *Proceedings of APNOMS 11*. Taipei, Taiwan: IEEE, New York, Sep. 2011, pp. 1 –7.

[19] H. Hajji, "Statistical Analysis of Network Traffic for Adaptive Faults Detection," *Trans. Neur. Netw.*, vol. 16, no. 5, pp. 1053–1063, Sep. 2005. [Online]. Available: http://dx.doi.org/10.1109/TNN.2005.853414

[20] B. Aggarwal, R. Bhagwan, and T. Das, "NetPrints: Diagnosing Home Network Misconfigurations Using Shared Knowledge," in *Proceedings of USENIX NSDI 09*. Boston, Massachusetts: USENIX Association, CA, USA, Apr. 2009, pp. 349–364.

[21] T. Reidemeister, M. Jiang, and P. Ward, "Mining Unstructured Log Files for Recurrent Fault Diagnosis," in *Proceedings of IM 11*. Dublin, Ireland: IEEE/IFIP, New York, May 2011, pp. 377 –384.

[22] S. Lee and H. S. Kim, "End-user perspectives of internet connectivity problems," *Comput. Netw.*, vol. 56, no. 6, pp. 1710–1722, Apr. 2012. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2012.01.009

[23] H. Dahmouni, S. Vaton, and D. Rossé, "A Markovian Signature-Based Approach to IP Traffic Classification," in *Proceedings of MineNet 07*. San Diego, California, USA: ACM, New York, 2007, pp. 29–34.

[24] C. Manikopoulos and S. Papavassiliou, "Network Intrusion and Fault Detection: A Statistical Anomaly Approach," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 76 – 82, Oct. 2002.

[25] M. Wolfgang, *Host Discovery with nmap*, nmap.org, Palo Alto, CA, USA, Nov. 2002.

[26] J. V. Gomes, P. R. Incio, M. Pereira, M. M. Freire, and P. P. Monteiro, "Exploring Behavioral Patterns Through Entropy in Multimedia Peer-to-Peer Traffic," *Comp. J.*, vol. 55, no. 6, pp. 740–755, 2012.

[27] Z. Chen, Y. Zhang, Z. Chen, and A. Delis, "A Digest and Pattern Matching-Based Intrusion Detection Engine," *Comp. J.*, vol. 52, no. 6, pp. 699–723, Aug. 2009.

[28] R. Vaarandi, "A Data Clustering Algorithm for Mining Patterns from Event Logs," in *IP Operations and Management, 2003.(IPOM 2003). 3rd IEEE Workshop on*. IEEE, 2003, pp. 119–126.

[29] J. Yang and J.-y. Yang, "Why can lda be performed in pca transformed space?" *Pattern recognition*, vol. 36, no. 2, pp. 563–566, 2003.

[30] G. Donato, M. S. Bartlett, J. C. Hager, P. Ekman, and T. J. Sejnowski, "Classifying facial actions," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 21, no. 10, pp. 974–989, 1999.

[31] C. Widanapathirana, J. Li, M. Ivanovich, P. Fitzpatrick, and Y. Şekercioğlu, "Adaptive Signatures of Soft-Failures in End-User Devices Using Aggregated TCP Statistics," in *Proceedings of IEEE/IFIP IM 13*. Ghent, Belgium: IEEE, New York, May 2013.

Chathuranga H. Widanapathirana is a Ph.D candidate in the Department of Electrical and Computer Systems Engineering at Monash University, Melbourne, Australia. He is also a data scientist working at Open Universities Australia specializing in analytics and big data. He received his B.Eng degree in Electronics with a major in Telecommunication Engineering at Multimedia University (MMU), Malaysia in 2009. His research interests include distributed cooperative networks, automated machine learning systems, data driven intelligent systems and end-user self-diagnostic services in multiuser networks.

X. Ang received the B.E degree in 2013 from Monash University and now studying towards a postgraduate degree in Electrical Engineering at the Department of Electrical and Computer Systems Engineering at Monash University, Melbourne, Australia

Jonathan C. Li received the B.E.in electrical and Electronic Engineering in 2001, B.Sc. degree in Computer Science and Information Technology Systems in 1999 from the University of Western Australia, and Ph.D. in Telecommunication from the University of Melbourne in 2010. He is currently a member of the academic staff at the Department of Electrical and Computer Systems Engineering of Monash University, Melbourne, Australia. His research interests are optical performance monitoring, routing in all-optical networks, network simulation and modeling, and Wireless TCP/IP optimization.

Milosh V. Ivanovich fills the role of Senior Emerging Technology Specialist within the Chief Technology Office of Telstra, and is an Honorary Research Fellow at Melbourne and Monash Universities in Australia. A Senior Member of IEEE, Milosh's interests lie in queuing theory, teletraffic modeling, performance analysis of wireless networks, and the study and enhancement of TCP/IP in hybrid fixed/wireless environments. Milosh obtained a B.E. (1st class Hons.) in Electrical and Computer Systems Engineering (1995), a Master of Computing (1996) and a Ph.D. in Information Technology (1998), all at Monash University.

Paul G. Fitzpatrick completed his Bachelor Degree in Electrical Engineering at Caulfield Institute of Technology, Melbourne in 1979 and his PhD in Electrical Engineering at Swinburne University, Melbourne in 1997 in the teletraffic performance of hierarchical wireless networks. Paul has over 30 years of experience working in the telecommunications industry and academia, including 15 years at Telstra Research Laboratories working on 2G, 3G and 4G wireless networks. His research interests focus on teletraffic modeling, quality of service, TCP performance modeling and analysis of telecommunication networks

Y. Ahmet Şekercioğlu is a member of the academic staff at the Department of Electrical and Computer Systems Engineering of Monash University, Melbourne, Australia. He has completed his Ph.D. degree at Swinburne University of Technology, and B.Sc., M.Sc. degrees at Middle East Technical University, Ankara, Turkey. He has lectured at Swinburne University of Technology, Melbourne, Australia for 8 years. His recent research interests are distributed algorithms for self-organization in wireless networks, application of intelligent techniques for multiservice networks as complex, distributed systems.

e-ONE:Enhanced ONE for Simulating Challenged Network Scenarios

Sujoy Saha[a], Rohit Verma[b], Somir Saika[a], Partha Sarathi Paul[b], Subrata Nandi[b]
[a] Department of Computer Applications, National Institute of Technology, Durgapur 713209, India
Email: {sujoy.ju, somirsaikia}@gmail.com
[b] Department of Computer Science & Engineering, National Institute of Technology, Durgapur 713209, India
Email: {rohitverma.kgp, mtc0113, subrata.nandi}@gmail.com

***Abstract*— Delay Tolerant Network (DTN) empowers sparse mobile ad-hoc networks and other challenged network environments, such as interplanetary communication network or deep sea communication network, where traditional networking protocols either fail to work completely or do not work well. The Opportunistic Networking Environment (ONE) Simulator has gained considerable popularity as an efficient tool for validating and analysing DTN routing and application protocols. It provides options for creating different mobility models and routing strategies as per the users' requirements. Nowadays, challenged networks such as rural internet connection, social networks, post-disaster communication systems, etc. use DTN along with some hybrid infrastructure networks. Incorporating such real life network systems in ONE needs extensive modification of the same. In this paper, we present the enhanced ONE (e-ONE) simulator as an extension of ONE to facilitate simulation of challenged networks and describe the enhancements we have added to the ONE. As a case study, we consider a challenged network, which we call a latency aware 4-tier planned hybrid architecture designed for post-disaster management. We describe, in detail, how this enhanced version of the ONE simulator is useful in analysis and evaluation of the scenario considered.**

***Index Terms*— e-ONE Simulator, Delay Tolerant Network, ONE Simulator, Ad Hoc Hybrid Network, Post Disaster Management**

I. Introduction

Delay Tolerant Networking (DTN) aims at partially supporting an architecture with heterogeneous networks where there is a lack of continuous network connectivity. The adaptation of the Interplanetary Internet (IPN) ideas to terrestrial networks led to the birth of Delay Tolerant Networking [1]. Since then, there has been a considerable amount of research in this field by several groups around the globe. The concept has been well utilized for Interplanetary Communication and Deep Sea Communication. Current Internet protocols (i.e., the TCP/IP protocol stack) suffer and sometimes fail under such testing conditions; so we require a different category of network (routing) and transport layer protocols, which are tailor-made for challenged environments.

In recent times, researchers have focused on the use of DTN in challenged networks, where nodes is sparse, which results in an intermittent connectivity [2][3][4], and where only low end devices are available. Such network

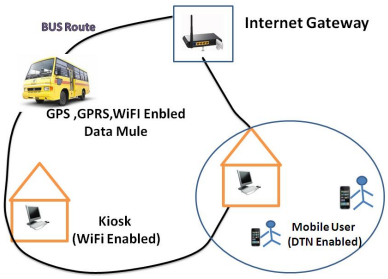


Figure 1. Low Cost Rural Internet Communication System

systems use, in addition to DTN, infrastructure networks comprising cellular networks, satellite communication systems, mesh networks etc. Examples include (i) heterogeneous architecture to provide low cost Internet service [5] and reliable connectivity to rural kiosks, using buses and cars as mechanical back-haul, [Figure 1] to ferry data to and from kiosks; (ii) hybrid architecture with different available technologies for post-disaster communication system [Figure 2] [6][7]; (iii) Twitter applications used in disaster mode relies on opportunistic communication and epidemic routing of tweets from phone to phone [8]. The tweets are transferred to the outside world when some pockets of network are eventually detected by the smart phones.

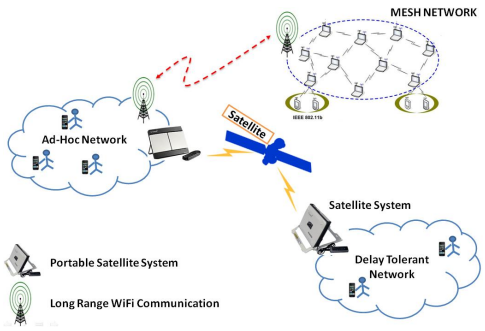


Figure 2. Hybrid Network for Post Disaster Management

All the above challenged network scenarios use hybrid network resources such as opportunistic/delay tolerant network at bottommost tier, some infrastructure based network, either through data mules (e.g bus,

doi:10.4304/jnw.9.12.3290-3304

ambulance, boat,UAV etc.) as mechanical back-haul or through MESH networks at middle tier, and long range WiFi/WiMax or satellite phone communication at topmost tier.

A. Objective

The objective in this paper is to identify what needs to be done on the ONE simulator, which is developed explicitly for DTN protocol evaluation, so that it can be used to simulate, analyse and evaluate above mentioned real-world challenged network scenarios. Furthermore, the identified changes need to be incorporated into the existing ONE simulator in order to extend it to the enhanced ONE simulator.

Simulation tools for DTN protocol evaluation are not available in abundance. The only simulators available for evaluation of DTN are the ONE Simulator [9] and DTNSim2 [10], the latter being based on the DTNSim. All these simulators have been developed in Java using object oriented characteristics. The Opportunistic Network Simulator (ONE) is a widely used simulator for DTN protocol evaluation. It has numerous in-built features to enhance its expertise. It supports (i) different routing algorithms such as Epidemic routing [11], Prophet routing [12], Spray and Wait routing [13], Spray and Focus routing [14], MaxProp routing [15] etc.; (ii) different mobility models such as Random Waypoint model, Random Walk model, Shortest Path Map Based model and so on. In addition to these, there is a provision for applying real-life mobility traces in the form of text file called external movement, which enables the users in ONE to use practical movement scenarios in simulation instead of artificial random simulation. (iii) Nice visualization tool and GUI is available to set the simulation parameters (dynamically in some cases) and to observe the simulation progress, with user-friendly graphical representation. (iv) It is an open source package, providing the flexibility to modify different modules according to specific requirements. (v) Every new release of ONE adds some new routing algorithms and mobility models; several new features have been added by the community working with ONE. (vi) ONE also provides several metrics to analyse simulations, like latency, packet delivery probability, overhead, etc., which are echoed in the form of report files. Map of any location can also be used as the play field for simulations and the the simulation can be designed accordingly. (vii) Extensive documentation of the software makes ONE developer-friendly.

B. Motivation

Although it is quite an effective simulator for DTNs, it still has a lot of ground to cover before being apt for the real world challenged network scenarios in general. It requires several major modifications to different modules in order to work with more realistic scenarios. The mobility of nodes needs to be modified in order to match with the real world requirements, such as group mobility, different types of path based movements, etc. There is a lack of several heterogeneous/smart interfaces, which need to be incorporated for further enhancement, such as the satellite phone interface and other infrastructure supporting nodes like long range WiFi, Mesh etc. These are essential for ONE to be compatible with a real-world challenged network system. Heterogeneous communication resources may yield a hybrid type of network in order to achieve better performance. Moreover, such enhancement would require inclusion of hybrid application-specific routing strategies, since different resources use different technologies to work.

In section 2, we have described the basic model of the ONE simulator and how it has been modified in the e-ONE. Also, we explain how the simulator has been customized as outlined. Section 3 presents a case study of a hybrid network and how e-ONE has been instrumental in analysing, evaluating and shaping it. In section 4, we have concluded the paper with directions for future research.

II. Customization of ONE simulator

Incorporating real world hybrid architecture in the simulator requires customization of most of the modules of ONE. Here, we discuss the major modifications incorporated in the simulator to develop e-ONE. These modifications include modification of the Cluster Movement Model, restricting the epidemic routing algorithm, making the nodes more intelligent and developing new modules for special types of communication. But a hybrid network would require more realistic mobility models, along with certain modifications in the routing strategies. Above all, it would require other types of nodes which operate on the principle of infrastructure based network. These modifications have been shown in Figure 3, which depicts a model of e-ONE simulator.

Novelty of e-ONE over ONE in terms of challenged network applications can be listed as follows:

- Mobility during and after any disaster is quite different from that in a normal scenario. Broken paths, destroyed bridges, scarcity of infrastructure networks restricts the movement of rescue personnels. In Mobility Model subsection, we introduced Postoffice Cluster Movement model that may fit in this scenario.
- Routing strategies for DTNs is different from that of infrastructure-based networks. But a hybrid network uses both types of network at different tiers. There are multiple categories of nodes existent in the network, and a node has to decide which node it will forward its packets to. The Routing Strategy subsection deals with this problem.
- At some tier we may use NLOS devices, which are layer 2 devices, for which it cannot operate in an interconnection which contain loops. So one needs

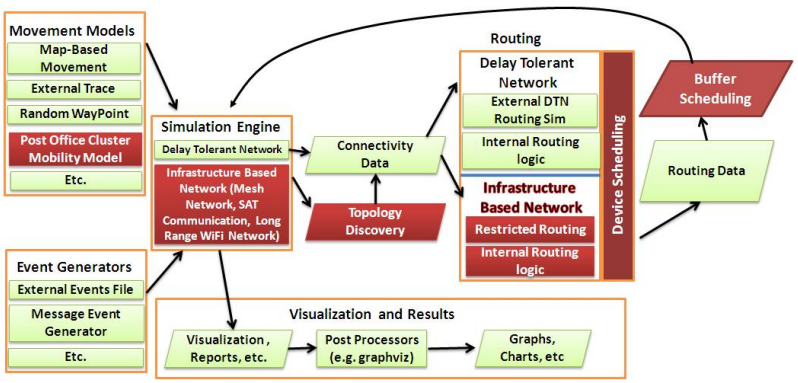


Figure 3. Existing ONE modules (in green) & added e-ONE modules (in red)

to implement a spanning tree algorithm, so that these devices can function.

- Since different types of networking devices are used, there exists the question of priorities for different nodes. In Device Scheduling subsection, we highlighted these priority scheduling of versatile types of networking devices used in our hybrid network.
- DTN nodes are accustomed in dealing with multiple copies of the same packet, which infrastructure-based networks are not. So suitable buffer scheduling is required for this.
- Depending on availability we may use sophisticated devices like satellite phones. So new interface modules needs to be implemented for such devices.

The above are our main thrust in upgrading ONE to e-ONE that may be used for simulating hybrid network models in challenged network scenarios.

A. Mobility Model

The ONE simulator has provided us with a wide variety of mobility models to choose from. But none of them exactly matches with post-disaster situation movements. To bridge the gap, we have incorporated *post office cluster movement model (PCM)* as a modification of the Cluster Movement Model [16], and *poisson post office cluster movement model (PPCM)* as a further modification to post office cluster movement model. Algorithm 1 describes PCM and algorithm 2 describes PPCM in details. Both the strategies restricts node to a cluster with a specific range. There can be different clusters of varying range, each having a dedicated set of nodes (DTN nodes) whose movements are restricted to the cluster. This scenario has been shown in Figure 4.1. In either of the model, a specific location within the cluster is marked as the location of dropbox, to which point the nodes within the cluster visit regularly. The dropbox locations usually symbolizes the shelter points in a disaster-affected region, or location of rural kiosks in rural internet scenario.

1) Post office cluster movement model: In this movement model, each node inside the cluster move following a random waypoint movement strategy within the cluster, but it visits the location of dropbox after a fixed number of waypoints (Referred in Algorithm 1), the fixed number being chosen as a random integer between two fixed parameters h_1 and h_2 of the movement model. Figure 4.2 shows this scenario. This approach uses all the attributes and functions of the *ClusterMovementModel* class, with only a slight modification in the *randomCoord* function and a few aiding variables. The new *randomCoord* function keeps track of the number of hops by the host, and automatically sets as its next waypoint (Step 3) the location of the dropbox, when the maximum hop count is reached (Step 2).

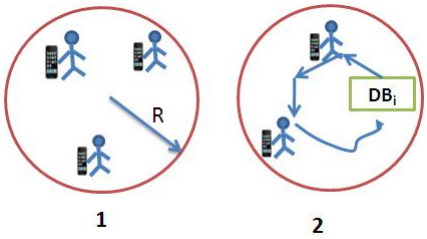


Figure 4. (4.1) Cluster Mobility Model (4.2) Post offfice Cluster Mobility Model

Algorithm 1: PostOfficeClusterMovement

Step 1: set random number of hops from the integer range [h1 , h2], between two consecutive visits within range R.
Step 2:**if** *(number of hops is equal to maximum hops)* **then**
  Step2.1: Bring the node back to center
end
Step 3: **else**
  Step3.1: Set next random coordinate
  Step3.2: Increase the number of hops by 1
  Step3.3: **return** *new coordinate*
end

2) Poisson Post office cluster movement model: In this movement model, inter-arrival times between two consec-

utive visits of a DTN node to the nearest Dropbox follows an exponential distribution. This is a one-parameter movement model in which the parameter λ represents the average inter-arrival time between two consecutive visits (i.e for the exponentially-distributed time gaps) to the dropbox. After generating the next inter-arrival time gap, T_1 say, randomly following the corresponding exponential distribution with parameter λ, Algorithm 2 finds one random waypoint (Say P_1), calculate time from DB to P_1 plus time from P_1 to dropbox (called roundtrip time), and check whether P_1 is reachable or not within T_1. If P_1 is found to be reachable, then the node moves to P_1, generate next random waypoint, P_2 say (Step 9.1, 9.2 and 9.4) and check the time from dropbox to P_1 plus time from P_1 to P_2 plus time from P_2 to dropbox is within T_1 or not. If reachable, then the node moves to P_2 and generate the next waypoint P_3, and so on. If one randomly generated waypoint P_i is found unreachable, then the corresponding point is regenerated and the same process is repeated. When the remaining time for returning the dropbox is too less (less than a threshold value T_{Th}, say) then it simply selects the dropbox as its next waypoint, returns the dropbox, and start the next iteration by generating the next inter-arrival time T_2, say.

Algorithm 2: PoissonPostOfficeClusterMovement

Step 1: Generate Next Poisson Number $T_{poisson}$.
Step 2: P $\leftarrow$ P_{DB} ; //Intial location of DTN node; Start from nearest DB
Step 3: Total $\leftarrow$ $Total_1 \leftarrow 0$;
Step 4: Generate new point P_1 , new velocity V_1 , new pause time T_{pause} .
//Time taken form point P to P_1
Step 5: T_{P,P_1} $\leftarrow$ Distance$(P, P_1)/V_1$;
Step 6: $T_{P_1,P_{DB}}$ $\leftarrow$ Distance$(P_1, P_{DB})/V_{Max}$;
Step 7: $Total_1 \leftarrow Total_1$ + T_{P,P_1} + Tpause ;
Step 8: Total $\leftarrow$ $Total_1$ + $T_{P_1,P_{DB}}$;
Step 9: **if** *(Total* $< T_{poisson}$*)* **then**
  Step 9.1: Move to P_1 with velocity V_1 and wait for pause time T_{pause} ;
  Step 9.2: P $\leftarrow$ P_1 ;
  Step 9.3: **if** *(Total* + $T_{Th} \geq T_{poisson}$*)* **then**
    Step 9.3.1: V_{next} $\leftarrow$ Distance(P_1,P_{DB})/ ($T_{poisson}$ - $Total_1$);
    Step 9.3.2: Return P_{DB} with speed V_{next} and wait for some Pause Time;
    Step 9.3.3: Go to Step 1;
  Step 9.4: **else**
    Go to Step 4 ;

B. Routing Strategy

We have devised a strategy to restrict flooding in the epidemic routing algorithm. The basic algorithm ensures that the message is flooded to all nodes in range of the host node. In our strategy, message is not relayed to those nodes which have already received the message. While this requires additional checks to determine if a node in range has already received a particular message, this ensures that flooding is limited.

Furthermore, rather than treating the entire network like a set of homogeneous nodes, we have divided the network into several entities. Messages from a particular entity are only allowed to be relayed to a sub-set of all other entities, to make communication more meaningful. For example, a message for the head office in a local office would only be relayed to someone having access to the head office and not to someone in the local office.

The desired constraints were met by modifying the *startTransfer* function and adding the boolean function *shouldSendMessage* for each stage, which checked the above constraints and returned true or false as per the algorithm.

The *shouldSendMessage* function is application-specific, and hence the modified routing strategy would depend on the context in which the user is using the simulator. As we have used the *PostOfficeClusterMovement*, let us take an example of a set of clusters, with a set of carrier nodes, denoted CN, between them. Let there be some control points in each cluster, known as CP, where the information dropbox(DB)/Postbox is placed. So the CNs would move between these clusters to collect and relay inter-cluster messages from the DB of the cluster. In this scenario, the DB must only relay a message to to specific CN which is moving towards the destination cluster (Step 2). If CNs are in the range of contact then one CN deliver the message to that CN which is towards the destination (Step 3). Algorithm 3 depicts the pseudo-code for this scenario.

C. Topology Discovery for Infrastructure Nodes with Fault detection and Recovery

As Long Range WiFi Communication(LWC) devices are layer - 2 devices (TCP/IP Protocol Stack), they lack in intelligence of alternate route discovery and thus existence of loops in the network may hang the whole communication system. To avoid such unwanted behaviour, a spanning tree formation is mandatory in the network.

Set of LWC devices forms the vertex set of the LWC graph (Referred in Algorithm 4). The vertices in the graph is connected by an edge if the corresponding LWCs are in the range. Vertex (S) is predefined starting vertex.

Initially, we start with an empty set of processed nodes $Processed$ and an empty queue Q.

Vertex S will be added to $Processed$ (Step 2) and in queue Q. Similar iterations will be carried out on other vertices until Q is empty. In each iteration, we delete an element X (Step 3.1) from Q and add all the nodes Y adjacent to X which has not been inserted to Q (Step 3.2), edge (X,Y) will also be added to the output graph H. When Q is empty, acyclic network of LWC devices is found in H, which is suitable for our purpose (Step 3).

Algorithm 3: Routing Strategy

Input: *Message m, Node Receiver_Node*
Step 1: Here, ***CN*** is the Carrier Node which moves among some Dropboxes (***DBs***); m is the message to be relayed currently in possession of host_node, and Receiver_Node is the node with which the host_node comes in contact with.
Step 2: **if** *(host_node is DB and Receiver_Node is CN)* **then**
  Step 2.1: **if** *(CN confirms DB to visits desired destination)* **then**
    Step 2.1.1: DB Transmit Packet to that particular CN.
  end
  Step2.2**else**
    Step 2.2.1: No Transmission of Packet
  end
end
Step 3: **else if** *(host_node and Receiver_Node both are CN type)* **then**
  Step3.1: **if** *(Receiver_Node is bounded towards the desired destination)* **then**
    Step3.1.1: Transmit Packet to that particular CN.
  end
  Step3.2: **else**
    Step3.2.2: No Transmission of Packet
  end
end

Algorithm 4: Topology Discovery Algorithm

Input: *Graph G(V,E) the graph network formed by the LWC devices where the Vertices are the LWC Devices and Edges represent devices in range, S : a Starting Station*
Step 1 : Processed = ϕ // a set of nodes which have been processed
  Q // an empty queue
  H // an empty graph
Step 2 : Add S to Processed
  Q.insert(S)
Step 3 : while *(Q is not empty)* **do**
  Step 3.1 : X = Q.delete()
  Step 3.2 : for *(all nodes Y which is Adjacent to X and not in Processed)* **do**
    Step 3.2.1 : add Y to Processed and Q.enqueue(Y)
    Step 3.2.2 : insert edge (X,Y) to graph H
  end
end
Step 5: Output: Graph H : the acyclic network of LWC devices (tree network)

The nodes periodically check the status of the nodes in their list with the help of *beacon* messages. If a node is found to be *down* (Step 1 of Algorithm 5), it is removed from the host's list and added to a temporary list. This

Algorithm 5: Fault Detection & Recovery

Input: *Connection C, Graph G*
Connection C is connection between two LWCs and Graph G(V,E) the graph network formed by the LWC Devices and Edges represent devices in range
Step 1: **if** *(Connection is Down in between two LWCs)* **then**
  Step 1.1: X=get first host of connection C
  Step 1.2: Y=get another host of connection C
  Step 1.3: **if** *(there is an edge between X & Y in Graph G)* **then**
    Step 1.3.1: Delete edge (X,Y) from graph G
    Step 1.3.2: Call Topology Discovery Algorithm on this new updated Graph G
  end
end
Step 2: **else**
  Step 2.1: **if** *(Connection* $< X, Y >$ *is up Between two LWCs)* **then**
    Step 2.1.1: **if** *(there is no edge between X & Y in Graph G)* **then**
      Step 2.1.1: Insert edge (X,Y) to graph G
      Step 2.1.2: Call Topology Discovery Algorithm on this new updated Graph G
    end
  end
end

list stores the node till it again becomes *active* (Step 2), which is again detected with the help of *beacon* messages. In the meantime, a new topology is followed for the nodes which are given by the algorithms 4 and 5.

D. Device Scheduling

When two types of devices are connected to a common device, a priority value for each type of devices is set by common device and higher priority device should be served first by common device.

Algorithm 6: Device Scheduling: Procedure start-Transfer(Node A , Node X)

L = List of all devices connected to A
for *(all i in L)* **do**
  if *(priority(i) > priority(X))* **then**
    return false;
  end
end
return true;

The routine *Device Scheduling* finds all connected node with device (Referred in Algorithm 6) A based on priority value and selects the highest priority device for packet transmission.

E. Buffer Scheduling

Buffer Scheduling is done by deletion of message from the buffer of the DTN nodes in the cluster, cluster

point/DropBox, carrier nodes and the LWC of the cluster point. These is done when transfer takes place between different types of nodes in the network. Detailed description is provided in Algorithm 7.

Algorithm 7: Buffer Scheduling

Step 1: **if** *(one DTN node encounters with another DTN node of the same cluster)* **then**
  Delete the message by checking their ACK list.
end
Step 2: **if** *(DTN node encounters with Cluster point/DropBox)* **then**
  Delete the message from DTN node after getting its Ack and updates ACk list for that message.
end
Step 3: **if** *(Cluster point/DropBox encounters with carrier node)* **then**
  Delete the message from the Cluster point/DropBox that has been sent to the carrier node and Delete the message also from the carrier node that has been sent to the Cluster point.
end
Step 4: **if** *(Cluster point/DropBox encounters with LWC)* **then**
  Delete the message from the Cluster point/DropBox that has been sent to the LWC.
end
Step 5: **if** *(LWC encounters with LWC(This LWC is towards internet gateway))* **then**
  Delete the message from the LWC that has been sent to the LWC towards the internet gateway.
end

F. Satellite Phone Module

An important aspect of satellite phones is the transfer of acknowledgement messages between nodes. Hence, it became necessary to facilitate acknowledgement messages for satellite phones. Primary DTN routing strategies does not include transfer of acknowledgement messages. This needs the modification in the super class of the *routing* package, i.e. the *MessageRouter* class and also to all the other routing classes.
Another issue is the propagation delay in message transfer through satellite phones. As the geosynchronous satellites are at a distance of about 35,792 km from the Earth, there is always an approximate propagation delay in message transfer which is stated in algorithm 8 and algorithm 9. It can be calculated as follows;

$Distance\ from\ satellite = 35792km$
$Speed\ of\ light = 299762km/sec$
$Hence,\ Time = 35792/299762 = 0.12seconds(approx.)$
$Propagation\ Delay = Uplink\ Time + Downlink\ Time$
$= 0.12 + 0.12 = 0.24seconds$

Algorithm 8: Satellite Module : Propagation Delay

if *(satellite phone)* **then**
  transferDoneTime = SimClock.getTime() + ((1.0*messagesize) / transmitspeed) + (0.24)
end
else
  transferDoneTime = SimClock.getTime() + ((1.0*messagesize) / transmitspeed)
end

Algorithm 9: Satellite Module : Emergency Message

if *(other node in the connection is satellite phone and message is emergency message)* **then**
  Transmission Message to encountered satellite phone
end

This additional delay parameter is required to be included in the simulator for all nodes having satellite phones. This modification requires a change in the code of *CBRConnection* class. The *startTransfer* function in ONE was manipulated by setting the transfer time equal to the above value.
Cost of message transfer is quite high for satellite phones. So only some important messages had to be transferred through the satellite phones. This involved change in the code of *ActiveRouter* class. The restriction that regular messages won't be transferred through satellite phone requires proper implementation of our routing strategies. The *startTrasfer* function was modified to check if the message being relayed through a satellite phone is an emergency message or not. The function returns false for normal messages in case of satellite phone, otherwise follows the normal procedure. Creation of a new event in the simulator for important/emergency messages helps in ensuring this property.

Table I summarises both built-in and incorporated modules and their respective methods with basic functionalities for developing e-ONE simulator.

III. Case Study:Hybrid Network Architecture for Post Disaster Management

In this case study, we describe a latency aware 4-tierd planned hybrid architecture [7][17]. Here, we have used DTN enabled smart phones, DropBoxes which may be high-end smart-phones or laptops, DataMules (e.g Ambulance, Boat etc.) which can move from one place to another and long-range WiFi Communication devices. In the next subsection we explain how we have used e-ONE to represent our communication architecture. Later, we analyze the results of simulations run using this architecture.

TABLE I.
REQUIRED MODIFICATION FOR E-ONE

Modification	Files Modified	Remarks
Mobility Model	PostOfficeCluster Movement.java	Modification of Cluster Movement Model
Routing	ActiveRouter.java: starttransfer(), shouldsendMessage()	Restricted routing is performed for inter cluster
LWC Network formation and message transfer	Graph.java(File added to the package routing) ActiveRouter.java: changedConnection(),startTransfer(), shouldsendMessage()	This is a class to perform basic functionalities of Graph & to form Tree Network. This class contains methods for Graph and Tree network formation inheriting *Graph.java* Restricted routing is performed based on Tree information.
Fault Detection and Recovery	Graph.java ActiveRouter.java: changedConnection()	Faulty node is detected by changedConnection() method. It obtains a new Graph and a tree network respectively.
Device Priority Scheduling	ActiveRouter.java	Higher priority nodes are served prior than lower priority nodes.
Buffer Scheduling	ActiveRouter.java starttransfer() Connnection.java finalizeTransfer()	The node which are recently involve in transfer of message are retrieve from finalize transfer of Connection.java. This is followed updatation and deletion of ACK List and message from the nodes. The function finalizeTransfer() is called by startTransfer() of ActiveRouter.java
Satellite Communication	MessageRouter.java & ActiveRouter.java	Transfer characteristics are implemented in MessageRouter.java, while the deciding a message transfer by ActiveRouter.java.

A. Post Disaster Communication Network Architecture

According to our perspective as shown in Figure 5., there is utilization of the low range and cheaper devices at the bottom layers and we have proceeded towards building the next higher ones with high range and costlier devices when the scenario cannot be handled by the lower layer. It has a fixed MCS to control centralized rescue/relief operations within affected area (AA) consisting of many shelter points (SPs). Rescue personnel within each SP carry smart phones which forms DTNs **[Tier-1]** to exchange information in the form of video clips, images, voice clips, and short text messages among

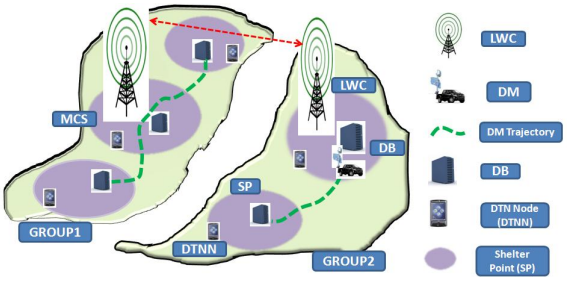


Figure 5. Four Tier hybrid Architecture using DTN Nodes,DBs,DMs and LWCs

themselves & deliver packets periodically to the nearest DB **[Tier-2]** belonging to each SP. As the DTNs formed are sparse, and DBs are far apart, we propose that, vehicles (i.e. boat, ambulance etc.) used by rescue/relief teams are equipped with Wi-Fi and VSAT (for emergency messages) and these act as DataMules (DMs) (mechanical back-hauls) **[Tier-3]** to carry information from DBs to MCS, within desired time L. If AA has a large diameter, deploying a dedicated DM per SP may not meet latency constraints and may also not be a feasible option. Hence we propose a grouping of DBs by using an efficient clustering algorithm. At the center of each such group, one (NLOS/near LOS)long range WiFi communicating device (LWC) **[Tier-4]**, accumulating data from a non-overlapping set of DBs, will be placed.

B. System Model Overview

The SP corresponds to the vertex set, DB signifies the dropbox at each vertex or SP and the pathways among the SP correspond to the edge set of that graph G (V,E) where $V = \{SP_i\}; 1 \leq i \leq m$ and $E = \{E_{ij}|E_{ij}$ is pathway between vertices SP_i & SP_j ; $1 \leq i \leq m$, $1 \leq j \leq m$ *and* $i \neq j\}$. Each vertex DB_i has service time $S_T(DB_i)$. The graph G(V,E) is divided into k sets of groups (*GR*). The vertex set of graph G is partitioned into 2 sets: one is Group Centers (GC) and another is the set of Group Members (GM) where GM =V$-GC$. Let N be total number of data mules deployed and each DM_{ip} has a distinct trajectory $T(DM_{ip})$.Let k LWCs with range R are deployed at each GC_j subject to the following:

$V = GC \bigcup GM$

DB_{ij} = j^{th} DB in i^{th} group $1 \leq i \leq k$ *and* $1 \leq j \leq m$

DM_{ip} = p^{th} DM in i^{th} group $1 \leq i \leq k$ *and* $1 \leq p \leq n$

GC_i = GC of i^{th} group

LWC_i = LWC of i^{th} group

$T(DM_{ip}) \leq$ *Latency*

$Distance(LWC_i, LWC_j) \leq$ R *if* LWC_i and LWC_j are connected.

The information packets have been differentiated into 2 types: (1) Packets generated at the DTN layer and destined to reach MCS (mostly), called *Relief Request Packet* (R_e); (2) Packets generated at MCS intended for DTN-enabled devices, called *Relief Response Packets* (R_s). list of conversion used to model our architecture as shown

in Table II. All these packets need to be delivered within a predefined required latency. Here we present the worst case calculations pertaining to all 4 layers/Tiers for both types of packets, so that we can model the system in such a way that it guarantees 100% packet delivery.

TABLE II.
LIST OF CONVERSION USED TO MODELED THE ARCHITECTURE

Variable Name	Meaning
N	Total DTN nodes surrounded by DB
g	Packet generation rate of Re packes
g'	Packet generation rate of Rs packets
p	Packet size of Re and Rs packets
F_1	Maximum time of DTN node to reach nearest DB
F_2	Time interval between 2 consecutive visits of DM to the particular dropbox DB
F_3	Time interval between two consecutive visits of DM to particular group center GC
L_d	Total load of Re packets
$L_{d'}$	Total load of Rs packets
DR	Data Rate
S_U	setup Time
S_T	Service Time
L	Latency
$E_T(DB_{ij}, DB_{ik})$	Travel Time by a DM from DB_{ij} to DB_{ik} without halting

Worst case latency calculation for Tier-1(T1) and Tier-2(T2): Let DR_{DTN-DB} be the data transfer rate from DTN to DB. $Q(R_e)$ be queuing delay for transfer of R_e packets from any particular DTN to DB and $Q(R_s)$ be queuing delay of R_s packet transfer from DB to DTN which is shown in figure 7,then:

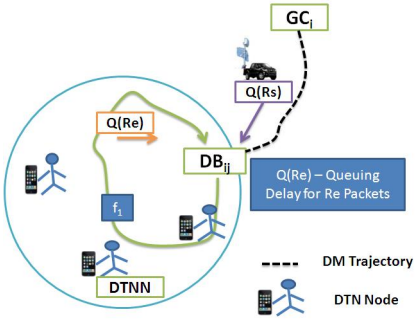


Figure 6. Tier-1 and Tier-2 Latency Calculation

$Q(R_e)$ = $F_1 \times g \times p \times (N-1)/DR_{DTN\_DB}$
$Q(R_s)$ = $L_{d'}(DB_{ij})/DR_{DTN\_DB}$ where $L_{d'}(DB_{ij})$ is total load of Rs packet at DB_{ij} which is calculated in Tier-3.

In Worst case, the 1st generated R_e packet come at the end of waiting queue at DB and it has to wait for other R_e packets from $(N-1)$ DTN nodes to be offloaded at the DB if they come at same time and belongs ahead of 1st R_e packet at queue . Also, packet bears delay because of setup time $S_U(DB_{ij})_{T1-T2}$ required at Dropbox between DTN and DB . Now, total service time required to serve a DTN at a particular DB_{ij} between Tiers 1 & 2 will be:

$S_T(DB_{ij})_{T1-T2}$ =$Q(R_e) + Q(R_s) + S_U(DB_{ij})_{T1-T2}$

Now total service time $S_T(DB_{ij})_{T1-T2}$ is calculated between T_1 and T_2 using $Q(R_e)$, $Q(R_s)$ and $S_U(DB_{ij})_{T1-T2}$.
so L_{T_2} = F_1 + $S_T(DB_{ij})_{T1-T2}$

Worst case latency calculation for Tier-3 (T3): At Tier-3, we consider the traversal of the packets using DMs. Here we assume that our DMs cover the DBs assigned to it in a circular manner as depicted in figure 7. Under such assumption, the DM serves each DB in its paths exactly once in one traversal. We now want to estimate the latency of a packet routed through DB_{ij} to reach GC_i.

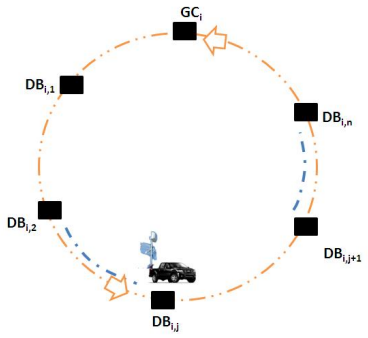


Figure 7. Circular DM Trajectory

At tier-3, the worst case may be a such scenario where a packet comes just immediately after a DM leaves the GC. In that case the packet has to wait almost the whole interval between two consecutive DM arrivals. Let $F_2(DB_{ij})$ be the time interval between 2 consecutive visits of DM_{ip} to the particular dropbox DB_{ij} and F_2 is also different for different DB_{ij}. $F_3(DM_{ip})$ is the time interval between two consecutive visits of DM_{ip} to particular group center GC_i. Let DR_{DB-DM} be the data transfer rate from DB to DM. DTN will dump packets at DB (F_2/F_1) times. Then, Total data accumulated(Load) at dropbox DB_{ij} will be:
$Ld(DB_{ij})$ =$F_2(DB_{ij}) \times g \times p \times N$.

Total data accumulated at dropbox DB_{ij} for Rs packet will be $L_{d'}(DB_{ij})$ = $(F_3(DM_{ip}) \times g' \times p)/m$ where m is the total no of DB in Graph G(V,E). Also, packet at DB suffers delay because of set up time $S_U(DB_{ij})_{L2-L3}$ required at DB_{ij} between DB and DM .
Total latency of Tier 3 should be included with the latency factor of previous layers and the total time of one or more DM visits to each of the DBs with waiting time between two consecutive visits which is basically the service time of other DBs coming into the DM trajectory. Hence, latency of Tier 3 comes as a function of Tier 2 latency, distance of DB from corresponding group center and service time of other DBs of that particular group. We have calculated total

latency (L_3) using $F_2(DB_{ij})$ and $S_T(GC_i)*$. $F_2(DB_{ij})$ varies with the topological structure of the DM trajectory.

In such a case, DM travels in circular fashion, and thus, it serves exactly once in one traversal from GC_i to current node and back to GC_i. Following is the mathematical model of circular trajectory:

$$L_{T_3} = L_{T_2} + F_2(DB_{ij}) + E_T(DB_{ij}, GC_i) + \sum_{j+1}^{1} S_T(DB_{ij})_{T2-T3} + S_T(GC_i)*$$

where

$$F_2(DB_{ij}) = E_T(DB_{ij}, GC_i) + E_T(GC_i, DB_{ij}) + \sum_{k=j}^{n} S_T(DB_{ik})_{T2-T3} + \sum_{k=1}^{j} S_T(DB_{ik})_{T2-T3}$$

Worst case latency calculation for Tier-4 (T4): Previous layers assures that R_e packets have been delivered to GC of all groups. Now,it is the fourth layer that takes care of R_e delivery to MCS. Similarly, Tier-4 also assures R_s packets to be delivered to GC of all groups.Thus, fourth layer modeling deals with latency incurred only due to LWC interconnections. Since LWCs ,being layer 2 network devices ,don't allow loops in the network , we reduce the graph network , where LWCs behave as vertices and connection active between adjacent LWCs behave as Edges, into tree like network based on a suitable heuristic. For now, we consider minimum no of hops count from MCS criterion to decide route to LWC . After topology has been defined for Tier-4 , we need to model it in terms of Latency (12) fulfilling the below mentioned constraints.

Constraints:

(i)At any timestamp, if two LWCs (say LWC_x and LWC_y) have their connections up, then neither LWC_x nor LWC_y can have connection up with any other LWC (say LWC_z) at the same time until and unless connection gets down.

(ii)However, any two LWCs (say LWC_a and LWC_b) other than LWC_x and LWC_y can have connection up at the same time provided that LWC_a and LWC_b are completely non-overlapping to LWC_x and LWC_y.

Given Tier 4 as tree like network with MCS as root and above mentioned constraints , our objective is to deliver Rs packets to GC and Re packets to MCS with minimum latency.Since both types of RELIEF packets use the same network , they affect each other's latency . Thus, we use an optimal strategy that minimizes latency for both types of packets.

C. Data Flow in PDCN using e-ONE Simulator

The fundamental to any planned approach is to design first and to test the performance of the design through some kind of dry run (simulation) before the actual deployment. In our case, we have a disaster-affected area for which two types of map are available to us. One map, which we call the *Path Matrix* for the simulation area, shows the SPs with possible vehicle connections between them. The other map, called the *Aerial Distance Matrix*, shows the SPs with Euclidean distance between them. The main design constraint in a post-disaster network design is the maximum allowed latency for the RELIEF packets. All the things mentioned above with few more relevant informations (shown in the flow diagram: Figure 8) are fed into a process called *Group Formation* which provide us with the complete deployment plan in which the SPs are divided into groups, one or more DMs are allotted to each group, the trajectories to each each DM allotted, the best placement of LWC towers inside each groups and the interconnection between the LWC towers. All the newly obtained group information along with original inputs are fed into our *e-ONE* simulator, which simulates the whole communication process and generate reports. The reports thus obtained are fed into our *Analysis Tool* to study the performance of our deployment plan. If the performance is found to be satisfactory, then it is ready for deployment.

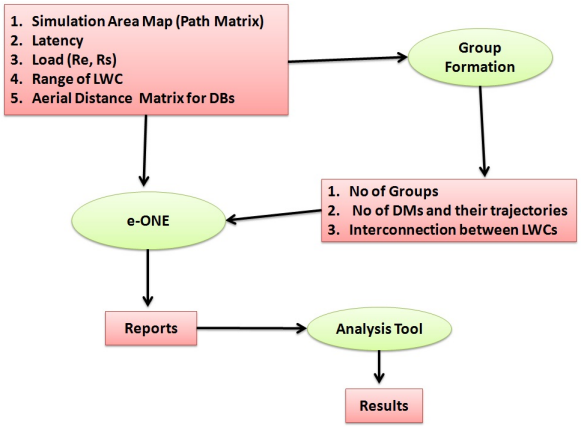


Figure 8. **Data Flow Diagram**

D. Algorithm

What is apparent from the previous subsection is that the group formation is a key step in the design process and the main constraint to this design process is the maximum allowed latency to any RELIEF packet.Now the latency of a packet is sum of the latencies at different tiers. But majority of the latency is observed at Tier 3, where the packets are carried by DMs. So from maximum allowed latency we subtract the maximum possible latencies at other layers to get maximum allowed latency at Tier 3. With this modified latency (L') value we form groups of SPs.

During group formation, we observe that a relief packet suffers maximum latency when it appeared to a DB immediately after the DM leave the DB, in which case the packet has to wait for a time equal to 3 times the the time required to travel from GC to corresponding DB including service time required at each intermediate DBs. Hence the maximum allowed time to reach a DB by a DM from from the GC is one third of L'.

Algorithm 10: Main Function for Modeling Algorithm

Step 1: Input: *MCS , L = Latency,* λ
// λ is initial randomly chosen T_4 latency value
$L' = L - (F_1 + \lambda)$
// L' is the maximum allowed latency for Tier-3
Step 2: for *(All unvisited DB)* **do**
  Step 2.1: GetGroups(MCS , GC , L', G(V,E)) Returns the number of groups, Number of DMs for each group and their trajectories
  Step 2.2: Verify the feasibility of the group formation using our system model. If found not feasible, reduce L' and go to step 2.
end
Step 3: Calculate Latency for Tier-4 using suitable heuristic and call it λ' .
step 4: if *(*$\lambda' \leq \lambda$ *)* **then**
  Exit with Success.
end
else
  $\lambda = \lambda'$ //Replace initial λ with calculated exact λ
  goto step 2
end

Algorithm 11: Group Formation :: GetGroups(MCS , GC , L, G(V,E))

step 1: GC = MCS
step 2: Deploy a DM and call it currentDM
step 3: for *(all DB's wich can be visited from GC in time* $\leq L/3$*)* **do**
  step 3.1 : if *(DB is already visited by some previous DM AND EdgeLength(GC,DB) for current DM < EdgeLength(GC,DB) for previous DM)* **then**
    visit DB by current DM
    Remove DB from the path of previous DM
    Update trajectory for previous DM
  step 3.2: else
    visit DB
    EdgeLength(GC, Next Unvisited DB) = EdgeLength(GC, DB) + min(EdgeLength(DB,Next Unvisited DB))
    DB = Next Unvisited DB
step 4:if *(There exist any unvisitd DB which can be traversed within L/3 from current GC)* **then**
  Go to step 2
step 5:else
  Deploy a new LWC at DB which can cover maximum number of unvisited DBs.
  That DB is included in GC set.
  Got to step 2.

We start by setting MCS as the first GC. We deploy a DM, and cover as many DBs as possible from that GC. If it covers all the DBs, we are through. If any more DB left, we deploy a second DM, if possible. Continue this way until no more addition of DM to the group can cover any more DB. If no more DBs left, we are through. Else, it is time to deploy LWC towers and add a new group. This starts by choosing best possible DB from the set of so far unvisited DBs as next GC and repeat the same process described above from the new GC. This process of forming group continues until no more DB left.

Our algorithm mostly follow a greedy approach. But the greedy approach has a tendency to stuck at a sub-optimal solution. To avoid this, we have taken a precaution as follows: if a DB can be reached by mor than one DMs, we assign that DM to the DB through which a GC can be reached in minimum possible time. Algorithm 10 and algorithm 11 describes the whole group formation procedure.

E. Customization e-ONE for PDCN

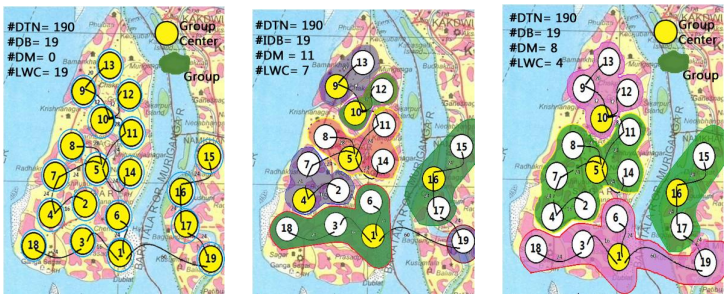
The PDCN architecture described above, being a hybrid architecture, requires several different features. The e-ONE can be utilized to provide these features to the architecture. Here, we describe how we have used the different features of e-ONE in PDCN.

1) Mobility Model: With the inclusion of the concept of the DropBox, it was evident that all the messages had to be relayed to it, as the DataMules could only establish connection with the DropBoxes. Hence, it became very important that all the nodes in the cluster should periodically visit the DropBox and drop the messages there. This was not the case for the Cluster Movement Model[ ] because the nodes in this movement were restricted to the cluster but followed Random Waypoint Model within. Hence, the periodic message dropping in the DropBox was not easy. Thus, the Post Office Cluster Movement Model was used to cope with this problem.

2) New Modules: Considering a disaster scenario, there might be some cases where emergency messages need to be delivered to the main control center as early as possible. The regular strategy is not particularly fast and thus satellite phones were used for relaying these emergency messages.

3) Restricted Routing Strategy: When the area was divided into various groups of clusters, there was a different type of restriction on the transfer of messages. Here the following restrictions were made to decrease the load in the system-

- If the message was for a node at the same cluster or at different cluster and the host was dtn node, (i) it would relay the message to the dtn node at the same cluster or (ii) if the dtn is in the range of DB then dtn not only will deliver message to the DB but also will receive ack from DB and this ack will be eventually propagated within the cluster for that particular message.
- If the message was for a node in the same cluster and the host was a DropBox, it would only relay the message to the DTN nodes.



(a) L=60 (b) L=180 (c) L=300

Figure 9. Number of Different Devices, Group Information for Latency 60,180 and 300 minutes of Planned Simulation

- If the message was for another cluster/shelter point in the same group and the host was a DropBox, it would only relay the message to the Data Mules.
- If the message was for another group and the host was a DropBox, it would relay the message to the LWC if the DropBox is in the group center, otherwise to the data mule.
- If the message was for another group and the host was a data mule, it would relay the message to the DropBox in the group center.
- If the message was for the same cluster/shelter point as the DropBox with which the host data mule is presently connected, it would relay the message to the DropBox.
- If the message is for the same group as the LWC, which is the host, then it would relay the message to the DropBox of the cluster it is in, otherwise to other LWCs.
- No data mule would relay a message to another data mule.

4) Buffer Scheduling: Buffering Scheduling is done by clearing of buffer from the nodes in the cluster, drop box, data mules and the LWC of the group center. These is done when transfer takes place between different types of nodes in the network.

- If one DTN node encounters with another DTN node of the same cluster then Delete the message by checking their ACK list.
- If DTN node encounters with dropbox then Delete the message from DTN node after getting its Ack and updates Ack list for that message.
- If dropbox encounters with data mules then (i) Delete the message from the dropbox that has been sent to the data mule and (ii) Delete the message also from the data mule that has been sent to the dropbox.
- If dropbox encounters with LWC then Delete the message from the Cluster point that has been sent to the LWC.
- If LWC encounters with LWC(This LWC is towards the MCS) then Delete the message from the LWC that has been sent to the LWC towards the MCS.

5) Device scheduling: Two types of devices encounters with dropboxes at each SP. One is DTN nodes & another one is DMs. Messages are uploaded and downloaded from both of them at DB. But a proper scheduling paradigm should be followed while both types of devices encounters DB at same time. DM should be served immediately with a higher priority than a DTN node. A miss arrival of DM will take longer time to get back again the opportunity of next arrival than DTN node to the particular DB. Because the roaming area of DM is larger than a DTN node. Henceforth DM is set to higher priority value than DTN Node.

F. Simulation Result and Analysis

In this subsection first we have described simulation specification based on our architecture and then analyse the results.

1) Simulation Setup: Simulation is carried out using e-ONE Simulator [18] for the area of Sundarban, India; an area of 225sq.km is divided into 19 SPs as shown in Figure 9(a) with a density of 10 smart phones per SP, each having a data rate of 8Mbps and coverage range of 10m; nodes follow the Post Office Cluster movement model [16]. These nodes follow the *restricted epidemic routing* strategy for message transfer. They only interact with either other smart phones or the DB at the center. The velocity of DMs is restricted to 10 km/hr. These DMs move (trajectory) between the group center SP to the other SPs which is also get from the modeling . The pause time at each SP for the DM is set from the modeling. The DMs are restricted to interact only with the group DBs and take messages only if it is entitled for some device outside the cluster it is presently in. The LWCs at the group centres have a coverage range of 9 kms. The data-rates for each type of device had been set based on lab-based experimental values. list of simulation parameters for our modeling as shown in Table III.

2) Simulation Settings: The use of e-ONE required some new settings to be included in the settings file for the ONE. In this section, we present the new settings used in e-ONE for PDCN.

Starting node number of all types of nodes

Group.first(type of Device)= first address of the node.

The networks needs to know the first address of the type of device implemented.

e.g.:- Group.firstBT = 53(first address of the DTN node)

Group.firstDM = 38(first address of the Data Mule)

Setting of total no of data mules

Group.DMS=n

TABLE III.
SIMULATION PARAMETERS USED TO SIMULATE THE ARCHITECTURE

Parameter	value
Total Area	225 sq.km
No of Shelter Points	19
Area surrounded by SP	12 sq. Km
No of DTNs/SP	10
Latecncy	200 minutes & 240 minutes
LWC Range	9 KM
Data Rate of DTN node	2 Mbps
Data Rate of DB to DM	20 Mbps
Data Rate of DB to LWC	18 Mbps
Data Rate of LWC to LWC	8 Mbps
Mean F_1	20 Minutes
Mean R_e Packet Generation Rate of DTN Node	10 Packets/DTN/Hr
Mean R_s Packet Generation Rate of MCS	3 Packets/minutes
Simulation Time	20 hours
Mean Packet Size	1 MB

Total no. of Data Mules in the network is n. E.g.:- Total no. of data mules for 200 latency is 9. Therefore in the Simulation setting it is give as below
Group.DMS=9
DataMule Trajectory
Group.DM(i)=a1, a2, a3
The above line says that Data Mule (DM) visits a1, a2, a3, Drop Box. It means that the Data Mule starts from Cluster Center and visits a1 Drop Box then a2 Drop Box and so on. i is the Data Mule no. starting from 1 to n. E.g:-
Group.DM1= 11
Group.DM2= 7,8
DM1 starts from cluster center and visits 11 no. Drop Box. DM2 starts from cluster center and visits 7 and 8 Drop Box.
Node number of the group center dropboxes
Dropboxes range from 19 to 37. Such that, 1 contains DB19 and similarly 19 contains DB37
Centres for 200AT are 1,4,5,10,13,16
$Group.group\_centers = 19, 22, 23, 28, 31, 34$

3) Planned Deployment: Figure 9 illustrates the effect of latency (L) on the process of group formation. We have also observed as we increase the value of L lesser the number of groups have been formed compared to lower latency. The size of a group is directly proportional to the coverage area of the DMs within L. The more is the value of L the more area will be covered by DMs resulting less number of group formation as shown in figure 9 (a) (b) and (c). The planned approach actually yields 100% packet delivery as shown in figure 10. The figure also shows that nearly 30% of all the packet from the system are delivered nearly within 25 minutes. We feel that these are from the DTN nodes near the GCs as well as the MCS. Again we observe that nearly 70% packets are delivered within the time equal to half the L.

Figure 11 illustrates mean delay at every tire with corresponding error bar highlighted in them. The observation suggests that majority of the delay is contributed by the traversal of the packets from IDBs to the respective GCs through the DMs.

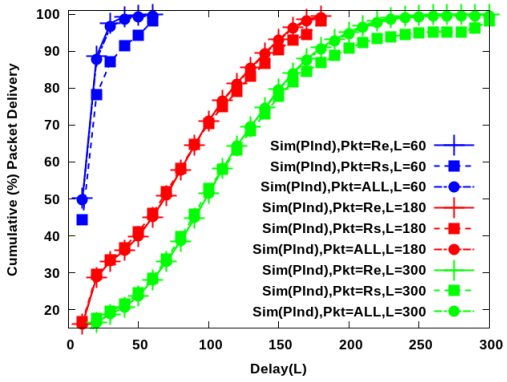


Figure 10. Cumulative Packet(%) Delivery for L=60, 180 and 300 of Planned Simulation

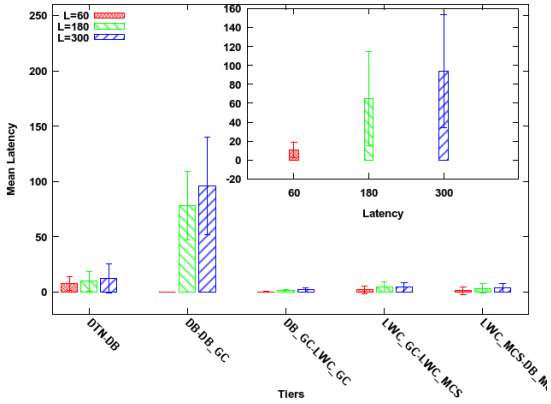
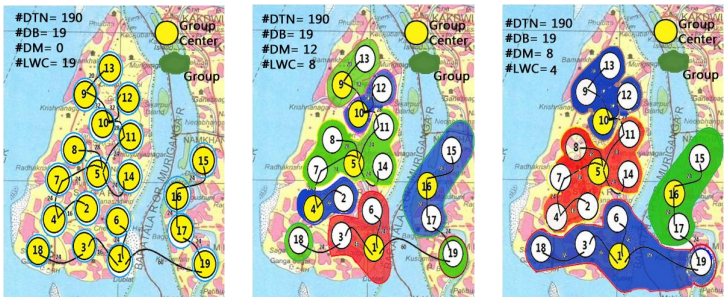


Figure 11. Mean Latency with error bar for L=60,180 & 300 of Planned Simulation

4) Unplanned Deployment: Parameters and logic of group formation are almost same for both planned and unplanned approach but for planned deployment the value of parameters are determined through some system model where as those are randomly taken some presumed values which can not be (service time) determined without mathematical model. We have also obtained same co-relation between no of groups and L which is shown in Figure 12 after some certain value of L_0 but the nature of relation between no of groups and L may be random for any value lesser than L_0.

Around 10% to 20% packet loss is observed in every case under unplanned solution, as seen from figure 13. We also noticed mean latency with error bar is always high compared to the planned simulation as shown in figure 14.

Figure 15 shows the lay out of our packet analysis tool which analyze performance (e.g cumulative packet delivery of different types of packet, Avarage latency , Tier wise latency). If packets are lost then our tool is capable of identifying the Tier/layer is responsible for that loss. It is also used to show the trace and associated graph of dropped packets. On selection of a dropped packet from



(a) L=60 (b) L=180 (c) L=300

Figure 12. Number of Different Devices, Group Information for Latency 60,180 and 300 minutes of Unplanned Simulation

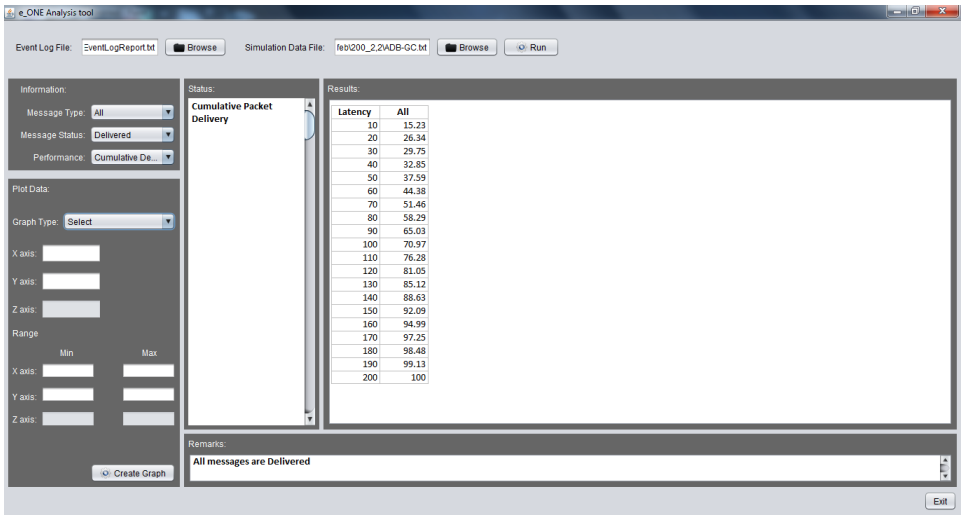


Figure 15. e-ONE Packet Analysis Tool

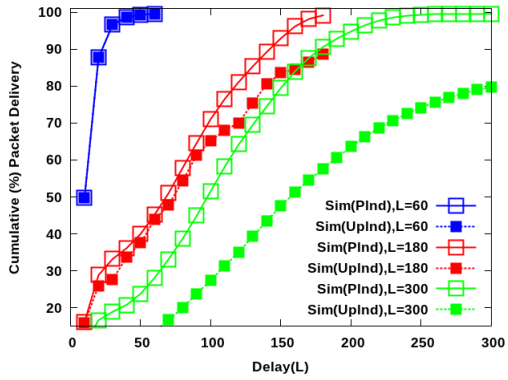


Figure 13. Mean Latency with error bar for L=60,180 & 300

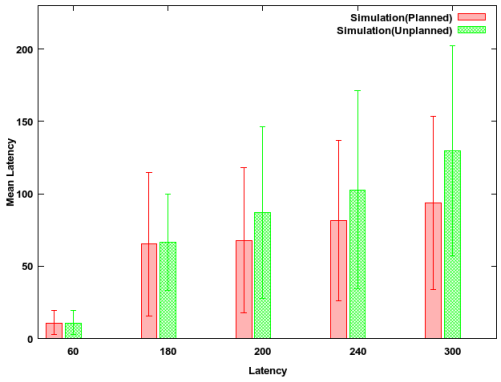


Figure 14. Cumulative Packet Delivery for L=60,180 & 300

its list, the tool shows the message path and possible reasons for packet dropping along with corresponding trace history. It also helps to draw different types plots for analysis the results.

IV. Conclusion & Future Work

Our proposed e-ONE simulator offers a heterogeneous or challenged network evaluation system with a variety of enhanced modules like mobility pattern, infrastructure network system (MESH, SAT, LWC), intelligent routing strategy, device scheduling, buffer scheduling etc. In this paper we have shown cent percent packet delivery within the given latency by our latency aware post disaster management architecture ; evaluated through e-one. We have also noticed that 70% to 74% packets are being delivered with half of the latency factor.

Future extension of e-ONE is to overcome a few limitations which still exist, such as,

(1) Shape of the cluster is a polygon in case of a real life scenario but here we have considered it as a circle

(2) Define movement pattern which is more realistic for post disaster management inside the cluster

(3) Combination of our Network Resource Allocation Software [19] and e-ONE for better post disaster network analysis & management;
(4) Deployment of an architecture in one of the disaster prone areas of the Sundarbans.

ACKNOWLEDGEMENT

The authors are grateful to the anonymous reviewers for constructive suggestions and insightful comments which greatly helped to improve the quality of the manuscript. This Publication is an outcome of the R&D work undertaken in the ITRA project of Media Lab Asia entitled Post-Disaster Situation Analysis and Resource Management Using Delay-Tolerant Peer-to-Peer Wireless Networks (DISARM). (Ref. No.: ITRA/15 (58) /Mobile/DISARM/01).

REFERENCES

[1] K. R. Fall, 'A Delay-Tolerant Network Architecture for Challenged Internets', *Proc.* ACM SIGCOMM (2003).
[2] A. Pentland, R. Fletcher and Hasson , 'DakNet: Rethinking Connectivity in Developing Nations', IEEE Computer, vol. 37, no.1, (2004).
[3] T. Hossmann, F. Legendre, P. Carta, P. Gunningberg, and C. Rohner,'Twitter in disaster mode: Opportunistic communication and distribution of sensor data in emergencies',ExtremeCom (2011).
[4] B. Braunstein, T. Trimble, R. Mishra, B. Manoj, L. Lenert and R. Rao, 'Challenges in using of distributed wireless mesh network in emergency response',3rd International ISCRAM Conference (2006).
[5] A. Seth, D. Kroeker, M. Zaharia, S. Guo and S. Keshav, 'Low-cost Communication for Rural Internet Kiosks using Mechanical Backhauls',Proc. MobiCom 2006, Los Angeles, USA (2006).
[6] S.M. George, W. Zhou, H. Chenji et al. 'DistressNet: A Wireless Ad Hoc and Sensor Network Architecture for Situation Management in Disaster Response',IEEE Communications Magazine, Volume: 48 , Issue: 3 (2010).
[7] S. Saha, V.K Shah, R. Verma, R. Mandal and S. Nandi, 'Is It Worth Taking a Planned Approach to Design Adhoc Infrastructure for Post Disaster Communication?'in Proceedings of the ACM CHANTS12, co-located with MobiCom 2012, Istanbul, Turkey (2012).
[8] T. Hossmann, F. Legendre, P. Gunningberg, C. Rohner,'Twitter in Disaster Mode: Opportunistic Communication and Distribution of Sensor Data in Emergencies'ExtremeCom2011, September 26-30, 2011, Manaus, Brazil.
[9] ONE: 'www.netlab.tkk.fi/tutkimus/dtn/theone/'.
[10] DTNSim2 :'http://www.codeforge.com/article/142062'
[11] A. Vahdat and D. Becker ,'Epidemic routing for partially connected ad hoc networks', Technical Report CS-200006,Duke University (2000).
[12] A. Lindgren, A. Doria and O. Schelen , 'Probabilistic Routing in Intermittently Connected Networks',SIGMOBILE Mobile Computing Communications Review (2003).
[13] T. Spyropoulos et al., 'Spray and wait: an efficient routing scheme for intermittently connected mobile networks',ACM SIGCOMM workshop on Delay-tolerant networking (2005).
[14] T. Spyropoulos et al., 'Spray and Focus: Efficient Mobility-Assisted Routing For Heterogeneous & Correlated Mobility',in Proc. Fifth IEEE PERCOM Workshops, 2007.
[15] J. Burgess et al., 'Maxprop: Routing for vehicle-based disruption-tolerant networking',in Proc. INFOCOM (2006).
[16] M. Romoozi et al.,'A Cluster-Based Mobility Model for Intelligent Nodes',at Proceeding ICCSA '09 Proceedings of the International Conference on Computational Science and Its Applications: Part I (2009).
[17] S. Saha, S. Nandia, P. S. Paul, V. K. Shah, A. Roy, S. K. Das, 'Designing delay constrained hybrid ad hoc network infrastructure for post-disaster communication', Journal of Ad Hoc Networks, Elsevier (DOI: 10.1016/j.adhoc.2014.08.009), 2014.
[18] http://www.nitdgp.ac.in/MCN-RG/eONE/eONE.html.
[19] S. Saha, N. Agarwal, P. Dhanuka and S. Nandi,'Google Map Based User Interface for Network Resource Planning in Post Disaster Management',in Proceedings of the ACM DEV 2013,co-located with COMSNETS 2013, Bangalore, India.

Sujoy Saha: He is presently a faculty member in the Department of Computer Applications, National Institute of Technology, Durgapur, India. He has completed B. Tech (Computer Science and Engineering) from NIT Calicut and M.Tech (Computer Science And Engineering), Jadavpur University in 2005. He is presently pursuing his Ph.D in designing Secure Resource Constrained DTN Architecture for Challenged Scenario under Dr. Subrata Nandi, Department of CSE, NIT Durgapur. His areas of research are Mobile Ad-hoc Network, Network Modeling, Delay Tolerant Networks and Network Security. He has published 9 papers in different International Conferences/Journals which includes leading conferences ACM Mobicom, ACM DEV, ICDCN, Journal of Ad Hoc Networks in Elsevier etc. He is also Project Co-Investigator of the project DISARM, Funded by Media Lab Asia /ITRA, MCIT, Govt. of India.

Rohit Verma: He is presently working at Schneider Electric India. He completed his B.Tech. in Computer Science and Engineering from National Institute of Technology, Durgapur, India in the year of 2013. He worked as a young researcher in a project entitled Post-Disaster Situation Analysis and Resource Management Using Delay-Tolerant Peer-to-Peer Wireless Networks (DISARM) which is funded by ITRA, Media Lab Asia, Government of India in 2013. He worked on security of Delay Tolerant Network & enhanced ONE simulator. He has published five international conference papers like in MOBICOM CHANTS workshop.

Partha Sarathi Paul: He is presently working as a Senior Research Fellow in the Department of Computer science & Engineering at National Institute of Technology Durgapur, India. He has received his B.Sc. degree from University of Calcutta with honours in Mathematics in the year of 1998. He then got his M.Sc. degree from the same university in pure mathematics in the year of 2000. After that he completed his M.Tech. in Computer Science program form Indian Statistical Institute, Calcutta in the year of 2003. Presently he is pursuing Ph.D. in the area of Modeling, Design & Analysis of Hybrid Networks Infrastructures, under Dr. Subrata Nandi at NIT Duragpur. His research interests include Mobile Ad-hoc Network, Network Modeling, Delay Tolerant Networks, etc.

Somir Saikia: He is presently working at Vantage Circle. He has got his M.C.A (Master of computer applications) from National Institute of Technology, Durgapur, India in the year of 2014. He worked as a young researcher in a project entitled Post-Disaster Situation Analysis and Resource Management Using Delay-Tolerant Peer-to-Peer Wireless Networks (DISARM) which is funded by ITRA, Media Lab Asia, Government of India.

Subrata Nandi: He is presently working as Associate Professor in the Department of Computer Science & Engineering, NIT, Durgapur,India. He has completed B.Tech (Computer Science & Engineering) from University of Calcutta and M.Tech (Computer Science & Engineering) from Jadavpur University. He has completed PhD (Titled: Information Management in Large Scale Networks) from the Department of Computer Science And Engineering, Indian Institute of Technology, Kharagpur in 2011. He worked as a project fellow in the Indo-German (DST-BMBF) project during 20082010. He visited Dept. of High Performance Computing, TU Dresden, Germany as visiting research scientist and received ACM SIGCOMM travel grant in 2008. He has published 25 papers in different International Conferences/Journals which includes Physical Review E, ACM Mobicom, ACM SIGCOMM, ACM DEV, etc. His broad interest lies in developing technologies for developing regions with specific focus on Peer to Peer Network, Mobile Ad-hoc Network, Delay Tolerant Network, Service-oriented Architecture, etc. He is also Project Investigator of the project DISARM, Funded by Media Lab Asia /ITRA, MCIT, Govt. of India.

A Load-Balanced On-Demand Routing for LEO Satellite Networks

Jingjing Yuan*, Peiying Chen, and Qinghua Liu
School of Phyisics and Electronic Engineering, Xingtai University, Xingtai, Hebei 054001, China
*Email: yuanjing0923@163.com

Heng Li
State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi 710071, China

***Abstract*—Due to population distribution and economic flourish diversity, the low earth orbit (LEO) satellite network carries unbalanced traffic load, which leads that parts of satellite links are congested while others are underutilized. Furthermore, the congested inter-satellite links result in high queuing delay and packet dropping ratio. To ensure an intelligent scheduling of traffic over entire satellite networks, a load-aware routing protocol named load-balanced on-demand routing (LBR) for LEO satellite networks is proposed in this paper. LBR integrates load judgment mechanism and location assistance strategy, which can reduce the time for path discovery and the control overhead. To evaluate the performance of the proposed protocol, the simulation is conducted on the platform of NS-2. Simulation results verify that, comparing with the existing protocols, LBR can achieve better load balancing, lower end-to-end delay and packet dropping ratio, and higher network throughput with the acceptable control overhead.**

***Index Terms*—LEO Satellite Networks; Routing; Load-Aware**

I. INTRODUCTION

The low earth orbit (LEO) satellite network is a type of wireless network system in space in which various LEO satellite nodes are interconnected by inter-satellite links (ISLs). Because of the particular features of LEO satellite networks, such as global coverage, near real time and high bandwidth, LEO satellite networks play a very important role in civil and military area [1, 2]. However, the population dispersion, the economic flourish diversity, the difference of geographical and time zones, the constellations' operation, and the Earth's rotation will lead to the unbalanced distribution of network traffic which results in some satellites that located in traffic-condensed area are congested. In addition, the problem will cause high queuing delay and packet dropping ratio in the phase of data transmission. Therefore, the network traffic load balancing must be considered as a key factor in routing protocol design for LEO satellite networks.

The satellite network routing strategies have been proposed can be divided into three categories which are virtual topology routings, virtual node routings, and dependent topology routing. In virtual topology routings [3-6], the constellation cycle is divided into several time slices. In each time slice, the network topology is seen as a fixed virtual topology. Therefore, this kind of routings can calculate the path between each pair of satellites in all time slices for each node in advance, according to the predictable network information. Virtual topology routings have poor adaptability for flow changes, congestions, failures, and other real-time conditions. The virtual node routing [7, 8] utilizes the rules of the topologies of the satellite networks to hidden the mobility of the satellite in routing protocols on the satellites. Because the virtual node routing only uses the local state information, the calculated route may not be optimal. But it can select a new route based on traffic load, failures, and other conditions in real time, so that this kind of routings has a strong adaptability. Meanwhile, it needs smaller storage space. The dependent topology routing [9, 10] is a dedicated routing which for satellites with specific topological features. It uses different routing strategies for different topologies by continuously analyzing the characteristics of the current network topology. This algorithm is strictly for a particular type of satellite constellations, so that it needs to design different algorithms for different satellite networks in general. It reduces the communication and processing overhead, but it cannot guarantee the route optimality. LEO satellite networks prone to appear the phenomenon of unbalanced load distribution, i.e. a part of links are overloaded and other links are idle, which will reduce the utilization of the valuable resources of the satellite. So, the unbalanced load distribution is one of the main problems of the communication in LEO satellite networks. However, the existing routing protocols in LEO satellite networks have two major problems in load balancing. For one hand, these routing protocols cannot calculate routes via the satellite network's real time states. For the other hand, most of the protocols use a global network status which will lead in a high control overhead.

To cope with the aforementioned limitations of current routing protocols, a load-balanced on-demand routing (LBR) protocol is proposed in this paper. The prior purpose of the LBR is to achieve better load balancing to adapt to high traffic changes. It limits the process of routing request with in a rectangular area. The

doi:10.4304/jnw.9.12.3305-3312

intermediate node load judgment mechanism and the location assistance strategy are introduced into the path discovery process of the LBR protocol. LBR uses a dynamic threshold to reflect the real-time state of the network average load. Each intermediate node compares its value of the load with the dynamic load threshold. If its value is greater than the threshold, it shows that the load on the intermediate node is heavy, and the request packet is discarded. Otherwise, the request packet will be forwarded to the next hop. When forwarding the request packet, the request packet is only transmitted to the ISLs, whose directions are consistent with the direction of the destination node, thereby reducing the blindness of the route discovery. The destination node selects the path that has the lightest load to reply a response packet. The intermediate node load judgment scheme is very effective to achieve load balancing and congestion avoidance. The location assistance strategy can reduce the control overhead and the time for path discovery procedure. Meanwhile, for node failures and other anomalies, using local repair strategy, LBR could repair the path timely and efficiently, improving the network's survivability.

The remainder of this paper is organized as follows. Section II introduces some related works about routing algorithms for efficient load balancing. Section III is the detail of the LBR protocol. The performance of LBR is evaluated and compared to other schemes in Section IV. Conclusion is drawn in Section V.

II. Related Works

Currently, a number of routing algorithms have been proposed for efficient load balancing over LEO satellite networks. These algorithms can be classified into two categories according to the place where the routing is performed: centralized algorithm and distributed algorithm. In the centralized algorithm, such as the routing strategies in [11-13], the source satellite nodes calculate the optimal route to the destination node according to the traffic information which is gathered globally from the whole network. In [11], a dynamic adaptive routing strategy is proposed for Non-Geostationary (NGEO) satellite systems. The adaptive routing can pick an optimized path according to transmission delay and link weight under predetermined statistical distribution model which is able to exactly portray traffic flows from the source to the destination worldwide. However the algorithm cannot adapt to a burst of traffic flow. In [12], a control route transmission (CRT) protocol is proposed. The routing protocol dynamically adjusts routes to balance the traffic load on the basis of congestion matrix. The congestion matrix accounts for the whole network load by updating control messages periodically. However, it cannot accurately reflect the actual condition of the network and then can not provide fast reaction to traffic changes. An agent-based load balancing routing (ALBR) protocol is presented in [13]. The mobile agent technology is introduced in LEO satellite networks. Local information of routing satellites is gathered by mobile agents to build routing information base for deploying routing table. However, its suitability to satellite networks has never been perfect solved. The disadvantage of the centralized algorithm is that it needs to periodically broadcast control messages to collect network status which will increase the control overhead. What's more, for loads dramatically change networks, the routes calculated based on the global information of network status may soon lapsed. Therefore, the centralized algorithm is not suitable for LEO satellite networks. While the distributed load balancing algorithms are proposed in [14-17]. In distributed schemes, each satellite balances the load and avoids the congestion independently based on the local traffic load. It can react to traffic changes faster than the centralized algorithm. In [14], a traffic load balancing scheme is proposed to resolve the congestion problem. The proposed scheme makes use of near-neighbor residual bandwidth information to apportion excess bandwidth from congested satellites to their underloaded neighbors in the network. The network model used in this algorithm is ATM which is a connection-oriented fast packet switching technology. When a target path is congested, the call on the path can be forwarded bypass through alternate paths in the same balanced domain. So, it solves the problem of local traffic congestion. Table et al. propose an explicit load balancing (ELB)[15] scheme, where a congested satellite sends a signal to its neighboring satellites to decrease their sending rate, and the neighbors search for alternate paths. It is a routing protocol that explicitly exchanges the congestion information between near satellites, and reduces the packet dropping ratio. The method is easy to implement and the overhead is low and can achieve local load balancing. However, since it uses a predetermined threshold, when the load dramatic changes, the threshold cannot guarantee an accurate reflection of the real-time network load status. So, it is difficult to achieve accurate load balancing. In [16], a location-assisted on-demand routing (LAOR) protocol is proposed. The optimal path is selected based on the total end-to-end delay, which is the sum of propagation and queuing delay. According to this strategy, it provides better estimation of the network state and avoids congested areas. However, in these distribution schemes above, signaling packets are sent so frequently that signaling overhead is obviously increased. Moreover, it does not consider the problems of the load balancing and the path repair. Literature [17] puts forward a distributed routing algorithm (DRA) for datagram traffic in LEO satellite networks. The method is based on virtual node routing algorithm, and the optimization objective of the method is to minimize the packet transmission delay. DRA uses the logical address, i.e. the virtual node's coordinates to represents the geographic coordinates of each constellation satellite. The satellite dynamically changes its logical address during operation. DRA calculates the shortest path through three phases, namely, direction estimation, direction correction and congestion handling. This method makes full use of the physical properties of the polar-orbiting constellation itself, and it solves the problem of routing failures in Polar Regions and seam zones. But, the algorithm's

robustness is poor and cannot fundamentally avoid the congestion. In addition, it can be used only in polar orbit LEO satellite networks and not apply to the inclined orbit satellite constellation. An approach of balancing network traffic by combining the merit of genetic algorithm (GA) and linear programming (LP) is given in [18]. Compare the new solution of obtained by the LP with the worst solution of the previous population obtained by the GA. If the new solution is better than the worst solution, then the worst solution is replaced with it. At the beginning of each time interval, take the solution of the previous time interval as the initial solution of the new population. In [19], a novel load balancing routing scheme is proposed. This scheme employs mobile agents to gather related routing information by migrating autonomously. Stationary agents estimate the ISL cost, the routing path cost and update routing items on satellites. Moreover, the ISL cost is calculated as the sum of propagation and queuing delays. Furthermore, ISL cost modification factor (ICMF) is designed considering the characteristic of polar-orbit satellite constellation as well as the traffic distribution on the earth. Finally, path cost is evaluated based on ICMF and ISL cost. An adaptive distributed load balancing routing mechanism (ADLB) is proposed in [20]. This mechanism makes well-performed routing decision based on the current and historical status of each ISL in each satellite node. With collecting historical information from network initiated, a proper mechanism is contained in ADLB for making required computing power and storage space in a reasonable range.

III. LBR Protocol Description

We propose a load-balanced on-demand routing (LBR) protocol for LEO satellite networks. The prior purpose of the LBR is to achieve better load balancing to adapt to high traffic changes. The LBR protocol mainly contains three processes, namely, the restricting network topology process, the path discovery process, and the route maintenance.

A. Restricting Network Topology Process

In this study, we use polar constellation as the network model. Each satellite has four ISLs: two intra-plane ISLs (links between adjacent satellites in the same orbital plane) and two inter-plane ISLs (links between adjacent satellites in the right-hand and left-hand orbital planes). While intra-plane ISLs are maintained for the whole satellite operation period, inter-plane ISLs cannot. It is because that when satellites come close to the poles and move to lower latitudes, due to adverse pointing, tracking conditions, and re-established, the inter-plane ISLs are broken. Moreover, on both sides of a seam, two adjacent orbits operate in counter direction, so there is no established inter-plane ISLs. The logical location of a satellite can be represented by a coordinate (P, S), where P=0, 1, … , N-1 is the plane number, and S=0, 1, … , M-1 is the satellite number on plane P.

Let us assume that the source satellite and the destination satellite are both known. When the source satellite has data to send, the restricting network topology process is invoked. We suppose the source satellite coordinate as (i, j) and the destination satellite coordinate as (k, l). Let $x_{\min}$, $x_{\max}$, $y_{\min}$ and $y_{\max}$ denote the boundaries of the restricted query area. The restricted query area is represented by the dash-dotted square as shown in Fig. 1. The source satellite calculates them according (1). The area where RREQs will be sent out is limited to the restricted query area, and that can minimize the signaling overhead. The reason of the expedition the area in the direction of the vertical axis is that when take the queue delay as the link cost standard, the shortest path may not within the minimum query area. To reduce this possibility, the ordinate region is amplified.

$$\begin{aligned} x_{\min} &= \min\{i,k\} \\ x_{\max} &= \max\{i,k\} \\ y_{\min} &= \min\{j,l\}-1 \\ y_{\max} &= \max\{j,l\}+1 \end{aligned} \quad . \tag{1}$$

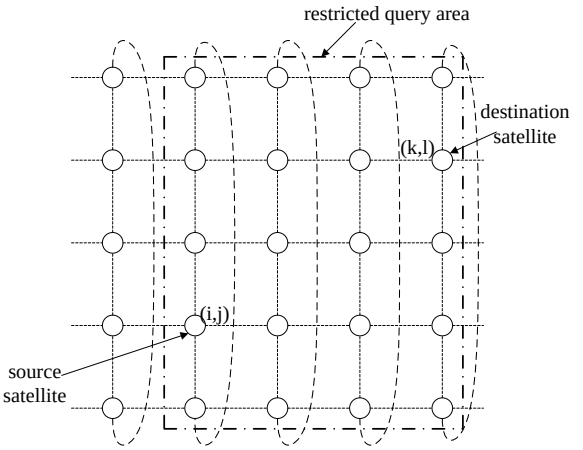


Figure 1. The concept of restricted query area

B. Path Discovery Process

The path discovery process has the following four steps.

Step 1: The source node sends the RREQ packet. After the restricted query area is formed, the source node checks its routing table for paths to the destination. If there is a valid path to destination node, then the source node sends data packets along the path. If the path not exists or exists but is expired, the source node initiates the path discovery process. That is generating and sending a RREQ packet to its neighbors in the boundaries of the predetermined restricted area.

Step 2: The intermediate node forwards the RREQ packet. When the intermediate node receives a RREQ packet, it first checks if it has already received a RREQ from the source with the same sequence number. The RREQ is dropped if the intermediate satellite has received the RREQ with the same sequence number; otherwise, the intermediate node starts the node load judgment mechanism. The idea of load judgment is introduced to judge whether an intermediate node is overloaded in the route discovery phase. Each node forwards RREQ packets selectively to exclude the heavily loaded satellite nodes from the requested paths.

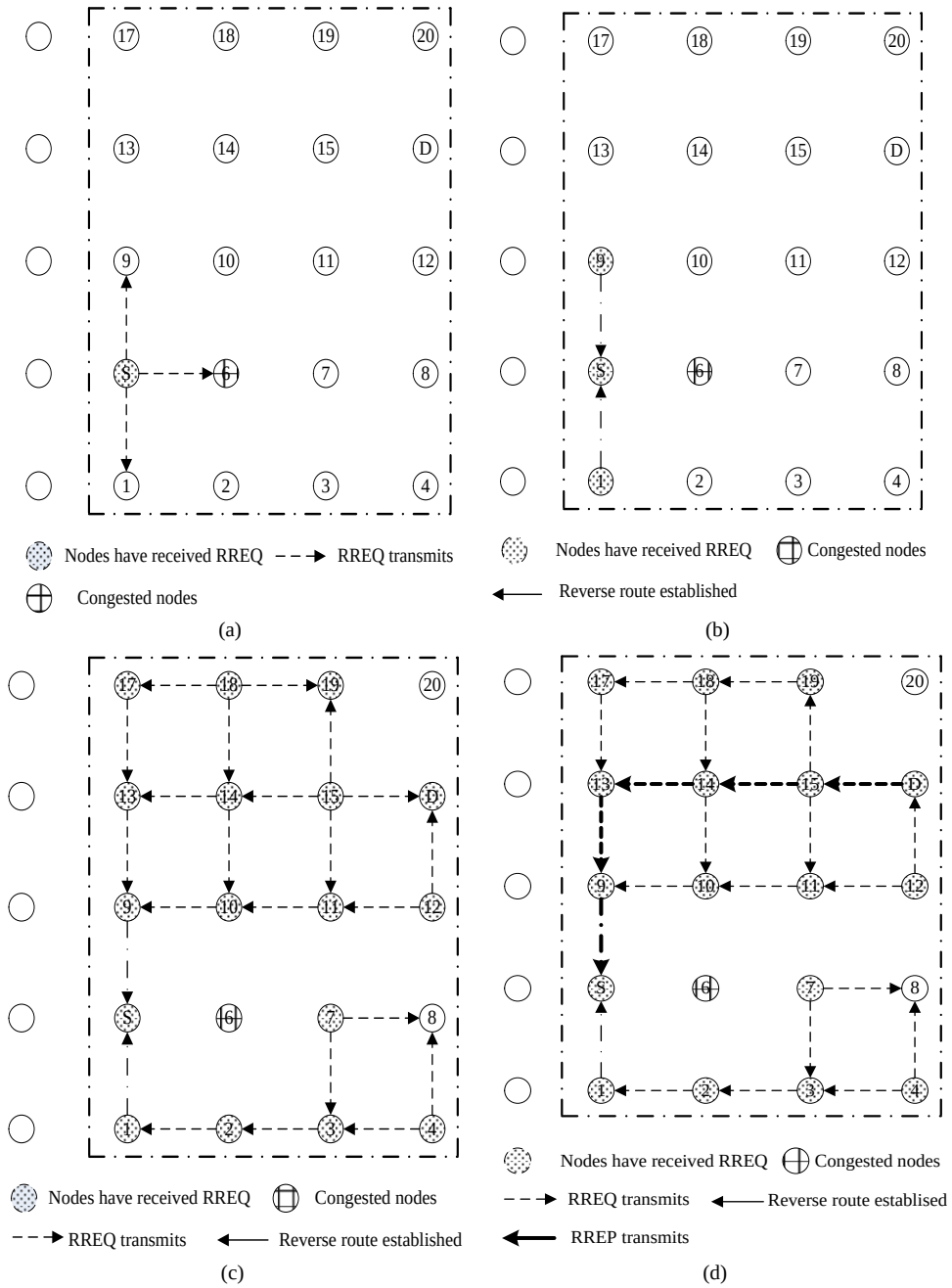


Figure 2. The path discovery process

In the proposed protocol, the node traffic load is computed according to the interface queue length of MAC layer. The average network load is defined as a dynamic threshold value. The dynamic threshold value is carried by RREQ. Let Γ denote the dynamic threshold value. The dynamic threshold value can be estimated by

$$\Gamma = \frac{\sum_{j=1}^{n_i} Q_j + L_{ave} + Q_i}{n_i + 2}. \quad (2)$$

where n_i denote the number of the neighboring satellite nodes of the current satellite node i. Q_i and Q_j respectively denote the traffic load value of the current satellite node i and that of the neighboring satellite node j. L_{ave} is included in RREQ packs to indicate the workload on the path.

The intermediate satellite node employs load judgment mechanism to forward RREQ packets selectively according to (3).

$$\begin{cases} \text{if } Q_i > \Gamma, & \text{drop RREQ;} \\ \text{else} & \text{, forward RREQ.} \end{cases} \quad (3)$$

If the node load value is greater than the dynamic threshold value, the node simply drops the RREQ. Otherwise, the node forwards the RREQ by rebroadcasting it with location assistance strategy. The location assistance strategy forwards RREQ packet to the intermediate node that forwards the destination and the

blind delivery of packets is reduced. By doing so, the overloaded nodes are naturally excluded from the newly requested paths and the time for path discovery procedure and the control overhead are both reduced. In LBR, the intermediate node does not reply the RREQ packs, even if there is a path from it to the destination node. It ensures that LBR always uses the latest load information in the path discovery process.

Step 3: The destination node replies the RREP packet. The destination node waits for an appropriate amount of time to learn all possible routes after receiving the first RREQ packet. In order to learn all routes and their qualities, the destination node accepts duplicate RREQ received from different previous nodes. When the waiting time is over, the destination then chooses the lightest load path and sends a RREP pack to the source via the selected path.

Step 4: The source node receives the RREP packet. When the source node receives the RREP packet, it starts to send data packets, and the path discovery process is finished.

Here we illustrate the process of the path discovery. As shown in Fig. 2 (a), the node S has data to send to node D. It first starts the process of restricting routing query region. Then, S sends the RREQ packet to its neighbor nodes 1, 6, and 9 which meet the coordinate conditions in the query region. When nodes 1, 6, and 9 receive the RREQ packet, they determine whether they have received the RREQ packet according to the broadcast number in the RREQ packet. The RREQ is dropped if they have received the RREQ with the same broadcast number; otherwise, they start the node load judgment mechanism, and determine whether they can afford some extra loads. After the judgment, nodes 1 and 9 can afford some extra loads, and then they establish a reverse route to the source node S. While node 6 not satisfies the load condition, it is a congested node, so the RREQ packet is discarded. We can see it from Fig. 2 (b). Nodes 1 and 9 forward the RREQ packet to nodes 2, 10, and 13, because they satisfy the coordinate conditions. And so on, until the RREQ packet reaches the destination node D as Fig. 2 (c) shows. The destination node D does not respond a RREP packet immediately after receiving the first RREQ packet, but waits for an appropriate amount of time to learn all possible routes. Node D compares and updates the path information received from the same source node. When the predetermined waiting time is over, the node D will response the updated lightest load path immediately by replying a RREP packet along the reverse path. As shown in Fig. 2 (d), after the path discovery process, LBR obtains the path S→9→13→14→15→D which from the source node to the destination node.

C. Route Maintenance

The path's expiration time is stored in each route entry. The purpose of this information is to purge the route entry for the destination satellite before the route is invalid. A new path should be established prior to the expiration of the previous one. The aim is to ensure that no packet will be in-flight when the path becomes invalid. If a node is on an active path, it periodically sends Hello packets to its neighbors to maintain connections with its neighbors. When a link is broken, the node that is located in the upstream of the broken chain starts a local repair strategy.

The route repair strategy in LBR replaces failed nodes by nodes near the scission, while other normal nodes on the path are retained. Add the last two-hop and next two-hop nodes addresses in the RREQ and RREP packets. The routing table entry also adds the next two-hop node address. When a node failure is detected, LBR immediately starts the local repair strategy rather than directly informs the source node re-routing.

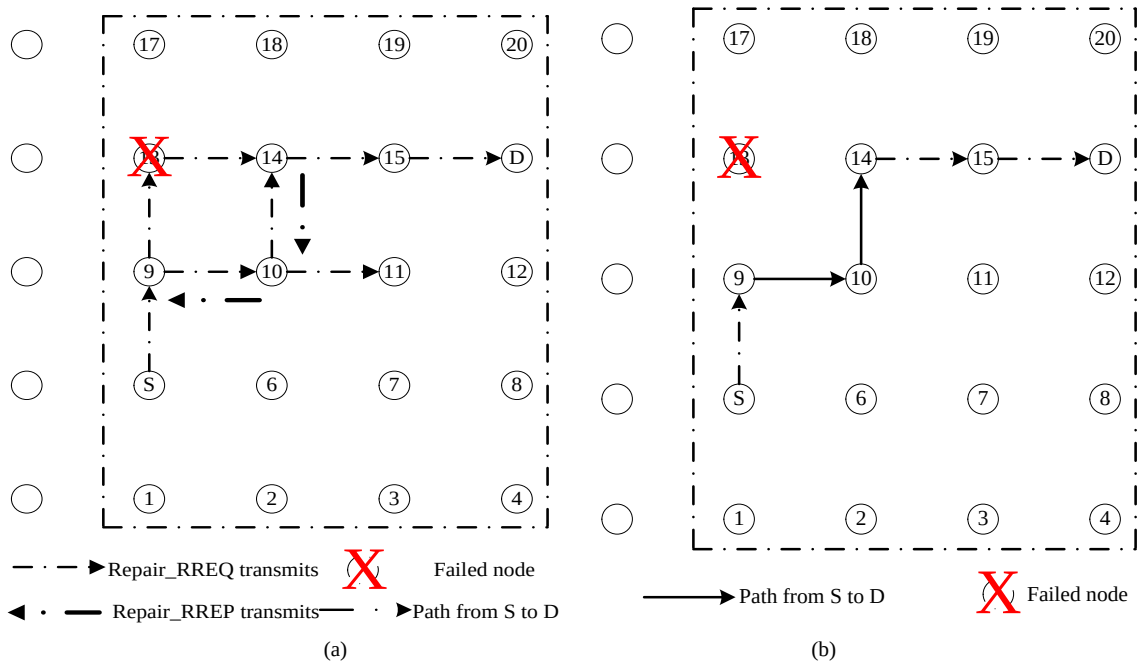


Figure 3. The local repair strategy

Here we illustrate the process of local repair strategy. As shown in Fig. 3 (a), when the node 13 is failed, the node 9 first set the route from it to D to invalid, and then it checks the routing table entry for the destination D. If its next two-hop node 14 exists and is valid, the node 9 pluses 1 to its destination sequence number. Then, broadcasts Repair_RREQ packet to the destination node 14. Except for the node 14, other nodes do not respond to the packet Repair_RREQ. When the node 14 receives the Repair_RREQ packet, it replies a Repair_RREP packet to the node 9 along the reverse path. Meanwhile, the node 14 generates a NOTICE packet and stores the destination node D's new sequence number in it. Then the node 14 transmits the NOTICE packet along the path from itself to the node D. When a node on the path receives the NOTICE packet, it updates its routing table entry for the new destination sequence number. The NOTICE packet finally reaches the node D, and D also updates its own sequence number. When the node 9 receives the Repair_RREP packet, it updates its routing to D and gets the local repair path 9 → 10 →14 as shown in Fig. 3 (b). The path from the source node to the destination node is updated to S→9→10→14→15→D.

If the local repair fails, LBR then sends the RERR packet to the upstream node to notify the source node to restart the route discovery process. Each path discovery process may fail to determine a path to destination. Since the existence of at least one path within the restricted route request area is guaranteed, failure to discover a path is the result of dropping RREQ or RREP packets due to congestion. In this case the path discovery process is repeated periodically until a path is found.

IV. Performance Evaluation

In this section, we study the performance of LBR by running a computer simulation with network simulator ns-2 [21]. We use LBR, ELB and LAOR as comparison terms. In ELB, a "soon-to-be-congested" satellite notifies its neighboring satellites of its current status and requests them to reduce their data forwarding rates. In response, neighboring satellites reduce their transmission rates of traffic originally destined to the "soon to be congested" satellite and search for other alternative paths that do not include the satellite. Regarding the LAOR protocol, the path cost takes account of queuing delay and the optimal path is selected based on the total end-to-end delay, which is the sum of propagation and queuing delay. According to this strategy, it provides better estimation of the network state and avoids congested areas.

A. Simulation Setup

The three protocols are tested in an Iridium-like constellation, which is the most representative of polar constellations. In this constellation, ISLs are switched off when satellites cross the Polar Regions; the latter are defined by a latitude threshold. The ISL and UDL bandwidths are 10 Mb/s and 15 Mb/s, respectively. The average length of all packets in the experiment is set to 1000 Bytes. The switching mode between the ground terminals and service satellites is asynchronous switching. Each terminal checks whether its service satellite meet the elevation angle requirements every 10s. The rest of the simulation parameters are presented in Table I.

For traffic generation, traffic inserted into the network is generated by 300 earth stations which are distributed over the six continents according to the hot spot scenario. Since earth stations represent traffic aggregation points, their number can be considered adequate for representing a real-life scenario. To model the traffic from each earth station, the bulk of the studies in this field used Poisson arrival process. In order to model traffic bursts, we use an exponential ON/OFF generator, which is a generalized version of the exponential process. This approach is closer to a real-life scenario. Table II tabulates the parameters of this traffic generation.

TABLE I. Parameters of Satellite Constellation

Number of orbits	6
Number of satellite pre plane	11
Satellite altitude	780km
Minimum elevation angle	8.2 º
Cross-seam ISLs	NO
Number of ISLs	2 Intra-plane + 2 inter-plane
ISL latitude threshold	±60 º
Drive type	data
Simulation duration	6060s

TABLE II. Parameters of Traffic Generator

ISL queue type	FIFO
ISL queue length	100 Packets
ISL bandwidth	10 Mb/s
UDL bandwidth	15 Mb/s
Size of packet	1000 Bytes
"On" period	0.4 s
"Off" period	0.8 s
Bit rate during "On" period	200-1200 kb/s

To evaluate the three proposed protocols, a terrestrial source-destination pair is selected. The source node of the pair is located at (120 ℃, 37 ℃) in Asia and the destination node is at (71 ℃, 33 ℃) in North America. Both terminals reside in areas with high traffic concentrations.

B. Simulation Results

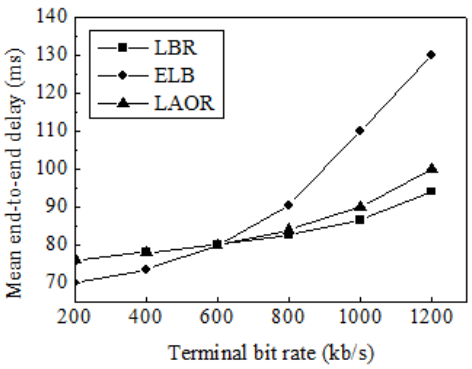


Figure 4. Mean end-to-end delay vs. terminal bit rate

Fig. 4 shows the performance of the end-to-end delay with the increasing terminal bit rate. The end-to-end

delays of LBR and LAOR are larger than that of ELB when the terminal bit rate is below 600kb/s. Once the bit rate is higher than 600kb/s, the end-to-end delays of LBR and LAOR are smaller than that of ELB. The reason is that both LBR and LAOR take the occupancy of the nodes and links in the network into account, and select the light load path. Each node allows additional traffic flows as long as it is not overloaded. In other words, the selected path does not include the overloaded nodes. However ELB does not consider the load balancing in the path discovery process, when the traffic is heavy, the path tends to be congested more easily. So, high delay occurs and packets are dropped more frequently. Moreover, the LBR's end-to-end delay increases much smoother than that of LAOR. This is due to LBR's inherent load balancing ability, which does not allow additional communications to set up through overloaded nodes so that they can be excluded from the requested paths within a specific period. It selects a path that has the lightest load to transmit the data, thus greatly reducing the average end-to-end delay. LBR achieves the load sharing, which means the load can be evenly distributed across the whole network. As a result, control the packet queuing time in the queue buffer and reduce the end-to-end delay.

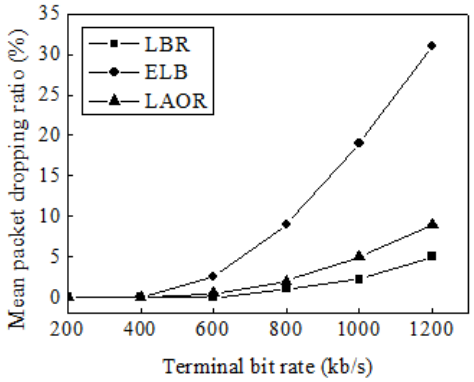


Figure 5. Mean packet dropping ratio vs. terminal bit rate

Fig. 5 illustrates the mean packet dropping ratio versus the terminal bit rate. It can be seen that, once the bit rate is higher than 400kb/s, the ELB's packet dropping ratio degenerates significantly. It is because when the bit rate is higher than 400 kb/s, some nodes switching into the "soon to be congested" state and these nodes' last hop neighbor will reduce the data transmission rate. Before finding the right path to bypass, this neighbor node caches the data packet has been received. The case that cannot find the right route at the end of the packet's life occurs in a great probability, which will result in packet dropping. However, unless the terminal bit rate is above 600kb/s, the packet dropping ratios of LBR and LAOR do not increase. We can see that when the terminal bit rate is below 600kb/s, the packet dropping ratios of the two schemes are very close. After that, the packet dropping ratio of LAOR is higher than that of LBR. The LBR's packet dropping ratio increases much smoother than that of LAOR. It is due to that when LBR establishes a path it does not contain heavy load nodes, which reducing the probability of congestion. In addition, LBR's local repair algorithm improves the ability of handing the link failures. Packets that are lost due to failing to find routes and are cached in buffer are less, thereby reducing the packet dropping ratio. In conclusion, the packet dropping ratios of the three schemes are similar in low traffic intensity, conversely LBR's performance is much better than that of LAOR and ELB for high terminal bit rate. The striking results of the LBR are ascribed to its ability to prevent heavily loaded satellite nodes from routing which stems from the fact that LBR forwards the RREQ message selectively according to the load status of each node in the route discovery phase.

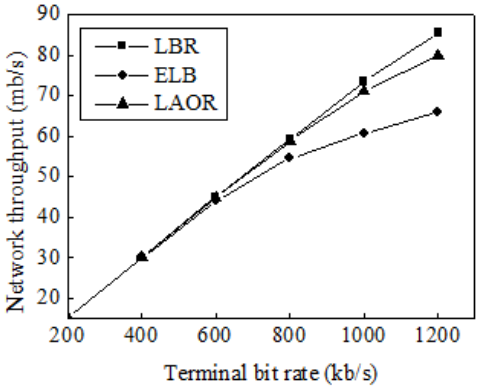


Figure 6. Network throughput vs. terminal bit rate.

Fig. 6 depicts the network throughput versus the terminal bit rate. The network throughputs of the three schemes are similar unless terminal bit rate is above 600kb/s. It becomes evident from this figure that LBR constitutes a significant improvement on ELB and LAOR in high bit rate. In particular, when the terminal bit rate is higher than 800kb/s, the network throughput of LBR achieves 9% and 29% average gain compared with that of ELB and LAOR, respectively. The outstanding network throughput of the LBR is due to its ability to share load within the whole network. LBR selects the path that has the lightest load to forward packet, so that reducing the probability of network congestion and the packet dropping ratio. Therefore, the network throughput is increased.

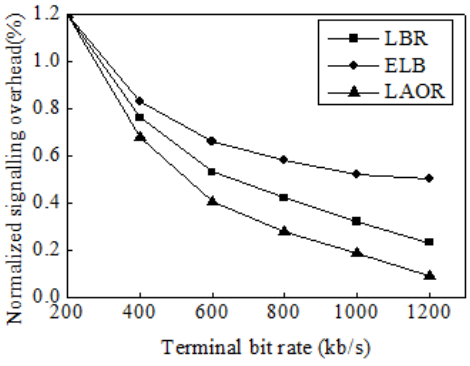


Figure 7. Normalized signaling overhead vs. terminal bit rate

Fig. 7 shows the variation of normalized signaling overhead with the increase of the terminal bit rate. We

can see that LBR's signaling overhead is significantly lower than that of ELB. It is because in LBR, the process of route discovery is performed in the minimum rectangle area. Meanwhile, LBR introduces the direction guidance strategy, which can reduce the blindness of forwarding RREQ packets, thereby reducing the number of transmitted RREQ packets. In addition, in LBR, the intermediate node does not reply RREP packets, which further reduces the signaling overhead. Also we can see, compared with LAOR, LBR's signaling overhead is higher. The reason is that in LBR, when the destination node first receives a RREQ packet, it not immediately replies a RREP packet, but waits for an appropriate amount of time to learn all possible routes. The destination node accepts duplicate RREQ received from different previous nodes, then chooses the lightest load path and sends a RREP pack to the source via the selected path. Moreover, in the process of routing maintenance in LBR, the length of the control packet is increased and a new packet is introduced, which increase the signaling overhead. However, the local repair can greatly shorten the time of path repair. From this point of view, we think the cost of a little signaling overhead is reasonable.

V. CONCLUSION

In this paper, we proposed a load-balanced on-demand routing (LBR) protocol for LEO satellite networks. The prior purpose of the LBR is to achieve better load balancing to adapt to dynamic traffic variations. A set of simulation was conducted to evaluate the performance of the LBR protocol, which is compared to LAOR and ELB protocols. Sufficient simulation results indicate that the LBR method is superior to other schemes. LBR can achieve better load balancing with acceptable control overhead at the high traffic concentration area. Moreover, LBR is shown to attain much lower end-to-end delay and packet dropping ratio, and higher network throughput. This fact renders it an excellent choice for future LEO satellite networks.

REFERENCES

[1] Abbas and Jamalipour, *Low Earth Orbital Satellite for Personal Communication Networks*, Boston-London: Artech House, 1998, pp. 31-35.

[2] Tarik Taleb, Nei Kato, and Yoshiaki Nemoto, "Recent Trends in IP/NGEO Satellite Communication Systems: Transport, Routing, and Mobility Management Concerns," *IEEE Wireless Communications*, vol. 12, no. 5, Oct. 2005, pp. 63-69.

[3] Markus Werner, Cecilia Delucchi, and Hans-Jorg Voge et al, "ATM-Based Routing in LEO/MEO Satellite Networks with Inter-satellite Links," *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 1, Jan. 1997, pp. 69-82.

[4] Markus Werner, "Dynamic Routing Concept for ATM-Based Satellite Personal Communication Networks," *IEEE JSAC*, vol. 15, no. 8, Oct. 1997, pp. 1636-1648.

[5] Hong Seong Chang, Byoung Wan Kim, and Chang Gun Lee et al, "FSA-based Link Assignment and Routing in Low Earth Orbit Satellite Networks," *IEEE Transactions on Vehicular Technology*, vol. 47, no. 3, Aug. 1998, pp. 1037-1048.

[6] Vidyashankar V Gounder, Ravi Prakash, and Hosame Abu-Amara, "Routing in LEO-based Satellite Networks," *Proceeding of IEEE Emerging Technologies Symposium. Wireless Communications and Systems*, Apr. 1999, pp. 22. 1-22. 6.

[7] Yukio Hashimoto and Behcet Sarikaya, "Design of IP-based Routing in a LEO Satellite Network," *Proc. of the 3rd International Workshop on Satellite-Based Information Services.* Oct. 1998, pp. 81-88.

[8] Tsung Han Chan, Boon Sain Yeo, and Laurie Turner, "A localized routing scheme for LEO satellite networks," *Proc. AIAA 21st International Communications Satellite Systems Conference and Exhibit*, Apr. 2003, pp. 2357-2364.

[9] Hüseyin Uzunalioglu, Lan F. Akyildiz, Yelena Yesha, and Wei Yen, "Footprint handover rerouting protocol for LEO satellite networks," *ACM-Blazer Journal of Wireless Networks (WINET)*, vol. 5, no. 5, Sept. 1999, pp. 327-337.

[10] Uzunalioglu Huseyin "Probabilistic routing protocol for low earth orbit satellite networks," *Proceeding of IEEE International Conference on Communications*. vol. 1, Jun. 1998, pp. 89-93.

[11] Hui Li and Xuemai Gu, "Adaptive ATM Routing in Walker Delta Satellite Communication Networks," *Proc. IEEE Symp. First International Symposium on Systems and Control in Aerospace and Astronautics (ISSCAA 06)*, IEEE Press, Jan. 2006, pp. 368-373.

[12] Yan He and Susanna Pelagatti, "CRT: an Adaptive Routing Protocol for LEO Satellite Networks," *Proc. IEEE Symp. International Conf. on Information and Communication Technologies: from Theory to Applications (ICTTA 06)*, IEEE Press, Apr. 2006, pp. 2496-2501.

[13] Yuan Rao and Ru-chuan Wang, "Agent-based Load Balancing Routing for LEO Satellite Networks," *Computer Networks*, vol. 54, no. 17, Dec. 2010, pp. 3187-3195.

[14] Yun Sik Kim, Young-Ho Bae, Youngjae Kim, and Chul Hye Park, "Traffic Load Balancing in Low Earth Orbit Satellite Networks," *Proc. 7th International Conference on Computer Communicaions and Networks*, IEEE Comput. Soc Press, Oct. 1998, pp. 191-195.

[15] Tarik Taleb, Daisuke Mashimo, Abbas Jamalipour, Kazuo Hashimoto, Yoshiaki Nemoto, and Nei Kato, "ELB: An Explicit Load Balancing Routing Protocol for Multi-Hop NGEO Satellite Constellations," *Proc. IEEE Globecom 2006*, IEEE Press, Nov. -Dec. 2006, pp. 2776-2780.

[16] Evangelos Papapetrou, Stylianos Karapantazis, and Fotini Niovi Pavlidou, "Distributed On-Demand Routing for LEO Satellite Systems," *Computer Networks*, vol. 51, Oct. 2007, pp. 4356-4376.

[17] Eylem Ekici, Ian F. Akyildiz, and Michael D. Bender. A Distributed Routing Algorithm for Datagram Traffic in LEO Satellite Networks. *IEEE/ACM TRANSACTIONS ON NETWORKING*, vol. 9, no. 2, Apr. 2001, pp. 137-147.

[18] Yan Hui Pan, Tao Wang, and Hua Li, "Research on Load Balancing Method of LEO Satellite Network Routing," Computer Engineering, vol. 37, no. 18, Sept. 2011, pp. 4-6.

[19] Jun Zhu, Yuan Rao, Leiyang Fu, Wei Chen, and Xing Shao, "Load Balancing Routing based on Agent for Polar-Orbit LEO Satellite Networks," *Journal of Information and Computational Science*, vol. 9, no. 5, May. 2012, pp. 1373-7-1384.

[20] Xiao Ma, "Adaptive Distributed Load Balancing Routing Mechanism for LEO Satellite IP Networks," *Journal of Networks*, vol. 9, no. 4, Apr. 2014, pp. 816-821.

[21] The network simulator ns-2, http://www.isi.edu/nsnam/ns/.

The faults of Data Security and Privacy in the Cloud Computing

AL-Museelem Waleed[1,a], Li Chunlin[2,b], Naji, Hasan.A.H[3,c]
[1, 2,3]School of Computer Science, Wuhan University of Technology, Wuhan, CHINA
[a]waleed_aboanas@hotmail.com, [b]waleedalmuseelem@gmail.com, [c]hasanye1985@gmail.com

Abstract—**According to Winkler [1], public cloud is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.**

The main benefits of using public cloud services include:

- **Easy and inexpensive set-up.**
- **Scalability to meet needs.**
- **No resource wastage.**

The term "public cloud" was invented to differentiate between the standard model and the private cloud, which is a proprietary network or data center that uses cloud-computing technologies, such as virtualization.

Examples of public clouds include Amazon Elastic Compute Cloud [2], IBM's Blue Cloud, and Sun Cloud. Despite of the advantages it also has some faults in its infrastructure. With the customer being unaware of their data storage over the internet, the problem is mainly the security and storage of client's data.

In the paper the faults on security of their data storage and it's privacy is reviewed. It also includes in it conducted experiment and statistical analysis using ubuntu simulation. The paper identifies the faults and proposes solutions to combat the identified problems.

I. INTRODUCTION

Cloud computing is a flexible delivery platform for business or consumer services provided over the internet. Public cloud computing delivers better services under pressure. The concept of cloud computing was initiated in the early 1960's and initially was used basically by telecommunication companies. By the year 2008 Gartner highlighted the characteristics for customer and service providers [3]. The paper outlines awareness of cloud computing power in the entire IT industry through addressing of global challenges and arising issues in implementation of the public cloud infrastructure.

Nowadays the topic of Cloud Computing use is considered to be a burning issue as this notion is rather new and still not studied enough. Therefore, its advantages and disadvantages are currently discussed by the specialists. According to the definition, Cloud Computing is "a model for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications, rather than a direct connection to a server. Data and software packages are stored in servers. However, cloud computing structure allows access to information as long as an electronic device has access to the web. This type of system allows employees to work remotely**." (**Hurwitz, Judith., Boor & Kaufman**).**

In spite of all the possible security and privacy risks, Cloud Computing is believed to be beneficial for the public and private IT organizations. According to the latest researches, this phenomenon is proved to have six main advantages that make it attractive for the potential users. There is a brief summary of these peculiarities:

1. Economy of cost (Cloud technology is usually paid incrementally, thus saving money for the company);
2. High level of automatism (this software product has the update function and IT personnel can escape this task);
3. Increase of Storage capacity (more data can be stored as compared to the private computer systems);
4. Flexibility (more flexible in comparison with the previous computing methods);
5. Mobility (the employees are able of accessing the information from the place of their location);
6. Freedom of actions to the organization (the company has the possibility to shift the focus and concentrate better on the innovations than on the constant server updates).

The principle of the Cloud Computing is related to the

doi:10.4304/jnw.9.12.3313-3320

searching for the connection between the main layers of the structure. It usually consists of five layers: client, application, platform, infrastructure and server. Correspondingly, each of them has its own characteristics and is considered to play important role in the process of Cloud Computing. Consequently, this trend is very interesting and useful to investigate as it may become a basis of the future IT structure for the organizations.

In the collection of information and statistics, experiments were conducted and analysis done using ubuntu simulation. With a review of cloud computing data storage, addressing the security faults and challenges faced in implementation of public cloud service, including mitigation steps [4].

The report gives out in details what are to be considered and guidelines on implementing cloud computing with computer organizations.

The paper is categorized into sections: Section one presenting the Abstract [5]. Section two provides the introduction, section three includes the literature review, section four represents the problem statement, section five contains the proposed solution , section six containing the experiment results and analysis using ubuntu simulation, section seven presents the conclusion and future work and finally the references in section eight.

II. Literature Review

The literature identifies the major broad service models used in cloud computing. The most recognizable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet [6]. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same-shared infrastructure.

The most salient examples of cloud computing tend to fall into the public cloud model because they are, by definition, publicly available. Software as a Service (SaaS) [7] offerings such as cloud storage and online office applications are perhaps the most familiar, but widely available Infrastructure as a Service (IaaS) [8] and Platform as a Service (PaaS) [9] offerings, including cloud based web hosting and development environments, can follow the model as well (although all can also exist within private clouds). Public clouds are used extensively in offerings for private individuals who are less likely to need the level of infrastructure and security offered by private clouds. However, enterprise can still utilize public clouds to make their operations significantly more efficient, for example, with the storage of non-sensitive content, online document and webmail [10].

The public model offers the following features and benefits:

A. Ultimate scalability

Cloud resources are available on demand from the public clouds' vast pools of resource so that the applications that run on them can respond seamlessly to fluctuations in activity

Cost effective; public clouds bring together greater levels of resource and so can benefit from the largest economies of scale. The centralized operation and management of the underlying resources is shared across all of the subsequent cloud services whilst components, such as servers, require less bespoke configuration. Some mass-market propositions can even be free to the client, relying on advertising for their revenue.

B. Utility style costing

Public cloud services often employ a pay-as-you-go charging model whereby the consumer will be able to access the resource they need, when they need it, and then only pay for what they use; therefore avoiding wasted capacity.

C. Reliability

The sheer number of servers and networks involved in creating a public cloud and the redundancy configurations mean that should one physical component fail, the cloud service would still run unaffected on the remaining components. In some cases, where clouds draw resource from multiple data centers, an entire data centre could go offline and individual cloud services would suffer no ill effect. There is, in other words, no single point of failure which would make a public cloud service vulnerable [11].

D. Flexibility

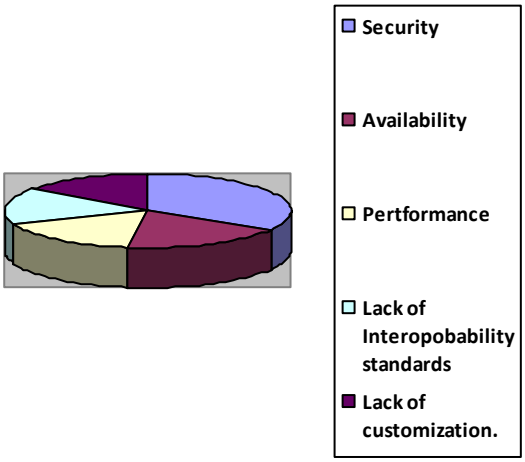
There are a myriad of IaaS, PaaS and SaaS services available on the market which follow the public cloud model and that are ready to be accessed as a service from any internet enabled device. These services can fulfill most computing requirements and can deliver their benefits to private and enterprise clients alike. Businesses can even integrate their public cloud services with private clouds, where they need to perform sensitive business functions, to create hybrid clouds [12].

E. Location independence

The availability of public cloud services through an internet connection ensures that the services are available wherever the client is located. This provides invaluable opportunities to enterprise such as remote access to IT infrastructure [13] or online document collaboration from multiple locations. The most recognizable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as

the internet. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same shared infrastructure.

The most salient examples of cloud computing tend to fall into the public cloud model because they are, by definition, publicly available. Software as a Service (SaaS) offerings such as cloud storage and online office applications are perhaps the most familiar, but widely available Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings, including cloud based web hosting and development environments, can follow the



model as well (although all can also exist within private clouds). Public clouds are used extensively in offerings for private individuals who are less likely to need the level of infrastructure and security offered by private clouds. However, enterprise can still utilize public clouds to make their operations significantly more efficient, for example, with the storage of non-sensitive content, online document collaboration and webmail [14].

III. Problem Statement

The capacitance of cloud computing that is to be used b y an information and technology organization. Giving inspirations for the implementation of cloud computing. The section is based on security issues of cloud computing, with results of a research conducted on cloud computing security.

A. Research Results on Cloud Computing Security

Figure 1. Note how the caption is centered in the column.

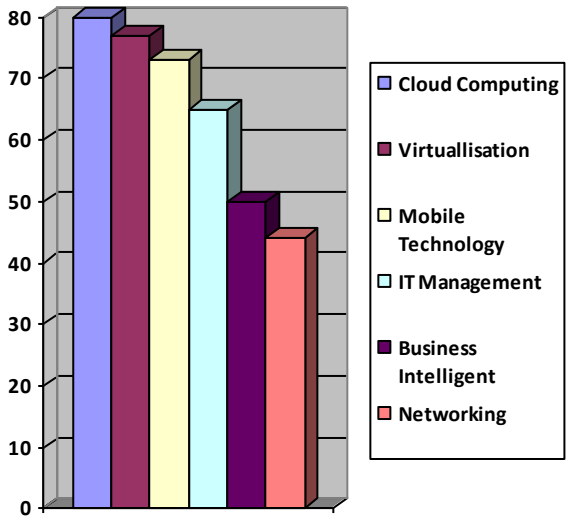


Figure 2. Cloud Computing Technology

B. Security Issues In Cloud Computing.

Cloud computing is a use of diverse computer resources like software and hardware introduced as a service within the certain network, especially Internet. Basically, there exist three kinds of cloud computing: service platform, infrastructure as a service and software service. The information flow is usually provided within the network and by means of central and remote servers.

This way, computer owners can track the work done and secure operational systems on remote computers. Virtualization is an aspect of cloud computing where virtual versions of operating systems, hardware platforms, network resources or storage devices are created. The main purpose of virtualization is to centralize administrative tasks, improving overall hardware-resource utilization. The ability to run two operating systems in parallel mode allows reducing overhead costs due to running the same programs within the same operating systems.

Both cloud computing and virtualization can have numerous benefits and drawbacks. First of all, let us speak about cloud computing. Cloud computing is favorable in terms of ability to achieve economies of scale. It allows increasing production output with fewer people. Respectively, the cost of projects is also slightly reduced because of that. Furthermore, cloud computing give an opportunity to globalize workforce for cheap. It means that everyone from everywhere can access the computer cloud via Internet. Cloud computing also reduces spending on technology infrastructure: minimal upfront spending is worth unlimited access to information.

Thanks to cloud computing, more work is usually done in less time. Once hardware and software are purchased, there is no need in constant replacement due to cloud computing, which significantly reduces capital costs. Cloud computing also allows tracking and planning projects within the certain budget, making reasonable business forecasts for the future.

Regarding the fact that cloud computing is based upon the utilization of hardware and software, it is easy to use and there is no need in personnel training. Minimizing licensing of software met due to cloud computing and this improves company flexibility. However, there are several disadvantages of cloud computing. The first is probable downtime. If Internet connection is not reliable, providers are expected to suffer server outages. Additionally, cloud computing may not always be favorable for large companies, which utilize huge resources and keep much information. Cloud computing provides availability of all details and in some cases it cannot be appreciated. Apart from that, there is a great chance of choosing ineffective cloud computing vendor who will offer ineffective and inflexible package.

Virtualization also has both benefits and drawbacks. Let us initially focus upon its benefits. The major benefit of virtualization is the amount of hardware required for all software applications. And this is a cost-saving factor. Additionally, application virtualization offers a flexible opportunity to run applications with various configuration settings. Virtualization eliminates the need to run numerous separate servers. This way, hardware is seen to be used efficiently. Living in the globalized world, we are always linked to computers. Virtualization support enables many organizations to outsource practically all their computing requirements.

Respectively, the costs related to central server are also slightly reduced. Additionally, numerous virtualization tools allow users rapidly maintain various testing environments with the opportunity to restore them to their original state. Finally, virtualization is easy to be applied, without fearing numerous hardware compatibility concerns, base computing environments and so on.

Thus, in some cases virtualization can be unfavorable. For example, virtualization has a single point of failure, which means when the central server breaks down, the rest crashes as well. In addition, visualization always demands expensive computers with powerful parts, which may be a costly solution for many small and medium-sized businesses. Finally, when dealing with databases, it would be extremely difficult to implement virtualization as databases and warehousing both require disk operations as well as numerous network updates.

Concerning cloud computing, one should also be aware that organizations must evaluate their existing governance against the cloud security model and understand the residual risks and what compensating controls need to be implemented. Governance areas for concern include risk management, legal and compliance, life-cycle management and portability [14].

Organizations must evaluate their existing governance against the cloud security model and understand the residual risks and what compensating controls need to be implemented. Governance areas for concern include risk management, legal and compliance, life-cycle management and portability [15].

Operational security concerns include business continuity, disaster recovery, incident response, encryption, vulnerability assessment, identity access management and virtualization [16].

The cloud multi-tenant environment security controls are developed for a general service offering which may or may not provide adequate security for every organization. Organizations need to assess their vulnerabilities and implement threat prevention policies and technologies; otherwise, reacting to breaches will become more the rule than the exception [17].

The cloud plays a critical role in helping organizations capitalize on the efficiency, flexibility and ease of operation. Companies must invest in people with the technical skills necessary to assess their readiness for implementing different cloud architectures that help move data in and out of public/private clouds and understand the security risks associated with changes related to cloud architecture.

Because of the organizational and cultural complexities of executing cloud strategies, companies are opting, to "out task" certain aspects of their operations because skilled resources are in short supply. Companies who understand the organizational impacts of cloud and who can acquire these skills, set the right security policies, and build closer relationships with the lines of business will be the best able to mitigate the two big risks associated with cloud security [18].

In the SAAS model control lies on the cloud service provider hands.

It is risk as delicate and sensitive information might be accessed someone else. Providing guidelines for the process.

7. Protection of transferred data.
8. Service provider giving clients security policies.
9. Back up Availability.
10. Lack of availably of data backups.
11. Multi-Tenancy.

A future of SAAS that allows a single program running in multiple machines It increases vulnerability.

IV. Proposed Solution

The authenticity and confidentiality of data are based on data encryption method. Encryption of data, which includes digital signatures, clients are provided with superset signatures and metadata along having querying results. Encryption variety incorporates querying encrypted data that utilizes several cryptographic

methods in data encryption Simulation tool.

The simulation tool is distributed file base system, which is downloadable in the Ubuntu and other operating systems. There is a critical need in information security, and one of the most crucial ways to localize possible threats is simulation and modeling. The simulation is the process of designing the real cyber-attacks models. This process is targeted to satisfy the expectations at the end. The simulation models can be continuous and discrete, depending on time characteristics. Constructing models, we test our system in the virtual world and want to shape our company strategy. Here it is obvious that the simulation model is effective as it depicts all the processes that are planned to happen in succession. Though each process is connected to the other one, they are supposed to be supported by the respective managers. The methods of modeling and simulation should be immediately introduced to every company that is interested in getting high incomes. Although the techniques can be observed only on the planning level, they are suggested to be used due to the balanced system of business organization. No matter what tools or techniques are used, it is necessary to be precisely sure that by means of software and planning management activities each company is more likely to be successful of business. Moreover, one should also consider that the success comes after prolific and productive efforts that can be the result of only highly qualified and experienced staff. In terms of analysis and simulation models it is proposed to give priority to team or group work and profound brainstorming. In terms of management processes it is suggested to implement the innovative software within each department that is recommended to be used only by the professional managers, who can bring positive results. As for the types of attacks performed in the system, they are as follows: Mandatory attacks, SQL injection attacks, and directory traversal attacks.

Indisputably, every particular organization is prone to threats, because in all times the competing companies are targeted to drive their rivals out of the market, gaining the competitive advantage over them. Generally, network security threats can combine various risks, problems and attacks, which are very frequently called the security vulnerabilities. The human behavior in the body of employees is the first danger in terms of security network. Apart from that, organizations can be also vulnerable for threats, because not all of them are engaged in using properly configured networks and not all of them have enforced the reasonable and sensible security policy without consulting the expert. That is why if we are targeted to design the secure network, we need to incorporate fault-tolerant solutions and systems.

Basically, it is crucial for the business organization to establish correct information security policy in order to function in accordance with the norms of law and at the same time preserve its interests. The majority of corporation and non-governmental organizations protect the information that can be damaged or used to threaten the national security or reveal some trade secrets of companies. There are also certain rules adopted by the state authorities for information clearance and the ways it should be gathered, stored, transmitted and damaged. These are security precautions that are needed for the organizations and individuals for ensuring their protection.

V. Experiment and analysis

The chart figures shows the attacks conducted on the simulation tools while using security models and when security models are not available. System with no security model is better than systems having the security model. Systems with security model require resources for the system. After conduction of the attack using the cloudism simulation tool and open stack process, the performance increases after each attacks making simulation of the cloud competing vital.

TABLE I.
CLOUD COMPUTING ATTACKS

Experiment results	Attacks	Using of SACS Extent	Not using SACS Extent
Cross VM attacks	10	25	70
Mandatory access attacks	15	43	90
Sql injection attacks	10	34	68
Directory traversal attacks	5	21	57
DDos attacks	25	35	68

System Performance against time

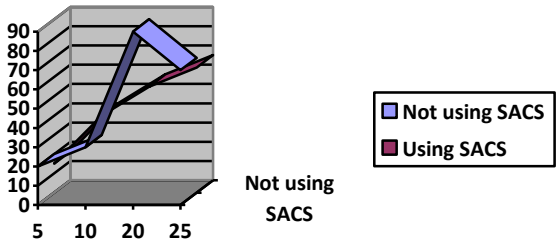


Figure 3. System Performance(1)

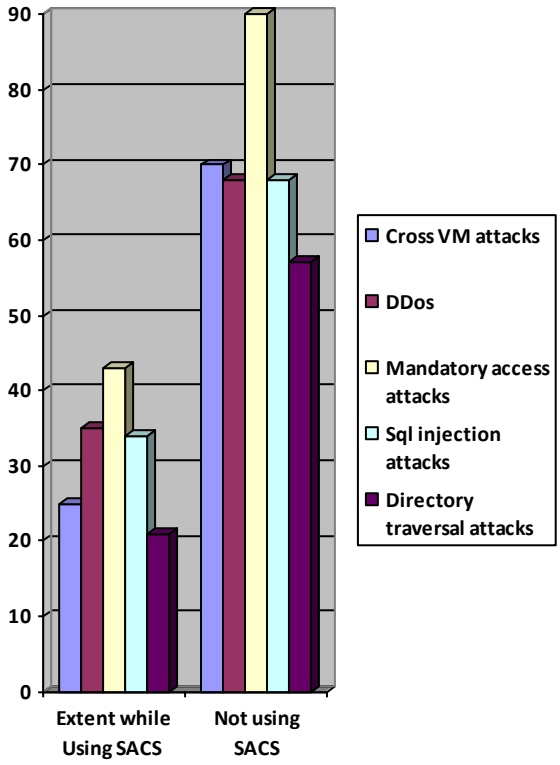


Figure 4. System Performance(2)

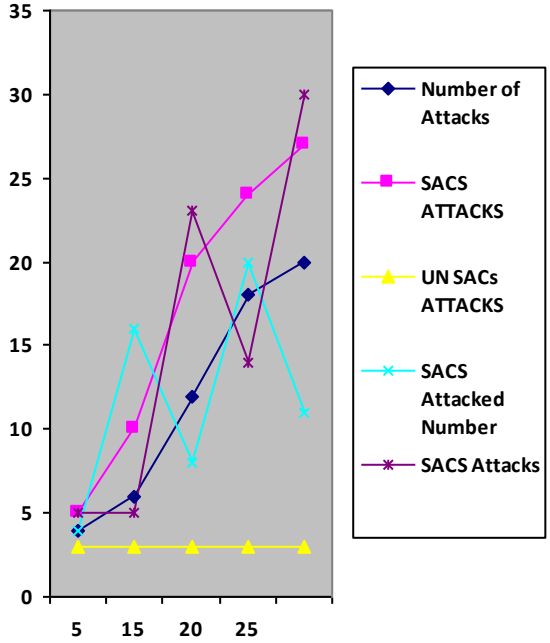


Figure 5 System Performance (5)

VI. Conclusion

Cloud computing serves as the latest development that provides for easy access to higher performance computing services and storage through the web. It offers unique opportunities to many countries in the world through the web services. After identification of problems in cloud computing steps for mitigation are identified and solutions are proposed.

VII. Future Work

Regarding cloud computing, it is necessary to take into account numerous security issues as an important part to consider. The security issues include data handling, management, governance, and data protection of personal information. Cloud computing regularly encounters security challenges. As for this paper, it has communicated the initial steps in the security challenge.

Acknowledgment

The work was supported by the National Natural Science Foundation (NSF) under grants (No.61171075), National Key Basic Research Program of China (973 Program) under Grant No.2011CB302601, Special Fund for Fast Sharing of Science Paper in Net Era by CSTD (FSSP) No.20130640001, Program for the High-end Talents of Hubei Province, Specialized Research Fund for the Doctoral Program of Higher Education under Grant

No.20120143110014 and the Open Fund of the State Key Laboratory of Software Development Environment (SKLSDE-2013KF). Any opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of the above agencies.

REFERENCES

[1] Winkler, Vic J. R. *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Burlington: Elsevier Science, 2011. Internet resource.

[2] "Research and Markets Adds Report: State of Cloud Computing Security in the UAE." *Manufacturing Close - Up* (2013)*ProQuest.* Web. 22 Dec. 2013.

[3] "Research and Markets Offers Report: State of Cloud Computing Security in the UAE." *Professional Services Close - Up* (2013)*ProQuest.* Web. 22 Dec. 2013.

[4] "SafeCentral Integrates Browser Security Solution with NetSuite's Cloud Computing Platform." *Business Wire*Dec 01 2010. *ProQuest.* Web. 22 Dec. 2013 .

[5] "Security Experts from Core Security and Invincea Lead Special Issue on Cloud Computing Security for IEEE Security & Privacy Magazine." *Business Wire*Dec 08 2010. *ProQuest.* Web. 22 Dec. 2013 .

[6] Alzain, Mohammed A., Ben Soh, and Eric Pardede. "A New Model to Ensure Security in Cloud Computing Services." *Journal of Service Science Research* 4.1 (2012): 49-70. *ProQuest.* Web. 22 Dec. 2013.

[7] Antonopoulos, Nick, and Lee Gillam. *Cloud Computing: Principles, Systems and Applications*. London: Springer, 2010. Print.*Auditing Cloud Computing: A Security and Privacy Guide*. Wiley, 2011. Internet resource.

[8] Badamas, Muhammed A. "Cyber Security Considerations when Moving to Public Cloud Computing." *Communications of the IIMA* 12.3 (2012): 1-18. *ProQuest.* Web. 22 Dec. 2013.

[9] Bradner, Scott. "Cloud Computing Security: Who Knew?" *Network World* 26.17 (2009): 16. *ProQuest.* Web. 22 Dec. 2013.

[10] Gutwirth, Serge. *Computers, Privacy and Data Protection: An Element of Choice*. Dordrecht, The Netherlands: Springer, 2011. Print.

[11] Howell, Donna. "Security Still Top Cloud Issue, Pair of Recent Surveys Confirm Majority See Vulnerability Moving to Internet-Based Computing Slowed as Top Executives Preach Caution." *Investor's Business Daily*Nov 07 2011. *ProQuest.* Web. 22 Dec. 2013 .

[12] Ismail, Noriswadi, and Edwin L. Y. Cieh. *Beyond Data Protection: Strategic Case Studies and Practical Guidance*. Berlin: Springer, 2013. Internet resource.

[13] Krutz, Ronald L, and Russell D. Vines. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Indianapolis, Ind: Wiley Pub, 2010. Internet resource.
Proceedings. Berlin: Springer, 2011. Print.

[14] Mantri, Archana. *High Performance Architecture and Grid Computing: International Conference, Hpagc 2011, Chandigarh, India, July 19-20, 2011. Proceedings*. Berlin: Springer, 2011. Print.

[15] Pohlmann, Norbert, Helmut Reimer, and Wolfgang Schneider. *Isse 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*. Wiesbaden: Vieweg + Teubner, 2011. Internet resource.

[16] Prasad, Sushil K. *Information Systems, Technology and Management: 4th International Conference, Icistm 2010, Bangkok, Thailand, March 11-13, 2010. : Proceedings*. Berlin: Springer, 2010.

[17] Qaisar, Sara, and Kausar Fiaz Khawaja. "CLOUD COMPUTING: NETWORK/SECURITY THREATS AND COUNTERMEASURES." *Interdisciplinary Journal of Contemporary Research In Business* 3.9 (2012): 1323-9. *ProQuest.* Web. 22 Dec. 2013.

[18] Sommer, Thomas, Tanya Nobile, and Paul Rozanski. "The Conundrum of Security in Modern Cloud Computing." *Communications of the IIMA* 12.4 (2012): 15-40. *ProQuest.* Web. 22 Dec. 2013.

[19] "How should Mobile and Cloud Computing be Treated in Cyber Security Budgets?" *The Controller's Report*.12 (2011): 3-5. *ProQuest.* Web. 22 Dec. 2013.

AL-Museelem Waleed, I'm from Kingdom of Saudi Arabia birth in 5th January 1981 at Capital City Riyadh. Currently I'm a PhD student in College of Computer Science and Technology at Wuhan University of Technology. I received M.S in Computer Science and Technology from Wuhan University of Technology, China, in 2012. My research interests are cloud computing security and data privacy.

Li Chunlin, she is a Professor of Computer Science in Wuhan University of Technology. She received the M.S in Computer Science from Wuhan Transportation University in 2000, and PhD in Computer Software and Theory from Huazhong University of Science and Technology in 2003. Her research interests include cloud computing and distributed computing.

Naji, Hasan.A.H, He is currently a PhD student in college of Computer Science and Technology at Wuhan University of Technology. He received his B.S and M.S from Wuhan University of Technology, China, in 2008 and 2010 respectively. His research interests are cloud computing, Service Oriented Computing (SOC) and ontology.

TTAF: TCP Timeout Adaptivity Based on Fast Retransmit over MANET

Wesam A. Almobaideen and Njoud O. Al-maitah
The University of Jordan/Computer Science, Amman, Jordan
Email: wesmoba@ju.edu.jo, njoud.maitah@yahoo.com

***Abstract*—Transmission Control Protocol (TCP) is one of the most widely deployed transport layer protocols. It responds to all packet losses, either due to congestion or link breakages, by invoking various congestion control mechanisms. All these mechanisms imply a reduction in the amount of transmitted data. Computing a proper value of the retransmission timeout (RTO) is a challenge for TCP. In mobile ad hoc networks (MANET), mobility and bit error cause a lot of packet losses which degrades TCP throughput. In this paper we introduce an adaptation of TCP NewReno in order to improve its performance during the fast recovery phase. Our adapted algorithm, which we called TTAF, does not rely only on round trip time samples but also takes into consideration fast retransmit events in tuning the value of RTO. A set of experiments have been conducted to evaluate the effect of TTAF over MANET with various mobility speed, traffic load, and bit error rates. Results have shown an improvement in TTAF throughput compared with that of TCP NewReno.**

***Index Terms*—TCP Timeout Adaptation; Fast Retransmit; Fast Recovery; Mobile Ad Hoc Networks**

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a decentralized wireless network which consists of mobile nodes that move freely and communicate via multi hop links. MANET has got a large attention in the ten past years and a number of researches have investigated its potential applications in many fields of our life. The need for MANEN clearly appears in situations where the infrastructure establishment is either expensive or impossible such as rescue missions and battle fields operations [1].

Transmission control protocol (TCP) is a reliable end-to-end protocol between pairs of processes over unreliable network. TCP achieves its reliability through sequence numbers, acknowledgment and retransmission. It provides flow control and congestion control. Congestion control is achieved via adapting the transmission rate of data based on the available network capacity. After sending a data packet, TCP sets an estimated RTO period within which it expect to get the corresponding ACK back. Packet loss is considered as a sign of congestion and is detected by timeout expiration. Should the destination receive an out of order packet, then it sends a duplicated ACK of the last packet that has been received in order [2-5].

Receiving a number of duplicated ACKs could be used as a sign of packet loss, an approach that is called fast retransmit [6]. Receiving one duplicated ACK could be interpreted as a delayed packet delivery and not necessary a lost one. For that reason, the TCP sender waits for three duplicative ACKs before invoking the fast retransmit procedure. This provides a kind of assurance that the packet is really lost and should be retransmitted immediately without the need to wait until the RTO expiration in order to retransmit that lost packet. Fast retransmission allows higher channel utilization and throughput [4].

TCP faces some challenges over wireless networks since it was not originally designed to work in such an environment which is characterized by very dynamic topology and high bit error rate [4]. The performance of TCP degrades with high mobility since it reduces the transmission rate due to link breakages and consequently packet dropping. TCP interprets the absence of ACK as congestion, and consequently, when the RTO expires it retransmits the corresponding packet and duplicates the value of RTO. Furthermore, TCP invokes slow start congestion control mechanism which decreases the window size to one segment [7-8].

TCP computes the value of RTO based on the Round Trip Time (RTT) samples. RTT is the period between the sending a packet and receiving its corresponding ACK [2]. Determining the appropriate RTO value is not an easy task since it is affected by many network factors such as multiple path existence, the dynamicity of the network topology, and the experienced bit error rate [10].

The original algorithm for computing the timeout keeps a running average of RTT and then computes the timeout value as a function of RTT. Specifically, TCP sender records the time of sending a packet and of receiving its corresponding ACK. A "SampleRTT" is then computed as the difference between these two time instances. Afterward, TCP computes an "EstematedRTT" as in (1), [10].

$$\begin{aligned}\text{EstematedRTT} = \alpha \times \text{EstimatedRTT} \\ + (1 - \alpha) \times \text{SampleRTT}\end{aligned} \quad (1)$$

where α is weighting parameter selected to make the EstimatedRTT changes smoothly. It is recommended to set α to a value that is not too small, which causes the EstematedRTT to follow the fluctuation of the

doi:10.4304/jnw.9.12.3321-3326

SampleRTT, and not too large since it then reduces the adaptivity of the EstematedRTT. The recommended value of α is 0.8. The RTO value, interchangeably called Timeout, is then computed as in (2):

$$\text{Timeout} = 2 \times \text{EstimatedRTT} \quad (2)$$

Jacobson and Karle noticed that the main problem of the original algorithm is that it doesn't take into account the variance between SampleRTT values. If the variance is small, then the EstimatedRTT can be better trusted and there is no reason for multiplying the EstematedRTT by 2 to compute the Timeout. On the other hand, a large variance in RTT samples suggests that the timeout value should not be too tightly coupled to the EstimatedRTT [11].

The standard algorithm of estimating TCP's RTO computes the Difference, the EstimatedRTT, and the variance between SampleRTTs (Deviation) as in (3), (4), and (5) respectively, [11].

$$\text{Difference} = \text{SampleRTT} - \text{EstimatedRTT} \quad (3)$$

$$\text{EstimatedRTT} = \text{EstimatedRTT} + (\beta \times \text{Difference}) \quad (4)$$

$$\text{Deviation} = \text{Deviation} + \sigma \times (|\text{Difference}| - \text{Deviation}) \quad (5)$$

where σ and β are two parameters used to give weight to the more important terms. The recommended value for each, according to the standard, is within (0, 1) for σ and 0.125 for β. TCP then computes the Timeout as in (6):

$$\textit{Timeout} = \mu \times \text{EstimatedRTT} + \varphi \times \text{Deviation} \quad (6)$$

where μ is set to 1 and φ is set to 4 as recommended values. This is done in order to allow for faster adaptation of timeout value according to the variance in SampleRTT [10].

The rest of this paper is organized as follows. The related work is presented in section II. Section III explains the proposed idea of TTAF. Section IV illustrates the setting of simulation environment and the results evaluation and discussion. Finally, section V concludes the paper.

II. Related Works

Alex Kesselman and Yishay Mansour in [2] have studied optimizing the RTO value depending on RTT and the TCP window size to maximize the throughput. They derive the RTO value based on several RTT distributions and found that TCP window size gets larger, the optimal RTO value services for longer period.

In [10] a transport layer and end-to-end approach was proposed to differentiate packet loss due to link failure from that due to congestion. It uses the history of queue usage rate where the ascending growth of queue usage refers to increased probability of congestion loss. On the other hand, a fixed averaged queue usage value can be considered as a sign of link failure losses. This study also has presented an approach that compares between the characteristics of the broken route and the re-established route in term of Relative On-way trip time (EROTT) and number of hops. EROTT helps TCP to set a suitable RTO for new route.

In [3], the authors have argued that computing the RTO based on only RTT is not enough. They proposed contention adaptive retransmission timeout (CA-RTO) algorithm. This algorithm uses a contention parameter which reflects the effect of contention into timeout. Furthermore, they introduced a randomization technique which adjusts/extends the timeout value in case of high contention.

In [13] a TCP Friendly Rate Control (TFRC) has been used to develop a cross-layer design that aims to improve the performance of video transmission over MANET. It gives priority to video packets via the utilization of information from the MAC layer. Signal to Noise Ratio (SNR) measurements through the routing path have been used to increase the efficiency of route reconstruction. Simulation results proved that traffic classification and the SNR utilization have improved the end-to-end and Quality of Service (QoS) provision.

A new variant of TCP called TCP AR (TCP Adaptive RTO) enhances the performance of standard TCP by adapting retransmission timeout to network conditions [14]. This approach combines between TCPW ABSE (TCP Westwood Adaptive Bandwidth Share Estimation) with new RTO back off mechanism. When packet loss is not due to congestion but to link failure, TCP AR prevents the RTO exponential back off. The key of this work is that if packet loss is detected by timeout and there are other signs which indicate that there is no congestion, then it is not necessary to trigger the TCP RTO exponential back off procedure. TCP AR detects the state of network by estimate network throughput using throughput filter that already exist in TCPW ABSE. The path congestion level is determined by comparing the throughput estimation with current CNWD which represents the instantaneous sending rate. If (throughput * RTT) is larger than the CNWD, this indicates that there is no congestion. Otherwise the packet loss is due to congestion so doubling the RTO.

In [5] ER-SRTO algorithm has been proposed to detect packet loss during delay spike. The proposed solution performs an efficient recovery in the RTO using the ACK of the retransmitted packet and without calling additional loss recovery mechanisms.

III. Idea of TTAF

The main idea of TTAF is to rely on fast retransmit events to more accurately adapt the value of Retransmission Time Out (RTO) calculation during the fast recovery period. The basic assumption of fast retransmit is that the network is not highly congested since the source TCP has received three duplicated ACKs safely. This allows the TCP source to retransmit the supposedly lost packet faster than waiting the RTO period to expire. After a fast retransmission event, TCP enters fast recovery phase. Since the sending side does not need to drastically reduce congestion window

(CNWD), fast recovery reduces CNWD to one-half of current CNWD. Furthermore, each time TCP sender gets additional duplicated ACKs, it transmits more one packet. In case of multiple losses in CNWD, TCP NewReno solves this issue using partial ACK, where TCP does not get out from fast recovery phase until it receives new ACK which acknowledges all packets in CNWD.

From the simulations traces analysis presented in [14], it is concluded that consecutive timeouts plays a major factor which affects TCP performance over wireless environment. A TCP source assumes that losses are due to congestion since TCP's RTO mechanism was originally designed for wired networks. When a timeout occurs, TCP assumes that the network is severely congested and accordingly invokes the congestion control mechanisms. These mechanisms imply lowering the CNWD value and doubling the RTO, which is calculated mainly based on the RTT value, so that the network could recover from the congestion state.

In MANET, consecutive timeouts could come as a result of route failures and not severe network congestion. Multipath routing could also play a role in delivering packet with more delay than other adjacent packets that have been sent over different paths [15]. Fast retransmit distinguishes between the two cases and allows the TCP source to reduce the time it waits to retransmit a packet that has been lost due to link failure or bit error. We think that more beneficial actions could be carried out based on a fast retransmit event. Such an action could be the modification of the value of the RTO. Furthermore, in case a loss has happened during fast recovery, the timeout expiration event is inevitable and there is a need to reduce RTO value in such case.

TTAF takes into consideration the difference of time between the event of receiving the third duplicated ACK and the end of the RTO period as shown in Fig. 1.

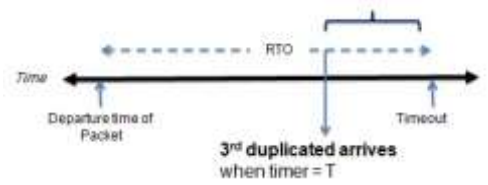


Figure 1. TTAF time line

This amount of time is used to lower the RTO value since it represents the unnecessary period of time a TCP source skipped after the reception of the third duplicated ACK. TTAF reduces the Timeout value by a fraction of this time difference, as shown in (7), since it could be risky to severely subtracting this whole time difference from the RTO value, see (8).

$$\text{FastDiff} = T \tag{7}$$

$$\text{FRTimeout} = \text{Timeout} - \omega \times \text{FastDiff} \tag{8}$$

where T is the remaining value of the TCP Timeout when the third duplicated ACK received, and ω is weighting factor that we recommend to be set to 0.25 based on some initial experiments.

It is worth to note here that fast retransmit does not displace timeout mechanism. The timeout mechanism is usually the sole player in determining lost packet for small window sizes or when the loss occurs at the end of a large window. This is because, in such cases, packets in transit are not enough to trigger fast retransmit. These cases are the target of TTAF and where it should be useful usage to increase the adaptivity of TCP Timeout. TTAF does this by anticipating such situations by lowering the RTO value to make it more close to the proper one based on previous fast retransmit events. Fig. 2 presents the idea in a form of a flow chart that could give more detailed illustration of TTAF.

IV. Results Evaluation and Discussion

We have conducted several simulated experiments to evaluate the performance of TTAF and compare it with TCP NewReno. The experiments were carried out using Glomosim 2.02 simulation package [16]. Different scenarios have been generated assuming 50 nodes in a 1200 meter by 1200 meter terrain area. The number of source nodes was 25 out of the 50 total nodes. The whole simulation time was 10 minutes. Each simulated scenario has been repeated several times with different simulation seeds in order to get confidence in the resulted average.

In the first three simulated experimental results, the nodes have moved randomly with a speed that varies in different scenarios as 0, 5, 10, 15, 20, 25, and 30 mps with a 30 seconds pause time. The throughput comparison between TTAF and TCP NewReno, shown in the first three figures of simulated results, measures the performance of both protocols as the mobility speed increases.

Figure 2. TTAF flow chart illustration

As we move from Fig. 3, Fig. 4, to Fig. 5, the number of packets sent by each TCP source increases from 1000, 2000, and up to 5000 data packets. This is done in order to evaluate the effect of increased traffic load over the simulated ad hoc network in addition to the effect of mobility speed.

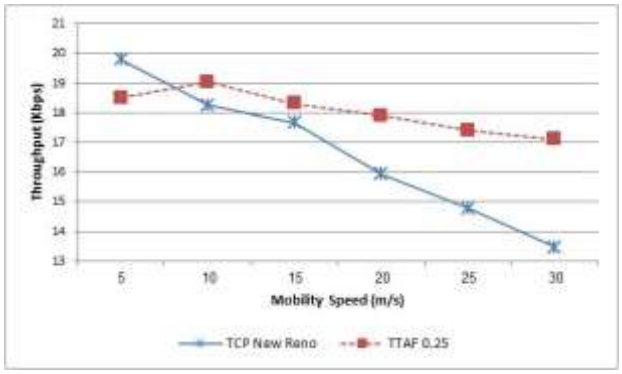


Figure 3. Throughput Vs. Mobility Speed (1000 Packets)

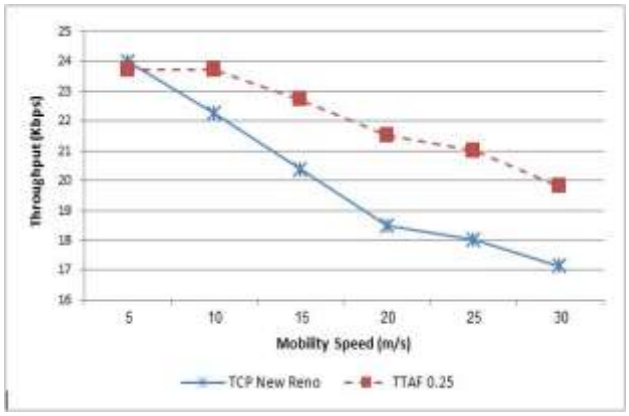


Figure 4. Throughput Vs. Mobility Speed (2000 packets)

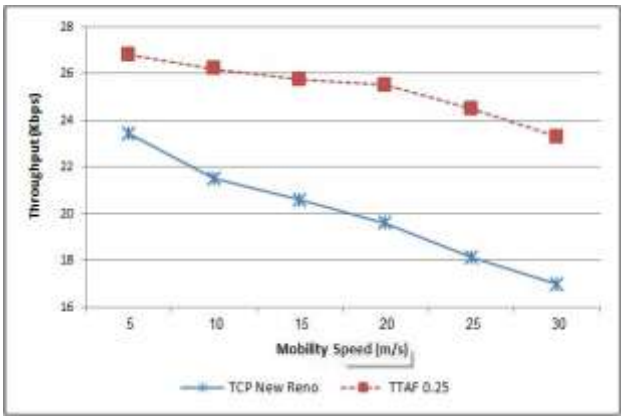


Figure 5. Throughput Vs. Mobility Speed (5000 Packet)

Fig. 3 shows that TTAF outperforms TCP NewReno for values of mobility speed start from 15 m/s when each TCP source sends 1000 packets. It shows that throughput decreases for both TTAF and TCP NewReno as the mobility speed increases. This occurs since the link breakages due to mobility increase which causes a more dropped data and ACK packets. In case of losing the retransmitted packet, timeout is invoked. This does not allow the TCP source in NewReno to figure out the real reason of data loss (i.e. whether it is due to severe congestion or link breakage). In contrast, TTAF makes its role in reducing the value of RTO based on the previously encountered FR. When the timeout during fast recovery phase is not avoidable, TCP sender waits for a shorter period of time to resend the lost packet and, accordingly, will be able to recover the size of the CNWD faster in TTAF than TCP NewReno.

Fig. 4 and Fig. 5 confirm the results that has been presented in Fig. 3. when we study these figures, we can notice that the difference in throughput between TTAF and TCP NewReno becomes bigger. In Fig. 5, it is noticeable that for all values of mobility speed TTAF is able to outperform TCP NewReno. This is because as the traffic load increases the number of packets in transmit increases, and this raises up the probability of FR occurrence and, as a result, elevates the utilization of TTAF improvement in the measurement of RTO during fast recovery. TTAF makes its role during this more frequently happing events with higher traffic load in reducing the value of RTO during fast recovery, based on previously encountered fast retransmit event. This is done by TTAF so that the source will not wait for long period of RTO when fast retransmit is not an option.

Fig. 6 illustrates a more detailed study of the effect of increasing traffic load on the behavior of the compared protocols while the nodes move with a mobility speed of 10 mps. One can notice that the throughput in TTAF TCP NewReno increases while traffic load increases up to a certain point after which the congestion become so severe and cause a drop in throughput. Fast retransmit can help in cases where there are enough packets that have been delivered after the lost one. In these situations, TTAF helps in reducing the value of RTO and so increasing the achieved throughput when fast retransmit is unable to help such as loss during fast recovery. TTAF is able to achieve its best performance and biggest difference, compared with TCP NewReno, with high traffic load as appeared in Fig. 6 for values higher than 3000 packets traffic load.

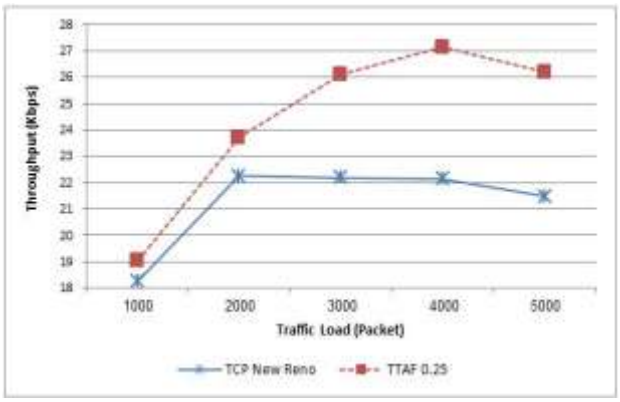


Figure 6. Throughput Vs. Traffic Load

In the results of next and last two experiments we show the evaluation of TTAF and TCP NewReno throughput while increasing the channel bit error rate from 10^{-7}, 10^{-6}, 10^{-5}, and up to 10^{-4}. The mobility speed of

each node has been assigned randomly within the rage from 5mps to 30 mps.

Fig. 7 shows a comparison of the achieved throughput when each source sends 3000 data packets during the simulation time. We can notice that TCP throughput decreases for both TCP NewReno and TTAF as the bit error rate increases. This is because as the bit error rate gets higher, the number of dropped erroneous data and ACK packets gets also higher. Consequently, TCP retransmits the dropped packets, backs off the RTO value, and reduces its CNWD more frequently. TTAF is able to outperform TCP NewReno with the existence of bit errors. This is because the lightly loaded network, in this case, is not suffering from a severe congestion which is detected by the invocation of fast retransmit. Based on fast retransmit invocation, TTAF is able to detect situations where packet loss is due to bit error and, accordingly, to decrease the RTO value. This allows TTAF sender, in contrast to TCP NewReno sender, to wait for shorter RTO in cases where waiting the timeout is inevitable during fast recovery.

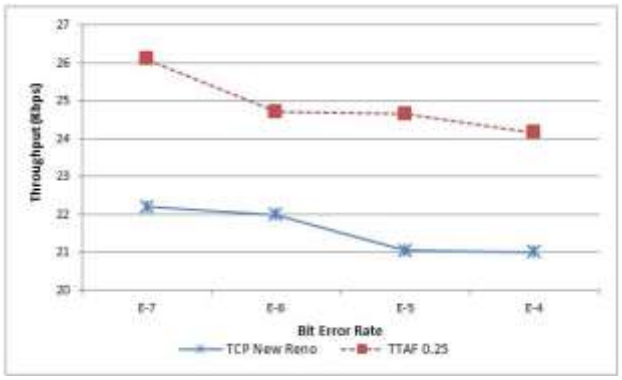


Figure 7. Throughput Vs. Bit Error Rate (3000 Packet)

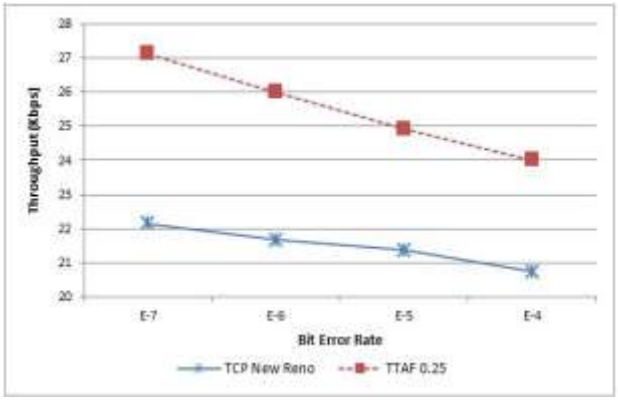


Figure 8. Throughput Vs. Bit Error Rate (4000 Packet)

Fig. 8 shows the comparison between the two TCP variants when the amount of data sent by each source has been raised to 4000 packets where each node moves by 10 mps. The figure shows that TTAF performance is more clearly better than TCP NewReno with this higher traffic load. The reason behind this is that with the increment of the data load on the network the effect of bit errors becomes more apparent and so becomes the effect of reducing the RTO.

With smaller RTO and when the timeout mechanism is the only way to detect lost packets, TTAF is able be faster in retransmitting those dropped packet and accordingly achieving higher throughput. On the other hand, TCP NewReno does not utilize the events of fast retransmit in reducing the RTO value, a fact that forces a TCP sender to wait for longer RTO in case when the packet loss is due to bit error. This decreases the throughput of TCP NewReno especially when the amount of data that is affected by the bit errors becomes higher.

V. CONCLUSION

In this paper we have presented TTAF which is a modification of TCP NewReno that tries to better adapt TCP behavior, and especially over MANET. The main aim of TTAF is to utilize the arrival of third duplicated ACK event not only to retransmit the supposedly lost packet faster than waiting for long RTO, but also to better adapt the RTO value to be closer to the proper one. The idea is that fast retransmit events indicate that the network is not severely congested and this allows the TCP sender to lower the value of RTO by a fraction of the time difference between RTO and the instance of time the third duplicated ACK has arrived.

This helps TCP sender in reducing the amount of time it has to wait for the expiration of RTO. Such a reduction in RTO value becomes very useful in certain situations like when the CNWD size is small such as the case during fast recovery phase. In such situation the timeout mechanism is normally the sole player in determining when to retransmit a lost packet. This is because the number of packets in transit is not high enough to trigger fast retransmit. Results of simulated experiments show that TTAF has achieved better throughput than TCP NewReno under various traffic loads, mobility speeds, and bit error rates.

REFERENCES

[1] Almobaideen, W., Al-Soub, R., and Sleit, A., "MSDM: Maximally Spatial Disjoint Multipath Routing Protocol for MANET," Communications and Networks, 5(4), pp. 316-322, 2013. doi: 10.4236/cn.2013.54039

[2] Mast, N., and Owens, T. J., "A Survey of Performance Enhancement of Transmission Control Protocol (TCP) in Wireless Ad Hoc," EURASIP Journal on Wireless Communications and Networking, vol. 1, pp. 1687-1499, 2011. doi:10.1186/1687-1499-2011-96

[3] Psaras, I., Tsaoussidis, V. and Mamatas, L., "CA-RTO: A Contention-Adaptive Retransmission Timeout," 14th International Conference on Computer Communications and Networks, 32(5), pp. 174-184, 2005. doi: 10.1109/ICCCN.2005.1523838

[4] Qaddoura, E., Daraiseh, A., Al Mobaideen, W., Muammar, R., Al-Walaie, S., "TCP Optimal Performance in Wireless Networks Applications," Journal of Computer Science, vol. 2, issue 5, pp. 455-459, 2006.

[5] Cho, I., Han, J., Le, J., "Enhanced Response Algorithm for Spurious TCP Timeout(ER-SRTO)," International Conference on Information Networking, ICOIN 2008, pp.1-5, 2008. doi: 10.1109/ICOIN.2008.4472748

[6] Henderson, T., Floyd, S., Gurtov, A., and Nishida, Y., "The New Reno Modification to TCP's Fast Recovery Algorithm," RFC 6582, 2012.
[7] Oliveria, R. d., and Braun, T., "A Smart TCP Acknowledgment Approach for Multihop Wireless Networks," IEEE Transaction on Mobile Computing, 6(2), pp. 192 – 205, 2007. doi: 10.1109/TMC.2007.19
[8] Almobaideen, W., Al-maitah, N., "TCP Karak: A New TCP AIMD Algorithm based on Duplicated Acknowledgements for MANET," International Journal Communication, Networks, and System Sciences, 2014, In press.
[9] Kesselman, A., and Mansour, Y., "Optimizing TCP Retransmission Timeout," ICN'05 Proceedings of the 4th international conference on Networking, Volume 2, pp. 133-140, 2005.
[10] Paxson, Vern and Allman, M., "Computing TCP's retransmission timer," RFC 2988, 2000.
[11] Sreenivas, B., Bhanu Prakash, G., and Ramakrishnan, K., "An Adaptive Congestion Control Technique for Improving TCP Performance over Ad-Hoc Networks," Elixir International Journal, vol. 44, pp. 7391-7395, 2012.
[12] Fard, M.A.K., Bakar, K.A., Karamizadeh, S., Foladizadeh, R.H., "Improve TCP Performance over Mobile Ad Hoc Network by Retransmission Timeout Adjustment," 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp. 437 – 441, 2011. doi: 10.1109/ICCSN.2011.6014086
[13] Adam, G., Bouras, C., Gkamas, A., Kapoulas, V., Kioumourtzis, G., "Cross Layer Design for Video Streaming in MANETs," Journal Of Networks, vol. 9, no. 2, 2014.
[14] Touati, H., Lengliz, I., and Kamoun, F., "TCP Adaptive RTO to Improve TCP Performance in Mobile Ad Hoc Networks," The Sixth Annual Mediterranean Ad Hoc Networking Work ShopCorfu, Greece, pp. 48-55, 2007.
[15] Almobaideen, W., Al-Khateeb, D., Sleit, A., Qatawneh, M., Al-Khdour, R., Abu Hafeeza, H.,"Improved Stability Based Partially Disjoint AOMDV", International Journal of Communications, Networks, and System Sciences, 6(5), pp. 244-250, 2013.
[16] Zeng, X., Bagrodia, R., Gerla, M., 1998, GloMoSim: a library for parallel simulation of large-scale wireless networks, PADS 98 Proceedings of Twelfth Workshop on Parallel and Distributed Simulation, pp. 154-161.

Wesam Almobaideen has received his Ph.D. in computer networks from the University of Bologna, Bologna, Italy in 2003, M.Sc. degree in computer science from the University of Jordan (UJ) in 1999, and B.Sc. degree in computer science from Mu'ta University, Karak, Jordan in 1997. He is currently an associate professor of Computer Science Department at UJ and the department Chairperson. Almobaideen also has served as the Director of the Computer Center at the University of Jordan for three years. He held several other administrative positions at UJ including the Assistant Dean of King Abdullah II School for Information Technology, the Assistant Dean of the Faculty of Graduate Studies, and the Director of the Accreditation and Quality Assurance Office. His research interests include mobile ad hoc networks protocols development especially over transport, network, and the data-link layers, edge and objection detection in moving and still images, and indexing algorithms, among others.

Njoud O. Al-maitah has received her M.Sc. degree in computer science from the University of Jordan (UJ) in 2014, and B.Sc. degree in computer science from Mu'ta University, Karak, Jordan in 2011. She is currently an internal auditor in IT auditing department at Central Bank of Jordan.

On-line Data Retrieval Algorithm with Restart Strategy in Wireless Networks

Ping He
School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China
Email: hepinglaver@126.com

Shuli Luan
Qingdao Agricultural University, Qingdao, China
Corresponding author, Email: yjlcsyl@163.com

***Abstract*—Data retrieval is an efficient scheme for data dissemination in mobile computing, and its primary goal is to improve the waiting time and save the energy of mobile devices. Existing data retrieval algorithms are developed at the basis of a-priori knowledge of wireless data broadcast. In practical, they are not suitable for on-line data retrieval where the knowledge is not known. In this paper, we study on-line data retrieval problem with Las Vegas strategy of randomized algorithm, called as LVDR, and reduce the competitive rate of this problem, $c = \frac{k-1}{2} + \frac{1}{2l}$, where k is the number of channels and l is the length of broadcast cycle. Thus, we observe that different schemes of choosing channel will generate the different efficiencies in randomized algorithm. Therefore, we propose another scheme introduced restart strategy to execute the other retrieval sequences of choosing channels when the client may not retrieve the requested data item in certain time, called as LVDR-RS. In addition, we adopt Markov chain to predict the optimal restart cycle for each requested data item. Through analysis, we obverse that the competitive rate is closely related with the number of restarts and restart cycle, $c = \frac{2 \cdot a \cdot t_{avg}}{l}$.**

***Index Terms*—Wireless Data Broadcast; On-Line Data Retrieval; Data Retrieval; Data Schedule; Indexing**

I. INTRODUCTION

With rapid development of technologies in mobile environment, data dissemination has become an important role for obtaining their requested information of clients in many applications. There are three major approaches to disseminate information between server and clients: unicast, multicast and broadcast. They have different advantages and disadvantages in practical and are suitable for different applications. Currently, data broadcast has paid more attention to many researchers in mobile computing environment due to its potential advantages. It can satisfy a large number of clients' requirements in same time but it is limited by certain range of dissemination. In wireless networks, many mobile devices have equipped with high configuration in these aspects of both software and hardware. And they have become most popular devices to receive information from server in a limited response time which guarantees quality of service (QoS). For example, a stock manager wants to know the prices of several companies by his phone at any time and any place, so the important metric is obviously the response time. It is an attractive field for more and more people to reduce the response time in wireless communication.

Recently, three typical data broadcast approaches are proposed to apply to wireless networks, such as push-based, pull-based and hybrid scheme [1]. The push-based scheme periodically and continually broadcasts a set of data items at multiple parallel channels by fixed or static manner. In this scheme, the broadcast system does not consider the requirements of current clients and it is based on existing a-priori knowledge of previous clients' requirements. However, the pull-based scheme, also called on-demand data broadcast, is broadcast data items by variable or dynamic manner. In this scheme, the broadcast system adjusts and schedules its broadcast data items according to the requirements of clients in the largest scale. The clients acquire multiple requests to the server by uplink channels, and the server schedules these requests to broadcast with its best effort such that the client can retrieve their requested data items in minimal response time. All of us know that the pull-based scheme cannot obtain the optimal or near-optimal performance. In addition, the hybrid scheme combines the above two schemes and fully utilizes the advantages of two schemes to improve the performance of data broadcast.

It is desired that researchers have deeply studied data broadcast based on the above data broadcast schemes from the aspects of indexing, data schedule, data retrieval and applications. Indexing is an efficient scheme to dramatically reduce two metrics: access time and tuning time. It adopts various index structures, such as alphabetic Huffman Tree, Hashing table, B^+ tree and exponential indexing, to determine the location of data items so that the client can quickly find the location of requested data items and conveniently learn the time offset of requested data items. After learning the time offset of requested data items, the client can enter into doze mode and just keep active mode in downloading process so that the energy can be significantly saved. Many existing literatures are proposed to study on the

doi:10.4304/jnw.9.12.3327-3335

indexing technology [2, 3, 4, 5, 6]. Data schedule is mainly based the push-based and pull-based schemes. The client has multiple requests with multiple data items and transmits requests to server by uplink channels. The server scheduler organizes all requested data items to broadcast at the downlink channels such that the client can receive them in shorter response time. Similarly, there also are many literatures, such as [7, 8, 9]. Data retrieval is another new field for data dissemination in wireless environment. From the perspective of client, based on indexing technology the client can know the locations of all requested data items. Here, the client does not simply wait for downloading the requested data items. The locations of requested data items are combined to obtain an optimal downloading sequence. It is studied from single antenna data retrieval [5, 10] and multiple antennae data retrieval [11].

From these above fields, the primary goal is to minimize the access latency that the requested data items of client can be satisfied in rational range. From the architecture, we can see that indexing and data schedule is based on server side, while data retrieval is based client side. In recent years, data retrieval is become an important research point. However, the existing literatures are focused on off-line algorithm. Obviously, it is not suitable for practical applications. In this study, we apply Las Vegas strategy of randomized algorithm to on-line data retrieval problem. Due to the uncertainty of randomized algorithm, each kind of channel's choice may result in different results, so when data retrieval algorithm does not find the requested data item, we introduce restart strategy to data retrieval algorithm and make it execute a new data retrieval sequence about channel selection.

The remainder of this paper is organized as follows. In Section II, we conclude the recent related works for wireless data broadcast. Section III shows the system architecture of wireless data broadcast. Section IV focuses on the description of proposed on-line Las Vegas data retrieval algorithm. We modify that the competitive rate of on-line Las Vegas data retrieval algorithm is $c = \frac{k-1}{2} + \frac{1}{2l}$. Section V extends on-line Las Vegas data retrieval algorithm and adopt existing restart strategy to solve data retrieval problem, and obtain the knowledge that the competitive rate of on-line Las Vegas algorithm with restart strategy is closely related to restart cycle and the number of restarts, $c = \frac{2 \cdot a \cdot t_{avg}}{l}$. We use Markov chain to get the near-optimal restart cycle in the retrieval process of each requested data item. Finally, Section VI concludes this paper.

II. Related Works

For the study of wireless data broadcast, there are mainly four focuses to achieve data dissemination, such as indexing, data schedule, data retrieval and applications. From different aspects, they are committed to minimize the waiting time of clients and save energy of mobile devices.

As the above description of indexing, indexing technique is currently divided into two types: first, a large number of existing studies suggest that index and data items are intermixed each other to be broadcast at same broadcast channel [12]; second, the broadcast channels are simply divided into index channel and data channel [8, 13]. They play different roles in data broadcast that index channel is responsible for broadcasting index structure, while data channel is responsible for broadcasting data items. Recently, the second type is more popular in indexing technique. All indexing structures are allocated in index channel. The client can firstly find the offset of requested data items from index channel. Then, according to the offset, the client downloads continually the requested data items in data channel. It is well known that the goal of indexing technique is to reduce access time. Various schemes are directly proposed to improve the performance of wireless data broadcast, all of which adopt alphabetic Huffman Tree, hashing table, B^+ tree and exponential indexing [8, 9, 13, 14, 15, 16, 17]. [7] firstly proposed an allocation model in server side through considering access frequencies of data items, data item's lengths, and bandwidth of different channels. [3] proposed a binary tree indexing structure. The structure is generally established for each channel and the nodes of all indexing trees are reasonably multiplexed on a well-known physical channel. [4] proposed a novel Huffman-Tree based distributed index scheme to answer this question. Alphabetic Huffman Tree can obviously provide better performance. [18] considered a novel parameterized index which usually had a linear distributed structure.

Data schedule is another scheme to achieve the primary goal of wireless data broadcast. It is studied from multiple views: push-based, pull-based and hybrid scheme. In push-based, broadcast disk [19] is the first and typical scheme to implement the skewed data dissemination from hot to clod. In addition, [20] proposed a greedy scheme in multi-channel data broadcast environment. However, due to pushed-based just periodically broadcasts the fixed data items, it is not suitable for dynamic environment. So pull-based is proposed to solve the above problem, also called as on-demand data broadcast. In early stage, FCFS [21] is the first on-demand broadcast scheme which always serves the first coming requests of clients. Consequently, LWF and MRF [22], $R \times W$ [23] and $\sin - \alpha$ [24] are proposed to solve the corresponding problem for multi-item requests. Recently, [25] proposed a data schedule scheme based on coding scheme. In all requests, according to the related requirements the server selects the outstanding request and combines the requested data item with the stored data item of client. [26] proposed another data broadcast schedule scheme based on coding technique. The scheme is applied to the existing many schemes, such as MRF, LWF and $R \times W$. The basic idea of this scheme is that data broadcast system is converted into undirected graph and finds the maximum clique in graph. For on-demand data broadcast environment with time critical and multi-item, [27] proposed a new schedule scheme (DPA) to solve the request starvation problem. Based on hybrid scheme, [28] is one on-line scheme to reduce access time from data schedule. The

strategy partitions the data items among broadcast channels in a balanced way, and adopts a hybrid push-pull data broadcast schedule.

With the increasing involvement of mobile applications in our daily life, data retrieval is another scheme to reduce access time from client side. Lu et al. [29] proposed a heuristic algorithm. It can employ the algebraic method to download a large number of data items. In addition, the optimal solution can be obtained in $O(2^k(nt)^{O(1)})$ time by the proposed AFPT algorithm, where k is the number of requested data items, n is the number of broadcast channels, and t is the least access time. [30] developed some efficient data retrieval protocols for client to download the requested data items. A new problem called Minimum Constraint Data Retrieval Problem (MCDR) is introduced, and prove NP-hard through using $VC \leq_p MCDR$, where VC is the decision problem of Vertex Cover. In [10], the authors also have studied the data retrieval problem from the point of mobile clients. The largest number of requested data items can be downloaded in given time such that the number of switching channels is minimized (called LNDR) and prove that LNDR is NP-hard by using $3CNF$ reduction. [5] largely reduced energy consumption through eliminating the maximum number of conflicts, retrieving the maximum number of data elements and minimizing the number of channel switches. However, this scheme cannot always attain the optimal switch such that the energy consumption can be significantly increased as the number of requested data items increases. Yet, these schemes are mostly concentrated at mobile devices with one antenna. With the development of wireless networks, the first scheme is adopted to directly apply to mobile devices with multiple antennae [11].

However, we should point out that almost indexing and data retrieval schemes are off-line algorithm. On the contrary, the existing studies of on-line algorithm are extremely few.

III. System Architecture

In general, wireless data broadcast system contains a server and a large number of clients. The system architecture is shown in Figure 1. In data retrieval problem of this paper, we assume that data broadcast is push-based data broadcast. The server is responsible for periodically broadcasting data items by several available downlink channels based on a-priori knowledge of requested data items. While clients require some data items transmitted to server by uplink channels and learn the locations of these requested data items through existing indexing schemes, then clients can combine the locations of all requested data items to obtain an optimal download sequence, not simply wait for the broadcast of requested data items. Obviously, the bandwidth of downlink channel is typically greater than that of uplink channel, due to the property of asymmetry.

The primary goal of data retrieval algorithm is to minimize the access latency and save energy such that the client can obtain all requested data items in rational range of time. For details of notations used in this study, it is referred to Table 1.

TABLE I. Summary of Notations

Notation	Description
CH, D, R, S	The set of broadcast channels, broadcast data items, requested data items, and retrieval sequence respectively
ch_i, d_i, r_i, s_i	Broadcast channel, broadcast data item, requested data item, and retrieval sequence respectively
AT	The total access latency
AT_i	The access latency of requested data item r_i
$AT_R^{r_i}$	The access latency of requested data item r_i in LVDR-RS algorithm
m_i	Whether channel ch_i is retrieved
m_R	The number of requested data items
k	The number of broadcast channels
l	The broadcast cycle
τ	The set of restart cycle
t_{avg}	The average restart cycle of all requested data items

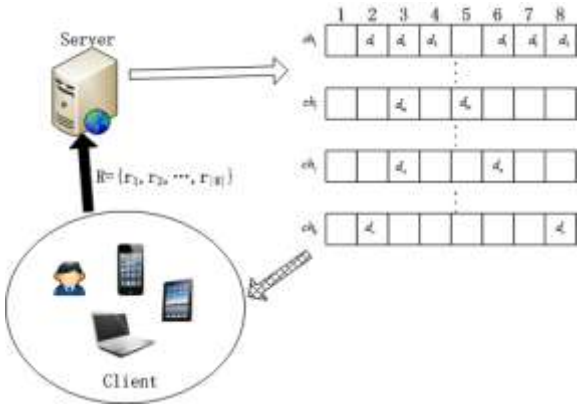


Figure 1. System architecture

IV. On-line Las Vegas Data Retrieval Algorithm

In this section, we adopt Las Vegas algorithm to solve data retrieval problem in order that we can analyze the performance of on-line data retrieval algorithm. Next, we introduce the description of Las Vegas algorithm.

A. Preliminary

The so-called random algorithm refers that makes a random choice in the executing process of algorithm. While Las Vegas algorithm is that the correct solution is also obtained and the difference when runs the algorithm two times is the running time.

Las Vegas algorithm belongs to a kind of random algorithm. Absolutely, it has all characteristics of random algorithm, as it allows to randomly selecting the next computing step in the executing process. Under many circumstances, when the algorithm needs to make the next choice, random choice always has less time and cost than optimal choice. Therefore, random algorithm can reduce the time complexity in larger degree. In general, Las Vegas algorithm does not obtain the error solution. Once it obtain a solution, the solution must be true. However, Las Vegas may not obtain the solution some times. The probability of Las Vegas for obtaining true

solution is increased as the computing time of algorithm is increased. For any an instance of this problem, we solve the instance enough times through using a same Las Vegas algorithm, it can make the probability of failure is arbitrarily small.

Usually, we use a Bool function to denote Las Vegas algorithm. When the algorithm finds a solution, it returns $true$, otherwise it returns $false$. The typical form of Las Vegas is followed: $Bool\, success = LV(x, y)$, where x denotes input parameter. When the value of $success$ is $true$, y returns the solution of problem. When the value of $success$ is $false$, it denotes that the algorithm does not obtain the solution of problem. In this time, we can independently call the same algorithm again for a same instance. Assume that $p(x)$ is the probability of solution which is obtained through calling Las Vegas algorithm for input parameter x. A true Las Vegas algorithm also has $p(x) > 0$ for all input parameters x. In a larger sense, it requires that there exists a constant $\delta > 0$ such that it also has $p(x) > \delta$ for all instances x. Suppose that $s(x)$ and $e(x)$ denote respectively the average time of successful or failure solution for a specific instance x. Due to $p(x) > 0$, so if only there has enough time, for any instance x Las Vegas always finds the solution of problem. Assume that $t(x)$ is the average time of algorithm for finding the solution of specific instance x, so the expression is followed as Equation (1).

$$t(x) = p(x) \cdot s(x) + (1 - p(x)) \cdot (e(x) + t(x)) \quad (1)$$

We concise the above equation, as shown in Equation (2).

$$t(x) = s(x) + \frac{1 - p(x)}{p(x)} \cdot e(x) \quad (2)$$

B. On-line Las Vegas Data Rretrieval Algorithm (LVDR)

We apply the above description of Las Vegas to solve on-line data retrieval problem. The main characteristic of this problem: the client does not any knowledge of broadcast channels and requested data items. When a requested data item needs to be retrieved, the client can only select a channel from the set of channels to retrieve blindly. If the requested data item does not broadcast at the selected channel, the client will randomly select and retrieve another channel until finding the requested data item. Therefore, we depict the definition of Las Vegas on-line data retrieval problem.

Definition 1. (On-line Las Vegas Data Retrieval Algorithm, **LVDR**) Assume that there exist multiple data items $D = \{d_1, d_2, d_3, \cdots, d_{|D|}\}$ which are broadcast at multiple parallel channels $CH = \{ch_1, ch_2, \cdots, ch_{|CH|}\}$. For the set of requested data items $R = \{r_1, r_2, \cdots, r_{|R|}\}$, on-line data retrieval problem is to find a retrieval sequence $S = \{s_1, s_2, \cdots, s_{|R|}\}$ such that the access latency of each requested data item is minimized $\min\limits_{s_i \in S} AT_i$ and total access latency of all requested data items is minimized, $AT = \sum\limits_{i=1}^{|R|} \min\limits_{s_i \in S} AT_i$.

Where s_i denotes the set of all channels $s_i = \{ch_1^{m_1}, ch_2^{m_2}, \cdots, ch_{|CH|}^{m_{|CH|}}\}$ which are retrieved by the client for obtaining the requested data items in on-line data retrieval algorithm. We use multivariate monomial to indicate s_i, $s_i = ch_1^{m_1} \cdot ch_2^{m_2} \cdot \cdots \cdot ch_{|CH|}^{m_{|CH|}}$, where $\{m_1, m_2, \cdots, m_{|CH|}\}$ is either 0 or 1 positive integer, and is applied to mark whether the channels $ch_1, ch_2, \cdots, ch_{|CH|}$ are retrieved respectively. If channel ch_i is retrieved, then $m_i = 1$, otherwise $m_i = 0$. The expression is concisely followed by Equation (3).

$$m_i = \begin{cases} 1 & ch_i\, is\, retrieved \\ 0 & ch_i\, is\, not\, retrieved \end{cases} \quad (3)$$

Assume that $s_i = ch_4 \cdot ch_3 \cdot ch_5$, it denotes that the client retrieves the requested data item r_i in channel ch_5 after retrieving channel ch_4 and ch_3. It also illustrates that the client does not retrieve the requested data item r_i in channel ch_4 and ch_3. Note that the last variable of monomial indicates that the requested data item is retrieved in this channel. Therefore, the retrieval of all requested data items can be indicated by polynomial. In on-line Las Vegas data retrieval algorithm, we perform Las Vegas algorithm in each channel. If the algorithm retrieves the requested data item, then Las Vegas algorithm returns $true$. Assume that the requested data item is not retrieved, Las Vegas returns $false$. Therefore, LVDR algorithm is shown in Algorithm 1 and Las Vegas algorithm is depicted in Algorithm 2. In Algorithm 1, we mark whether the requested data item is retrieved in line 3, and we initiate the flag of channel for the retrieval of each requested data item in line 4-6. In line 7-13, we retrieve the requested data item in each channel until we retrieve it. Finally, we update the retrieval sequence S in line 14-16 and compute total access latency AT in line 18. Here, we adopt a sub-function $LV(sucess, r_i, ch_j, s_i)$ to retrieve the requested data item r_i from the selected channel ch_j, as depicted in Algorithm 2. If the selected channel ch_j exists the requested data items r_i, we set that the value of $success$ is $true$ and the flag of selected channel is $true$ in line 5-6. Otherwise, the value of $success$ is $false$ and the flag of selected channel is $retrieved$ in line 8-9. At last, we return the value of $success$ to LVDR algorithm in line 12.

ALGORITHM 1. on-line Las Vegas data retrieval algorithm (LVDR)
Input: the set of channels $\{ch_1, ch_2, \cdots, ch_{|CH|}\}$, the set of requested data items $R = \{r_1, r_2, \cdots, r_{|R|}\}$;
Output: total access latency AT;
1: for $i = 1$ to $|R|$ do
2: *bool* $success = false$;
3: $s_i = NULL$;
4: for $j = 1$ to $|CH|$ do
5: $ch_j.flag = false$;
6: end for
7: select randomly a channel ch_j with $false$;
8: while (!$success$) do
9: $success = LV(sucess, r_i, ch_j, s_i)$;
10: if !$success$ then
11: select randomly a channel ch_j with $false$;

12: end if
13: end while
14: if $ch_j.flag = true$
15: $S \leftarrow s_i$;
16: end if
17: end for
18: according to S, compute total access latency AT;

C. The Analysis of LVDR

In worst case, the time complexity of LVDR algorithm is $O(m_R \cdot k \cdot l)$, where $m_R = |R|$ denotes the number of all requested data items, $k = |CH|$ denotes the number of all broadcast channels, and l denotes the broadcast cycle of each channel that the client needs to retrieve the whole broadcast cycle of each channel for downloading each requested data item. Assume that the broadcast cycle of each channel is different, the time complexity is expressed as $O(m_R \cdot (l_1 + l_2 + \cdots + l_k))$.

Lemma 1. The competitive rate of LVDR algorithm is $c = \frac{k-1}{2} + \frac{1}{2l}$.

Proof: We have held the competitive rate of on-line randomized data retrieval algorithm is $\frac{k}{2}$ in previous study. However, we suggest that if the client finds the requested data item from a channel, the client does not need to continually stay at the channel until the broadcast cycle is end. The client can switch to another channel for retrieving the next requested data item. Based on the above description, if the broadcast cycle is l, then the probability of a requested data item which is broadcast at first time slot is $\frac{1}{l}$. Similarly, the probability of requested data item which is broadcast at second, third, ... , and last time slot is also $\frac{1}{l}$. Therefore, the competitive rate of saving part is concisely computed in Equation (4). If the requested data item is broadcast at first time slot, access latency will be saved $l-1$, if the requested data item is broadcast at second time slot, access latency will be saved $l-2, \cdots$, if the requested data item is broadcast at last time slot, access latency will be saved 0. According to the probability, we can compute the average of saving access latency. While in original result the access latency is l.

ALGORITHM 2. Las Vegas Algorithm (LV)
Input: the requested data item r_i, the selected channel ch_j, the retrieved channels s_i, and the flag of Las Vegas $success$;
Output: the update retrieved channels s_i;

1: $bool\ LV(r_i, \&ch_j, \&s_i)$
2: {
3: if r_i is retrieved in channel ch_j then
4: append channel ch_j to s_i, $s_i \leftarrow ch_j$;
5: $ch_j.flag = true$;
6: $sucess = true$;
7: else
8: $ch_j.flag = retrieved$;
9: $sucess = false$;
10: append channel ch_j to s_i, $s_i \leftarrow ch_j$;
11: end if
12: return $success$;
13: }

Finally, the competitive rate of LVDR algorithm is expressed $c = \frac{k}{2} - \frac{1}{2} + \frac{1}{2l} = \frac{k-1}{2} + \frac{1}{2l}$.

$$\begin{aligned} \frac{L_1}{L} &= \frac{\frac{1}{l} \cdot (0+1+2+3+\cdots+l-1)}{l} \\ &= \frac{1}{l^2} \cdot \frac{l \cdot (l-1)}{2} \\ &= \frac{1}{2} - \frac{1}{2l} \end{aligned} \tag{4}$$

Next, we estimate the average probability of selecting channel with the requested data item from k channels. For each requested data item, the probability of finding the true channel with the requested data item is $p = \frac{1}{k}$, while the probability of not finding the true channel with the requested data item is $q = \frac{k-1}{k}$. Note, we assume that data items are different in each channel. We perform k groups of random selection experiment. In each experiment, we select randomly k times from k channels. Assume that the time of selecting the required channel with the requested data item is $1, 2, 3, \cdots, k$ respectively. The experiment belongs to Bernoulli trial. Therefore, the probability that the client selects the channel with the requested data item one time is $P_k(1) = C_k^1 p^1 q^{k-1}$, the probability that the client selects the channel with the requested data item two times is $P_k(2) = C_k^2 p^2 q^{k-2}, \cdots$, the probability that the client selects the channel with the requested data item k times is $P_k(k) = C_k^k p^k$. So the average probability is concisely expressed by Equation (5).

$$\begin{aligned} P &= \frac{P_k(1)+P_k(2)+\cdots+P_k(k)}{k} \\ &= \frac{C_k^1 p^1 q^{k-1} + C_k^2 p^2 q^{k-2} + \cdots + C_k^k p^k}{k} \\ &= \frac{\sum_{i=1}^{k} C_k^i p^i q^{k-i}}{k} \\ &= \frac{\sum_{i=1}^{k} C_k^i (\frac{1}{k})^i (\frac{k-1}{k})^{k-i}}{k} \end{aligned} \tag{5}$$

where $k - i > 0$ and $\frac{k-1}{k} < 1$, so Equation (5) can be simply denoted by Equation (6).

$$\begin{aligned} P &\leqslant \frac{\sum_{i=1}^{k} C_k^i (\frac{1}{k})^i}{k} \\ &= \sum_{i=1}^{k} C_k^i (\frac{1}{k})^{i+1} \end{aligned} \tag{6}$$

V. On-line Las Vegas Data Retrieval Algorithm with Restart Strategy

The above Las Vegas random algorithm always obtains true solution at the end of running process, however the time of obtaining solution is different in each execution. In previous, the performance of random algorithm is usually unstable at solving NP-hard problem. Even if there is identical input instance, the performance of algorithm may have magnitude difference. It results that the average performance of algorithm is reduced. To improve the performance and stability of algorithm, we need to optimize random algorithm. According to restart strategy, we optimize Las Vegas random algorithm. In other words, we adopt restart strategy to optimize on-line Las Vegas data retrieval algorithm (LVDR-RS) and obtain the better performance. In next subsection, we illustrate the basic description of restart strategy.

A. Preliminary

The restart strategy is very common in daily life. For example, when the client browses web pages from Internet, he often meets the case that the page can not be normally displayed in long time. If the client breaks off the download of page and refresh the page to continue restart, the page is commonly displayed in shorter time. When a path of network occurs stoppage, restart strategy can choose another new path to continue the transmission. Suppose that the transmission of page is viewed as a random algorithm, and the time of transmission is the running time of algorithm. This is the basic idea to optimize random algorithm through using restart strategy.

Restart strategy is that if the algorithm is still not ended when it performs in some time, then we stop the algorithm and restart the running of algorithm with a new seed of random number. The step is repeatedly executed until the algorithm is ended, where the threshold of running time can be different, as shown in Figure 2.

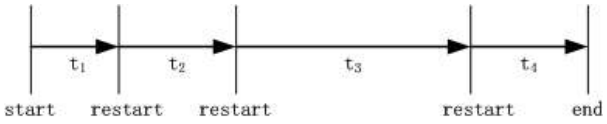


Figure 2. The example of restart strategy

The key point of designing restart strategy is to determine the number of restarts and the time of each restart. According to different number of restarts, we can classify it into two types: finite restart strategy and infinite restart strategy. However, if the algorithm is allowed, the restart time is set to infinity.

B. On-line Las Vegas Data Retrieval Algorithm with Restart Strategy (LVDR-RS)

Although the performance distribution of algorithm is not a continuous distribution, it approximated a continuous distribution cannot change the characteristic of algorithm and it can simplify the process of analysis. From these problems, We analyze the performance of randomized algorithm by using Markov chain modeling of random process, and analyze the best restart cycle in restart strategy, furthermore, analyze the access latency of on-line data retrieval problem based on above description. Markov chain is applied to on-line data retrieval problem and predicts the probability of a channel existing requested data item in future time from this time. But it is irrelevant how the algorithm reaches to this state before this time.

First, we depict the definition of Markov chain.

Definition 2. (**Continuous-time Markov chain**) Assume that the state space E of random process $\{X_t : t \geqslant 0\}$ is a most countable set. For any an integer $n \geqslant 1$, parameters $0 \leqslant t_0 \leqslant t_1 \leqslant \cdots \leqslant t_n \leqslant t_{n+1}$ and states $i_0, i_1, \cdots, i_{n+1} \in E$, there is an Equation (7). Then we call that $\{X_t : t \geqslant 0\}$ is continuous-time Markov chain.

$$\begin{aligned} &P(X_{t_{n+1}} = i_{n+1} | X_{t_0} = i_0, \cdots, X_{t_n} = i_n) \\ &= P\{X_{t_{n+1}} = X_{t_{n+1}} | X_{t_n} = i_n\} \end{aligned} \quad (7)$$

Similarly, in order to determine the located channel of a requested data item $r_i \in R = \{r_1, r_2, \cdots, r_{m_{|R|}}\}$, we also depict the followed definition in on-line data retrieval problem.

Definition 3. (**Conditional probability of LVDR-RS**) Assume that random process is $X_t : t \geqslant 0$, where X_t denotes the retrieved channel of client in time slot t, channel set CH is a most countable set. For any an integer $n \geqslant 0$, these parameters of channel's access time $0 \leqslant t_0 \leqslant t_1 \leqslant \cdots \leqslant t_n \leqslant t_{n+1}$ and the responding channels $i_0, i_1, \cdots, i_{n+1} \in CH$, there exists Equation (8), where i_{n+1} denotes the channel ch_{r_i} of requested data item r_i.

$$\begin{aligned} &P\{X_{t_{n+1}} = i_{n+1} | X_{t_0} = i_0, \cdots X_{t_n} = i_n\} \\ &= P\{X_{t_{n+1}} = X_{n+1} | X_{t_n} = i_n\} \end{aligned} \quad (8)$$

Based on Markov property and non-after effect property, we simplify conditional probability, as followed Equation (9).

$$\begin{aligned} &P\{X_{t+s} = ch_{r_i} | X_s = ch_{r_j}\}, s, t \geqslant 0 \\ &ch_{r_i} \in CH, ch_{r_j} \in CH, i > 0, j > 0 \end{aligned} \quad (9)$$

It denotes transition probability function that the client retrieves channel ch_{r_j} in time slot s, after t time slots the client transforms to the channel ch_{r_i} of current requested data items, as followed Equation (10).

$$p_{ch_{r_j}, ch_{r_i}}(s, s+t) = P\{X_{t+s} = ch_{r_i} | X_s = ch_{r_j}\} \quad (10)$$

Obviously, transition probability function $p_{ch_{r_j}, ch_{r_i}}$ is not related to the size of s, where s denotes the time from the channel ch_{r_j} of previous requested data item r_j to the channel ch_{r_i} of current requested data item r_i, in other words, the waiting time of client between two requested data items. We use Equation (11) to denote the transition probability fiction matrix of random process $\{X_t : t \geqslant 0\}$, where $ch_{r_i}, ch_{r_j} \in CH$, $i > 0$, $j > 0$, $t > 0$ and $\sum_{i,j \in N} p_{ch_{r_j}, ch_{r_i}}(t) = 1$, where $ch_{r_i}, ch_{r_j} \in CH$.

$$P(t) = [p_{ch_{r_j}, ch_{r_i}}(t)]_{ch_{r_i}, ch_{r_j} \in CH} \quad (11)$$

Assume that there are k channels, the transition probability function matrix of on-line randomized data retrieval algorithm is followed as Equation (12). In the process of data retrieval, the probability may be different for switch from a channel to another channel.

$$\begin{bmatrix} 0 & p_{ch_{r_1}, ch_{r_2}}(t) & \cdots & p_{ch_{r_1}, ch_{r_{|R|}}}(t) \\ p_{ch_{r_2}, ch_{r_1}}(t) & 0 & \cdots & p_{ch_{r_2}, ch_{r_{|R|}}}(t) \\ p_{ch_{r_3}, ch_{r_1}}(t) & p_{ch_{r_{31}}, ch_{r_2}}(t) & \cdots & p_{ch_{r_3}, ch_{r_{|R|}}}(t) \\ \vdots & \vdots & \vdots & \\ p_{ch_{r_{|R|}}, ch_{r_1}}(t) & p_{ch_{r_{|R|}}, ch_{r_2}}(t) & \cdots & 0 \end{bmatrix} \quad (12)$$

Next, we define the performance distribution of access latency through using Las Vegas algorithm.

Definition 4. (**Performance distribution of LVDR-RS's access latency**) For a requested data item $r_i \in R, R = \{r_1, r_2, \cdots, r_{|R|}\}$ of on-line data retrieval problem, we define its access latency as $AT_R^{r_i}$ through

Las Vegas algorithm, where the transition probability function from previous requested data item r_j to current requested data item r_i is defined as $p_{ch_{r_j},ch_{r_i}}(s,s+t)$. We call $AT_R^{r_i}$ as the performance distribution of LVDR-RS's access latency.

We know that restart cycle plays an important role in this LVDR-RS, so it is a critical problem how to determine the restart cycle t in on-line data retrieval algorithm. Next, we define LVDR-RS algorithm.

Definition 5. (**LVDR-RS algorithm**) For on-line data retrieval problem with restart strategy of Las Vegas, we define time sequence $\tau = \{t_1, t_2, \cdots, t_{ts}, \cdots\}$, where $t_{ts} > 0$, $ts \in Z^+$. For each requested data item r_i, LVDR-RS executes time τ in proper order. If it satisfies the ending condition, we find the located channel ch_{r_i} of the requested data item and the algorithm is end.

We conclude the above descriptions. For restart strategy $\tau = \{t_1, t_2, \cdots, t_{ts}, \cdots\}$, there is $\forall ts > 0$, $t_0 \in \tau$, where t_0 is a constant, we call τ as cycle restart strategy, and t_0 is the cycle of strategy τ. $AT_R^{r_i}(t_0)$, $i \in Z^+$ is the running time of a input requested data item r_i in on-line data retrieval problem with restart strategy.

Lemma 2. Under circumstance of current channel ch_{r_j}, we can obtain the probability (as shown in Equation (13)) that the requested data item r_i is located at channel ch_{r_i}. Through computing, we can obtain the cycle t_0 with highest probability.

ALGORITHM 3. on-line Las Vegas data retrieval algorithm with restart strategy (LVDR-RS)

Input: the set of channels $\{ch_1, ch_2, \cdots, ch_{|CH|}\}$, the set of requested data items $R = \{r_1, r_2, \cdots, r_{|R|}\}$, restart strategy $\tau = \{t_1, t_2, \cdots, t_{ts}, \cdots\}$;

Output**: total access latency** AT**;**

1: **for** $i = 1$ to $|R|$ **do**
2: **while** r_i is not retrieved
3: $bool\ success = false$;
4: $s_i = NULL$;
5: **for** $j = 1$ to $|CH|$ **do**
6: $ch_j.flag = false$;
7: **end for**
8: computing the restart cycle t_0 based on restart strategy $\tau = \{t_1, t_2, \cdots, t_{ts}, \cdots\}$;
9: initiate the executing time of algorithm t_{sum};
10: select randomly a channel ch_j with $false$;
11: **while** (!$success$) **do**
12: $success = LV(sucess, r_i, ch_j, s_i)$;
13: compute the executing time t_{sum} in each data retrieval for requested data item r_i;
14: if the retrieval time is larger than t_0 and r_i is not retrieved then
15: **break**;
16: **end if**
17: **if** !$success$ **then**
18: select randomly a channel ch_j with $false$;
19: **end if**
20: **end while**
21: **if** $ch_j.flag = true$
22: $S \leftarrow s_i$;
23: **end if**
24: **end while**
25: **end for**
26: according to S, compute total access latency AT;

$$
\begin{aligned}
&p_{ch_{r_j},ch_{r_i}}(t_1) = P\{X_{s+t_1} = ch_{r_i} | X_{t_1} = ch_{r_j}\} \\
&p_{ch_{r_j},ch_{r_i}}(t_2) = P\{X_{s+t_2} = ch_{r_i} | X_{t_2} = ch_{r_j}\} \\
&\cdots \\
&p_{ch_{r_j},ch_{r_i}}(t_{ts}) = P\{X_{s+t_{ts}} = ch_{r_i} | X_{t_i} = ch_{r_j}\}
\end{aligned} \tag{13}
$$

The LVDR-RS algorithm is shown in Algorithm 3. The difference compared with Algorithm 1 is that Algorithm 3 needs to compute the restart cycle, in line 8. The computing process is shown in the above description. We initiate the executing time of algorithm, such as line 9, and compute the executing time t_{sum} in the process of data retrieval for requested data item r_i, such as line 13, so that we can compare with the restart cycle t_0. If the executing time t_{sum} is larger than restart cycle t_0 and the requested data item is not retrieved, we break the process of data retrieval for downloading the requested data item r_i and restart to compute the restart cycle t_0, in line 14-16. In a new restart cycle, we continue to retrieve the requested data item r_i until it is retrieved. Here, Las Vegas algorithm in line 12 is same as Algorithm 2.

C. The Analysis of LVDR-RS

First, we analyze the time complexity of LVDR-RS through considering Algorithm 3. The time complexity of LVDR-RS is $O(t_{sum_1} + t_{sum_2} + \cdots + t_{sum_{|R|}})$, where t_{sum_i} indicates the total of retrieving the requested data item r_i. In the process of retrieving the requested data item r_i, the requested data item may be retrieved in one restart cycle, or the requested data item may be retrieved in several restart cycles. Therefore, t_{sum_i} is the sum of these restart cycles. Similarly, the other requested data items have the same operation. The total access latency is $AT = t_{sum_1} + t_{sum_2} + \cdots + t_{sum_{|R|}}$. The best time complexity of LVDR-RS is that each requested data item is retrieved in first restart cycle, $AT = |R| \cdot t_{avg}$, where t_{avg} denotes the average restart cycle of all requested data items, and $|R|$ denotes the number of requested data items.

Next, we consider the competitive rate of LVDR-RS. Before analysis of competitive rate, we describe a division criterion for all requested data items.

Definition 6. (**Division criterion**) Assume that we can partition all requested data items to several segments, $P(0), P(1), P(2), \cdots$, such that $P(0)$ has at most $k-1$ channel switches, while for the other segments $P(i)$ each segment has $k-1$ channel switches.

Assume that the partition is feasible. We scan all requested data items from the end. If we meet $k-1$ channel switches, the set of these requested data items is defined as a segment. Then, we continually scan the remaining requested data items to execute the partition operation until all requested data items are partitioned. Obviously, the last segment has at most $k-1$ channel switches.

Lemma 3. The competitive rate of LVDR-RS is $c = \frac{2 \cdot a \cdot t_{avg}}{l}$.

Proof: We compare with the access latency of off-line optimal algorithm OPT. Suppose that k_i denotes the number of channel switches in i^{th} iteration. According to the division criterion, the requested data items are broadcast at k_i different channels in i^{th} iteration. Therefore, the optimal off-line algorithm OPT needs $k_i - 1$ switches in i^{th} iteration. Assume that the channel has same broadcast cycle l, the access latency of i^{th} iteration is $(k_i - 1) \cdot l$. Finally, we sum all requested data items in m iterations, so it can clearly be seen that the total access latency of optimal off-line algorithm OPT is $AT_{OPT} = \sum_{i=1}^{m}((k_i - 1) \cdot l)$.

For on-line LVDR-RS algorithm, we also compute its total access latency of data retrieval process. We also know that restart cycle and the number of restarts play an important role in restart strategy of randomized algorithm. Note that we adopt the average restart cycle t_{avg} and the average number of restarts a in on-line LVDR-RS algorithm. They indicate that the access latency of each requested data item is at most $a \cdot t_{avg}$. For i^{th} iteration, the access latency is obviously $a \cdot t_{avg} \cdot k_i$, where k_i denotes the number of channels. Finally, the total access latency is $AT_{LVDR-RS} = \sum_{i=1}^{m} a \cdot t_{avg} \cdot k_i$.

Therefore, the competitive rate is computed by Equation (14).

$$\begin{aligned} c &= \frac{AT_{LVDR-RS}}{AT_{OPT}} \\ &= \frac{\sum_{i=1}^{m} a \cdot t_{avg} \cdot k_i}{\sum_{i=1}^{m} (k_i - 1) \cdot l} \\ &= \frac{\sum_{i=1}^{m} (a \cdot t_{avg} \cdot (k_i - 1) + a \cdot t_{avg})}{\sum_{i=1}^{m} (k_i - 1) \cdot l} \\ &< \frac{\sum_{i=1}^{m} (a \cdot t_{avg} \cdot (k_i - 1) + a \cdot t_{avg} \cdot (k_i - 1))}{\sum_{i=1}^{m} (k_i - 1) \cdot l} \\ &= \frac{\sum_{i=1}^{m} 2 \cdot a \cdot t_{avg} \cdot (k_i - 1)}{\sum_{i=1}^{m} (k_i - 1) \cdot l} \\ &= \frac{2 \cdot a \cdot t_{avg}}{l} \end{aligned} \quad (14)$$

From the above description, the competitive rate of LVDR-RS is closely related to restart cycle t_{avg} and the number of restarts a.

D. Comparison between LVDR and LVDR-RS

In this subsection, we describe the comparison between LVDR and LVDR-RS from two views: time complexity and competitive rate.

First, the time complexity of LVDR is $O(m_R \cdot (l_1 + l_2 + \cdots + l_k))$, while the time complexity of LVDR-RS is $O(t_{sum_1} + t_{sum_2} + \cdots + t_{sum_{|R|}})$, so it is obvious that LVDR-RS has less time complexity.

Second, we observe that the longest restart cycle is l. The reason is that the longest retrieval time of a requested data items is l, so the client will find this requested data items in one broadcast cycle. If a requested data item cannot be retrieved in one broadcast cycle, it denotes that this requested data item is not broadcast and the algorithm does not need to execute. From the above description, $max(t_{avg}) = l$, therefore the competitive rate of LVDR-RS is $c = \frac{2 \cdot a \cdot t_{avg}}{l} \leq 2a$. If we compare the competitive rate between LVDR and LVDR-RS, $2a \leq \frac{k-1}{2} + \frac{1}{2l}$, we can obtain $a \leq \frac{k-1}{4} + \frac{1}{4l}$. Therefore, we conclude that when $a \leq \frac{k-1}{4} + \frac{1}{4l}$, the performance of LVDR-RS will better than that of LVDR.

VI. CONCLUSION

Most of these recent related literatures have studied on wireless data broadcast from several fields, such as indexing, data schedule and data retrieval, they are committed to reduce the waiting time and save the energy of mobile devices. We argue that existing algorithms of data retrieval problem are mainly focused on off-line, so we study on-line data retrieval algorithm from different aspects for more emerging mobile applications. We introduce existing Las Vegas strategy of randomized algorithm into on-line data retrieval algorithm for multi-channel wireless data broadcast environment, called LVDR. Upon a comprehensive analysis, the competitive rate of LVDR is $c = \frac{k-1}{2} + \frac{1}{2l}$. However, we know that different randomized styles of selecting channel may result in different results of wireless data broadcast, so we propose another scheme through adopting restart strategy of randomized algorithm, called LVDR-RS. And we compute the optimal restart cycle for each requested data item and the competitive rate of this LVDR-RS, $c = \frac{2 \cdot a \cdot t_{avg}}{l}$. We observe that it is closely related to restart cycle and the number of restarts.

ACKNOWLEDGMENT

This research was partially supported by National Science Foundation of China under its General Projects funding #61170232 and Youth funding #61100218, Fundamental Research Funds for the Central Universities #2012JBZ017, National Key Laboratory Research Funds RCS2011ZT009.

REFERENCES

[1] S. Acharya, M. Franklin, and S. Zdonik, "Balancing push and pull for data broadcast," *SIGMOD Rec.*, vol. 26, no. 2, pp. 183–194, June 1997.

[2] W. Sun, P. Yu, Y. Qing, Z. Zhang, and B. Zheng, "Twotier air indexing for on-demand xml data broadcast," *in Proceedings of the 2009 29th IEEE International Conference on Distributed Computing Systems, ser. ICDCS '09. Washington, DC, USA: IEEE Computer Society*, 2009, pp. 199–206.

[3] S. Wang and H. -L. Chen, "Tmbt: An efficient index allocation method for multi-channel data broadcast," *in Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on*, vol. 2, May 2007, pp. 236 –242.

[4] J. Zhong, W. Wu, Y. Shi, and X. Gao, "Energy efficient tree-based indexing schemes for information retrieval in wireless data broadcast," *in Proceedings of the 16th*

international conference on Database systems for advanced applications: Part II, ser. DASFAA'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 335–351. [Online]. Available:http://dl. acm. org/citation. cfm?id=1997251. 1997282.

[5] A. R. Hurson, A. M. Mu˜noz Avila, N. Orchowski, B. Shirazi, and Y. Jiao, "Power-aware data retrieval protocols for indexed broadcast parallel channels," *Pervasive Mob. Comput.*, vol. 2, no. 1, pp. 85–107, Feb. 2006.

[6] Y. D. Chung and J. Y. Lee, "An indexing method for wireless broadcast xml data," *Inf. Sci.*, vol. 177, no. 9, pp. 1931– 953, May 2007.

[7] B. Zheng, "Tosa: a near-optimal scheduling algorithm for multi-channel data broadcast," *in In MEM'05: Proceedings of the 6th international conference on Mobile data management. Springer*, 2005, pp. 29–37.

[8] C. -C. Chen, C. Lee, and S. -C. Wang, "On optimal scheduling for time-constrained services in multichannel data dissemination systems," *Information Systems*, vol. 34, no. 1, pp. 164 – 177, 2009.

[9] E. Ardizzoni, A. Bertossi, M. Pinotti, S. Ramaprasad, R. Rizzi, and M. Shashanka, "Optimal skewed data allocation on multiple channels with flat broadcast per channel," *Computers, IEEE Transactions on*, vol. 54, no. 5, pp. 558 – 572, may 2005.

[10] Z. Lu, Y. Shi, W. Wu, and B. Fu, "Efficient data retrieval scheduling for multi-channel wireless data broadcast," *in INFOCOM, 2012 Proceedings IEEE*, march 2012, pp. 891–899.

[11] Y. Shi, X. Gao, J. Zhong, and W. Wu, "Efficient parallel data retrieval protocols with mimo antennae for data broadcast in 4g wireless communications," *in Proceedings of the 21st international conference on Database and expert systems applications: Part II, ser. DEXA'10. Berlin, Heidelberg: Springer-Verlag*, 2010, pp. 80–95.

[12] W. -C. Lee and D. L. Lee, "Using signature techniques for information filtering in wireless and mobile environments," *Distributed and Parallel Databases*, vol. 4, pp. 205–227, 1996, 10. 1007/BF00140950.

[13] J. -L. Huang and M. -S. Chen, "Broadcast program generation for unordered queries with data replication," *in Proceedings of the 2003 ACM symposium on Applied computing, ser. SAC '03. New York, NY, USA: ACM*, 2003, pp. 866–870.

[14] G. Lee, M. -S. Yeh, S. -C. Lo, and A. Chen, "A strategy for efficient access of multiple data items in mobile environments," *in Mobile Data Management, 2002. Proceedings. Third International Conference on*, Jan. 2002, pp. 71 – 78.

[15] J. -L. Huang, M. -S. Chen, and W. -C. Peng, "Broadcasting dependent data for ordered queries without replication in a multi-channel mobile environment," *in Data Engineering, 2003. Proceedings. 19th International Conference on*, March 2003, pp. 692 – 694.

[16] K. Foltz, L. Xu, and J. Bruck, "Scheduling for efficient data broadcast over two channels," *in Information Theory, 2004. ISIT 2004. Proceedings. International Symposium* on, june-2 july 2004, p. 113.

[17] S. Jung, B. Lee, and S. Pramanik, "A tree-structured index allocation method with replication over multiple broadcast channels in wireless environments," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 17, no. 3, pp. 311– 325, march 2005.

[18] J. Xu, W. -C. Lee, X. Tang, Q. Gao, and S. Li, "An error resilient and tunable distributed indexing scheme for wireless data broadcast," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 18, no. 3, pp. 392 – 404, march 2006.

[19] S. Acharya, R. Alonso, M. Franklin, and S. Zdonik, "Broadcast disks: data management for asymmetric communication environments," *SIGMOD Rec.*, vol. 24, no. 2, pp. 199–210, May 1995.

[20] W. G. Yee, S. Navathe, E. Omiecinski, and C. Jermaine, "Efficient data allocation over multiple channels at broadcast servers," *Computers, IEEE Transactions on*, vol. 51, no. 10, pp. 1231 – 1236, oct 2002.

[21] J. W. Wong and M. H. Ammar, "Analysis of broadcast delivery in a videotex system," *IEEE Trans. Comput.*, vol. 34, no. 9, pp. 863–866, Sept. 1985.

[22] J. Wong, "Broadcast delivery," *Proceedings of the IEEE*, vol. 76, no. 12, pp. 1566–1577, 1988.

[23] D. Aksoy and M. Franklin, "R*W: a scheduling approach for large-scale on-demand data broadcast," *Networking, IEEE/ACM Transactions on*, vol. 7, no. 6, pp. 846–860, 1999.

[24] J. Xu, X. Tang, and W. -C. Lee, "Time-critical on-demand data broadcast: algorithms, analysis, and performance evaluation," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 17, no. 1, pp. 3–14, 2006.

[25] C. -H. Chu, D. -N. Yang, and M. -S. Chen, "Multi-data delivery based on network coding in on-demand broadcast," *in Mobile Data Management, 2008. MDM '08. 9th International Conference on*, 2008, pp. 181–188.

[26] C. Zhan, V. C. S. Lee, J. Wang, and Y. Xu, "Coding based data broadcast scheduling in on-demand broadcast," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 11, pp. 3774–3783, 2011.

[27] J. Chen, V. C. S. Lee, and J. -Y. Ng, "Scheduling real-time multi-item requests in on-demand broadcast," *in Embedded and Real-Time Computing Systems and Applications, 2008. RTCSA '08. 14th IEEE International Conference on*, 2008, pp. 207–216.

[28] N. Saxena and M. C. Pinottti, "On-line balanced k-channel data allocation with hybrid schedule per channel," *in Proceedings of the 6th international conference on Mobile data management, ser. MDM '05. New York, NY, USA: ACM*, 2005, pp. 239–246.

[29] Z. Lu, W. Wu, and B. Fu, "Optimal data retrieval scheduling in the multi-channel wireless broadcast environments," *Computers, IEEE Transactions on*, vol. PP, no. 99, p. 1-8, 2012.

[30] X. Gao, Z. Lu, W. Wu, and B. Fu, "Algebraic data retrieval algorithms for multi-channel wireless data broadcast," *Theoretical Computer Science*, pp. 1 – 8, 2011.

Ping He received her B.E. degree from Shandong University of Finance and Economics in June 2007, and her M.S. degree from Qingdao University in June 2011. She is working her Ph.D at Beijing Jiaotong University from September 2011. Her research interests include parallel and distributed computing, design and analysis of data disseminating algorithms for optimization problems, routing algorithms, multicast protocols and various schemes of data retrieval and scheduling in wireless networks.

Shuli Luan is currently working at Qingdao Agricultural University, China. Her current research interests include wireless network security and applied cryptography.

Trail Coverage : A Coverage Model for Efficient Intruder Detection near Geographical Obstacles in WSNs

G Sanjiv Rao[a], V Valli Kumari[b]
[a] Sri Sai Aditya Institute of Science and Technology ,Suramplem ,Andhra Pradesh,INDIA
Email: sanjivgsr@yahoo.com
[b] Professsor , Department of Computer Science and Systems Engineering ,Andhra University ,VSP,INDIA
Email: vallikumari@gmail.com

***Abstract*— In wireless sensor network (WSNs), the coverage strategy for achieving higher performance in intruder detection probability near irregular geographical obstacles inside a military terrain, is studied in this paper. The real life problem of the of intruder detection near irregular geographical obstacles has not been focused so far, in which coverage requirement is very high, hard and expensive, if we require the entire boundary of an obstacle in the region has to be covered. Therefore, a novel coverage problem based on data fusion detection system, called *Trail Coverage* is proposed in this paper. A sensor network with *Trail Coverage* provides higher performance rate in detection probability of any intruder that moves along the shortest passes between the geographical obstacles inside a military terrain. We consider various preliminary steps to provide a strong basement for this *Trail Coverage* model. We state a probabilistic model to locate the obstacles inside the region, with randomly deployed sensor nodes, during initial network configuration. Based on computational geometry techniques we design a O^1- *Continuous Obstacle Hull* to find the trail region between the obstacles, for the node deployment, to achieve *Trail Coverage*. We adopt fusion based target detection technique to obtain effective performance in intruder detection probability at the trail region. Through analytical results, we show, the significance of the *Trail Coverage* strategy to meet the desired performance requirements of an intruder detection system, while maintaining greater network coverage with a given fusion range.**

***Index Terms*— Trail Coverage, Fusion range, Obstacle's hull, Detection probability.**

I. Introduction

WIRELESS sensor Networks (WSNs) for battle field surveillance have received a high potential in recent years. This application requires a network with large number of sensor nodes deployed in hostile environments, where random deployment is the only feasible choice. Sensor nodes, limited in terms of sensing, processing and transmitting capabilities, are often affected by the environmental influences. Therefore, battlefield surveillance applications are concerned about how to achieve high performance, in terms of effective intruder detection, which is a basic requirement. For instance, a surveillance application may require, any intruder to be detected with a high probability (e.g. $> 90\%$) and a low false alarm rate (e.g. $< 1\%$)[1].

Coverage plays an important role in achieving optimal detection performance of WSNs, which determines how effectively an area of interest is monitored by sensors [2][3][4][5][6][7]. There exist three types of coverage models for randomly deployed WSNs, namely, area coverage, target coverage, and barrier coverage [8]. Other types of coverage models for intruder detection applications also exist, such as, trap coverage [3], which generalizes the de-facto model of full coverage by allowing holes of a given maximum diameter. However, in reality, achieving the optimal coverage for effective intruder detection is a challenging task.

In particular, in a military terrain, existing obstacles (e.g.natural/cultured), are obstacles that are present on the battle field as inherent aspects of the terrain, where sensor network coverage become critical, because, these obstacles does not allow either to deploy sensors or the sensing signals to pass through. For instance, we consider, jungle and forested areas for military surveillance. There is always moisture present. There are densely packed trees. The jungle can also contain mountains with more plant life, and no two mountains are alike. There can be avalanches, rock slides, cliffs and there are almost caves some where in the mountains.

We argue that these physical locations, known to be obstacles, influence the military operations, based on WSNs. The unit would be at a risk, if the enemy would have chosen these obstacles inside the terrain, as a point to ambush the unit, as it passed through. It is unrealistic and impossible to cover the boundaries, around the obstacles with as many sensors as necessary as in [9], to detect intruders, inside the terrain. However, if we consider the case, when the intruders prefer to travel along a shortest pass, that exist between the obstacles in order to improve its attacking probability, the existing coverage methods such as [3] does not provide a solution for coverage problem to handle the intruder detection at irregular geographical obstacles. So we address the coverage problem for the effective detection probability of intruders in the terrain, by considering the shapes of obstacle's boundaries and using computational geometry concepts.

To the best of our knowledge, this effort to model the coverage to improve intruder detection probability by using computational geometry concepts has not been

doi:10.4304/jnw.9.12.3336-3346

investigated before. In this paper, Therefore, we propose a new problem of coverage, called, *Trail Coverage*, to maximize the intruder detection system performance that scales well with surveillance regions with geographical obstacles. We define the shapes of geographical obstacles in a target region of deployment R^2, to be closed concave curves of set of boundary points inside R^2. The trail region of set of obstacles is a concave, non-intersecting bounding area envelope with finite area, through which, intruders are expected to travel.

A sensor network is said to provide a trail coverage, if the trail region between the obstacles is covered with more number of sensors, than other regions of the deployment area, according to [10]. When the sensor node deployment provides trail coverage, with K number of sensors, the network guarantees intruder that moves along the shortest passes between the obstacles, will surely be detected with maximum probability. Fig.1. shows an example deployment region with several geographical obstacles, where the concave closed curves of set of points reflects the boundaries of the obstacles inside the deployment region. The dotted lines represent the existence of shortest passes between the obstacles, which refer the trail regions, through which the intruders travel for being undetected. The research can improve the efficiency of detection system performance for real time military applications using WSNs, with coverage efficiency, sensor deployment, redeployment over trail regions, while adopting data fusion concepts for detection system.

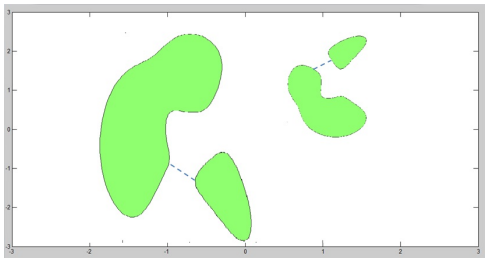


Figure 1: Existence of several Geographical Obstacles inside the deployment region,influence intruder detection system performance.

In this paper, we make several contributions of independent interest, to introduce a new model, *Trail Coverage*, that enhances coverage efficiency of WSNs for improving the performance of a detection system, especially in networks with geographical obstacles inside the deployment area.

- We provide an *Obstacle Locating Model* (similar as in [11]) needed to locate boundary nodes on obstacles inside the deployment region. During initial network configuration, when sensors deployed using poission point process, the probabilistic model for node distribution around the obstacle boundaries is also specified.
- An *Obstacle Distribution Model* explains how to obtain an O^1-*Continuous Obstacle Hull* of set of closed geographical obstacles inside the terrain, which is needed to identify trail regions between the obstacles. Under some network assumptions such as data fusion concept etc., the *Trail Coverage* Network Model is built.
- Once the sensors have been deployed on the trail regions, we specify the impact of trail coverage on the performance of a detection system.

The rest of the paper is organized as follows. In section II, previous works on coverage, deployment, data fusion and intruder detection of WSNs are summarized. In section III, the preliminary work related to the *Trail Coverage* problem is presented. Section IV describes the specification of the problem. Section V illustrates the *Trail Coverage* in detail. Section VI provides the probability analysis of intruder detection system performance under *Trail Coverage*. Section VII specifies significance evaluation for the proposed coverage model. Section VIII gives the conclusion of the paper.

II. Related Work

Arora et al.[12] analysed intrusion detection problem in WSNs as a surveillance problem, (aims at detecting the presence of an intruder effectively and conserving network resources). The authors examined the intrusion detection problem *A line in the sand*, in the context of security scenario. Then, by assuming uniform density for node deployment, they quantitatively analysed the effect of network unreliability on application performance.

Wang et al.[13] analysed the problem of intrusion detection probability in both homogeneous and heterogeneous WSNs, with respect to various network settings. Under various application scenarios, the authors provided an analytical model to formulate the intrusion detection probability within a certain intrusion distance, assuming an intruder is moving on a straight line.

In[14], the authors proposed a new model called *Sine-curve Mobility Mode1*, to examine the effects of different intrusion paths of the intruder on the intrusion detection probability. The authors studied and explored the impact of various intrusion patterns on the WSNs detection probability. Their theoretical and experimental results proved that, when the moving distance is fixed, the straight line path provides the maximum possible intrusion progress towards the destination.

Rang et al.[15] presented a novel intrusion detection algorithm for WSNs, based on data aggregation scheme, which does not require prior knowledge of network behaviour. They proved that the algorithm can detect the compromised nodes with high accuracy and low false alarm probability.

All the above researches aim at detecting the presence of an intruder effectively and conserving network resources under various metrics, assumptions and detection accuracy constraints. In this paper, the major difference of the *Trail Coverage* problem is to examine effect of geographical obstacles present inside the WSN, on the intrusion detection probability.

Other works study impact of deployment strategies and coverage as metrics to measure the detection quality of the WSNs. Zhao et al.[16]proposed a new model called *Surface Coverage* in WSNs. The authors derived expected coverage ratio on surface coverage for stochastic deployment. Then, they formulated the planned deployment problem and proposed three approximation algorithms.

Bai et al.[17] proposed an *Optimal Multiple-Coverage Problem* in sensor networks, where the authors proposed to cover each point in the monitored region with more than one sensor,to improve detection quality. The authors proposed two-coverage patterns for deployment, with a bound on optimal deployment density.

Li and Kao [18] demonstrated a new, distributed, self-location estimation scheme, based on voronoi diagram, to achieve K-coverage with minimum number of mobile nodes, in WSNs.Here their aim is to maximize the area coverage by a given number of sensors.

The authors of [19], used a probabilistic coverage protocol for WSNs, based on probabilistic sensing model. The main idea of this protocol is to ensure the coverage at a least-covered point in the monitored area, exceeds a given threshold value.

XU and Sahni[20] have formulated an integer linear programming model to provide the desired target coverage for minimum cost sensor deployment. Then, they developed a greedy algorithm for solving the ILP model.The authors considered the deployment cost and placement capacity as the constraint conditions for the deployment at every point in the monitored region.

In [21], the authors presented a new algorithm pSPIEL,which is a polynomial-time,data-driven algorithm, to select optimal sensor placement locations for the deployment.The authors considered, communication cost and minimum number of sensors at maximum informative locations as constraints.

Nene et al.[22] have proposed a new algorithm as a sensor deployment strategy, called *Uncovered Region Exploration Algorithm(UREA)*, to enhance the coverage after the initial random deployment of sensors. Under the assumptions of bounded, homogeneous and mobile ad hoc properties of WSNs, the authors proposed to identify effective locations for sensor positions on the uncovered region around the node in consideration. Then, they proposed the redeployment of the sensors through one time displacement of each node at the new positions, to achieve best network coverage.

Wang et al.[23] examined the problem of intrusion detection in randomly distributed WSNs. The authors compared the detection performance of a random deployed WSN with a Gaussian, a truncated Gaussian and a uniformly distributed WSN, under the same application scenario. The authors investigated the problem of intrusion detection under both single and multiple sensing detection. This work illustrates how the network parameters, such as, number of deployed sensors, sensing range, deployment deviation, maximal allowable intrusion distance and intruder starting distance etc., affect the detection probability.

Chen et al.[24], worked on the concept of barrier coverage, where sensors are deployed in a narrow belt region to detect intruders. The authors theoretically analysed the problem of detection probability of arbitrary path across the barrier of sensors,under the consideration of intruders speed as constraint. The authors proposed an algorithm called MWBA (ie)*Minimum Weight Barrier Algorithm*,to schedule the activation of sensors energy-efficiently to form a $\epsilon - barrier$ in a random WSN.

Fang et al.[25] proposed an algorithm to find out the boundaries of routing holes. The authors considered the holes as important topological features and proposed two simple and distributed algorithms, the *TENT* rule and *BOUNDHOlE* to identify and build routes around the holes.

However, in all the above works,the authors in their research strategies did not take into consideration the influence of geographical obstacles inside the terrain,on the intrusion detection performance of a WSN in a military surveillance region, which believe is an important factor to consider while designing a sensor network for effective intrusion detection.

In this paper, compared to the above schemes, we have adopted different assumptions, metrics and computational geometry concepts to achieve effective detection quality in the presence of geographical obstacles inside the WSN of a military surveillance application. The theoretical results demonstrate the superiority of our proposed model.

III. Preliminaries

A. Assumptions

- We consider a cluster based WSN with n sensors distributed in clusters, with in the deployment region, for the initial configuration.
- We study homogeneous WSN, where all sensor nodes are identical in terms of sensing and forwarding abilities.
- We assume, the entire network is under the supervision of a central base station, which controls the initial network configuration by choosing the cluster heads, and obtain the information about boundary nodes either at the obstacles inside the deployed region (or) the outer boundary of the network.
- However, in this paper, we focus only on the nodes, that are closer to the *obstacles* inside the deployment region, and the outer boundary can be ignored here.
- We consider only *opaque obstacles*, which does not allow either to deploy sensors inside or allow the sensing signal to pass through.
- Further, we note that, the cluster head is responsible for making a detection decision, based on the fused measurement from member sensors inside the cluster.
- We also assume, adding new nodes to the network is under the control of the base station.

B. Obstacle-locating Model

We assume a large 2-dimensional geographical region R^2 for the WSN deployment. We consider, n number of sensors are uniformly distributed within the field of interest (FOI). Generally, sensors may be dropped in battle field (or) hostile environments using airplanes. Such a random distribution is desirable for the initial configuration of the network, where there is no prior knowledge of the network due to the existence of geographical holes/obstacles such as hills, ponds, lakes, etc. In our work, to locate the boundaries of the obstacles (or) the outer boundary of the FOI, we make use of the topology of the *Connectivity Graph*. Formally, we assume that each sensor can communicate with any other sensor located within certain transmit range r_t. And this r_t is considerably larger than the sensing range r_s. This corresponds to assuming the communication graph defined by the wireless nodes is a *Unit Disk Graph(UDG)* as specified in [11]. A UDG has an edge between two nodes, if the euclidean distance between the two nodes is less than transmit range r_t. Further more, we assume that the graph is connected, when the sensors are initially configured at random positions within the FOI.

To model the *Initial Configuration* of the network, we can use a poisson point process over R^2 with constant density λ, which results in *Boolean model*. In poisson point process, each sensor covers a disk of radios r_s and the sensor network *Connectivity* can be studied from the connected components set.

$$\mathcal{I}(\lambda, r_s) := \cup_i C(X_i, r_s) \tag{1}$$

Where (X_i) denotes the poisson process points called nodes. $C(X, r_s)$ denotes the disk centered on X and $r_s = r_t/2$.

Further, the average number of neighbours located inside a disk of radius r_t, centred on a arbitrary location of region R_2 is

$$\gamma := \lambda \pi r_t^2 \tag{2}$$

Now, we would employ a hole finding algorithm by considering a sub-graph of *UDG* induced by each connected component of $\mathcal{I}(\lambda, r_s)$, and compute hop distances of all the network nodes to a dedicated network node $\in R^2$ i.e., cluster head. Therefore we can determine the boundary nodes, which do not have a 2-hop neighbours as illustrated in[11].

Moreover, the percolation theory addresses the existence of a giant connected component $G(A)$ in the random set $\mathcal{I}(\lambda, r_s)$, which is the union of connected components of $\mathcal{I}(\lambda, r_s)$, that have non-empty intersection with $G(A)$ as described in [26]. Under all these considerations, we can state the main results of Boolean Model [27] and the Hole Finding algorithm [11] as follows.

Theorem 1. $\exists$ a value $\gamma_c < \infty$ such that

- If $\gamma = 4\lambda\pi r_s^2 < \gamma_c, \mathbb{P}(diam(G(C(X_i, r_s))) = \infty) = 0$, and there are holes in the network since the contour of connected components in $\mathcal{I}(\lambda, r_s)$ is always *broken* either at the boundary of a hole (or) outer boundary.
- If $\gamma = 4\lambda\pi r_s^2 \geq \gamma_c, \mathbb{P}(diam(G(C(X_i, r_s))) = \infty) > 0$ and the network is free of holes with a giant connected component $G(A)$ in the random set $\mathcal{I}(\lambda, r_s)$, where γ_c is known as percolation threshold. $\mathbb{P}(diam(G(C(X_i, r_s))) = \infty)$ is the percolation function which is defined as the probability that a node placed at X_i, belongs to the region which is free of holes i.e., non-obstacle parts of R^2.

In the context of connectivity, *Theorem 1* implies that when $\gamma < \gamma_c$ i.e., when node density is too low (or) the radius of disk is too small, the network is split into number of sub network of connected components with the presence of hole boundary (or) outer boundary of R^2. Therefore, in this case, the network cannot achieve good connectivity. On the other hand, if $\gamma > \gamma_c$ the network is free of holes and therefore, all nodes are connected together to provide higher connectivity. Here, we make some remarks on the effect of hole boundaries (or) outer boundary on network coverage and connectivity. Generally, the coverage is more likely to fail at the boundary than interior [28]. Moreover, it is shown in [11] that the non-hole parts of the network exhibits high node distribution with greater network connectivity. Clearly, if in a sufficiently large region, sensors mostly break down and can not perform effective detection, especially which are close to the outer boundary (or) to a boundary of some hole. And we require that sensors are connected to a cluster head in order to perform effective detection. Under these assumptions, as mentioned in this section, we can obtain the initial network configuration , by locating the boundaries of the holes in the geographical region R^2 as shown in Fig.2.

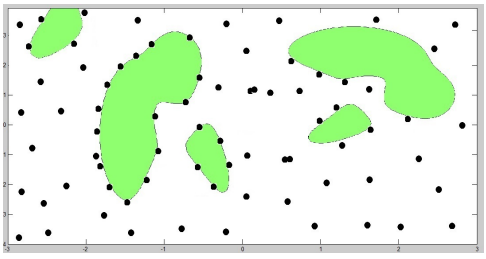


Figure 2: Locating the boundaries of obstacles inside the deloyment area during intial network configuration.

Fig.2. depicts the network model during the initial configuration, where the dark-filled circles representing the randomly deployed sensor nodes are locating the boundaries of set of concave closed curves of various geographical obstacles inside the deployment region R^2 of a military terrain.

In addition to the initial configuration model, we need to add a probabilistic model to estimate the node distribution around the obstacle (or) hole boundaries within the field of interest.

In the following theorem, we show that the probability that deployed nodes to be on the boundaries of hole/obstacle inside the field of interest R^n.

Theorem 2. Let R^n be a FOI of area $|R^n|$, perimeter $|\partial R^n|$. Assume, R be a hole caused by an obstacle (concave (or) convex) with in R^n (i.e)$R \subseteq R^n$. Let the area of R is $|R|$, its boundary (or) perimeter is $|\partial R|$. Let $n = \gamma |R^n|$ be the number of sensors distributed with in the FOI R^n, by considering a *Poisson Deployment* with intensity γ and a common radius of r_t. Then,

- Let P be a point at which a sensor is located. The sensor is said to be on the boundary of any hole/obstacle inside the terrain, iff, there is no sensor located within the disc of radius r_t centered at P. Let X is a set of points within the disc of radius r_t centered at P. Then,
- The probability that the point P is on the boundary of an obstracle is equal to the probability that X contains no sensor nodes (i.e.,)

$$\mathbb{P}(P \in |\partial R|) = e^{-\lambda\gamma} = e^{-\lambda\pi r_t^2} \tag{3}$$

C. Obstacle Distribution Model

In practical intruder detection applications, one of the WSNs essential responsibilities is to capture the information about geographic obstacles inside the terrain. Ambushes can be easily conducted in this environment since, the tanks and other vehicles have a hard time maneuvering through and around the obstacles, such as, small rivers, brooks, ravines etc., serve to break the *army's* front. The obstacles such as, large river, lakes, an impenetrable morass which are absolutely impassable. These obstacles however, are very rare, and a complete protection, therefore, is hard to find. Hence, the coverage requirement may differ from trail regions to other regions. The sensing devices should be placed according to the distribution of obstacles. It is required to model the obstacle distribution, based on computational geometry techniques before going for the deployment. In order to obtain this distribution model, the relevant definitions are given as follows.

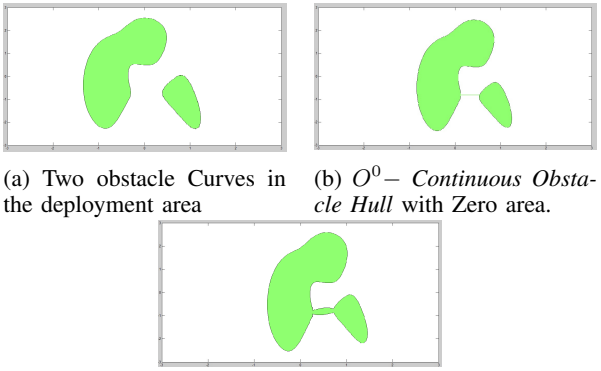
Definition 1: O^1- *Continuous Obstacle Hull* of set of closed obstacle curves is a concave, non-intersecting and bounding area envelope, with finite area (or trial region) as shown in Fig.3.c

Definition 2: Free-form obstacle curves means, they are represented using *Bezier (or) B-Spline* representations which are *parametric ones*.

Definition 3: Inflection point refers to a point on a curve of an obstacle, at which the curvature changes its sign.

Definition 4: Antipodal points on obstacle refer to the points on the obstacle which are diametrically opposite to each other, are connected by a straight line, gives the true diameter.

Definition 5: Minimum Antipodal Distance between two closed O^1- *Continuous*, non-intersecting curves of



(a) Two obstacle Curves in the deployment area

(b) O^0- *Continuous Obstacle Hull* with Zero area.

(c) O^1- *Continuous Obstacle Hull* with finite area.

Figure 3: Closed concave/convex obstacle curves

obstacles occurs, when, the normals of the corresponding points on respective obstacle curves are antipodal, as shown in Fig.4

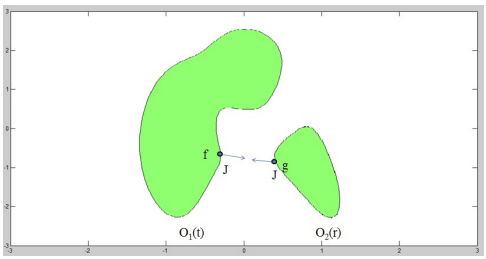


Figure 4: Minimum Antipodal distance for two free - form planar obstacle curves in R^2

where f and g are the antipodal points on the curves $O_1(t)$ and $O_2(r)$ respectively. J is the outward normal.

Definition 6: Obstacle Distribution Model depicts the O^1- *Continuous Obstacle Hull* of the concave obstacle hull of set of closed obstacle curves inside the deployment region. The model can be represented by the Obstacle Distribution Function $O(U, \delta)$ which is constructed according to the O^1- *Continuous Obstacle Hull* with finite area (or trial region), for the set of free form concave obstacle curves of R^2

Let U be a set of disjoint free form concave/convex obstacle curves with inflection points. δ be the minimum antipodal distance between any two closed obstacle curves and having no discontinuities in R^2.

It is to be noted that, as the closed obstacle curves have well defined boundary and interior, the concave hull of set of closed obstacle curves also should have a well-defined interior. It is assumed that, the interior of a concave hull lies to its left as we travel along the increasing direction of parametrization.

In this paper, we adopt, an algorithm, that consider the problem of computing an approximate O^1- *Continuous Obstacle Hull*, for a set of free form obstacle curves, that are closed O^1- *Continuous*, non-self intersecting and contains no straight line segments. Our approach, consists of several necessary processes for acquiring the

obstacle distribution function.

While determining the concave hull for two obstacle curves, the following cases can be observed.

Case :1 Both obstacles intersect with each other, where the minimum antipodal distance between them is zero. i.e $\delta = 0$

Case :2 One obstacle lies completely outside the other, with minimum antipodal distance is other than zero (i.e) $\delta > 0$
We exclude the case where one obstacle is inside the other.

However, in our work, we consider the obstacles lies completely outside the other, with minimum antipodal distance should be $\epsilon \leq \delta \leq \eta$, where ϵ, η represents minimum and maximum allowable distances between the obstacles respectively.
Initially, for the obstacle curves, that lie completely outside, we find the inflection points on the curves by following *antipodal constraints* of two obstacle curves in R^2:

$$\begin{aligned} \langle O_1^1(t), O_1(t) - \frac{O_1(t) + O_2(r)}{2} \rangle = 0 \\ \langle O_2^1(r), O_2(r) - \frac{O_1(t) + O_2(r)}{2} \rangle = 0 \end{aligned} \quad (4)$$

Where $O_1(t), O_2(r)$ are the two planar closed O^1- *Continuous* curves of two obstacles and $O_1^1(t), O_2^1(r)$ are the tangents of the curve at the parameters t and r respectively, here t and r are unknowns. By solving equation(4), we will get a finite set of candidates for t and r values, which can be evaluated to get minimum distance points on the respective curves. Theses are the starting points for the concave hull. We repeat the same process for each pair of non-intersecting obstacle curves with $\epsilon \leq \delta \leq \eta$, in the set U, and compute the minimum antipodal distances, $\delta_1, \delta_2 \ldots$. Then find $\delta = min\{\delta_1, \delta_2 \ldots\}, \exists$ and $\epsilon > 0$and $\epsilon <<< \delta$.
At this moment, the concave hull for each obstacle curve, can be viewed as a O^0- *Continuous*(with zero area)concave hull. Now, we need to attain O^1- *Continuity* by applying Bezier (or) B-spline fitting method, where, a small number ϵ, can be used to define two sets of control points, which are used to fit a Bezier (or) B-spline curve. Given the minimum distance antipodal points f and g on the two curves$O^1(t), O^2(r)$ respectively, we can represent its antipodal line $\overline{fg}$ in parametric form as $f + v(g - f)$, where v is the parameter. Now, Generally, Given a point L, on the curve $O(t)$, with normal $J(t)$, we can find closest tangent points to L on its either side:

$$\langle L - O(t), J(t) \rangle = 0 \quad (5)$$

This process results in two control polygons with vertices $\{T_1, r, s, T_3\}$ and $\{T_2, r, s, T_4\}$. Here r, s are the control points on the antipodal line $\overline{fg}$, Where $r = f + \epsilon$ and $s = g - \epsilon$. And T_1, T_2 are the closest tangent points on either side of r on $O_1(t)$. Similarly, T_3, T_4 are the closest tangent points on either side of s on $O_2(r)$ as shown in Fig.5. Now, a Bezier/B-spline curve can be

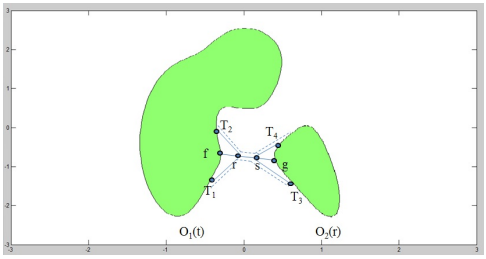


Figure 5: Fitting of curves to ensure O^1- *Continuity*

generated between for each set of control points ensuring O^1- *Continuity* for the concave hull by removing the portion of the curve between the parameters at which the tangents were identified as shown in Fig.6.

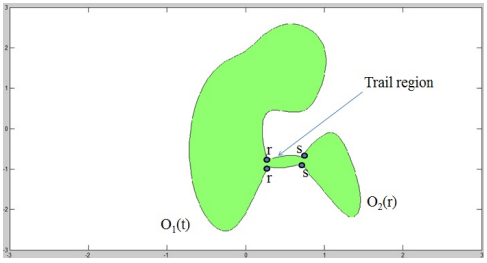


Figure 6: AttainingO^1- *Continuity* by removing $T_1 - f - T_2$from $O_1(t)$ and $T_3 - g - T_4$ from $O_2(r)$

These Bezier/B-spline curves are called *Auxiliary Curves*, and the area or region between them represents the trail region between the obstacles, justifies our assumptions. Repeat the same process for the remaining curves in the set U, in ascending order of $\delta's$, finally results in the tight envelope of a concave hull, with finite bounded area (or) trail region for the set of obstacle curves.

For complete details of the concave hull construction algorithm refer to [29].

D. Sensing model

The sensing model is another important factor to address the coverage quality for detecting intruders using WSNs. The coverage be expanded by the cooperation of sensors through data fusion. In our work, we adopt the signal decay model which depicts the sensors sensing capability interns of signal energy attenuation [4]. We assume, that sensors (i.e.,cluster heads) with isotropic sensing capability can detect intruders by measuring the signal energy emitted by the signal sources (or member sensors) located at a certain distance from it. In practice, as the signal energy attenuates with distance from the signal source, the sensor (or cluster head) sensing capability is not constant over a given area, and vanishes gradually towards boundaries and completely outside.

As in [1], if we denote the original energy emitted by the signal source is P_0 , the decaying factor k is from 2 to 5, and the constant d_0 determined by the size of the sensor (or cluster head) and the signal source (or member sensor). Then, the decreasing function $P(d)$ as the signal energy measured by a sensor (cluster head) located d meters away from the signal source (member sensor) is given as follows

$$P(d) = \begin{cases} \frac{P_0}{(d/d_0)^k} & \text{if } d > d_0 \\ P_0 & \text{if } d \leq d_0 \end{cases}$$

..... (6)

Since, there are many factors affecting the sensor nodes measurements such as back ground noise, which follows the zero-mean normal distribution with a variance of σ^2. The signal energy measured by some sensors located d_i meters away from the signal source will be of the form

$$S_i = P(d_i) + q_i^2 \tag{7}$$

Where q_i is noise strength

E. Fusion-Based Detection Model

The performance of detection systems can be improved by adopting *Data Fusion Techniques* [4], for cluster based sensor network, with uniformly distributed sensors in clusters within the network area.

There are two types of basic data fusion schemes, which are *decision fusion* and *value fusion*. The *value fusion* scheme depicts, each sensor sends its measure including noise, to the cluster head, which makes the final detection decision, based on the received snapshot measurement from the member sensors in the cluster. We adopt the above data fusion model for intruder detection as follows.

In a detection process, which can be executed periodically, the intruder is detected, when the aggregated value of the sensors energy measurements, over the routing path, to the cluster head, has exceeded, some detection threshold τ. As in [1], if we denote by P_I be the probability that an intruder can be detected when, K sensors take part in the data fusion. Under the value fusion scheme, the detection probability is given by

$$P_I = \mathbb{P}(\frac{1}{K}\sum_{i=1}^{K} S_i > \tau) \tag{8}$$

Also, the false alarm rate too, affects the detection system's performance, the probability of making a false alarm is given by

$$P_I^1 = \mathbb{P}(\frac{1}{K}\sum_{i=1}^{K} q_i^2 > \tau) \tag{9}$$

F. Network Model

In military applications of WSNs, the terrain usually have many natural geographical obstacles, that are a common and inherent consequence, due to environmental influences. We assume that intruders try to hide themselves, using the obstacles, and they defend themselves by following, the shortest passes between the obstacles. We define such passes to be *Trails* in the network model. We are only concerned with the coverage, for such kind of *trails* between the obstacles. Due to the assumption that, the base station has a complete meta information about the initially configured network using poisson point process, we propose that, the base station acquires the phenomenon of the obstacle regions inside the network, with much *lower sensor density* than other regions.

We define, *obstacles* to be simple concave regions enclosed by polygonal cycle, which contains all the boundary nodes inside the network. We note, that the sensor nodes close to the obstacles experience low SNR with high noise rate. Hence, these nodes make little contribution to the effective intruder detection, and some times result in false alarms too. Also, the fusion range limits the quality of information fused at the cluster head, due to spatial decay of signal energy. Such a fusion range concept is adopted as an important design parameter in previous works on detection performance [1][4].

In our work, we define the *fusion range* or *coverage threshold* as, disc of radius R, centred at any point on the trail. There fore, we propose that, more sensors are deployed along the trails, between the obstacles, by following a two dimensional Gaussian distribution, to participate in the data fusion as shown in Fig.7.

Let the Trail $T = \{X \in R^2 : \|X\| \leq 1\}$ in R^2. Let $G_i = (x_i, y_i)$ be any physical location represents point of interest (POI) on the trail, and, it is associated with a minimum coverage threshold, denoted by R_i , $r_s \leq R_i \leq R$. Following Gaussian Distribution, the *probability density function (PDF)* that a sensor located at the point (x, y) with respect to the deployment point with coordinates (x_i, y_i), as $(0, 0)$ is given by [30]:

$$f(x, y, \sigma_x, \sigma_y) = \frac{1}{2\pi\sigma_x\sigma_y} e^{-}(\frac{x^2}{2\sigma_x^2} + \frac{y^2}{2\sigma_y^2}) \tag{10}$$

Where σ_x, σ_y denotes deployment deviation, which are assumed to be the different, along the two dimensions respectively.

Fig.7. illustrates the network model. In the figure, the finite area between the two obstacle curves reflects the trail region between the obstacles, and the dotted lines represent the fusion range or coverage threshold with in which, sensor nodes are Gaussian distributed with respect to any POI on trial. Thus, forms a cluster to detect the intruder, by comparing the fused energy measurements in the cluster, with a threshold value.

IV. Problem Specification

Let T is to-be-deployed trail area, consists of a set of points of interest (POI), depicts a barycentric coordinate

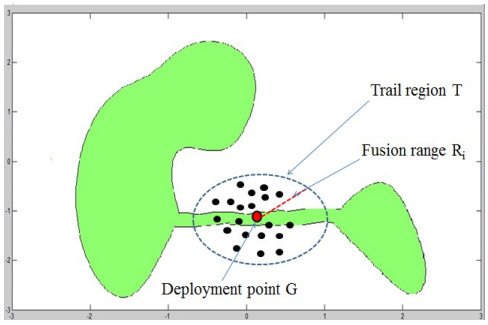


Figure 7: Gaussian Distribution of sensors to form cluster along the trial between the two obstacles

system, where, the two POI are separated at a barycentric distance as in [10]. As we assumed that each POI, $G_i = (x_i, y_i) \in T$ is associated with a minimum coverage threshold, denoted by R_i, $r_s \leq R_i \leq R$. After Gaussian deployment over the trail region, let each POI is covered with a PDF, $f(x, y, \sigma_x, \sigma_y)$, defined by (10). For each physical location $G_i = (x_i, y_i) \in T$, we assume, $P_I(G_i)$ be the probability of successfully detecting an intruder located within the fusion range (or) coverage threshold, R_i of G_i, with K number of sensors, which can be calculated by (8), must be maximum, i.e, between 0.5 and 1.

Similarly P_I be the problem of false alarm, calculated by (9), must be minimum, i.e, between 0 and 0.5, and is location independent [4]. As mentioned before, the detection system's performance can be characterized by the coverage efficiency of the network. Our focus is to study the coverage, to improve the intruder detection system's performance, by a new metric called *Trail Coverage*, which is defined as follows

Definition 7: Given a Trail region T, a physical point $G_i = (x_i, y_i) \in T$ is covered, if $s = \{s_1, s_2, ...s_K\}$ denote K deployed sensors with sensing range r_s, are, within R_i of G_i.

The *Trail Coverage* defines the data fusion quality provided by the network at any point on trail-region. Our problem is to place more sensors using Gaussian distribution along, all the trail-regions, in order to maximize the detection system's performance. Our problem is formulated as below.

Problem 1 Given a trail-region T and a set of physical locations on it, deploy sensors using Gaussian distribution along the trail region, with respect to the deployment point $G_i = (x_i, y_i) \in T$, such that, the intruder detection system's performance is improved subject to the following constraint,

$$P_I(G_i) \geq \beta, \beta \in (0.5, 1) \tag{11}$$

β is high detection probability.

V. Trail Coverage

In this section, we derive the trail coverage probability by considering Gaussian distributed sensor nodes, around a deployment point on the trail region, with different deployment deviations in x, y dimensions (i.e.,) $\sigma_x \neq \sigma_y$. In military terrain monitoring applications, the trail regions, which are the regions of interest in this paper, may not be as regular as disk. Therefore, we adopt an elliptical network domain as in [30] for our analysis. When sensors are distributed with respect to a deployment point of a trail region, the PDF for a point (x,y) to be located within the coverage threshold, R_i, of the deployment point G, is given by (8). In particular, as shown in Fig.8, we consider, the deployment point on a trail region is located at the center of the ellipse, as in [30]. The coverage probability

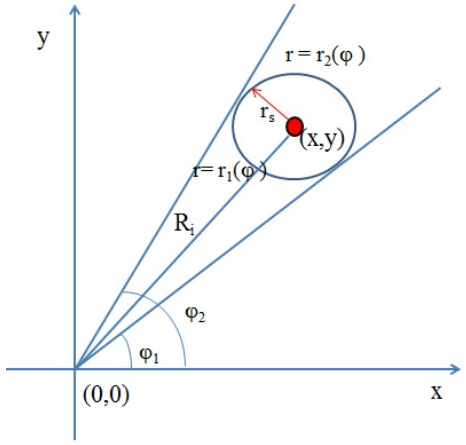


Figure 8: Coverage probability of a point (x,y) using polar co-ordinate system for an elliptical area (Figure is redrawn from [30]).

that a sensor node is located to cover any point (x, y) in the ellipse is given by

$$P_s = \iint_{\pi * r_s^2} f(x, y, \sigma_x, \sigma_y)\, dx\, dy \tag{12}$$

The coverage probability given by (12) follows a Cartesian coordinate system. However, since, we consider the deployment deviations differently in x, y directions, we note that, we adopt to use the polar coordinate system as in [30], for describing the coverage probability equivalent to (12) as follows

$$P_s = \int_{sin^{-1}(\frac{y}{R_i}) - sin^{-1}(\frac{r_s}{R_i})}^{sin^{-1}(\frac{y}{R_i}) + sin^{-1}(\frac{r_s}{R_i})} d\varphi \int_{r_1}^{r_2} \frac{1}{2\pi\sigma_x\sigma_y} e^{-(\frac{r^2 cos^2\varphi}{2\sigma_x^2} + \frac{r^2 sin^2\varphi}{2\sigma_y^2})} r dr \tag{13}$$

Here, r_1 and r_2 can be obtained from the equation,

$$r_s^2 = (r cos\varphi - x)^2 + (r cos\varphi - y)^2 \tag{14}$$

Where r is variable.

Let $S = \{s_1, s_2 ... s_m\}$ be the set of nodes deployed on the trail point, whose sensing range cover the point (x,y) in the ellipse. Then, the total coverage probability of the

point (x, y) with atleast K number of sensors is defined as

$$P_S = 1 - \sum_{i=1}^{K} \binom{m}{k} (1 - P_s)^{m-i} * P_s^i \qquad (15)$$

Where P_s is the coverage probability given by (13). We note that the total coverage probability given by (15) reflects the trail coverage probability of the network.

VI. Intruder Detection in Trail Covered WSNs

In this section, we provide the probability analysis for the intrusion detection system under data fusion detection model in a *Trail Covered* WSN. In many target detection applications, it is required to maintain a high level coverage over the target regions to perform effective intruder detection. According to [4], data fusion improves the coverage of WSNs. Also, the detection probability increases, when the number of sensors taking part in the data fusion is large enough.

Now, we discuss, how the *Trail Covered* network with data fusion detection model performs with respect to the intruder detection system's performance. This leads to the Theorem 3 as follows.

Theorem 3. The intruder detection probability, denoted by $P_I(G)$ on trail, maximizes, only if, there exists at least one point on the trail, which has been covered with at least K number of sensors to participate in the data fusion with in the R_i of G. It can be given by:

$$\mathbb{P}(P_I(G) \geq \beta) = 1 - (1 - P_S) \qquad (16)$$

where P_S is given by equation (15).

Proof. In order to analyse the probability of intrusion detection system's performance in a *Trail Covered* WSN, we assume a trail region as depicted in Fig.9 based on the network model. The region is covered under the fusion range (or) coverage threshold R_i of any deployment point G on the trail, exploit the collaboration among the sensors to detect intruders.

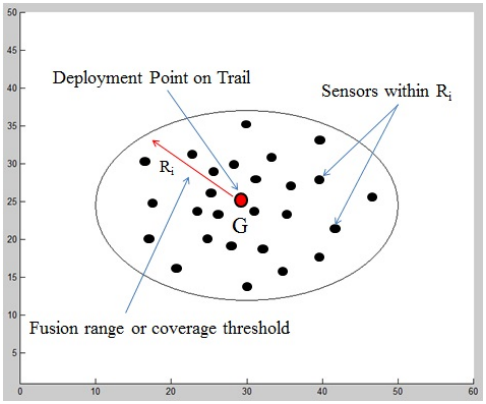


Figure 9: Trial Coverage to perform Intruder Detection at G.

Under this *Trail Coverage* model, at least one point on the trail region should be covered with K number of sensors for improving the performance of the detection system. The probability that there is no point on the trail that has been covered with K number of sensors is $(1 - P_S)$. Then, the complement of $(1 - P_S)$ is the probability that there is at least one point on the trail that has been covered with at least K number of sensors and can be given as: $1-(1-P_S)$. Thus, the probability that the detection probability of an intruder at a point on the trail, maximizes, under the *Trail Coverage* model in WSNs is $\mathbb{P}(P_I(G) \geq \beta) = 1 - (1 - P_S)$.

Based on *Theorem 3*, it is clear that, the intruder's detection probability $P_I(G)$ is no lower than a detection probability value β, where $\beta \in (0.5, 1)$, when a trail point G is covered with atleast K number of sensors, given M nodes, to participate in the data fusion.

Therefore, if a point on a trail region is covered with Gaussian Distributed sensors, under data fusion detection model, the sensors within the fusion range of that trail point, provide higher coverage, which in turn leads to increased detection probability at that point of deployment. Detailed analytical based discussions are presented in the next section.

VII. Significance Evaluation

In this section, we theoretically evaluate the significance of *Trail Coverage* scheme proposed in Section 5 to improve the network performance in various intrusion detection systems using WSNs. To support our discussions, we present the impact of *Trail Coverage* on Detection probability in Section 7.1. Further we analyse the effect of various network deployment parameters such as *Number of Nodes* deployed on trail and *Deployment Deviations* on *Trail Coverage* probability that in turn effect the quality of intrusion detection in WSNs in Sections 7.2 and 7.3 respectively.

To follow up our work, we fix the parameters of deployment point, sensing range for each sensor and the number of nodes to participate in data fusion detection and the optimal fusion range, are as follows:

$G(0, 0)$, $r_s = 10m$, $K = 3$, $40 < R_i < 70$. The trail domain T is a $60mX50m$ elliptical area. The detection probability of an intruder, at any point on trail region is set to be between 50% and 100%, i.e., $\beta \in (0.5, 1)$

A. Impact on Intruder Detection Probability

We first, analyse the effect of Trail Coverage on the detection probability of an intruder at any point on the trail region in MATLAB. We set the deployment deviations in X,Y directions and the number of deployed nodes as $\sigma_x = 45, \sigma_y = 25$ and $M = 500$ respectively. Fig.10. plots the Trail Coverage versus the Intruder Detection Probability under K-node data fusion detection model $(e.g., K = 3)$.

From the Fig.10, the intruder detection probability increases with increasing of the trail coverage probability. This is because when sensors are gaussian deployed with

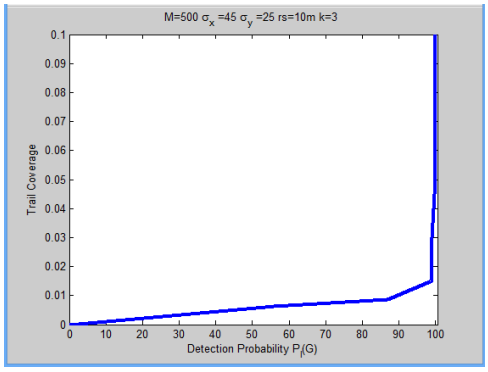


Figure 10: Intruder Detection probability versus Trial Coverage

respect to $G(0,0)$ on the trail region, the optimal fusion range in between $40m$ and $70m$ maximizes the *Trail Coverage*. Hence more sensors contribute to the data fusion, leads to higher detection performance. Intuitively, an increase in the *Trail Coverage* with gaussian deployed sensors within the optimal fusion range on a trail region, resulting in better detection probability. Hence, *Trail Coverage* plays an important role in maximizing the intruder detection probability of a WSN.

B. Impact of Number of Deployed Nodes M on Trail

In order to analyse the impact of number of nodes deployed on a trail region coverage , we set a point in the elliptical trail domain, deployment deviations in X,Y directions as $(x,y) = (35,40)$, $\sigma_x = 45$ and $\sigma_y = 25$ respectively. Fig.11, shows Trail Coverage probability at a point $(35,40)$ in the trail domain under 3-node data fusion detection model with varying number of deployed sensor nodes on the trail domain.

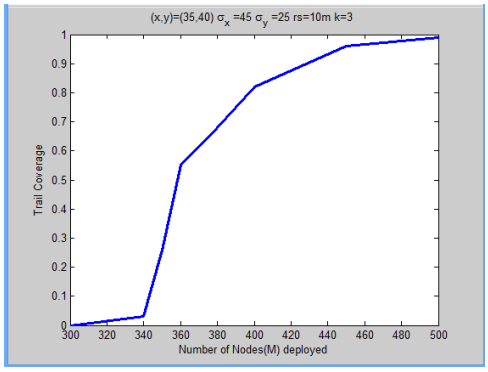


Figure 11: Trial Coverage versus Number of Nodes

From the Fig.11, the trail coverage probability increases with increase of number of deployed nodes on the trail domain. The reason for this is, given a fusion range(e.g., $R_i = 53$), the deployment of more sensors on the trail domain improves the node density which results in greater *Trail Coverage* for effective intruder detection.

C. Impact of Deployment Deviations

We now explore, the impact of non uniform deployment deviations in X, Y directions, on *Trail Coverage* probability. We set the fusion range, number of deployed nodes as $R_i = 53$ and $M = 500$ respectively. Fig.12. depicts the *Trail Coverage* Probability with varying Deployment Deviations σ_x and σ_y, under 3-node data fusion detection model.

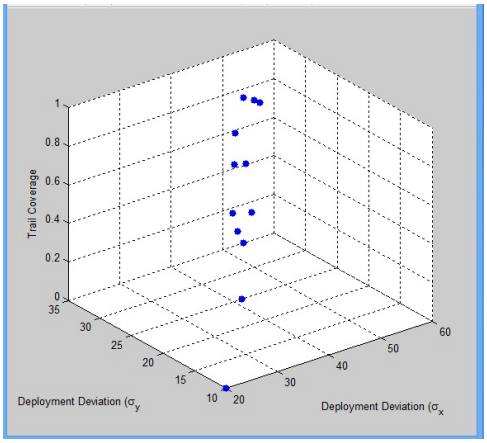


Figure 12: Trail Coverage versus Deployment Deviations

We can see from Fig.12. that the *Trail Coverage* initially increases with the deployment deviations but decreases to zero eventually. This is due to the fact that, when the deployment deviations increases, more number of sensors can be deployed around the deployment point to increase the *Trail Coverage*. However, as the deployment deviations becomes very large, the sensors will be distributed far away from the deployment point, thus reduces the *Trail Coverage* probability.
Hence, an Optimal choice of deployment deviations can maximize the trail coverage probabilities.

VIII. Conclusions

In this paper, we present a novel *Trail Coverage* strategy as the coverage problem of a wireless sensor network. More specifically, we address network coverage at geographical obstacles inside a military terrain, in order to detect intruders more effectively. By adopting the concept of fusion–based target detection, the research on the problem contributes to improve the efficiency of network coverage while enhancing, the performance of intruder detection probability, especially near irregular geographical obstacles. For the initial network configuration and the obstacles locating model, we have shown that the area near the geographical obstacles suffers with least sensor node density, which results in poor network coverage, that has a great impact on the detection probability of an intruder that passes through the obstacles. And for obstacle distribution model, we use computational geometry techniques to find the trail region between the obstacles, by assuming, that an intruder moves along the trail regions. We take a Gaussian approach to deploy nodes to cover a point on the trail region. Under the

consideration of the data-fusion detection model, trail coverage model is constructed for improved detection probability of an intruder near geographical obstacles. The analytical results showed the significance of the novel coverage scheme that can improve the detection probability of an intruder near irregular geographical obstacles inside a military terrain.

ACKNOWLEDGMENT

The authors would like to thank to College of Engineering, Andhra University, Visakhapatnam and Sri Sai Aditya Institute of Science and Technology, Surampalem authorities for their constant support and cooperation!

REFERENCES

[1] Yuan, Z., Tan, R., Xing, G.L., Lu, C., Chen, Y., Wang, J.: Fast sensor placement algorithms for fusion-based target detection. Proc. IEEE RTSS, 2008, pp. 103112.
[2] Liu, B., Brass, P., Dousse, O., Nain, P., Towsky, D.: Mobility improves coverage of sensor networks. Proc. ACM MOBIHOC, May 2005, pp. 300308
[3] Balister, P., Zheng, Z., Kumar, S., Sinha, P.: Trap coverage: Allowing coverage holes of bounded diameter in wireless sensor networks. Proc. IEEE INFOCOM, April 2009, pp. 136144
[4] Xing, G., Tan, R., Liu, B., Wang, J., Jia, X., Yi, C.W.: Data fusion improves the coverage of wireless sensor networks. Proc. ACM MOBICOM, September 2009, pp. 157168
[5] Zhang, L., Li, D., Zhu, H., Cui, L.: OPEN: an optimisation scheme of N-node coverage in wireless sensor networks. Proc. IET Wirel. Sens. Syst., 2012, Vol. 2, Iss. 1, pp. 4051
[6] Liu, B., Towsley, D.: A study of the coverage of large-scale sensor networks. Proc IEEE MOBIHOC, October 2004,pp. 475483
[7] Wang, Y., Fu, W., and D.P. Agrawal.: Intrusion Detection in Gaussian Distributed Wireless Sensor Networks. Proc. Sixth IEEE Intl Conf. Mobile Ad Hoc and Sensor Systems, 2009.
[8] Hao, Q., Guruswamy, M.: Lifetime Maximization for Connected Target Coverage in Wireless Sensor Networks. IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 16, NO. 6. DECEMBER 2008
[9] Tan, H., Wang, Y., Hao, X., Hua, Q., Lau, F.: Arbitrary Obstacles Constrained Full Coverage in Wireless Sensor Networks. Proc. WASA 2010, LNCS 6221, PP. 1-10
[10] Li, Y., Song, Y., Zhu, Y., and Schott, R.: Deploying Wireless Sensors for Differentiated Coverage and Probabilistic Connectivity,. Proc.IEEE Wireless Comm. and Networking Conf. (WCNC), pp. 1-6, 2010.
[11] Funke, S.: Topological Hole Detection in Wireless Sensor Networks and its Applications. Proc. ACM, September 2005.
[12] Arora, A., Dutta, P., Bapat, S., Kulathumani, V., Zhang, H., Naik, V., Mittal, V., Cao, H., Demirbas, M., and Gouda, M.: A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking. Computer Networks, vol. 46, no. 5, pp. 605-634, 2004.
[13] Wang, Y., Wang, X., Xie, B., Wang, D., and D.P. Agrawal.:Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks .IEEE Trans. Mobile Computing, vol. 7, no. 6, pp. 698- 711, June 2008.
[14] Wang, Y., Leow, Y.,and Yin, J.:Is Straight-Line Path Always the Best for Intrusion Detection in Wireless Sensor Networks. Proc. Intl Conf. Parallel and Distributed Systems, pp. 564-571, 2009.
[15] Rong, Ch., Eggen, S., Chen, H.: A Novel Intrusion Detection Algorithm for Wireless Sensor networks. Proc. IEEE, 2011.
[16] Zhao, M.C., Lei, J.Y., Wu, M.Y., Liu, Y.H., Shu, W.: Surface coverage in wireless sensor networks. Proc. IEEE, INFOCOM, April 2009, pp. 109117
[17] Bai, X.L., Yun, Z.Q., Xuan, D., Chen, B., Zhao, W.: Optimal multiple-coverage of sensor networks. Proc. IEEE INFOCOM, April 2011, pp. 21222132
[18] Li, J.S., Kao, H.C.: Distributed k-coverage self-location estimation scheme based on Voronoi diagram. IET Commun., 2010, 4, pp. 167177.
[19] Hefeeda, M., Ahmadi, H.: A probabilistic coverage protocol for wireless sensor networks. Proc. IEEE ICNP, 2007, pp. 4150
[20] Xu, X.C., Sartaj, S.: Approximation algorithms for sensor deployment. IEEE Trans Comput., 2007, 56, pp. 16811695
[21] Andreas, K., Carlos, G., Anupam, G., Jon, K.: Near optimal sensor placements: maximizing information while minimizing communication cost. Proc. IEEE/ACM IPSN, April 2006, pp. 1921
[22] Nene, M., Deodhar, R., Patnaik, L.: UREA: Uncovered Region Exploration Algorithm for Reorganization of Mobile sensor Nodes to maximize Coverage. Proc, IEEE, 2010.
[23] Wang, Y., Fu, W., Agarwal, D.P.: Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks. IEEE Trans.Parallel and Distributed Systems, vol. 24, no. 2, February 2013.
[24] Chen, J., Li, J., Lai, T.H.: Energy-Efficient Intrusion Detection with a Barrier of Probabilistic Sensors: Global and Local. IEEE Trans. Wireless Communications, vol. 12, no. 9, September 2013.
[25] Fang, Q., Gao, J., and Guibas, L.J.: Locating and Bypassing Routing Holes in Sensor Networks. Proc. INFOCOM, 2004.
[26] Dousse, O., Tavoularis, C., and Thiran, P.: Delay of Intrusion Detection in Wireless Sensor Networks. Proc. MobiHoc, 2006.
[27] Meester, R.,and Roy, R.: Continuum percolation. Cambridge University Press, 1996.
[28] Balister, P., Bollobas, B., Sarkar, A., and Kumar, A.: Reliable Density Estimates for Coverage and Connectivity in Thin Strips of Finite Length.Proc. ACM MobiCom, 2007.
[29] Srivatsan, R., Viswanath, A., Ramanathan, M.: Concave hull of freeform planar curves.
[30] Wang, D., Xie, B., Agarwal, D.P.: Coverage and Lifetime Optimization of Wireless Sensor Networks with Gaussian Distribution. .IEEE Trans. Mobile Computing, vol. 7, no. 12, December 2008.

G Sanjiv Rao is an Associate Professor of CSE, at the Sri Sai Aditya Institute of Science and Technology Surampalem, Andhra Pradesh , India. He has been working towards Ph.D at the College of Engineering, Andhra University. He received his M.Tech from the same institute. His research interests include Security and Wireless Sensor Networks.

Dr. V Valli Kumari is a Professor of Department of Computer and Systems Engineering, at the College of Engineering, Andhra University Visakhapatnam, Andhra Pradesh, India. She has received her Ph.D from the Andhra University. Her research interests include Security and Privacy issues in Data Engineering, Network Security and E-Commerce. She is a member of the IEEE and ACM and fellow of the IETE.

Verifying Online User Identity using Stylometric Analysis for Short Messages

Marcelo Luiz Brocardo[a], Issa Traore[a], Sherif Saad[a], Isaac Woungang[b]
[a] Department of Electrical and Computer Engineering, University of Victoria, Victoria, British Columbia, Canada
Email:{marcelo.brocardo, itraore, shsaad}@ece.uvic.ca
[b] Department of Computer Science, Ryerson University, Toronto, Ontario, Canada
Email: iwoungan@scs.ryerson.ca

***Abstract*—Stylometry consists of the analysis of linguistic styles and writing characteristics of the authors for identification, characterization, or verification purposes. In this paper, we investigate authorship verification for the purpose of user authentication process. In this setting, authentication consists of comparing sample writing of an individual against the model or profile associated with the identity claimed by that individual at login time (i.e. 1-to-1 identity matching). In addition, the authentication process must be done in a short period of time, which means analyzing short messages. Although a significant amount of literature has been produced showing high accuracy rates for long documents, it is still challenging to identify accurately authors of short unstructured documents, in particular when dealing with large authors populations. In this paper, we pose some steps toward achieving that goal by proposing a supervised learning technique combined with *n-grams* analysis for authorship verification for short texts. We introduce a new *n-gram* metric and study several sizes of *n-grams* using a relatively large dataset. The experimental evaluation shows increased effectiveness of our approach compared to the existing approaches published in the literature.**

***Index Terms*—Authentication and access control; biometrics systems; authorship verification; stylometry; *n-gram* features; short message verification.**

I. Introduction

THE writing style is an unconscious habit, which varies from one author to another in the way he/she uses words and grammar to express an idea. The patterns of vocabulary and grammar could be a reliable indicator of the authorship. The linguistic characteristics used to identify the author of a text is referred to as stylometry [1], [2]. Although the writing style may change a bit with time [3], each author has a unique stylistic tendency.

Forensic authorship analysis consists of inferring the authorship of a document by extracting and analyzing the writing styles or stylometric features from the document content. Authorship analysis of physical and electronic documents has generated a significant amount of interest over the years and led to a rich body of research literature [4]–[7]. Authorship analysis can be carried from three different perspectives including authorship attribution or identification, authorship verification, and authorship profiling or characterization. Authorship attribution consists of determining the most likely author of a target document among a list of known individuals. Authorship verification consists of checking whether a target document was written or not by a specific individual. Authorship profiling or characterization consists of determining the characteristics (e.g. gender, age, and race) of the author of an anonymous document.

According to Koppel et al., "verification is significantly more difficult than basic attribution and virtually no work has been done on it, outside the framework of plagiarism detection" [6]. Most previous works on authorship verification focus on general text documents. However, authorship verification for online documents can play a critical role in various criminal cases such as blackmailing and terrorist activities, to name a few. To our knowledge, only a handful of studies have been done on authorship verification for online documents. Authorship verification of online documents is difficult because of their relatively short lengths and also because these documents are quite poorly structured or written (as opposed to literary works).

We address the above challenge by proposing a new supervised learning technique combined with a new *n-gram* analysis approach to check the identity of the author of a short online document. We evaluate experimentally our approach using the Enron emails dataset and compute the following performance metrics:

- False Acceptance Rate (FAR): measures the likelihood that the system may falsely recognize someone as the genuine author of a document while they are not;
- False Rejection Rate (FRR): measures the likelihood that the system will fail to recognize the genuine author of a document;
- Equal Error Rate (ERR): corresponds to the operating point where FAR and FRR have the same value.

Our evaluation yields an EER of 14.35%, which is very encouraging considering the existing works on authorship verification using stylometry.

The rest of the paper is structured as follows. Section II summarizes and discusses related works. Section III introduces our proposed approach. Section IV presents our experimental evaluation by describing the underlying methodology and discussing the obtained results. Section V discusses the strengths and shortcomings of our approach and outlines the ground for future works. Section

doi:10.4304/jnw.9.12.3347-3355

VI makes some concluding remarks.

II. Related Work

A large number of studies have used stylometric techniques not only for authorship identification, but also for authorship verification and authorship characterization. Some of the previous studies on authorship identification investigated ways to identify patterns of terrorist communications [8], the author of a particular e-mail for computer forensic purposes [9]–[11], as well as how to collect digital evidence for investigations [12] or to solve a disputed literary, historical [13], or musical authorship [14]–[16]. Work on authorship characterization has targeted primarily gender attribution [17]–[19] and the classification of the author education level [20]. In this section, we present related works on stylometry for authorship attribution, characterization, and verification.

A. Authorship Attribution or Identification

Despite significant progress achieved on the identification of an author within a small group of individuals, it is still challenging to identify an author when the number of candidates increases or when the sample text is short as in the case of e-mails or online messages.

For instance, Chaski (2005) reported 95.70% accuracy in their work on authorship identification, the evaluation sample consisted of only 10 authors [12]. Similarly, Iqbal et al. (2010) achieved when using k-means for author identification, classification accuracy of 90% with 3 authors; the rate decreased to 80% when the number of authors increased to 10 [21]. Iqbal et al. (2008) also proposed another approach named AuthorMiner [9], which consists of an algorithm that captures frequent lexical, syntactical, structural and content-specific patterns. The experimental evaluation used a subset of the Enron dataset, varying from 6 to 10 authors, with 10 to 20 text samples per author. The authorship identification accuracy decreased from 80.5% to 77% when the authors population size increased from 6 to 10.

Hadjidj et al. (2009) used the C4.5 and SVM classifiers to determine authorship [22], and evaluated the proposed approach using a subset of three authors from the Enron dataset. They obtained as correct classification rates 77% and 71% for sender identification, 73% and 69% for sender-recipient identification, and 83% and 83% for sender-cluster identification, for C4.5 and SVM, respectively.

B. Authorship Characterization

Works on authorship characterization have targeted the determination of various traits or characteristics of an author such as gender and education level.

Cheng et al. (2011) investigated the author gender identification from text by using Adaboost and SVM classifiers to analyze 29 lexical character-based features, 101 lexical word-based features, 10 syntactic, 13 structural, and 392 functional words. Evaluation of the proposed approach involving 108 authors from the Enron dataset yielded classification accuracies of 73% and 82.23%, for Adaboost and SVM, respectively [19].

Abbasi and Chen (2005) analyzed the individual characteristics of participants in an extremist group web forum using decision tree and SVM classifiers. Experimental evaluation yielded 90.1% and 97% success rates in identifying the correct author among 5 possible individuals for decision tree and SVM, respectively [8].

Kucukyilmaz et al. (2008) used k-NN classifier to identify the gender, age, and educational environment of a user. Experimental evaluation involving 100 participants grouped in gender (2 groups), age (4 groups), and educational environment (10 groups), yielded accuracies of 82.2%, 75.4% and 68.8%, respectively [23].

C. Authorship Verification

Among the few studies available on authorship verification are works by Koppel et al. [6], Iqbal et al. [21], Chen and Hao's [24], and Canales et al. [5] .

Koppel et al. proposed an authorship verification method named "unmasking" where an attempt is made to quantify the dissimilarity between the sample document produced by the suspect and that of other users (i.e. imposters) [6]. The experimental evaluation of the approach yields 95.70% of correct verification, but shows that the proposed approach can provide trustable results only for documents of at least 500 words long, which is not realistic in the case of online verification.

Iqbal et al. studied email authorship verification by extracting 292 different features and analyzing these features using different classification and regression algorithms [21]. Experimental evaluation of the proposed approach using the Enron e-mail corpus yielded EER ranging from 17.1% to 22.4%.

Chen and Hao's (2011) extracted 150 stylistic features from e-mail messages for authorship verification [24]. Experimental evaluation involving 40 authors from the Enron dataset yielded varying classification accuracy rates based on the number of e-mails analyzed. More specifically, 84% and 89% classification accuracy rates were obtained for 10 and 15 short e-mails, respectively.

Canales et al. extracted keystroke dynamics and stylistic features from sample exam documents for the purpose of authenticating online test takers [5]. The extracted features consisting of keystroke timing features and 82 stylistic features were analyzed using a K-Nearest Neighbor (KNN) classifier. Experimental evaluation involving 40 students with sample document size between 1,710 to 70,300 characters yielded (FRR=20.25%, FAR=4.18%) and (FRR= 93.46%, FRR=4.84%) when using separately keystroke and stylometry, respectively. The combination of both types of features yielded an EER of 30%.

In an earlier version of the current paper, presented at the 2013 Conference on Computer, Information and Telecommunication Systems (CITS 2013), we investigated only the presence or not of a specific *n-gram* [25].

The current paper extends our previous work by considering all unique and non-unique *n-grams*, and also all *n-grams* with frequency equal or higher than some number f. We validate our approach by performing experiments using different sets of configurations and varying the size of *n-grams* from 3 to 5 characters.

III. Authorship Verification Approach

In this section, we present our approach by discussing feature selection and describing in detail our classification model.

A. Feature Selection

Over a thousand stylistic features have already been identified and used in the literature along with a wide variety of analysis methods. The stylistic features can be categorized as lexical, syntactic, semantic, and application specific.

Lexical features are related to the words or vocabulary of a language. Lexical analysis consists of breaking a text into a single atomic unit of language called token. A token can be a word or a character [26]. While earlier studies used a set of 100 frequent words to determine the author of a document [27], recent studies have used more than 1000 frequently used words to represent the style of an author [28]. However, lexical features encompass not only the frequency of characters or words found in a text but also vocabulary richness, sentence/line length, word length distribution, n-grams and lexical errors [5], [29].

Some lexical features measure the frequency of characters, which include letters (upper-case and lower-case), digits, and special characters (e.g. '@', '#', '$', '%', '(', ')', '{', '}', etc.). Other lexical features are obtained by extracting *n-grams* from a text. *N-grams* are tokens formed by a contiguous sequence of *n* items. The most frequent *n-grams* constitute the most important feature for stylistic purposes. Importantly, *n-grams* are noise tolerant since their representation is not affected dramatically by factors such as misspelling [29].

Vocabulary richness measures the diversity of vocabulary in a text by quantifying the total number of unique vocabulary, the number of *hapax legomenon* (i.e., a word which occurs only once in a text) and the number of *hapax dis legomenon* (e.g., dis legomenon or tris legomenon, referring to double or triple occurrences). This metric is computed by dividing the total number of unique vocabulary (hapax legomenon or dis legomenon) by the total number of tokens (each token is a word).

Syntactic features can be divided into average of punctuation and part-of-speech (POS). Syntactic pattern is an unconscious characteristic and it is considered to be more reliable than lexical information [30]. Punctuation is an important rule to define boundaries and identify meaning (quotation, exclamation, etc.) by splitting a paragraph into sentences and each sentence into various tokens. However, it is not sufficient to analyze only the punctuation of a document, as certain words such as 'Ph.D.' or 'uvic.ca' include punctuation characters too. Therefore, it is necessary to format the text before analyzing it. The part-of-speech tagging (POS tag or POST) is to categorize the tokens according to their function in the context. Basic POS tags include the functional words that express a grammatical relationship (i.e. articles, auxiliary verbs, personal pronouns, possessive adjectives) [16], [19], [20], [22].

Semantic features are related to the meaning of language and involve factors such as the meaning of words, grammatical construction, semantic relationships, and content-specific features [31]. Content-specific features are derived by measuring the use of certain vocabulary in the text. These features can be useful when they identify the gender, age, or a specific group the author may be part of. For example, within the same group, authors tend to use identical taxonomy in their communication and each generation has its own unique vocabulary [22], [23], [32]. In addition, some approaches measure the use of words indicative of the individual's race, nationality, and even tendency towards certain types of violence [8], as well as the number of gender-specific words [18], and psycho-linguistic cues [19]. However, these features are more useful when the context of the text being analyzed does not vary, avoiding the confounding factor of cross-topic texts [33].

Application specific features can easily be extracted from documents by analyzing structural and content-specific characteristics [22], [24], [32], [34]. Structural characteristics are related to the organization and format of a text and are usually more flexible in online documents such as e-mail. These features can be categorized at the message-level, paragraph-level or according to the technical structure of the document [4].

As a matter of fact, analyzing a large number of features does not necessarily provide the best results, as some features provide very little or no predictive information. Previous studies yielded encouraging results with lexical features, specially *n-grams* [5], [28]. In particular, since *n-gram* features are noise tolerant and effective, and e-mails are non-structured documents, we will focus in this paper only on these types of features.

Although *n-gram* features have been shown to be effective, classification based on such feature is complex while the data processing is time consuming. While the approach used so far in the literature has consisted of computing *n-gram* frequency in given sample document, we propose an innovative approach that analyzes *n-grams* and their relationship with the training dataset. This allows us to reduce the number of *n-grams* features to one, and address the above mentioned challenges.

B. Basic Classification Model

Our model consists of a collection of profiles generated separately for individual users. The model involves two modes of operations, namely, training and verification, where the users profiles are built and then checked, respectively. The training phase involves two steps. During

the first step, the user profile is derived by extracting *n-grams* from sample documents. During the second step, a user specific threshold is computed and used later in the verification phase.

Given a user U, we divide randomly her training data into two subsets, denoted T_1^U and T_2^U, corresponding to $2/3$ and $1/3$ of the training data, respectively. Let $N(T_1^U)$ denote the set of all unique *n-grams* occurring in T_1^U. We divide T_2^U into p blocks of characters of equal size: $b_1^U, ..., b_p^U$.

Given a block b_i^U, let $N(b_i^U)$ denote the set of all unique *n-grams* occurring in b_i^U.

Given two users U and I, let $r_U(b_i^I)$ denote the percentage of unique *n-grams* shared by block b_i^I (of user I) and (training set) T_1^U, giving:

$$r_U(b_i^I) = \frac{|N(b_i^I) \cap N(T_1^U)|}{|N(b_i^I)|} \quad (1)$$

where $|X|$ denotes the cardinality of set X.

Given a user U, our model approximates the actual (but unknown) distribution of the ratios $(r_U(b_1^U), ..., r_U(b_p^U))$ (extracted from T_2^U) by computing the sample mean denoted μ_U and the sample variance σ_U^2 during the training.

A block b is said to be a genuine sample of user U if and only if $|r_U(b)| \geq (\epsilon_U + \gamma)$, where ϵ_U is a specific threshold for user U, and γ is a predefined constant.

$$\begin{cases} \text{genuine or 1 if } |r_U(b)| \geq (\epsilon_U + \gamma) \\ 0, \text{otherwise} \end{cases} \quad (2)$$

We derive the value of ϵ_U for user U using a supervised learning technique outlined by $Algorithm$ 1 when given when given training samples from other users $I_1, ..., I_k$ ($I_i \neq U$). Let up and $down$ be local variables (in the algorithm) used to verify whether the difference between FRR and FAR is increasing or decreasing, and δ be a local variable that denote the increment/decrement for the value of ϵ_U. The threshold is initialized (i.e. $\epsilon_U = \mu_U - (\sigma_U/2)$), and then varied incrementally by minimizing the difference between FRR and FAR values for the user, the goal being to obtain an operating point that is as close as possible to the EER (i.e. FRR = FAR) for $\gamma = 0$.

In each iteration, the FRR and FAR for user U denoted FRR_U and FAR_U, respectively, are calculated for the current values of ϵ_U and γ. Let δ be a local variable (in the algorithm) that denote the increment/decrement for the ϵ_U value. If $(FRR_U - FAR_U) > 0$, a true value is assigned to the variable $down$ and the threshold is decreased by δ. If $(FRR_U - FAR_U) < 0$, a true value is assigned to the variable up and the threshold is increased by δ. Finally, we test if up and $down$ are true, which means that a local optimum was found. In this case, the values of up and $down$ are reset to false and δ is divided by 10. This process is repeated until δ is lower than 0.0001.

$Algorithm$ 2 returns the FAR and FRR for a user U given some training data, a user-specific threshold value, and some constant value assigned to γ.

```
/* U a user for whom the threshold
   is being calculated                    */
/* I_1, ..., I_k: a set of other users
   (I_i ≠ U)                              */
/* ε_U: threshold computed for user U
   */
Input: Training data for U, I_1, ..., I_k
Output: ε_U
1  begin
2      up ← false;
3      down ← false;
4      δ ← 1;
5      ε_U  μ_U − (σ_U/2);
6      γ ← 0;
7      while δ > 0.0001 do
           /* Calculating FAR and FRR for
              user U                      */
8          FRR_U, FAR_U =
               calculate(U, I_1, ..., I_k, ε_U, γ);
               /* Minimizing the difference
               between FAR and FRR        */
9          if (FRR_U − FAR_U) > 0 then
10             down ← true;
11             ε_U  ε_U − δ;
12         else if (FRR_U − FAR_U) < 0 then
13             up ← true;
14             ε_U ← ε_U + δ;
15         else
16             return ε_U;
17         end
18         if (up & down) then
19             up ← false;
20             down ← false;
21             δ ← δ/10;
22         end
23     end
24     return ε_U;
25 end
```

Algorithm 1: Threshold calculation for a given user.

C. Extended Classification Model

We extend the above basic classification model by introducing two new variables, named frequency and mode, in order to capture repeated *n-grams* in the training dataset (frequency) and in the testing (mode), respectively. Given a user U, we divide her training data into two subsets, denoted $T(f)_1^U$ and T_2^U. Let $N(T(f)_1^U)$ denote the set of all unique *n-grams* occurring in $T(f)_1^U$ with frequency f.

Let m denote a binary variable (i.e., $m \in \{1, 0\}$) that represents the mode of calculation of the n-grams.

Given a block b, let $N_m(b)$ denote the following:

$$\begin{cases} \text{- the set of all unique } \textit{n-grams} \text{ occurring in } b, \text{ if } m = 0 \\ \text{- the set of all } \textit{n-grams} \text{ occurring in } b, \text{ otherwise.} \end{cases} \quad (3)$$

Therefore, the basic classification model, expressed in

Input: ϵ_U, γ, Training data for $U, I_1, ..., I_k$
Output: (FAR_U, FRR_U)

```
begin
    /* Calculating FRR for user U   */
    for i → 1 to p do
        FR ← 0;
        if r_U(b_i^U)) < (ε_U + γ) then
            FR ← FR + 1;
        end
    end
    FRR_U ← FR/p;
    /* Calculating FAR for user U   */
    for i → 1 to k do
        for j → 1 to n do
            FA ← 0;
            if r_U(b_j^{I_i}) ≥ (ε_U + γ) then
                FA ← FA + 1;
            end
        end
    end
    FAR_U ← FA/(p×k); return (FAR_U, FRR_U);
end
```

Algorithm 2: FAR and FRR calculation for a given user

the equation 1, has the same output when f and m are set to 0 in the following equation:

$$r_U(b) = \frac{|N_m(b) \cap N(T(f)_1^U)|}{|N_m(b)|} \quad (4)$$

IV. Experimental Evaluation

In this section, we present in this section the experimental evaluation of our proposed approach by describing our dataset and data preprocessing technique, and then outlining our evaluation method and results.

A. Dataset and Data Preprocessing

In order to validate our system, we performed experiments on a real-life dataset from Enron e-mail corpus[1]. Enron was an energy company (located in Houston, Texas) that was bankrupt in 2001 due to white collar fraud The e-mails of Enron's employees were made public by the Federal Energy Regulatory Commission during the fraud investigation. The e-mail dataset contains more than 200 thousands messages from about 150 users. The average number of words per e-mail is 200. The e-mails are plain texts and cover various topics ranging from business communications to technical reports and personal chats.

While traditional documents are very well structured and large in size providing several stylometric features, an e-mail typically consists of a few paragraphs, wrote quickly and often with syntactic and grammatical errors. In our approach, we grouped all the sample e-mails used to build a given author profile into a single document that could be subsequently divided into small blocks.

In order to obtain the same structural data and improve classification accuracy, we performed several preprocessing steps to the data as follows:

- E-mails from the folders "sent" and "sent items" within each user's folder were selected, with all duplicate e-mails removed;
- JavaMail API was used to parse each e-mail and extract the body of the message;
- Since different texts must be logically equivalent, (i.e., must have the same canonical form), the following filters were applied:
  - Strip e-mail replay;
  - Replace e-mail address by double @ character (i.e. @@);
  - Replace http address by a meta tag http;
  - Replace currency by $XX;
  - Replace percentage by XX%;
  - Replace numbers by the digit 0;
  - Normalize the document to printable ASCII;
  - Convert the document to lower-case characters;
  - Strip white space;
  - Strip any punctuation from the document.
- All messages, per author, were grouped creating a long text or stream of characters that was divided into blocks.

B. Evaluation Method

After the preprocessing phase, the dataset was reduced from 150 authors to sets of 107, 92 and 87 authors to ensure that only streams of text with 12,500, 18,750 and 25,000 characters were used in our analysis, respectively.

We assess experimentally the effectiveness of our approach through a 10-fold cross-validation test. We randomly sorted the dataset, and allocated in each (validation) round 90% of the dataset for training and the remaining 10% for testing. The 90% training data allocated to a given user U was further divided as follows: $2/3$ of the training data allocated to subset T_1^U and $1/3$ of the data for subset T_2^U, respectively. The 10% test data for user U was divided in p blocks of equal size s. We tested two different block sizes, $s = 250$ and $s = 500$ characters, respectively. The number of blocks per user p varied from 25 to 100. In addition, we investigated separately *n-grams* of sizes (n=) 3, 4, and 5, for each of these analyses yielding in total 18 different experiments.

Our experiments cover three different values for the frequency f (i.e. f= {0, 1, 2}) and two different values for the mode of calculation of the *n-grams* (i.e. m= {0, 1}). Table I shows the configuration of our experiments.

For each user U, we computed a corresponding profile by using their training data and training data from other users considered as impostors. This allows computing the acceptance threshold ϵ_U for user U as explained before. A given block b is considered to belong to an hypothesized genuine user U when the ratio $|r_U(b)|$ is greater than

[1]available at http://www.cs.cmu.edu/~enron/

TABLE I
CONFIGURATION OF EXPERIMENTS

Experiment configuration #	Number of Users (k)	Number of blocks per author (p)	Block size (s)
1	107	50	250
2	92	75	
3	87	100	
4	107	25	500
5	92	37	
6	87	50	

$\epsilon_U + \gamma$, where γ is a predefined constant and ϵ_U is the user specific threshold.

We compute the FRR for user U by comparing each of the blocks from her test data against her profile. A false rejection (FR) is counted when the system rejects one of these blocks. The FAR is computed by comparing each of the test blocks from the other users (i.e. the impostors) against the profile of user U. A false acceptance (FA) occurs when the system categorizes any of these blocks as belonging to user U. By repeating the above process for each of the users, we compute the overall FAR and FRR by averaging the individual measures.

C. Evaluation Results

Table II shows the overall FRR and FAR for the 18 experiments, where the constants $\gamma = 0$, $f = 0$, and $m = 0$. It can be noted that the accuracy decreases not only when the number of authors increases, but also when the number of blocks per user p and the block size s decreases.

Experiments using 5-*grams* achieve better results than those using 3 and 4-*grams* for large number of blocks per user and block size. Experiments using 4-*grams* yield better results when the number of blocks per user decreases. Overall, the best result is achieved in experiment 6, with 87 authors, 50 blocks per user, and a block size of 500 characters (FRR=14.71%, FAR=13.93%).

TABLE II
PERFORMANCE RESULTS FOR THE DIFFERENT EXPERIMENTS
($\gamma = 0, f = 0, m = 0$)

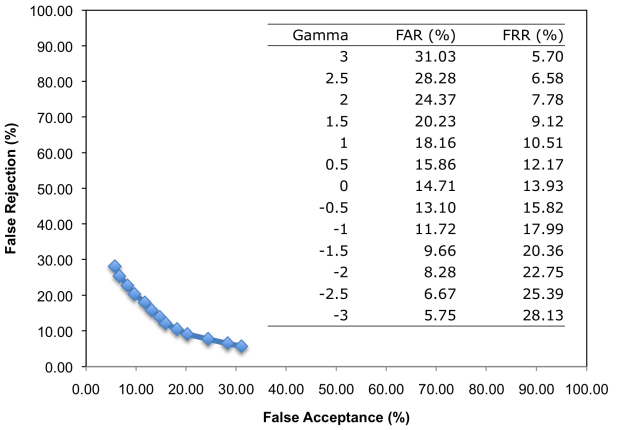
No.	*3-gram*		*4-gram*		*5-gram*	
	FRR	FAR	FRR	FAR	FRR	FAR
1	24.85	28.61	22.05	24.09	24.11	20.50
2	26.76	26.82	23.64	21.68	25.13	19.39
3	24.82	28.15	23.56	21.15	17.24	20.39
4	26.47	22.70	23.67	17.81	23.98	16.29
5	23.36	21.81	18.75	18.01	18.20	15.40
6	22.29	22.21	19.77	16.11	**14.71**	**13.93**

Based on configuration 6 (which yields the best results), we assess the impact of the frequency f and mode m on the system performance, by varying the frequency from 0 to 2 and the mode between 0 and 1. Table III lists the obtained results.

Figure 1 depicts the receiver operating characteristic (ROC) curve for experiment configuration # 6 (from Table I) using 5-*gram*, $f = 0$, and $m = 0$. The curve illustrates the relationship between the FRR and FAR for different values of γ. The equal error rate (ERR) was estimated as 14.35% and achieved when $\gamma = -0.25$.

TABLE III
PERFORMANCE RESULTS VARYING f AND m FOR EXPERIMENT NUMBER 6 ($\gamma = 0$)

f	m	*3-gram*		*4-gram*		*5-gram*	
		FRR	FAR	FRR	FAR	FRR	FAR
0	0	22.29	22.21	19.77	16.11	14.71	13.93
	1	21.83	22.16	19.08	16.02	15.40	13.90
1	0	21.60	22.93	21.83	17.09	19.54	15.45
	1	21.60	22.87	22.75	17.30	20.68	15.46
2	0	23.21	22.20	21.83	18.11	21.37	16.38
	1	22.75	22.78	21.60	18.47	22.98	16.46



Gamma	FAR (%)	FRR (%)
3	31.03	5.70
2.5	28.28	6.58
2	24.37	7.78
1.5	20.23	9.12
1	18.16	10.51
0.5	15.86	12.17
0	14.71	13.93
-0.5	13.10	15.82
-1	11.72	17.99
-1.5	9.66	20.36
-2	8.28	22.75
-2.5	6.67	25.39
-3	5.75	28.13

Fig. 1. Receiver Operating Characteristic curve for experiment configuration #6 using 5-*gram* and sample performance values for different values of γ.

V. DISCUSSIONS

The Enron dataset has previously been used not only in authorship verification [24], but also in authorship identification [4], [9], [11], [21], [22] and authorship characterization [11], [18], [19]. These previous experiments used a number of users ranging from 3 to 114, and achieved in the best cases EER varying from 17% to 30%. In the present study, the best configuration was achieved with block size of 500 characters, achieving EER below 15% which is better compared to the accuracy obtained using similar techniques in the literature. Table IV summarizes the performances, block sizes, and population size of previous stylometry studies.

Despite our encouraging results, more works must be done to improve the accuracy to an acceptable level for authorship verification in forensics investigation. We believe that our proposed scheme is a good step toward achieving that goal. It is important to notice that these results were obtained using only one type of features out of hundreds of potential stylometric features. We believe that we can reduce significantly our error rates by incorporating other types of features in our framework.

We investigated in this work block sizes of 250 and 500 characters, respectively, which represent significantly

shorter messages compared to the messages used so far in the literature for identity verification. To our knowledge, one of the few works that have investigated comparable message sizes includes the work by Sanderson and Guenter, who split a long text in chunks of 500 characters [7].

They achieved similar results using block size of 500 characters, although with a relatively smaller dataset (i.e. 50 users) [7]. Furthermore, it is important to mention that their dataset consisted of newspapers' articles, which are known to be well structured compared to e-mail messages.

Our experiments varying f and m showed a slight increase of FRR and FAR across different size of *n-grams*. However, we note that a block can be classified correctly by one configuration and misclassified by another, suggesting that a combination of different configurations submitted to a machine learning classifier (e.g. SVM, Logistic Regression) could improve the general results.

We still need to investigate even shorter messages (e.g. 10 to 50 characters) to be able to cover (beyond emails) a broader range of online messages such as twitter feeds and text messages. However, attempting to reduce at the same time the block size and verification error rates is a difficult task in the sense that these attributes are loosely related to each other. A smaller verification block may lead to increased verification error rates and vice-versa. We intend to tackle such challenge in the future.

Another important limitation of many previous stylometry studies is that the performance metrics computed during their evaluations cover only one side of the story, and this is clearly emphasized by Table IV. Accuracy is traditionally measured using the following two different types of errors:

1) Type I error, which corresponds to the FRR, also referred to as False Non-Match Rate (FNMR) or False Positive Rate (FPR);
2) Type II error, which corresponds to the FAR, also referred to as False Match Rate (FMR) or False Negative Rate.

However, most previous studies calculate the so-called (classification) accuracy (see Table IV) which actually corresponds to the true match rate and allows deriving only one type of error, namely, Type II error: $FAR = 1 - Accuracy$. Nothing is said about Type I error in these studies, which makes it difficult to judge their real strength in terms of accuracy. As shown by Table IV, only few studies have provided both types of errors, among which our work can be considered as one of the most strongest in terms of sample population size, block size, and accuracy.

VI. Conclusion

In this paper, we have introduced a new approach and investigated the effectiveness of using stylometry for authorship verification for short online messages. Our proposed model combines supervised learning and *n-gram* analysis. We have validated our system by performing experiments on a real-life dataset from Enron, where the e-mails were combined to produce a single long message per individual, and then divided into smaller blocks used for authorship verification. Our experimental evaluation yields an EER 14.35% for 87 users for relatively small block sizes. While the obtained results are promising, it is clear that more work must be done for the proposed scheme to be usable in real-world authentication of online users. We discussed the limitations of our approach and plan to address them in our future work.

In particular, we will improve verification accuracy by creating new *n-grams* features based on different values for the frequency f (i.e. f = 1 and f = 2) and for the mode of calculation of the *n-grams* (i.e. m = 0 and m = 1), and by expanding our feature set beyond *n-grams*. We will also improve the robustness of the scheme in handling shorter and shorter message structures.

Acknowledgement

This research has been enabled by the use of computing resources provided by WestGrid and Compute/Calcul Canada. The research is funded by a Vanier scholarship from the Natural Sciences and Engineering Research Council of Canada (NSERC) and CNPq scholarship (Brazil).

References

[1] J. Li, R. Zheng, and H. Chen, "From fingerprint to writeprint," *Commun. ACM*, vol. 49, pp. 76–82, April 2006.
[2] J. L. Hilton, *On verifying wordprint studies: Book of Mormon authorship*, ser. Reprint (Foundation for Ancient Research and Mormon Studies). F.A.R.M.S., 1991.
[3] F. Can and J. M. Patton, *Change of Writing Style With Time*. Kluwer Academic Publishers, 2004, vol. 38.
[4] A. Abbasi and H. Chen, "Writeprints: A stylometric approach to identity-level identification and similarity detection in cyberspace," *ACM Trans. Inf. Syst.*, vol. 26, pp. 1–29, April 2008.
[5] O. Canales, V. Monaco, T. Murphy, E. Zych, J. Stewart, C. T. A. Castro, O. Sotoye, L. Torres, and G. Truley, "A stylometry system for authenticating students taking online tests," P. of Student-Faculty Research Day, Ed., CSIS. Pace University, May 6 2011.
[6] M. Koppel and J. Schler, "Authorship verification as a one-class classification problem," in *Proceedings of the 21st international conference on Machine learning*, ser. ICML '04. Banff, Alberta, Canada: ACM, 2004, pp. 62–69.
[7] C. Sanderson and S. Guenter, "Short text authorship attribution via sequence kernels, markov chains and author unmasking: an investigation," in *Proceedings of the 2006 Conference on Empirical Methods in Natural Language Processing*, ser. EMNLP '06. Stroudsburg, PA, USA: Association for Computational Linguistics, 2006, pp. 482–491.
[8] A. Abbasi and H. Chen, "Applying authorship analysis to extremist-group web forum messages," *IEEE Intelligent Systems*, vol. 20, pp. 67–75, September 2005.
[9] F. Iqbal, R. Hadjidj, B. C. Fung, and M. Debbabi, "A novel approach of mining write-prints for authorship attribution in e-mail forensics," *Digital Investigation*, vol. 5, pp. S42–S51, 2008.
[10] F. Iqbal, L. A. Khan, B. C. M. Fung, and M. Debbabi, "E-mail authorship verification for forensic investigation," in *Proceedings of the 2010 ACM Symposium on Applied Computing*, ser. SAC '10. New York, NY, USA: ACM, 2010, pp. 1591–1598.
[11] F. Iqbal, H. Binsalleeh, B. C. Fung, and M. Debbabi, "A unified data mining solution for authorship analysis in anonymous textual communications," *Information Sciences*, vol. 231, pp. 98–112, 2013.
[12] C. E. Chaski, "Who's at the keyboard: Authorship attribution in digital evidence investigations," *International Journal of Digital Evidence*, vol. 4, no. 1, pp. 1–13, Spring 2005.
[13] F. Mosteller and D. L. Wallace, *Inference and Disputed Authorship: The Federalist*. Addison-Wesley, 1964.

TABLE IV
COMPARATIVE PERFORMANCES, BLOCK SIZES AND, POPULATION SIZES FOR STYLOMETRY STUDIES.

Category	Reference	Sample Population Size	Block Size	Accuracy* (%)	EER (%)
Attribution	[4]	100 **	277 words	83.10	- -
	[12]	10	200 words	95.70	- -
	[35]	2 - 4	60,000 words	93.8 - 97.8	- -
	[22]	3 **	200 words	69 -83	- -
	[28]	87	287 words	50 - 60	- -
	[21]	3 - 10 **	200 words	80 - 90	- -
	[11]	4 - 20 **	300 words	69.75 - 88.37	- -
	[9]	6 - 10 **	200 words	77 - 80.5	- -
	[36]	1000	500 words	42.2 - 93.2	- -
	[1]	20	169 words	99.01	- -
	[37]	20	600 words	84.30	- -
	[7]	50	500 characters	- -	8.08 - 30.88
	[36]	10,000	500 words	46	- -
	[38]	100,000	335 words	20	- -
Characterization	[8]	5	76 words	90.1 - 97	- -
	[19]	108 **	50 - 200 words	73 - 82.23	- -
	[18]	114 **	50 - 200 words	80.08 - 82.20	- -
	[39]	325	50 - 200 words	70.20	- -
	[11]	4 - 20 **	300 words	39.13% - 60.44%	- -
	[23]	100	300 words	39.0 - 99.70	- -
	[17]	10 - 40	450 words	68.3 - 91.5	- -
Verification	[5]	40	1710 - 70300 characters	- -	30
	[24]	25 - 40 **	30 - 50 words	83.90 - 88.31	
	[40]	8	628 - 1342 words	- -	3
	[6]	10	500 words	95.70	- -
	[41]	29	2400 words	- -	22
	Proposed Approach	87	500 character	- -	14.35%

* The accuracy is measured by the percentage of correctly matched authors in the testing set.
** Used Enron dataset for testing.

[14] J. Burrows, "Delta: a measure of stylistic difference and a guide to likely authorship," *Literary and Linguistic Computing*, vol. 17, no. 3, pp. 267–287, 2002.

[15] E. Backer and P. van Kranenburg, "On musical stylometry pattern recognition approach," *Pattern Recognition Letters*, vol. 26, no. 3, pp. 299–309, 2005.

[16] Y. Zhao and J. Zobel, "Searching with style: authorship attribution in classic literature," in *Proceedings of the thirtieth Australasian conference on Computer science - Volume 62*, ser. ACSC '07. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2007, pp. 59–68.

[17] K. G. Ruchita Sarawgi and Y. Choi, "Gender attribution: tracing stylometric evidence beyond topic and genre," in *Proceedings of the 15th Conference on Computational Natural Language Learning*, ser. CoNLL '11. Stroudsburg, PA, USA: Association for Computational Linguistics, 2011, pp. 78–86.

[18] N. Cheng, X. Chen, R. Chandramouli, and K. Subbalakshmi, "Gender identification from e-mails," in *Computational Intelligence and Data Mining, 2009. CIDM '09. IEEE Symposium on*, 30 2009-april 2 2009, pp. 154–158.

[19] N. Cheng, R. Chandramouli, and K. Subbalakshmi, "Author gender identification from text," *Digital Investigation*, vol. 8, no. 1, pp. 78–88, 2011.

[20] P. Juola and R. H. Baayen, "A controlled-corpus experiment in authorship identification by cross-entropy," *Literary and Linguistic Computing*, vol. 20, no. Suppl, pp. 59–67, 2005.

[21] F. Iqbal, H. Binsalleeh, B. C. Fung, and M. Debbabi, "Mining writeprints from anonymous e-mails for forensic investigation," *Digital Investigation*, vol. 7, no. 1-2, pp. 56–64, 2010.

[22] R. Hadjidj, M. Debbabi, H. Lounis, F. Iqbal, A. Szporer, and D. Benredjem, "Towards an integrated e-mail forensic analysis framework," *Digital Investigation*, vol. 5, no. 3-4, pp. 124–137, 2009.

[23] T. Kucukyilmaz, B. B. Cambazoglu, C. Aykanat, and F. Can, "Chat mining: Predicting user and message attributes in computer-mediated communication," *Information Processing Management*, vol. 44, no. 4, pp. 1448–1466, 2008.

[24] X. Chen, P. Hao, R. Chandramouli, and K. P. Subbalakshmi, "Authorship similarity detection from email messages," in *Proceedings of the 7th international conference on Machine learning and data mining in pattern recognition*, ser. MLDM'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 375–386.

[25] M. L. Brocardo, I. Traore, S. Saad, and I. Woungang, "Authorship verification for short messages using stylometry," in *In Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS)*. Piraeus-Athens, Greece, May 2013, pp. 1–6.

[26] S. M. Alzahrani, N. Salim, and A. Abraham, "Understanding plagiarism linguistic patterns, textual features, and detection methods," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 42, no. 2, pp. 133–149, March 2012.

[27] J. F. Burrows, "Word patterns and story shapes: The statistical analysis of narrative style," *Literary and Linguistic Computing*, vol. 2, no. 1, pp. 61–70, 1987.

[28] N. Homem and J. Carvalho, "Authorship identification and author fuzzy fingerprints," in *Fuzzy Information Processing Society (NAFIPS), 2011 Annual Meeting of the North American*, march 2011, pp. 1–6.

[29] E. Stamatatos, "A survey of modern authorship attribution methods," *J. Am. Soc. Inf. Sci. Technol.*, vol. 60, pp. 538–556, March 2009.

[30] H. Baayen, H. van Halteren, and F. Tweedie, "Outside the cave of shadows: using syntactic annotation to enhance authorship attribution," *Literary and Linguistic Computing*, vol. 11, no. 3, pp. 121–132, 1996.

[31] D. Jurafsky and J. H. Martin, *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics and Speech Recognition*, 2nd ed. Prentice Hall, Feb. 2008.

[32] R. Zheng, J. Li, H. Chen, and Z. Huang, "A framework for authorship identification of online messages: Writing-style features and classification techniques," *J. Am. Soc. Inf. Sci. Technol.*, vol. 57, pp. 378–393, February 2006.

[33] E. Stamatatos, "Ensemble-based author identification using character n-grams," in *3rd International Workshop on Text-based Information Retrieval*, 2006, pp. 41–46.

[34] O. de Vel, A. Anderson, M. Corney, and G. Mohay, "Mining e-

mail content for author identification forensics," *Sigmod Record*, vol. 30, no. 4, pp. 55–64, 2001.
[35] J. H. Clark and C. J. Hannon, "A classifier system for author recognition using synonym-based features," in *Proceedings of the 6th Mexican international conference on Advances in artificial intelligence*, ser. MICAI'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 839–849.
[36] M. Koppel, J. Schler, and S. Argamon, "Authorship attribution in the wild," *Lang. Resour. Eval.*, vol. 45, pp. 83–94, March 2010.
[37] D. Pavelec, L. Oliveira, E. Justino, F. Neto, and L. Batista, "Author identification using compression models," in *Document Analysis and Recognition, 2009. ICDAR '09. 10th International Conference on*, july 2009, pp. 936–940.
[38] A. Narayanan, H. Paskov, N. Z. Gong, J. Bethencourt, E. Stefanov, E. C. R. Shin, and D. Song, "On the feasibility of internet-scale author identification," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, ser. SP '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 300–314.
[39] M. Corney, O. de Vel, A. Anderson, and G. Mohay, "Gender-preferential text mining of e-mail discourse," in *Proceedings of the 18th Annual Computer Security Applications Conference*, 2002, pp. 282–289.
[40] H. V. Halteren, "Author verification by linguistic profiling: An exploration of the parameter space," *ACM Trans. Speech Lang. Process.*, vol. 4, pp. 1–17, February 2007.
[41] I. Krsul and E. H. Spafford, "Authorship analysis: identifying the author of a program," *Computers and Security*, vol. 16, no. 3, pp. 233–257, 1997.

M.Sc Marcelo Luiz Brocardo received his B.Sc. in Computer Science from Regional University of Blumenau, Brazil (1995), M.Sc in Computer Science from Federal University of Santa Catarina, Brazil (2001). In 2011 started his PhD in the Department of Electrical and Computer Engineering of the University of Victoria. His primary research interests are in continuous authentication using stylometry.

Dr. Issa Traore is the CEO and co-founder of Plurilock Security Solutions Inc. (www.plurilock.com) He has been with the faculty of the Electrical and Computer Engineering Department of the University of Victoria since 1999, where he is currently a Professor. Dr. Traore is also the founder and Director of the Information Security and Object Technology (ISOT) Lab (www.isot.ece.uvic.ca). He obtained in 1998 a PhD in Software Engineering from the Institute Nationale Polytechnique of Toulouse, France. His main research interests are biometrics technologies, intrusion detection systems, and software security.

M.Sc Sherif Saad received his B.Sc. in Computer Science from Helwan University, Egypt (2003), M.Sc in Computer Science from Arab Academy for Science, Technology and Maritime Transport, Egypt (2007). In 2008 he received the University of Victoria Fellowship and started his PhD in the Department of Electrical and Computer Engineering of the University of Victoria. His primary research interests are in advancing machine-learning methods and their application to computer and network security. Since 2009, he is working as an information security engineer for Plurilock Security Solutions (www.plurilock.com/).

Dr. Isaac Woungang received his M.S. & Ph. D degrees, in Mathematics, from the Universite de la Mediterranee- Aix Marseille II, France, and Universite du Sud, Toulon & Var, France, in 1990 and 1994 respectively. In 1999, he received a M.S degree from the INRS-Materials and Telecommunications, University of Quebec, Montreal, Canada. From 1999 to 2002, he worked as a software engineer at Nortel Networks. . Since 2002, he has been with Ryerson University, where he is now an Associate Professor of Computer Science and Coordinator of the Distributed Applications and Broadband (DABNEL) Lab (http//www.scs.ryerson.ca/iwoungan).

Topology Control Mechanism Based on Link Available Probability in Aeronautical Ad Hoc Network

Zhong Dong, Zhu Yian, and You Tao
School of Computer Science; Northwestern Polytechnical University; Xi'an; P. R. China
Email: zhongyl@nwpu.edu.cn

Kong Jie
School of Computer Science; Xi'an Shiyou University; Xi'an; P. R. China

***Abstract*—In this paper; we consider traffic network with high-speed mobility nodes scenario; and give a new network topology control mechanism to rise the routing path duration in Aeronautical ad hoc network. The mechanism can use different methods to construct topology according to the node densities. For network regions having a high density of aircraft; the packets are preferentially routed over the long available links created by the aircraft moving in same direction. For low density of aircraft; the routing preferentially uses the short available links created by the aircraft moving in both directions. The mechanism can effectively decrease the probability of routing path breaks; when the nodes move with a high velocity. It can be also integrated with existing Ad hoc network routing protocols smoothly. We combine the mechanism with Optimized Link-State Routing Protocol (OLSR); and give a Path Link Availability Routing Protocol (PLAR). The performance of PLAR protocol is compared with several routing protocols in different scenes. The metrics include end-to-end delay; availability and length of path. Experimental results show that PLAR protocol exhibits a significant improvement over most routing protocols base on topology and position.**

***Index Terms*—Topology Control; Routing Protocol; Ad Hoc; Mobile Computing; Wireless Network**

I. INTRODUCTION

AANET (Aeronautical Ad Hoc Network) is a kind of Ad Hoc Network. AANET has its own features compared with the traditional MANET. In the AANET; the mobile speed of nodes is generally higher. The mobility of aircraft is usually constrained by flight path. And the nodes are not constrained excessively in terms of energy. The rapid change of network topology in course of moving leads to frequent link break between nodes. And it will cause frequent routing path interruption; which can bring great influence for the persistent session established by applications. These problems have brought new challenges to routing protocol in AANET; which require the routing protocol can detect the frequent network topology change and cope with it with effective methods. Comparing AANET with MANET; the mobility of nodes in AANET has certain regularity and controllability. And the available time of link is considered a crucial metric for high mobility of AANET. The routing protocols adopt the links with long available time in the process of routing path build; which can increase the stability and reliability of the routing path greatly.

The current routing protocols used in MANET can be divided into two categories [1-2]: topology-based and position-based.

In topology-based routing mechanisms; the nodes need store routing tables or routes which depend on the topology. This kind of protocols includes the AODV (Ad hoc On-Demand Distance Vector Routing); OLSR (Optimized Link State Routing) and others (DSDV; DSR; TORA and FSR). Strictly speaking; these protocols were proposed for MANET; where the nodes are assumed to move with low velocity and frequency. On this condition; these protocols are allowed to establish available end-to-end paths within a reasonable time range. And they only occasionally need repair the path according to the movement features. Consequently; this kind of protocol is used for AANET; which is not easy to meet various requirements of applications. Especially when various aircrafts move with high-speed; these protocols are difficult to meet the demand of real-time data transmission. Therefore; the protocols based on topology in MANET are used for AANET; which faces some challenges. One of the key problems is nodes in AANET usually require updating the routing information in quasi real time; in order to perceive the change of network topology in time. And it can cause high cyber resources consumption. And some optimization can alleviate the consumption; such as the design of a lightweight protocol based on link state aware in [3]. For high mobility scenarios; the nodes exhibit some special characteristics in [4]; which shows some routing protocols proposed for MANET can not perform well in AANET.

The position-based routing protocols mainly include GSR; GPSR; LORA_CBF; RBVT; GyTAR and COALS; etc [5-10]. This class of protocol often uses the location of the neighbor nodes and destination node to determine the next hop node. In most cases; the nodes do not need

doi:10.4304/jnw.9.12.3356-3365

record any address or routing table for forwarding packets; only record the corresponding position of nodes. But these protocols also have their negative side. For example; when a fault occurs in positioning system of node; in order to inform other nodes of its new location; the node must broadcast its location to other nodes; which will increase the consumption of cyber resource.

The comparison study about routing protocols for AANET is few currently. Literature [5] has compared the data transmission performance of AODV and OLSR protocol in mobile Ad hoc network with mobile trajectory constraint; including the routing path length; packet delivery ratio; routing overhead and end-to-end delay. It makes a conclusion that the performance of OLSR protocol is better than AODV protocol in above scenario. The performance of AODV; DSR; TORA and FSR routing protocols have been compared in high speed mobile Ad hoc networks [6]. And the study results show the performance of AODV and FSR are better; the DSR and TORA are unsuitable for high speed mobile ad hoc networks. Since the forwarding efficiency of TORA shows poor performance and the end to end delay of DSR is too high. A comparison of city traffic models based on high speed mobile ad hoc network is carried out in [7]. The different routing algorithms in MANET are compared in several traditional performance metrics [11-12]; such as path length; end to end delay; packet forwarding rate; routing overhead and so on. However; the available time; an important metric for routing in AANET; is still lacking for network stability metrics. Literature [13] takes TCP protocol as an example; and point out that the routing failure occasioned by path break lead to TCP connection interruption. And the handshake mechanism of TCP may cause entire network serious instability; which demonstrates that the path available time plays an important role in network stability.

This paper focus on routing mechanism based on topology in AANET. We aim to provide an ideal environment for the applications in AANET; which is not relying on positioning system. The rest of the paper is organized as follows. Section 2 introduces the nodes mobility models in AANET. In Section 3 we describe a topology control mechanism based on nodes mobility models in AANET. Section 4 describes a routing mechanism based on high mobility of node in AANET. Section 5 addresses the simulations and the evaluation metrics that we adopted. Section 6 presents the analysis of simulation results. Finally; the summary and outlook are given in Section 7.

II. NODES MOBILITY MODEL IN AANET

Mobile nodes in AANET are usually all kinds of air vehicles. Each air vehicle always moves along different flight routes in accordance with all assigned missions. And the flight path is always a straight line. The same flight route usually has two different directions; one is the direction which air vehicles start off on their missions; another is direction homed at end of missions.

Our research focuses on the theoretical method of network construction; when air vehicles flight along bidirectional straight line route. The following is an instance of the theoretical model.

We adopt the following assumptions: set the distance between two air vehicles m_1 and m_2 to d; the radio communication range of each node is r; the velocity of two air vehicle nodes m_1 and m_2 are represented by the vectors $\overrightarrow{v_1}$ and $\overrightarrow{v_2}$ respectively. A link between two nodes is created if d≤r. We consider two cases: when the nodes move with high speed; the link between the nodes will remain active in the case of $\overrightarrow{v_1}=\overrightarrow{v_2}$; the link will be broken after some time if $\overrightarrow{v_1}\neq\overrightarrow{v_2}$. According to the flight characteristics of the air vehicles on the same route; $\overrightarrow{v_1}$ and $\overrightarrow{v_2}$ can be represented in polar coordinates (v_1, θ_1)and(v_2, θ_2)with v_1, $v_2\in[V_{\min};V_{\max}]$ and θ_1, $\theta_2\in\{0;\pi\}$, the relative velocity of the nodes is represented by

$$\overrightarrow{v_r}=\overrightarrow{v_1}-\overrightarrow{v_2}=(v_1\cos(\theta_1)-v_2\cos(\theta_2),v_1 sin(\theta_1)-v_2 sin(\theta_2)) \quad (1)$$

And we define its absolute value as

$$\left|\overrightarrow{V_r}\right|=\psi(v_1,v_2,\theta_1,\theta_2)=\sqrt{v_1^2+v_2^2-2v_1v_2\cos(\theta_1-\theta_2)} \quad (2)$$

The relative velocity is a function depending on the random variables v_1, v_2, θ_1 and θ_2; which are mutually independents. We use a random variable V_r to express the relative velocity; and define the expected relative velocity value as

$$E(V_r)=\int_{-\infty}^{+\infty}\psi(v_1,v_2,\theta_1,\theta_2)f(V_r)dV_r \quad (3)$$

As the random variables in (3) are independent; the joint distribution function $f(V_r)$ is equal to the product of the marginal distribution function

$$f(V_r)=f(v_1)f(v_2)f(\theta_1)f(\theta_2)$$

The mathematical expectation of relative velocity can be expressed as

$$E(V_r)=\int_{V_{\min}}^{V_{\max}}\int_{V_{\min}}^{V_{\max}}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\frac{f(v_1)f(v_2)f(\theta_1)f(\theta_2)}{\sqrt{v_1^2+v_2^2-2v_1v_2\cos(\theta_1-\theta_2)}}d\theta_1d\theta_2dv_1dv_2 \quad (4)$$

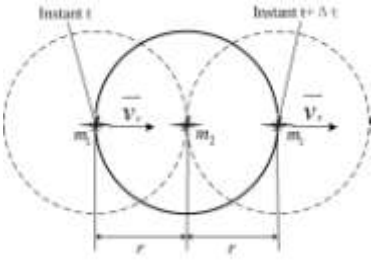


Figure 1. Maximum relative displacement between two mobile nodes without broken their link

We assume that two nodes m_1 and m_2 form $link_{12}$ at instant t; and consider that node m_1 moves with velocity $\overrightarrow{v_r}$ relative to node m_2; the $link_{12}$ will be considered broken after some time if $\left|\overrightarrow{v_r}\right|>0$. If nodes do not change their velocity and the relative distance traveled never

exceeds $2r$ during the interval $(t, t+\Delta t)$; the nodes will maintain the $link_{12}$ active. This scenario is depicted in Fig. 1.

The probability of a link formed at a time t remaining active at a time $t+\Delta t$ is related with the spatial intersection of the covered areas at instants t and $t+\Delta t$; which is represented by the white area in Fig. 2.

The radio covering area of the node m_1 at instant t can be depicted by following formula

$$C_t = 2\int_{-r}^{r} \sqrt{r^2 - x^2}\, dx \tag{5}$$

The radio covering overlap area in the instant t and $t+\Delta t$ can be represented by function $O_{t+\Delta t}(d)$;which is the node m_1 move with velocity v_1 in the interval$(t;t+\Delta t)$(the distance $d\geq 0$)

$$O_{t+\Delta t}(d) = \begin{cases} \pi r^2 - 2\int_{-d/2}^{d/2} \sqrt{r^2 - x^2}\, dx & 0 \leq d \leq 2r \\ 0, & d > 2r \end{cases} \tag{6}$$

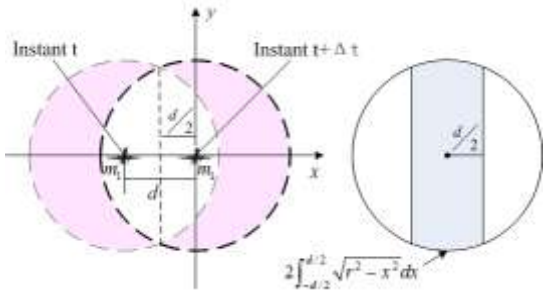


Figure 2. Radio covering circumference change of the node m_1 moved d length units between instant t and the time instants $t+\Delta t$

Now we take the hello message in routing mechanism based on topology (DSDV; AODV or OLSR protocol) as an example; and introduce the method for calculating link available probability in the process of nodes moving. We consider that the Hello messages are broadcasted every T seconds to discover and/or maintain an active link. The distance; which the node m_1 move relative to the node m_2 during the period T; can be calculated by $E(V_r)T$. Therefore; the probability of the link remaining active after nT periods is approximately depicted by Formula (7). (N denotes the set of natural numbers)

$$p_{connected}(n) \approx \frac{O_{t+\Delta t}(nTE(V_r))}{\pi r^2} \quad n \in N \tag{7}$$

We consider the nodes moving with high speed only have two opposite directions. When the nodes move in the same direction; the mathematical expectation of relative velocity can be calculated by the formula (8); which is simplified by formula (4).

$$E_{same\,direction}(V_r) = \int_{V_{\min}}^{V_{\max}} \int_{V_{\min}}^{V_{\max}} \frac{f(v_1) f(v_2)}{\sqrt{v_1^2 + v_2^2 - 2v_1 v_2}}\, dv_1 dv_2 \tag{8}$$

When the nodes move in the opposite direction; the mathematical expectation of relative velocity can be calculated by the formula (9) which is simplified by formula (4).

$$E_{opposite\,direction}(V_r) = \int_{V_{\min}}^{V_{\max}} \int_{V_{\min}}^{V_{\max}} \frac{f(v_1) f(v_2)}{\sqrt{v_1^2 + v_2^2 + 2v_1 v_2}}\, dv_1 dv_2 \tag{9}$$

Proposition 1. The links established by the nodes flight in the same direction take on a higher probability of keeping long time available than in opposite direction on one air line.

Proof. The known periodic T is a constant. And the relative distance $d=E(V_r)nT$ between two moving nodes is proportional to the expected relative velocity $E(V_r)$. We can get $E(V_r)_{opposite\,direction} > E(V_r)_{same\,direction}$ by formulas (8) and (9). And $O_{t+\Delta t}(d)$ is a decreasing function in $0 \leq d \leq 2r$. By the known conditions and formula (7) can infer

$$\frac{O_{t+\Delta t}(nTE_{oppositedirection}(V_r))}{\pi r^2} < \frac{O_{t+\Delta t}(nTE_{samedirection}(V_r))}{\pi r^2}$$

Therefore; when the nodes move in the same direction; the probability which the links between two nodes keep long time available is higher.

When the routing protocols in AANET create multi hop routing path; using proposition 1 can effectively reduce the probability of link break; thereby reducing the probability of routing path interrupt. When the density of air vehicles is smaller; the links created by the air vehicles in the same direction may not ensure the interactive data between the two nodes can be delivered each other. So we need use the links created by the nodes flight in the opposite direction. Under the circumstances; the proposition 2 can be introduced to optimize the routing mechanism and increase the available time of routing path.

Proposition 2. The newest links established by the nodes flight in the opposite direction take on a higher probability of keeping long time available than older links on one air line.

Proof. Set a time period T and two links $link_1$ and $link_2$ created at different time. At the time instant t; the $link_1$ has lasted for nT ($n \in N$); and the $link_2$ has lasted for $(n-\beta)$T ($0<\beta<n$; $\beta \in N$). According to the formula (7); the probabilities that the $link_1$ and $link_2$ keep available at the time instant t are respectively represented by

$$p_{connected}(n) \approx \frac{O_{t+\Delta t}(nTE_{opposite\,direction}(V_r))}{\pi r^2}$$

and

$$p_{connected}(n-\beta) \approx \frac{O_{t+\Delta t}((n-\beta)TE_{opposite\,direction}(V_r))}{\pi r^2}$$

Since $O_{t+\Delta t}(d)$ is a decreasing function in $0 \leq d \leq 2r$; Thus; we can get $p_{connected}(n) < p_{connected}(n-\beta)$. And the probability which the older $link_1$ keeps available is smaller.

III. Topology Control Base on Mobility Model

This section introduces a solution which uses topology control mechanism to detect and recognize the available link established by two nodes flight on one air line in AANET. In routing mechanisms based on topology

control; we mainly adopt regular exchange of Hello packets to discovery and maintenance the link between two nodes. Therefore; we represent the available time of a link by the number of Hello packets received; and introduce the concept of node logic neighbor set which is the set of 1-hop nodes that can exchange Hello packets directly from one node.

Table I shows a parameter list of a logic neighbor set of m_i (here i=1); M_i characterizes logic neighbor set of m_i. $t_i(m_x)$ is the time instant when the node m_i firstly receives a Hello packet from its neighbor node m_x and creates a unidirectional link between them. $\varphi_i(m_x)$ is the stability between m_i and m_x used to measure the duration of link. Formula (10) is the calculation method; t is current time instant; T characterizes the period received Hello message; $[x]$ is the largest integer not greater than x.

$$\varphi_i(m_x) = \left\lfloor \frac{t - t_i(m_x)}{T} \right\rfloor + 1 \tag{10}$$

TABLE I. LOGICAL NEIGHBORS OF NODE M_I (T=132.6S;T=1S;I=1)

M_i={m_2;m_3;m_5}	$\varphi_i(m_x), \forall m_x \in M_i$	$t_i(m_x)$	$N_i(m_x)$
m_2	69	63.8	n_2
m_5	12	121.1	n_5
m_3	4	129.3	n_3

$N_i(m_x)$ is overtime threshold. If no exchange time of Hello packets between two nodes is over the threshold $N_i(m_x)$; we consider the link is broken. And the function of $N_i(m_x)$ is to avoid that links are wrongly considered broken when occasional interference leads to Hello packet loss. Here; we just consider a fixed value: $N_i(m_x)$ = 4T; which means that the link detection mechanism tolerates up to three consecutive missed Hello packets and does not deem it broken. The probability of more than three consecutive missed Hello packets is small [14-15]. And when there is not Hello packet exchanged via a link for 4 periods; the link is considered broken; the routing algorithm no longer chooses this link; its stability value is reset. However; when the stability value reaches a threshold again; the link will be reconsidered as an available link again.

A. Recognition of Long Time Available Links

This subsection gives a method using the stability value to detect the long time available link between the air vehicles flight in the same direction. As shown in the formula (11); a link is considered to have high stability if its stability value $\varphi_i(m_x)$ is greater than a given value n_{stab}. And we define the link with high stability as a long time available link (represent with $link_{ix\text{-}l}$).

$$\varphi_i(m_x) \geq n_{stab} \tag{11}$$

Following is the calculation method of n_{stab}. Based on the formula (6) and (7); a link created by two nodes flight in the opposite direction presents an improbability of keeping the link available when d > 2r and $E(V_r) \neq 0$. Due to $d=E(V_r)nT$;we can infer $p_{connected}(n)=0$ when $n>2r/E(V_r)T$. The literature[14] finds that keeping the link available in high speed Ad hoc network; relative velocity is approximated by a normal distribution; 99.7% of the velocity observations are within $E(V_r) \pm 3\sigma (\sigma < E(V_r)/3)$; where σ denotes the standard deviation of the distribution. And we use the lower limit $E(V_r)$-3σ of relative velocity distribution to get a larger n_{stab} value. The computational method is shown in formula (12).

$$n_{stab} = \frac{2r}{(E(V_r) - 3\sigma)T} \tag{12}$$

In other words; after the link is created between two nodes flight in same direction; more than n_{stab} Hello packets are transmitted; which means the link is a long time available link.

B. Recognition of Short Time Available Links

The links between nodes are not always long time available links for the mobility of the nodes in AANET. Sometimes all existing long time available links can not establish a routing path. On this condition; we need some short time available links to patch the routing path for reliable data transmission. When the condition $\varphi_i(m_x) < n_{stab}$ holds; a link is considered to be unstable. The unstable link with longer duration is defined as short time available link. And corresponding recognition algorithm uses the proposition 2 to select the nodes which create link with minimum stability value from logic neighbor set; as shown in the formula (13).

$$link_{ix-s} = \min(\varphi_i(m_x)), \quad \forall m_x \in M_i \tag{13}$$

For the unstable links; we do not distinguish the links created by the nodes flight in the same direction or the opposite direction; and just choose the link with minimum value of $\varphi_i(m_x)$ as the short time available link.

C. Topology Control Based on Link Stability

When majority of logical neighbor nodes have created long time available links between themselves and a node; we consider the node as a stable node. It can be used for broadcasting the messages about network topology change. To avoid a large amount of messages broadcast causing flooding phenomenon; we propose a broadcast agent vote algorithm; which can select an agent node to broadcast the messages about network topology change. In addition; the topology consists of long time available links can be effectively used for information dissemination and transfer in whole network.

We assume A(m_i) is the broadcast agent selected by node m_i; and only one broadcast agent can be selected by node m_i. The m_i also can learn of other broadcast agents selected by the nodes in its logical neighbor set via the Hello message. The detail is shown in algorithm 1.

Algorithm 1. The node m_i selects its broadcast agent.
Input:M_i;{ $\varphi_i(m_x)$; $A_i(m_x)$; $t_i(m_x)$} $\forall$ $m_x \in M_i$
Output:A(m_i)
1 φ_{max} ←*return_*φ_{max}*_from_table*();
2 *address*←*MAX_INT*;
3 A_{mid}← -1;
4 *thershold*← -1;
5 IF *if_stable_node* (m_i) THEN
6 FOR each neighbor $m_x \in M_i$ DO
7 *insert_list*($A_i(m_x)$;*list_BA*);

8 END
9 IF (m_i is BA) THEN
10 *insert_list*(m_i ; *list_BA*);
11 END
12 FOR each $A_x \in$ *list_BA* DO
13 FOR each neighbor $m_x \in M_i$ DO
14 IF (m_x=A_x) AND *if_stable_node*(m_x) THEN
15 $A_{mid} \leftarrow m_x$;
16 END
17 END
18 IF($A_{mid} \neq$ -1)THEN;
19 BREAK;
20 END
21 IF (m_i=A_x) THEN
22 $A_{mid} \leftarrow m_i$;
23 BREAK;
24 END
25 END
26 IF(A_{mid} = -1)THEN
27 FOR each neighbor $m_x \in M_i$ DO
28 IF(φ_{max} -$\varphi_i(m_x)$-*thershold*≤0)
AND (*address*_ m_x < *address*) THEN
29 *address*←*address*_ m_x;
30 $A_{mid} \leftarrow m_x$;
31 END
32 END
33 END
34 END
35 A(m_i)= A_{mid};

The principle of the algorithm as follows:

First; when there is not long time available link between m_i and its logic neighbor nodes (meaning that m_i does not have stable neighbors); m_i does not select any node as its broadcast agent;

Second; when the logic neighbor nodes of m_i do not select m_i as their broadcast agent; and there is at least one neighbor node m_x is already a broadcast agent; m_i select m_x as its broadcast agent. We can merge multiple broadcast groups into one through this rule.

Third; when m_i is one of broadcast agents selected by the logic neighbor nodes of m_i; and the address of m_i is lower than broadcast agents of its neighbor nodes; m_i selects itself as a broadcast agent. The function of this rule is to merge multiple broadcast groups into one when m_i act as the broadcast agent of the group.

Last; when none of logic neighbor nodes of m_i has a broadcast agent; m_i selects the node; which has maximal stability value and lowest address in logic neighbor nodes of m_i; as its broadcast agent. This rule is used to select the first broadcast agent in the network.

IV. Routing Mechenism Base on Mobile Feature of Nodes in AAnet

This section introduces a new protocol Path Link Availability Routing Protocol (PLAR) based on OLSR. And one feature of PLAR is using the stability of link to control the network topology. A core technology used in OLSR is Multipoint relaying (MPR); which can reduce the number of redundant retransmission message when the messages are broadcasted in the network. The Multipoint Relay Set (MPRs) is a set of Multipoint Relay nodes. In OLSR; MPRs are chosen as the minimum set of m_i's 1-hop neighbor nodes which cover all its 2-hops neighbor nodes. Therefore MPR nodes can guarantee 2-hops full coverage. Algorithm 1 can generate a broadcast agent set which send the massage about topology change; and construct a stable topology which diffuse the message in whole network. Then we introduce the algorithms 2 and 3; which select and generate the MPRs based on the algorithms 1. The algorithm 2 relates to the method of generating MPRs; when the density of mobile nodes is high. And Algorithm 3 is used to generate MPRs and supplementary MPRs for low density of nodes.

A. Generation of MPRs for High Density of Nodes

This subsection introduces a new method (algorithm 2) generating MPRs for the OLSR protocol based on algorithm 1. The basic principle of the method is the choice of nodes with long time available links to generate MPRs. Following is an example about algorithm 2. If a given node m_i runs the algorithm 2; only need to know its logic neighbor set M_i; stability value $\varphi_i(m_x)$ and 2-hop neighbor set M_{2i}. In the OLSR; 2-hop neighbor set includes all 2-hop neighbor nodes of m_i. In our algorithm; we select the 2-hop neighbor nodes; which the m_i' 1-hop stable neighbor nodes m_x can connect with; to form the 2-hop neighbor set. The set can meet the requirement of broadcast well for topology update when the density of nodes is high. And the reason is the nodes with long time available links are enough. The core principle of the algorithm 2 is MPRs in OLSR consists of broadcast agents.

In algorithm 2, The MPRs selected in line 4 can not guarantee 100% coverage of 2-hops neighbor nodes. For example; a given 1-hop neighbor node m_x may be stable; but not be a broadcast agent. It is not selected as a MPR node in line 4. And it can be the only one that can arrive at a given 2-hops neighbor node (initially inserted in M_{2i}). All nodes contained in M_{2i} are verified in line 10; where M_{2i} should be empty if all nodes initially inserted in M_{2i} are accessible for the nodes already inserted in the MPR list. When M_{2i} is not empty; the algorithm selects the node; which has the highest stability values and can access at least one of the nodes contained in M_{2i} (selected in line 12); as the MPR node. So all 1-hop nodes have stable link to m_i can access the nodes initially contained in M_{2i}. And the process of verifying and revising the MPRs is described in lines 10–15 of algorithm 2.

Algorithm 2. Generation of MPRs for high density of nodes
Input:M_i; M_{2i};{ $\varphi_i(m_x)$; $A_i(m_x)$; $t_i(m_x)$} $\forall$ $m_x \in M_i$
Output:*MPRs*(m_i)
1 *MPRs*(m_i)←*Ø*
2 $M_{2i} \leftarrow$*2_hop_neighbor*( )
3 FOR each neighbor $m_x \in M_i$ DO
4 IF $\varphi_i(m_x) > n_{stab}$ AND m_x is BA THEN
5 *MPRs*(m_i)← *MPRs*(m_i) $\cup$ m_x
6 *remove_2_hops_from*(M_{2i})
7 *remove_1_hops_from_set*(m_x;M_i)
8 END
9 END
10 M_{order}=*sort_stability_by_descendent*(M_i)
11 WHILE $M_{2i} \neq$ Ø DO
12 m_x=*get_first_element*(M_{order})
13 *MPRs*(m_i)← *MPRs*(m_i) $\cup$ m_x
14 *remove_2_hops_from*(M_{2i})
15 *remove_1_hops_from_set*(m_x;M_i)
16 *rm_redundance_cover*N_{2a}*_from_set*(*MPRs*(m_i); M_{order})
17 END;

Algorithm 2 shows better results than the MPRs generation algorithm of original OLSR when the number of stable links associated with m_i is above a given threshold (4 stable links). If the number of stable links is not above this threshold; the number of nodes contained in MPRs (Algorithm 2 in line 5) is small. But the number may become bigger in line 12. However; when the number of long time available links between m_i and its neighbors is small; the nodes initially inserted in M_{2i} is also small; which leads to the number of nodes in MPRs is small. Under this condition; the result of utilization proposition 2 is better than proposition 1 for the algorithm design. In the next subsection; we will introduce an additional algorithm; which is better suited for the case that the number of long time available links of m_i is below the threshold.

B. Generation of MPRs for Low Density of Nodes

When the density of air vehicles is low; the number of long time available links created between the air vehicle and its neighbors is small. The result of algorithms 2 is not ideal. Under this condition; we can utilize more short time available links to increase the amount of routing path; thereby improving the routing efficiency. Therefore; this subsection gives the algorithm 3 based on proposition 2 to generate MPRs for the lower density of nodes.

Algorithm 3. Generation of MPRs for low density of nodes
Input:M_i; M_{2i};{ $\varphi_i(m_x)$; $A_i(m_x)$; $t_i(m_x)$} $\forall$ $m_x \in M_i$
Output:$MPRs(m_i)$
1 $MPRs(m_i) \leftarrow \emptyset$
2 $M_{2i} \leftarrow 2\_hop\_neighbor(\ )$
3 FOR each neighbor $m_x \in M_i$ DO
4 IF $\varphi_i(m_x) > n_{stab}$ AND m_x is BA THEN
5 $MPRs(m_i) \leftarrow MPRs(m_i) \cup m_x$
6 $remove\_2\_hops\_from(M_{2i})$
7 $remove\_1\_hops\_from\_set(m_x;M_i)$
8 END
9 END
10 $M_{order}=sort\_stability\_by\_ascendent(M_i)$
11 WHILE $M_{2i} \neq \emptyset$ DO
12 $m_x=get\_first\_element(M_{order})$
13 $MPRs(m_i) \leftarrow MPRs(m_i) \cup m_x$
14 $remove\_2\_hops\_from(M_{2i})$
15 $remove\_1\_hops\_from\_set(m_x;M_i)$
16 $rm\_redundance\_coverN_{2a}\_from\_set(MPRs(m_i); M_{order})$
17 END;

Algorithm 3 has the same rationale with algorithm 2. The 1-hop neighbor nodes of m_i ;which have been selected as broadcast agents and have long time available links with m_i; are inserted in MPRs (lines 3–8); since these links are stable. Proposition 1 indicate that they have higher probability of keeping available for a long time. If the nodes contained in MPRs generated based on proposition 1 can not access all 2-hops neighbor nodes; the algorithm inserts more unstable nodes into MPRs (lines 10 to 15). For this case; the density of nodes is low; and algorithm 3 uses proposition 2 to select the 1-hop neighbor nodes; which have lowest stability value links to m_i; as the nodes of MPRs. And the link between m_i and its neighbor nodes with lowest stability value has higher probability of keeping long time available.

C. Selection Policy of Algorithm in PLAR

The difference between the algorithm 2 and algorithm 3 is the way of generating the MPRs. When the density of air vehicles is high; the probability of creating more long time available links between m_i and its neighbor nodes (stable neighbor nodes) is high. So the algorithm 2 is applied. For low density of air vehicles (scenario proposed for Algorithm 3); the probability which the 1-hop stable neighbor nodes of m_i can access all 2-hop neighbor nodes of m_i is lower. At this moment; algorithm 3 is more suitable.

A given node m_i running our method uses Algorithm 2 or Algorithm 3 depending on the number of its long time available links. We set a threshold. If the number of long time available links associate with m_i is not greater than the threshold. The node m_i adopts the Algorithm 3. Otherwise; Algorithm 2 is used to generate the MPRs. In our work; we set the threshold at four; which was achieved by simulating different threshold values for both Algorithms 2 and 3. From the results of simulations performed; we conclude that the performance of algorithm 3 is better than the Algorithm 2 when the number of long time available links is less than 5. If the number of long time available links is more than four; Algorithm 2 presents better performance than algorithm 3.

V. SIMULATIONS

A. Simulation Model

In the simulation; we develop a traffic simulator to simulate air traffic scenarios. The simulator is integrated into the NS2 (network simulation platform) to simulate the AANET. We have simulated a 100 kilometer air line with three lanes in each direction. At the same time; the bidirectional air traffic with different air vehicles density is simulated. The radio range of air vehicle is 10 kilometer. We define three different classes of air vehicles according to the flying speed for a classic scenario.

We define four different scenes regarding the density of air vehicles; described in table II; which differs in the average number of 1-hop neighbor nodes. Average numbers of neighbors in simulation are adopted with 4; 6; 8 and 10 respectively; which means 5; 7; 9; 11 air vehicles per $10^2\pi$ km^2. The density and the simulation time of flight nodes are shown in table II. The density and simulation time setting in table II are based on real air traffic; which can reflect the normal flight states of different aircraft.

In the simulation process; we use NS2 to run the commands of air traffic simulator for aircraft communication simulation. The scheme of generating network traffic is as follows: the air vehicles flight from west to east generate the packets; which are randomly sent to another mobile nodes. The air vehicles flight from east to west do not generate packets but are able to forward them. The number of packets generated on each density scene was maintained constant at approximately 3500 packets.

TABLE II. CLASSIFICATION OF AIRCRAFT BY DENSITY IN THE SIMULATIONS

scene	Number of aircrafts	Average number of neighbors	Simulation Time (s)
scene 1	80	4.0	807
scene 2	120	6.0	786
scene 3	160	8.0	834
scene 4	200	10.0	865

B. The Setting of Threshold n_{stab}

In order to compute the threshold n_{stab}; we assume that the flying velocities of the three classes of air vehicles are normally distributed approximately. For this case; applying (8) and (9); the average relative velocity between two air vehicles flight in the opposite directions ($E(V_r)_{opposite\ direction}$) is 589 m/s; and the average relative velocity between two air vehicles flight in the same direction ($E(V_r)_{same\ direction}$) is approximately 15 m/s. The transmission frequency of Hello packets ($1/T_B$) which we adopt is 1 Hz; the maximum communication distance between nodes is 10 kilometers; the standard deviation of mobile velocities is 5 m/s. According to (12); we can yield n_{stab} = 68; which indicates the links created by the air vehicles flight in the opposite direction have low probability of lasting longer than 68 s (the probability is lower than 0.3%); and the probability in the same direction lasting for 68 s is 95.1% ($p_{connected}(68)= O_{t+\Delta t}(68*15*1)/(\pi*10000^2)\approx 95.1\%$).

C. Metrics and Measure Methods

This subsection introduces the metrics and evaluation mechanisms in the simulations. We developed a packet tracking tool based on NS2. The tool is able to generate and follow every PING/PROBE packet on its way from source to destination; and record the node sequence of a routing path passed. We can easily measure the path availability; path length and end-to-end delay by simulating a specific traffic. The measurement steps are as follows:

Step 1; we choose randomly two aircrafts on the same route to compose a source-destination node pair; and one act as source; another is destination. The source node sends a PING packet to the destination node. If the PING packet can arrive at the destination node; the path is considered available; and the path availability is updated further. We use the path resolving rate to compute the path availability. The time intervals of source-destination pairs generated have exponential distribution.

Step 2; when we have confirmed the path available by using the PING packet; the time instant t_{first} when the PING packet arrives at the destination node is recorded. And the destination node stores the sequence of nodes visited by the PING. We consider the sequence as the original path $Path_k$ and use it to compute the path length. At the same time; the source node sends a PROBE packet to the destination node along the $Path_k$ every 1 s.

Step 3; the calculation of the path available time can utilize the time instant t_{last} which the PROBE packet arrives at the destination node. When the PROBE packet is transmitted between a node pair; the destination node can verify whether the packet is transmitted along the original path $Path_k$. If the PROBE packet arrives at the destination node through the original path; the time instant which the last PROBE packets arrive at the destination node is recorded; and t_{last} is updated. The path available time is computed by the time instant difference t_{last}-t_{first}. If the path followed by the PROBE packet is different from the original one; then the path is considered broken. And the t_{last} is no longer updated. The final path available time is the time interval t_{last}-t_{first}; the destination node recorded lastly. And the periodic transmission of PROBE packets is canceled.

Step 4; the end-to-end delay between the node pair is computed at the destination node by the time difference (t_{end}- t_{begin}) between arrival time instant and departure time instant of one packet. We adopt the average of the time difference of packet transmission; including the PING and all PROBE packets.

VI. ANALYSIS OF SIMULATION RESULTS

We compared the simulation scenarios to the real scene; the approximation degree of all parameters and data is close to 95%. In the simulation; the performance of PLAR is compared with OLSR, DSR, AODV and GPSR.

First; the results that we analyze the end-to-end delay in simulation are shown in table III. For each protocol; the results of end-to-end delay have a common feature; that is; the end-to-end delay will increase with the increase in node density. This is mainly because the number of nodes increase will bring the number of control messages of protocol increase; which makes the ratio of network management data flow to network bandwidth increase; and increases the end-to-end delay of general data packets. However; the DSR protocol shown in Table III is an exception. Initially with the increase in density of nodes; the end-to-end delay is not increased but decreased. When the node density increases to a certain degree; the delay will increase. This is mainly because DSR uses available sub-paths contained in the cache of each node to form routing paths. When the density of nodes small; the increase of probability reusing the same sub-paths for different destination which causes the paths saturation easily. Thus end-to-end delay is increased. In addition; if the number of sub paths is small; once a sub path is break; it is hard to find other sub path to transmit the data. For this case; the packets will be discarded; resulting in higher end to end delay.

In addition; from the simulation results in table III; we also found that; with the increase in density of nodes; the end-to-end delay of DSR and GPSR is much higher than other protocols. This is because GPSR floods the position of the nodes in whole network; and DSR uses flooding to discover the path. Flooding technology is the main reason leading to the end to end delay high. And it can generate large amounts of network management data flow in the process of protocol resolving path. Therefore; DSR and GPSR are not suitable for AANET when the load of network is heavy.

TABLE III. COMPARISON OF END-TO-END DELAY(MS)

scene	OLSR	PLAR	AODV	DSR	GPSR
1	2.71±0.08	2.72±0.07	8.53±0.15	191.12±18.91	10.65±0.41
2	3.39±0.11	4.06±0.18	8.71±0.21	117.73±11.23	18.12±0.39
3	3.82±0.15	5.91±0.21	10.03±0.31	90.09±5.17	20.08±0.49
4	4.33±0.16	6.83±0.21	11.06±0.28	112.83±4.35	29.32±0.69

TABLE IV. COMPARISON OF AVERAGE PATH LENGTH (HOPS)

scene	OLSR	PLAR	AODV	DSR	GPSR
1	2.51±0.05	3.33±0.05	3.83±0.06	4.94±0.05	4.16±0.05
2	2.61±0.05	3.24±0.06	4.03±0.06	5.19±0.05	3.99±0.05
3	2.55±0.05	3.61±0.06	4.11±0.06	5.53±0.05	4.07±0.05
4	2.51±0.04	3.69±0.06	4.15±0.05	5.61±0.05	3.93±0.06

TABLE V. COMPARISON OF PATH AVAILABILITY RATE(%)

scene	OLSR	PLAR	AODV	DSR	GPSR
1	41.93±0.89	71.05±0.67	69.71±0.71	96.97±0.36	92.08±0.71
2	45.87±0.96	66.93±1.64	68.92±0.81	96.48±0.27	90.11±0.75
3	48.01±1.12	72.13±1.69	68.24±0.91	97.05±0.21	89.81±1.02
4	46.72±0.63	69.84±1.07	71.17±0.85	96.69±0.39	91.09±0.65

The overall simulation results demonstrate that the end-to-end delay of PLAR proposed in this paper is obviously much lower than DSR and GPSR protocols; between OLSR and AODV. In point of end to end delay; performance of OLSR is slightly better than PLAR. This is mainly because the number of nodes in MPRs of PLAR is more than in MPRs optimized by OLSR; which cause more topology control messages generated and broadcasted in PLAR when the network topology update. While the bandwidth of broadcast and unicast in the simulation are 2 Mbps and 11Mbps respectively; the topology control data streams will occupy the part of common data flow bandwidth; thereby increasing the end to end delay in the process of data transmission. But compared with AODV; DSR and GPSR; PLAR has shown better performance; because the MPRs generation algorithm in PLAR preferentially selects the nodes flight in the same direction; which reduces the probability of link break; thereby decreasing the average of end to end delay.

Table IV describes the average path length of different protocols in different simulation scenarios. The OLSR shows the lowest average path length in all scenes; while DSR has the highest values for almost all scenes. Comparing the tables III and IV; we can find that the increase in average path length cause the increase of end to end delay in general. However; this does not hold for all scenes in simulation. For example; the path length in the simulation of GPSR smoothly decreases from Scene3 to Scene4; but the end-to-end delay increases from 20.08 to 29.32 ms.

In addition; for the simulation scene 2; the average path length of AODV is higher than GPSR; but GPSR shows higher end to end delay. This is because each routing protocol has their own features; can not be generalized in terms of the relationship; which the end-to-end delay is always proportionate to average path length. But when the average path length for a given protocol is smaller; and the path saturation degree is higher; it will show a higher end to end delay.

In this paper; we use the percentage of resolved paths to a given destination to define the average path availability rate. In table V; DSR and GPRS is shown higher path availability rates; the reason is a common feature of the two protocols is messages routed on demand. In addition; table V also shows the path availability rate of PLAR and AODV is very close; far higher than the OLSR. For end users; path availability rate is an important metric; but available time is also important for the network stability [13]. Although the path availability rate of DSR and GPSR in the simulation is highest; but their end-to-end delay is the highest too. In addition; there is a common shortcoming in DSR and GPSR; although they can resolve large amounts of paths to a given destination; but from the available time point view; the quality of these paths is not high.

We choose the simulation results of a medium-low (scene 2) and medium-high (scene 3) density air traffic scenes to analyze the path available time. While the results obtained from scene 1 and 4 are similar to that obtained from scene 2 and 3; respectively; so we no longer analyze the simulation results of scene 1 and 4. In the process of analysis; we utilize the path available time cumulative distribution function (CDF) to analyze the simulation results of different protocols; as shown in figure 3. Figure 3(a) and 3(b) show the simulation results of path available time in scene 2 and 3 respectively. Combined with the results in table V; we can find GPSR and DSR have higher path availability rate; but the path available time CDF indicates that approximately 45% of the paths lasting no longer than 1 s. These values are significantly reduced in PLAR. The path available time CDF indicates the percentage of paths lasting no longer than 1 s in PLAR is smaller than 9%; significantly lower than GPSR and DSR protocols. It means the paths created by the PLAR have longer available time. In addition; figure 3(a) shows the number of paths that last no longer than 6 s is approximately 28%; while the percentages of other protocols are between approximately 55% and 78%.

All simulation results show that the method proposed in this paper is applied to the PLAR; which can increase the path available time significantly. When the routing paths are created by air vehicles flight in one direction; the available rate of routing paths established by OLSR can reach 72.18%. When we choose the nodes bidirectional flight to create the routing paths; the available rate of routing paths established by OLSR is only 45.27%. The table V shows the available rate of routing paths established by PLAR using the nodes bidirectional flight can reach 66.93%; which is closer to the performance of OLSR used in a single direction. In addition; the PLAR is also shown good performance in the end to end delay; only the OLSR is superior to it. But the path available rate of PLAR is better than OLSR; which can be comparable with the AODV. Therefore; the PLAR improves on the available time for routing paths; which shows PLAR is more suitable for the AANET with higher demand on the network stability.

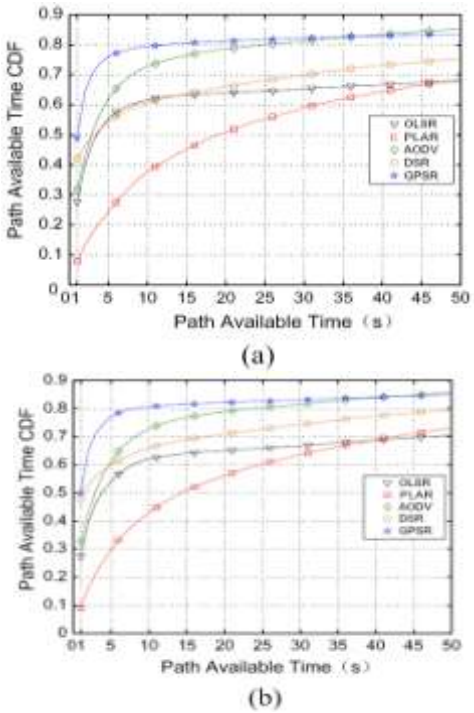


Figure 3. Performance comparison of path available time

VII. CONCLUTION

In this paper; we propose a new routing mechanism for AANET network. This mechanism can reduce the probability of routing path broken by increasing the available time of links in the AANET; so as to improve the performance of routing protocols. The complexity of algorithms in the mechanism are all O(n).The experimental results show that the method proposed in this paper can effectively improve the performance of routing protocols based on topology and location; mainly reflected in the path available time. The end-to-end delay and path available rate is also enhanced to an ideal level. The innovation of this paper lies in that the node mobility model of AANET is applied to the routing mechanism design and implementation. In the future; we can further research on probability model representing the real-time parameters of node mobility model; which can provide a theoretical basis for the adaptive routing behavior in AANET.

ACKNOWLEDGMENT

The author wishes to thank the anonymous reviewers for their valuable comments and suggestions. This work was is sponsored by the Natural Science Foundation of China (NSFC) under Grant No. 61303225; the Natural Science Foundation of Shaanxi Province of China under Grant No. 2013JQ8046; the Basic Research Foundation of Northwestern Polytechnical University under Grant No. GBKY1004.

REFERENCES

[1] Li F; Wang Y. Routing in vehicular ad hoc networks: a survey. *Vehicular Technology Magazine IEEE;* 2007; 2(2) pp. 12-22.

[2] Bernsen J; Manivannan D. Review: unicast routing protocols for vehicular ad hoc networks: a critical comparison and classification. *Pervasive and Mobile Computing;* 2009; 5 (1) pp. 1-18.

[3] Shen H; Wang XD; Zhou XM; Xia GM. Link-Ware Based Routing Protocol for VANET. *Journal of Software;* 2011; 22(Suppl. (1)) pp. 157-164.

[4] Blum JJ; Eskandarian A; Hoffman LJ. Challenges of intervehicle ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems;* 2004; 5 (4) pp. 347-351.

[5] Santos RA; Edwards A; Edwards RM; Seed NL. Performance evaluation of routing protocols in vehicular ad hoc networks. *International Journal of Ad Hoc and Ubiquitous Computing*; 2005; 1(1/2) pp. 80-91.

[6] Nzouonta J; Rajgure N; Wang GL; Borcea C. VANET routing on city roads using real-time vehicular traffic information. *IEEE Transactions on Vehicular Technology;* 2009; 58 (7) pp. 3609-3626.

[7] Jerbi M; Senouci SM; Rasheed T; Ghamri-Doudane Y. Towards efficient geographic routing in urban vehicular networks. *IEEE Transactions on Vehicular Technology;* 2009; 58 (9) pp. 5048-5059.

[8] Wang Y; Su H; Fang DY. A Geographic Surface Routing Algorithm in 3D Ad Hoc Networks. *Journal of Software;* 2010; 21(Suppl. (12)) pp. 318-329.

[9] Zhang LL; Zheng Y; Chen H. Position-Based and Connectivity Aware Routing Algorithm in Vehicular Ad Hoc Networks. *Journal of Software;* 2012; 23(Suppl. (1)) pp. 141-148.

[10] Zong M; Wang XD; Zhou XM. Cost-Optimizing Adaptive Location Service Protocol in MANET. *Journal of Computer Research and Development;* 2012; 49(12) pp. 2515-2528.

[11] Xia H; Jia ZP; Zhang ZY; Edwin H. S. A Link Stability Prediction-Based Multicast Routing Protocol in Mobile Ad hoc Network. *Chinese Journal of Computer;* 2013; 36(5) pp. 926-936.

[12] Sun J; Guo W. Cross Layer Transmission Control Protocol Interacting with Link Reliable Routing in MANET. *Journal of Software;* 2011; 22(5) pp. 1041□ 1052

[13] Nahm K; Helmy A; Kuo CC. Cross-layer interaction of TCP and ad hoc routing protocols in multihop IEEE 802.

11 networks. *mIEEE Transactions on Mobile Computing; 2008;* 7(4) pp. 458-469.
[14] Oliveira R; Bernardo L; Pinto P. The influence of broadcast traffic on IEEE 802. 11 DCF networks. *Elsevier Computer Communications;* 2009; 32(2) pp. 439-452.
[15] Oliveira R; Luis M; Bernardo L; Dinis R. Towards reliable broadcast in ad hoc networks. *IEEE Communications Letters;* 2012; 16(3) pp. 314-317.

Zhong Dong received the BEng degree of information security in 2002; MEng degree of software engineering in 2005; and PhD degree of engineering in computer science and technology in 2010; respectively; from the Northwestern Polytechnical University. He is currently a lecture at the School of Computer Science; Northwestern Polytechnical University; P.R. China. His research interests include mobile computing; Aeronautical Ad Hoc Network; and Internet of things. He is a member of the IEEE; ACM and CCF.

An Energy-Efficient Routing Mechanism Based On Genetic Ant Colony Algorithm for Wireless Body Area Networks

Guangxia Xu
School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
Corresponding author, Email: xugx@cqupt.edu.cn

Manman Wang
School of Communication Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
Email: {manmanw68}@163.com

***Abstract*—As an important branch of Wireless Sensor Network (WSN), Wireless Body Area Network (WBAN) has received extensive attention of various fields as it is portable and removeable. However, energy consumption is highlighting increasingly as nodes are hard to be recharged or replaced. Up to now, many energy efficient routing algorithms or protocols have been proposed with techniques like clustering, data aggregation and location tracking etc. However, many of them aim to minimize parameters like total energy consumption, latency etc. In order to optimize network routing and prolong the life of network, this paper proposes an energy-efficient routing algorithm in WBAN which is based on Genetic Ant Colony Algorithm (GACA). GACA makes full use of Genetic Agorithm (GA) and Ant Colony Algorithm (ACA). Choosing the optimal routing is to take advantages of both GA and ACA. At the early stage of algorithm, it uses GA to generate the initial pheromone distribution quickly and comprehensively, and then converts the evolved pheromones distribution into pheromones that can be used by ACA and finally uses the positive feedback and parallelism of ACA to find out the optimal solution. It is the fusion of the two algorithms, gaining an improvement of both time and quality. Then it reduces and balances energy consumption for all sensor nodes through a Distance-based Energy Aware Routing (DEAR) algorithm in order to prolong the lifetime of network.**

***Index Terms*—Wireless Body Area Network; Genetic Ant Colony Algorithm; Optimal Routing; Network Lifetime**

I. INTRODUCTION

Wireless Sensor Network, as the hot topic being studied by researchers all the time, includes many nodes that have ability of sensing and processing. It can collect and manage information such as temperature, humidity, pressure, voice and other information people need in many cases. So it is widely applied in areas like public security, environmental monitoring, ITS, biomedicine, etc. People's demand for short-distance wireless communication is increasing with the rapid development of communication technology. Mobile communication system is developing towards personalization and miniaturization. Therefore, people-centered small network WBAN is proposed at the very moment.

As a branch of sensor network, WBAN is an important public application network. It can meet the huge application demand in the field of electronic medical services, especially in remote medical treatment, special crowd monitoring, community health care, etc. WBAN, also called as Body Area Sensor Networks (BASN) [1], is a kind of communications network whose center is human and components are network elements related with human body. It senses and collects some important physical parameters such as body temperature, blood pressure, heart rate, blood oxygen concentration, etc. and some environmental parameters around human such as temperature, humidity, light intensity, etc. with the sensor nodes that are in or around human. Then it will send the parameters to the Base Station (BS) or the Mobile Unit (MU) near human body in a wireless way. Finally, it will upload the parameters to the terminal server through internet to have them analyzed and processed. It will be shown in Fig. 1. WBAN is not only a new solution to universal health care, disease control and disease prevention, but also an important perception part of Internet of Things (IOT).

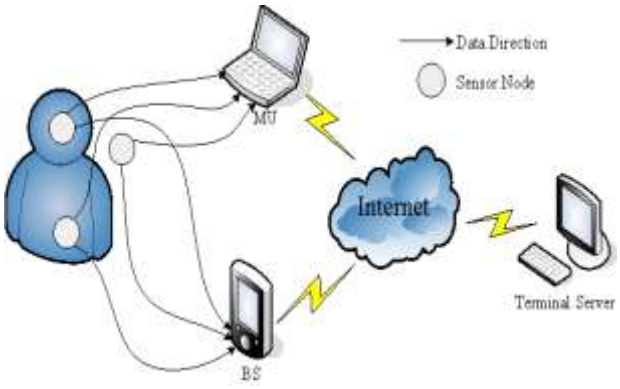


Figure 1. The basic framework of wireless body area network

doi:10.4304/jnw.9.12.3366-3372

The increase of aging population around the world and the shortage of medical relative resources (budget outlay, doctor, nurse and sickbeds) make the development of medical and health care systems become a the global demand. Applications of WBAN technology are automated and intelligent. And it can effectively solve the difficulty of expensive medical treatment problem, especially for users located in rural areas. It is to provide a convenient means of quick medical services. And conventional medical treatments methods are taken after symptoms, and not real-time disease surveillance or prevention, while the real-time of features WBAN can satisfy this demand. However, on the one hand, WBAN has brought us much convenience. On the other hand, energy constrained problem of nodes in body area sensor work has aroused concern..Secure access between sensor nodes. It ensures network access only to eligible SMD and biosensors, they need to make an authentication before starting data transmission among them.

Most of the sensor nodes of WBAN are powered by micro batteries, so the system energy resources are limited. The nodes' channel quality changes as the link is wireless channel and human body movement is unpredictable. Medical sensor close to the person physically, out of consideration of human radiation, wireless communication capabilities are limited. Due to the limitation of node energy, if some of the nodes are used too frequently for data forwarding, it can easily lead to energy depletion of those nodes and reduction of network connectivity, which ultimately results in a loss of network lifetime. The most important and critical task in the design of WBAN is how to design an efficient routing protocol according to the characteristics of the WBAN. The application scenarios of the WBAN are particular. It must improve the existing energy-efficient strategies, keep the high balance of energy as well as extend the network life cycle as long as possible.

In order to optimize the routing quality and the energy consumption, it is needed to achieve the tradeoff between route hops and the energy consumption. In this paper, we optimized a DEAR algorithm proposed by Wang Jin [2]. An Energy-efficient Routing Mechanism Based on GACA is proposed, which optimizes the energy consumption of WBAN and prolongs the lifetime of network obviously.

This paper is organized as follows. Section 2 states some related works in routing protocol. Section 3 describes the system model of WBAN. Section 4 introduces the design of An Energy-efficient Routing Mechanism Based on GACA. Section 5 evaluates the performance of GACA. Finally, a conclusion is given in Section 6.

II. Related Work

Due to the dynamic nature of WBAN, the optimization of network metrics like shortest path, minimal energy consumption can be viewed as a combinatorial optimization problem which is hard to solve. Since heuristic bionic evolution algorithm based techniques can dynamically adjust their parameters during the search of the optimal value, it is very suitable to be used to solve these kinds of dynamic optimization problems, such as NP-hard problems.

Rahul C. Shal et al proposed an energy multipath routing mechanism, which makes it possible for data to be transmitted through multipath, balances the consumption of energy of whole network and prolongs the lifetime of whole network. However, all these algorithms have assumptions that physical channel is ideal, all nodes in network are equal, data sent by nodes are of same importance and all nodes in network won't exit network in advance. Unfortunately WBAN does not meet these assumptions. The channel transmission model that WBAN depends on is a mixed wireless environment. The concurrence of body channel and free space propagation leads to the time variance of channel quality [3]. A hierarchical structured energy efficient routing protocol called LEACH is presented in literature [4]. A multi-path routing protocol based on dynamic clustering and ant colony optimization (ACO) is proposed in literature [5], so as to reduce energy consumption and maximize network lifetime. The ACO technique is used during the search for multi-paths between cluster head and sink node. An improved version of LEACH is presented in literature [6] to improve energy efficiency and system stability where GA is utilized during the selection of cluster head nodes. GA can also be applied to minimize data latency once the number of gateways and their positions are determined [7]. Each swarm agent can carry and exchange the residual energy information during the route selection process in order to maximize the network lifetime in ad hoc and sensor networks [8].

III. System Model

As is shown in Figure 2, there are 19 wireless sensor nodes being placed in human body or on the surface which make a WBAN. Each sensor node (except Sink Node) is powered by batteries. It collects one or more physical data and then sends the collected data from child nodes to the parent node and finally sends them to sink node through multiple hops. Each sensor node has the ability to forward information automatically and dynamically so as to adjust the transmitting signal power according to the distance of the next hop node.

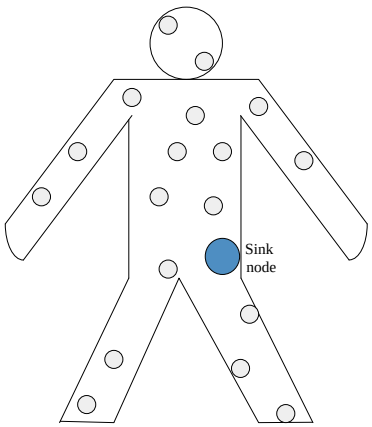


Figure 2. Wireless body area network structure

The network topology in Fig. 2 can be abstracted as a topology diagram $G(V,E)$ in Fig. 3. (V is the set of sensor nodes and E is the set of links). It is an undirected graph $G=<V,E>$ where V represents the set of vertices and E represents the set of edges (or links) [9]. Sink node (or BS) can be placed either inside or outside where can be monitored. This paper assumes that there are N nodes randomly scattered in a two dimensional square field $[X,Y]$. There exists a link $E(i,j)$ between node i and node j if the Euclidean distance $d(i,j)$ is not larger than the radio transmission radius R, namely $d(i,j) \le R$. The objective in this paper is to find a set of optimal or sub-optimal individual distances during routing process so that the energy is consumed at similar rate for all involved sensors.

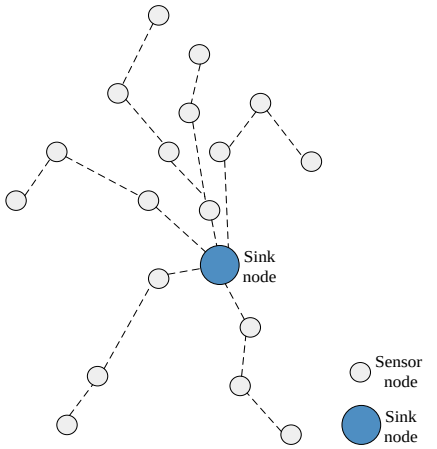


Figure 3. Wireless body area network topology structure

According to the deployment of sensor nodes in human body, we can make the following assumptions of the network topology:

The bi-direction link is used in networks. That is to say, if sensor A can communicate with sensor B, then sensor B can communicate with sensor A.

All sensor nodes are static after deployment.

The initial energy in sensors is equal. During the early period of network's life, sensors have enough energy to communicate with border sensors.

The communication links are symmetric.

Each sensor node can control its power level to the neighbors.

Each sensor node can know the distance to its neighbors and to the sink node.

The sensor has all-direction antenna.

This paper assumes ideal MAC layer conditions.

IV. Proposed Approach

The proposed solution to ensuring energy-efficient in WBAN through an optimized routing algorithm is comprised of two phases. At the first phase this paper proposes a DEAR algorithm. The objective of this phase is to balance the available amount of energy in the whole WBAN as well as to maximize the network lifetime. At the second phase this paper proposed GACA. The objective of this phase is to select an optimal path through GACA. Fig. 4 shows the complete architecture of the proposed model. GACA will be adopted for searching an optimal path from the source node to the base station.

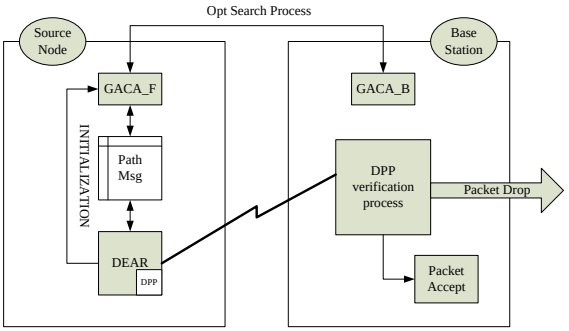


Figure 4. Energy-efficient Routing Mechanism General Architecture

There are three types of packets in the scheme: data packets, ant packets, and neighbour packets. Data packets refer to the data that is carried in the sensor network. The routing algorithm has no interest in what the contents of these packets are, it is just responsible for routing these packets from the source to the destination. Forward and backward ants named GACA_F and GACA_B respectively are represented by control packets. These packets are used to update the routing table. These packets contain four parts: the final destination address, the start time, the arrival time to the final destination, and a stack of each visited node. The final destination is required to let the ant know that it has finished its journey and can be replaced by a backward ant. The start time and arrival time are used to calculate the total trip time, and the stack of each visited node is needed so that the backward ant can retrace the forward ant's trip exactly in reverse.

Information or result got from control packets will be stored in a Path_msg repository. Path_msg repository can be used to maintain or store all available optimal selected results and send them to DEAR on the event based for load balancing. When the event boost the initialization has to be sent on GACA to initiate the already obtained optimal path. The actual sensed data will be sent under the control of Data Privacy Protection (DPP) for protecting the sensory data readings from malicious.

Then sensor will send the obfuscated collected data via a well selected path to a command center known as the base station or sink. The DPP verification process will be performed for ensuring the authenticity and integrity on the actual sensed data. Therefore, the packets will be accepted or dropped according to a verification process.

A. Distance-Based Energy Aware Routing Phase

The following are the steps for distance-based energy aware routing [10]: "This algorithm is used for balancing the energy in a whole network as well as maximizing the network lifetime"

The Implementation of Algorithm in detail:

Input: sensor nodes, distance from each sensor node to base station, base station address and distance to neighbor nodes.

Output: maximizing network lifetime through best routing.

Step 1: Calculate optimal distance value, where $\alpha \in [2,4]$ $\varepsilon_{amp}=\varepsilon_{fs}$ when $\alpha = 2$ and $\varepsilon_{amp}=\varepsilon_{mp}$ when $\alpha = 4$.

$$d_i = d / n_{opt} = \sqrt[\alpha]{\frac{2E_{elec}}{\varepsilon_{amp}(\alpha-1)}}$$

Step 2: Neighbors selection

S_i =select (neighbours)

Step 3: Calculate distance from source to neighbors

$d_i = d(S,N)$

Step 4: Compare optimal distance d_i with d_j

$d_{temp} = near(d_i, d(S,N)).energy \geq ength$

Step 5: End

Iteratively other nodes also repeat the same process. As is shown in Fig. 3, each sensor node will consume the following E_{Tx} amount of energy to transmit a l -bits message over distance d, E_{Tx} can be represented as (1):

$$E_{Tx}(l,d) = \begin{cases} l \cdot E_{elec} + l \cdot \varepsilon_{fs} \cdot d^2, & if\ d < d_0 \\ l \cdot E_{elec} + l \cdot \varepsilon_{mp} \cdot d^4, & if\ d \geq d_0, \end{cases} \quad (1)$$

E_{Rx} the energy to receive this message is (2):

$$E_{Rx}(l) = l \cdot E_{elec} \quad (2)$$

E_{Fx} the energy to forward this message is (3):

$$E_{Fx}(l,d) = E_{Tx}(l,d) + E_{Rx}(l) = \begin{cases} 2l \cdot E_{elec} + l \cdot \varepsilon_{fs} \cdot d^2, & if\ d < d_0 \\ 2l \cdot E_{elec} + l \cdot \varepsilon_{mp} \cdot d^4, & if\ d \geq d_0. \end{cases} \quad (3)$$

For other parameters E_{elec} is the Energy dissipation to run the radio device, ε_{fs} represents free space model of transmitter amplifier, ε_{mp} represents multi-path model of transmitter amplifier and d_0 stands for the distance threshold.

B. Select Optimal Path Phase

This paper proposes a distance based energy aware routing algorithm on selected optimal path through GACA, GACA is put forward on the basis of the genetic GA and ACA. The GACA gives full play to their strength, compensates for their shortcomings and greatly improves the efficiency of seeking the optimal solution.

1) GA Algorithm

For the problems to be solved, it is the first thing to generate a population which presents the potential solution set. The population consists of some individuals which are coded through gene. After the generation of the initial population, the better approximate solutions will be generated according to the principle of survival of the fittest and the evolution. In each generation, the individuals are selected according to their fitness in the problem domain and each generation will make a combination crossover and mutation according to genetic operator of nature genetics to produce a population of new solution set. In this process, the population is like a natural evolution whose offspring are more adaptive to the environment than its previous generation. The best individual in the last population can be used as approximate optimal solution of the problem after being decoded [11].

2) ACA Algorithm

The main idea of ACA is to generate a number of ant colonies initially. Each ant is responsible for building a feasible solution or a part of it by path search. At the beginning of the algorithm, the ants are placed at several random initial nodes. Each ant starts from the initial node and chooses the next node in a certain probability according to the pheromone concentration and the heuristic information on the path until a feasible solution is set up. According to the quality of the solution, each ant releases pheromone which is proportional to the quality of the solution. Then, each ant will start a new search until the ant colony finds the global optimal solution [12].

3) GACA Algorithm

The reason of choosing GACA is due to the basic mutation operation is stochastic through the mutation of GA, lacking the use of heuristic information in the search space. GA has a strong ability of global searching. However, it is a fact that it is weak in local search. Ant colony optimization, inspired by the study of the evolutionary ability of the real ants to choose routes, is a distributed and heuristic search algorithm. Ant colony optimization can make full use of local heuristic information through the positive feedback mechanism of pheromones. However, at the initial period of algorithm, it can only use the heuristic information in the path to guide the move of the ants because of lacking pheromones. With the expansion of question scale, other problems, such as longer searching time, slower solution speed and easier convergence at local optimum likely lead to premature convergence.

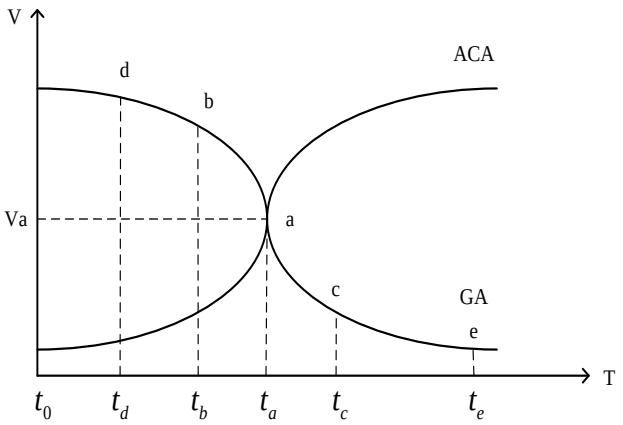


Figure 5. Velocity-time image

In order to overcome their shortcomings, the best way is to combine the two algorithms organically, bringing their advantages to full play. Currently using genetic ant

colony algorithm to solve the NP problems has brought good results [13]. Through the study and experiment of the genetic algorithm and ant colony algorithm, we find that it can be shown in the velocity-time image in Fig. 5 [14].

From the above image it can be seen that the speed of ant colony algorithm to search a problem in the early period ($t_0 - t_a$) is slow and the convergence to the optimal solution significantly won't speed up until the pheromones accumulate to a certain degree (after t_a). Genetic algorithm has a high speed of convergence to the optimal solution at the beginning of the search ($t_0 - t_a$). But after t_a , the efficiency of searching the optimal solution decreases obviously.

In order to overcome their shortcomings, the best way is to combine the two algorithms organically, bringing their advantages to full play. The main idea of the fusion is to take advantage of the rapidity and global convergence of genetic algorithm before the best point (point a) to solve the problem and convert the results into the initial pheromone of ant colony algorithm and then make full use of parallelism, positive feedback mechanism and high problem-solving efficiency of ant colony algorithm to solve the problem. Then the advantages of genetic algorithm and ant colony algorithm are made full use of. The algorithm fused are superior to ant colony algorithm in time efficiency and to genetic algorithm in problem-solving quality, realizing the complementary advantages of both methods and forming a solution with high efficiency and quality. The fused algorithm of genetic algorithm and ant colony algorithm is called Genetic Ant Colony Algorithm, namely GACA.

In order to make full use of the high quality of genetic algorithm at early stage, it is essential to give the stop condition. The genetic control function is defined as (4):

$$G = (\cos t(T(s,u))_m - \cos t(T(s,u))_{m+1}) < 10^{-3} \quad (4)$$

In the formula (4), $(\cos t(T(s,u))_m$ is the cost of the m^{th} iteration. $1 \le m \le M_{\max}$, $M_{\max}$ is the maximum number of iterations of genetic algorithm. When it is in the maximum number of iterations and $G<10^{-3}$, the ant colony algorithm can take the place of genetic algorithm.

As the result of genetic algorithm is the path from the source node to destination node, when used the path information must be converted into pheromone on each path. To ensure the pheromone concentration becomes higher with less cost under the given constraints, we should assume the result of genetic algorithm as path set v, and take the first 20% as initialization pheromone path, by analyzing we get (5):

$$\tau_{ij}(t) = \frac{C}{\cos t(T(s,u)) \times \cos t(v_i, v_j)} \quad (5)$$

In the formula (5), C is a constant and (v_i, v_j) is the adjacent nodes of v . i ,j And n obeys the constraint is $0 \le i, j \le n$. N is the number of network nodes. τ_{ij} processed by superposition method when there are multiple paths spread through (v_i, v_j) in genetic algorithm.

As the load will be balanced under an optimal obtained route, the path selection possibility $s_{i,j}(t)$ for a searching from v_i to v_j the searching period t is defined by (6):

$$s_{i,j}(t) = \frac{[\tau_{ij}(t)]^{\alpha} * [\eta_{ij}(t)]^{\beta}}{\sum_{ij} [\tau_{ij}(t)]^{\alpha} * [\eta_{ij}(t)]^{\beta}} \quad (6)$$

In the formula (6), $\tau_{ij}(t)$ is the density of pheromone accumulated on the path segment (v_i, v_j) by ants in the period t ; $\eta_{ij}(t)$ is the information of searching for that path segment, and is the inverse distance of the arc from v_i to v_j ; $\alpha, \beta > 0$ are called the pheromone index and cost index respectively.

The Implementation of GACA Algorithm in detail:

Step 1: Initialize the network and delete the paths that cannot conduct data communication, namely all the paths under the constraint $d(v_i, v_j) > R$ and the effective communication radius whose wireless network node is R .

Step 2: Describe the problem as WBAN network routing problem, and preprocess it

Step 3: Initialize the genetic parameters

Step 4: Initialize the population according to population initialization method

Step 5: Calculate the individual adaptive value in initial population

Step 6: Set the number of iterations $m = 1$

Step 7: Include the iterative process in genetic algorithm

While $m < M_{\max}$

Use roulette and best individual reserve strategy to select new species

Carry out the single-point crossover operation and mutational operation of species

$m = m + 1$

If $(\cos t(T(s,u))_m - \cos t(T(s,u))_{m+1}) < 10^{-3}$

Break

End while

Step 8: By using the transformation method of initial pheromone value, convert the first 20% of the result of genetic algorithm into the initial pheromone value in the path of ant colony algorithm.

$$Perm = \tau_{ij}(t) = \frac{C}{\cos t(T(s,u)) \times \cos t(v_i, v_j)}$$

Step 9: Initialize the pheromone value on the sensor nodes

$Perm\_node = Perm$

Step 10: Place the ants for searching optimal path

Ants = till the tour complete

Step 11: Initialize the Constant

$\alpha \in [2, 4]$

$\varepsilon_{amp} = \varepsilon_{fs}$ When α =2 and ε_{mp} when α =4

Step 12: Searching an optimal path

If (S_i !=BS)

While p=1 to $p_{\max}$

If (S_i = visited node)

S_i =0

End if

$$s_{i,j}(t)=\frac{[\tau_{ij}(t)]^{\alpha}*[\eta_{ij}(t)]\beta}{\sum_{ij}[\tau_{ij}(t)]^{\alpha}*[\eta_{ij}(t)]\beta}$$

End while

d_i =Active (backward)

Then else

d_i =Active (backward)

Return d_i

End if

Step 13: Calculate optimal distance value

$$d_i = d_{opt} = \sqrt[\alpha]{\frac{2E_{elec}}{\varepsilon_{amp}(\alpha-1)}}$$

Step 14: Neighbors selection

S_i =select (neighbours)

Step 15: Calculate distance from source to neighbors

$d_i = d$ (S, N)

Step 16: Compare optimal distance d_i with d_j

d_{temp} =near (d_i , d (S, N)).energy $\geq$ length

Step 17: Return the optimal path

Return d_{temp}

Anyhow, GACA algorithm can make full use of advantages of both methods and find routings that satisfy the constraints in a relatively short time, thus reducing the transmitting delay and saving much time for multipath routing protocol in choosing the shortest path.

V. Simulations and Analysis

In order to validate the superiority of the proposed routing mechanism which is based on genetic ant colony algorithm (GACA) in routing choice and network cycle, experimental simulations are proposed in this paper. This paper analyzes genetic ant colony algorithm from two aspects of optimal path and shortest time and also compares it with routing mechanisms based on genetic algorithm(GA) and ant colony algorithm(ACA).

A. Network Initialization

Take the practical application of WBAN into consideration, it is assumed that there are 15 data acquisition nodes in the network and their ability of dealing with data is same. According to the network partitioning algorithm, in this paper 15 acquisition nodes are randomly generated in a matrix space of 300*300. The specific distribution of nodes is shown in Fig. 6:

B. Optimal Path

Fig. 7 shows the optimal paths of the three routing mechanisms. It can be seen from the figure that the three shortest paths of GA, ACA and GACA are 1476.8635, 1196.9816, 978.1286. In the experiment, the parameters of genetic algorithm are valued: population size is 500 and maxEvolution is 100. The parameters of ant algorithm are also valued: maximum iteration is 1000, ant-quantity is 8000, and the rate of evaporation is 0.01. It can be seen from the simulation that the shortest path of GACA is significantly less than that of GA and ACA.

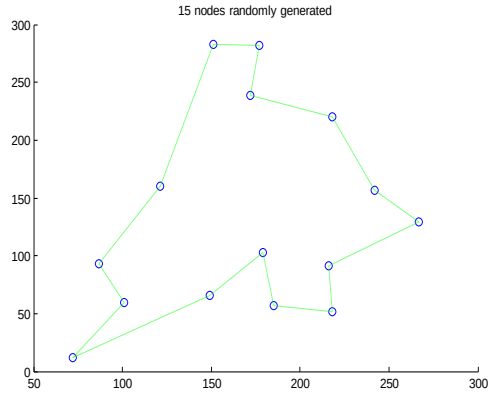


Figure 6. Distribution of network nodes

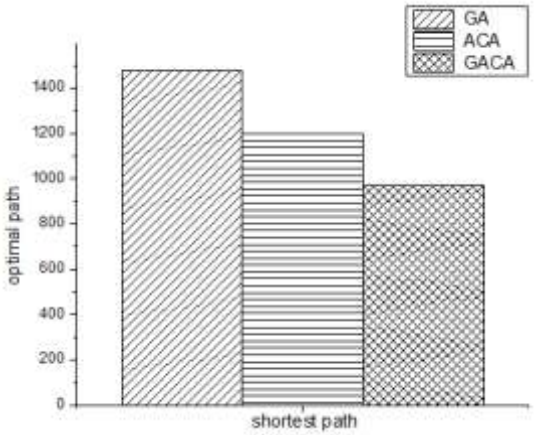


Figure 7. Optimal path contrast

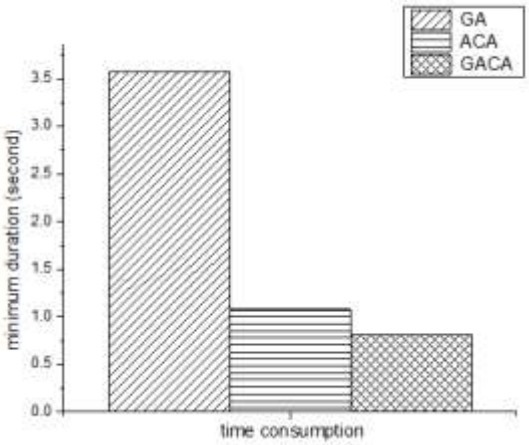


Figure 8. Time consumption contrast

C. Time Consumption

Figure 8 shows the time consumption of the three routing mechanisms in searching for optimal path. GA has rapid global searching ability, but it can't make use of

the feedback information of the system and it has to do a large redundancy repeat for the result. So the efficiency to solve results is reduced. ACA approaches to the optimal path through the accumulation and renewal of information pheromone. It has the ability of parallel processing and global searching. However, in the primary period of searching, information pheromone is of shortage, so the speed is slow and time consumption is large. GACA keeps the advantages and discards the disadvantages of GA and ACA and gains a best result of high efficiency and low time consumption.

VI. Conclusion

This paper proposes An Energy-efficient Routing Mechanism Based on genetic ant colony algorithm for Wireless body area network. In genetic ant colony algorithm, Genetic ant colony algorithm makes full use of genetic algorithm and ant colony algorithm. At the early stage of algorithm, it uses genetic algorithm to generate the initial pheromone distribution quickly and comprehensively, then converts the evolved pheromones distribution to pheromones that can be used by ant colony algorithm and finally uses the positive feedback and high parallelism of the ant colony algorithm to find out the optimal solution. It is the fusion of the two methods, gaining an improvement of both time and quality. Following by a Distance-based Energy Aware Routing algorithm achieved the energy balancing on all the nodes from the source node to base station along the transmission path.

In future work, plans to further stimulation comparison of the three algorithms in order to further illustrate the superiority of the ant colony genetic algorithm between the other two algorithms. To consider its overall performance, we will take some factors such as residual energy, node degree and multi-path routing algorithm into consideration in future research.

Acknowledgment

This work is supported by the Natural Science Foundation of Chongqing (cstc2012jjA40053); The Scientific Research Found of Chongqing University of Posts and Telecommunications (A2012-12); The National Natural Science Foundation of China (Grant No. 61309032), Chongqing Innovative Team Fund for College Development Project (No. KJTD201310) and the Chongqing medical research project (No.2013-1-049).

References

[1] Ehyaie A, Hashemi M, Khadivi P. Using relay network to increase life time in wireless body area sensor networks. *Kos: Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops.* 2009, pp. 1-6.

[2] Wang J, Kim J-U, Shu L, Niu Y, Lee S. A Distance-Based Energy Aware Routing Algorithm for Wireless Sensor Networks. *Sensors*, Vol. 10, No. 10, 2010, pp. 9493-9511.

[3] Ryckaert J, Doncker PD. Channel model for wireless communication around human body. *Electron. Lett.*, Vol. 40, No. 9, 2004, pp. 543-544.

[4] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless sensor networks, *Proc. of the International Conference System Sciences, Hawaii, Jan*. 2000, pp. 1-10.

[5] J. Yang, M. Xu, W. Zhao, B. Xu. A Multipath Routing Protocol Based on Clustering and Ant Colony Optimization for Wireless Sensor Networks, *Sensors* 2010, pp. 4521-4540.

[6] X. Li, L. Xu, H. Wang, J. Song, S. X. Yang. A Differential Evolution-Based Routing Algorithm for Environmental Monitoring Wireless Sensor Networks, *Sensors* 2010, pp. 5425-5442.

[7] W. Youssef, M. Younis. Optimized Asset Planning for Minimizing Latency in Wireless Sensor Networks, *Wireless Networks*, 2010.

[8] H. Yang, F. Ye, B. Sikdar. A Swarm-Intelligence-Based Protocol for Data Acquisition in Networks with Mobile Sinks, *IEEE Trans. on Mobile Computing*, 2008, pp. 931-945.

[9] J. N. Al-Karaki, A. E Kamal. Routing Techniques in Wireless Sensor Networks: A Survey, *IEEE Wireless Communications* 2004, pp. 6-28.

[10] I. J. de Dieu, J. Wang, D. J. Asturias, Young-Koo Lee. EDPPS: An Energy-efficient Data Privacy Protection Scheme for wireless sensor networks, *Computer Sciences and Convergence Information Technology (ICCIT)*, 2010 *5th International Conference on*, 2010, pp. 451-456.

[11] Zhao Y W, Niu Q Y, Wang X C. Study on combination of genetic algorithm and ant algorithm, *Science Technology and Engineering*, Vol. 10, No. 16, 2010, pp. 4017-4020.

[12] X. Jiang, B. Hong. ACO Based Energy-Balance Routing Algorithm for WSNs, *In proceedings of Advances in Swarm Intelligence, LNCS 6145*, 2010, pp. 298-305.

[13] Ding J L, Chen Z Q, Yuan Z Z. On the combination of genetic algorithm and ant algorithm, *Journal of Computer Research and Development*, Vol. 40, No. 9, 2003, pp. 1351-1356.

[14] Xiong ZH, Li SK, Chen JH. Hardware/Software partitioning based on dynamic combination of genetic algorithm and ant algorithm, *Journal of Software*, Vol. 16, No. 4, 2005, pp. 503-512.

GuangXia Xu earned her Ph.D. degree at Chongqing University in 2011. She is an associate professor of the School of Software Engineering at Chongqing University of Posts and Telecommunications. Her current research interests include network security and management control, big data analytics.

ManMan Wang Graduate student of Chongqing University of Posts and Telecommunications. Her research interests include network security and management control, internet of things and body sensor network.

An Improved Mix Transmission Algorithm for Privacy-Preserving

Guangxia Xu
School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
Email: xugx@cqupt.edu.cn

Fuyi Lin and Yu Liu
School of Communication Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
Email: {linfuyi.colin@gmail.com, freefish426@hotmail.com}

***Abstract*—With the rapid development of the internet of things (IOT), personal privacy has been realized as the most important security issue in wireless sensor networks, especially in the Body Area Network (BAN) used in the medical field. Traditional encryption methods cannot defense against the attacks in which the communication signal vector is analyzed in time and space dimensions, while the data is transmitting in the wireless space. Based on the above requirements, an improved security data mix transmission algorithm for medical applications in the BAN is presented in this paper. Combined with the practical application scenarios, this algorithm can realize anonymous privacy protection of data transmission in the transmission process and present better transmission performance by dividing the whole network into many smaller ring networks and generating more tokens in the network. transmission simulations are conducted and the results show the method proposed offers less energy consumption and time delay.**

***Index Terms*—BAN; K-Anonymity; Privacy-Preserving; Data Transmission**

I. INTRODUCTION

The body area network (BAN) is a new type of network which is composed of small wearable or implantable sensors that have the function of detecting physiological data and coordinators that are responsible for store-and-forward data collected. The coordinator is a medium of communication and data exchange between BAN and external network, which could be special equipment or consists of mobile personal server, BAN head, base station, and so on [1,2]. BAN provides the technical motivity for the development of a new generation of health care system, and also provides a broad prospect for the rapid development of e-healthcare [3]. No matter the BAN is for medical or non-medical applications, it must satisfy stringent security and privacy requirements, which are based on different applications from medical to non-medical applications [4]. The openness of wireless channel causes the sensor-based BAN to face with security threats including transmission monitoring and position exposure. The traditional cryptography method is not enough to protect the patient's privacy. Because of BAN's network structure and application scenarios, its privacy protection is particular. Both the existing mature method of content encryption and policy of privacy protection of communication entity are not applied to BANs according to application requirements and operating environment. It has specific privacy requirements such as confidentiality, dependability, integrity, access control and authenticity etc.

The security and privacy protection of user's sensitive information from a BAN has some challenges coming from low-power and resource constrained devices, and high requirement for both security and practicality. The security and privacy of BAN is divided into the privacy of data content and the privacy of data transmission. In this paper, the issues of the privacy of data transmission in BANs are discussed and an improved security data mix transmission algorithm (SDMT) for medical applications in BANs based on fixed token-based k-anonymous transfer mix (FTATM) in [5] is presented. In FTATM, the whole network is a single ring network and there is only one token in the network, those cause a big data delay and a weak transmission performance. Since the operation cycle of single token network is too long, the network should produce more tokens to reduce the data delay and improve the real-time of data. However, this can also increase the load of the whole network and affect performance. The network structure is divided into many smaller ring networks according to k-anonymous condition and another new token with data storage time-limit is generated in SDMT. Combined with the practical application scenarios, this algorithm not only realize anonymous privacy protection of data transmission in the transmission process, but decrease the data delay and power consumption.

The rest of this paper is organized as follows. Section 2 describes security and privacy of data transmission. Sect. 3 states application scenarios and transmission privacy attacks. Sect. 4 introduces our mix transmission algorithm. Section 5 presents simulation results. Section 6 concludes this paper.

doi:10.4304/jnw.9.12.3373-3380

II. Related Work

The privacy and security of the data transmission means adversary does not need to get the content of encrypted messages in transmission, but acquires privacy information of both transmission parties in another ways. In BANs, wireless communication environment is vulnerable to be attacked. Adversarys can acquire user's other privacy except data content by probing the position of the nodes that send data packages, the time of receiving and sending data, the flow direction of data traffic in the network and corresponding relationship of services between communication parties.

In [6], the routing problems of source location privacy in the sensitive target monitoring network and the "panda-hunter" model and the phantom routing protocol is studied in the privacy of the user transmission mode. In [7], a deep analysis of oriented random technology in phantom routing protocol, and a random walk protocol that made neighbors of a node adjust themselves according to coordinate quadrant is proposed. However, the essence of phantom routing protocol is used in homogeneous network of distributed nodes. This protocol is not suitable for the problem of privacy protection under the circumstances of BANs. In [8], a message preemptive sending method which could reduce the delay in the light of the length of sending queue time is studied in timing privacy issues. In [9], a statistical anonymous protection method is presented and made the traffic randomly generated according to the probability distribution when nodes generate data. However, the overhead of this method is too high. In [10], period collection and source simulation to protect privacy of source nodes are proposed, but the problem is that traffic will be larger and real-time property is not high.

III. System Model

A. Scenario Assumption

In the application of disease monitoring in the hospital, the different floor sets many wards of different department. According to actual requirement, the physiological parameters of every patient in the ward could be collected by small wearable or implantable sensors. Due to the limitation of data transmission distance and the processing capability of sensors, every department ward or several wards need a cluster-head node to collect and forward the data within its communication range. For the upper network of medical applications, it may be provide a way to access remote data for external people like family members of the patient and medical researchers. The patient's medical data may be viewed by patient, doctors, nurses, family members and government staffs. In such case, the patients do not want their personal information or communication relationship between themselves and doctors to be known by outside world. That is because the patient's disease or other privacy information may be deduced by adversarys. In the similar scenario of BANs, the deployment architecture of the general BAN is shown in Fig. 1.

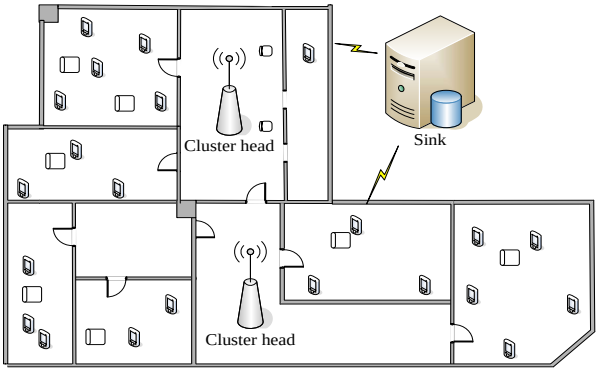


Figure 1. The typical application model of BANs

B. The Definition of Model

For the above analysis of the scenario, the network structure is assumed to divide into three-layer architecture. According to the hierarchical architecture, the base stations of the hospital data center are in the first layer of the network and responsible for aggregating, storing, and handling user data collected in the network. As a transmission intermediary between the lower-layer network and the upper-layer network, the cluster-head nodes are in the second layer of network. All the sensors deployed on the patients' body to collect physiological information are in the third layer of the network. This hierarchical architecture meets the need of the practical application and could expand more levels based on the practical application. The network structure is described as below:

This hierarchical scenario is assumed to has M sensor nodes $S=\{s_1,s_2,\cdots s_M\}$ to collect physiological information of users. The nodes are divided into N clusters $C=\{c_1,c_2,\cdots c_N\}$ according to automatic or scheduled clustering method. $|c_i|$ means the number of sensor nodes of cluster c_i, $M \gg N$. And there are N cluster-head nodes $CH=\{ch_1,ch_2,\cdots ch_N\}$ in the second layer.

The data sent from sensor nodes to cluster-head node is defined as $r=\{r_1,r_2,\cdots r_M\}$, $r_i=r(s_i,t), i\in M$, that is, the data r is sent by each sensor node s_i at certain time t. The data set stored in the cluster-head node is $R=\{R_1,R_2,\cdots R_N\}$, $R_i=\bigcup_{j=1}^{|R_i|} r_j$. $|R_i|$ means the number of data contained by the data set. Maybe R stores the same or different data $r=\{r_1,r_2,\cdots r_M\}$ sent by several sensor nodes $S=\{s_1,s_2,\cdots s_M\}$ at different sampling time.

C. Transmission Privacy Attacks

The attack behavior on transmission privacy is not the initiative attack of damaging or decrypting encrypted data and inserting data flag, but uses statistical methods on the nodes within the entire system to divide time or space by analyzing the time of transmitting data or data transmission frequency. The attack behavior ought to be

"external", "passive" and "variable" [11]. This paper has considered two kinds of privacy threats, which are shown as below:

One is the time-correlated attack according to the correlation of sending and receiving data [12]. Adversary can acquire the time sequence of the data sent from the partial or all nodes by monitoring for a long time, and can find high probabilistic correlated time of sending and receiving data in the time sequence. Therefore, the corresponding relation of both communication parties has been cracked.

The other one is the linking attack, which adds context information obtained occasionally into the attack to guess the identity of the sender with a certain probability. With the increasing development of the attack's ability and based on the feature of distributed deployment of the BAN, the attack pattern is not limited to all kinds of privacy attack on the partial nodes, but is the attack on the node position of the entire network and the eigenvector of the data transmission behavior [13]. Adversary maybe also capture the data set in the process of transmission with a probability and use the linking attack to crack the data set, and verify the result through context knowledge [14].

D. Loose Cluster Network

If the number of the clusters and the nodes in the cluster is small (less than k), the overall structure of the network becomes a typical distributed network that is called the loose cluster network. This is also the most popular and common type of networks in the practical application. At this time, the monitoring targets of adversary may be turned to several or a single node-cluster in the BAN from monitoring the entire nodes of the network and data transmission. Because the number of adversary's target nodes could be decreased to the number of nodes in the cluster ($|c_i| \ll K$), even if adversary obtains the communication relationship between the senders and receivers without analyzing the transmission time and the transmission rate of the data, the privacy security cannot reach the requirement of k-anonymity. Therefore, the number of the data is needed to increase in the anonymous set in order to meet the requirement of k-anonymity. According to the above division of the network model, the data set stored in N cluster-head nodes is $R=\{R_1,R_2,\cdots R_N\}$. For the special cluster-head node CH_α that has stored data set R_α , and the probability that the corresponding sender may be guessed is (1):

$$P=\{p \mid p=\frac{1}{|R_\alpha|}>\frac{1}{k}\} \tag{1}$$

Since the number of nodes in the cluster C_α is less than k , the minimum of the probability of guessing the communication relationship between the data and its sending node is more than $1/k$. And this cannot achieve the purpose of privacy protection.

IV. PROPOSED APPROACH

A. Basic Principle of Algorithm

If the network structure belongs to the loose cluster and the probability of gaining the relationship between the data within the cluster and its sender should be reduced. In this paper, this algorithm refers to the thought of the Mix communication to make mix transmission operation with the data stored in the cluster-head node and other cluster-head nodes. Then it forms a token of data set matched the condition of k-anonymity in a single cluster-head node that can transfer and mix data to reduce the probability of gaining the relationship between data and its sender.

When the network is set up initially, the attacking probability matrix can be expressed in (2).

$$\begin{aligned}\mathbf{\Lambda}(0)&=\begin{bmatrix}\theta_1P_{11}(0) & \theta_1P_{12}(0) & \cdots & \theta_1P_{1N}(0)\\ \theta_2P_{21}(0) & \theta_2P_{22}(0) & \cdots & \theta_2P_{2N}(0)\\ \vdots & \vdots & \vdots & \vdots\\ \theta_NP_{N1}(0) & \theta_NP_{N2}(0) & \cdots & \theta_NP_{NN}(0)\end{bmatrix}\\ &=\begin{bmatrix}\frac{1}{|R_1|} & \cdots & 0 & 0 & \cdots & 0\\ \vdots & \ddots & 0 & 0 & \vdots & \vdots\\ 0 & 0 & \frac{1}{|R_a|} & 0 & 0 & 0\\ 0 & 0 & 0 & \frac{1}{|R_b|} & 0 & 0\\ \vdots & \vdots & 0 & 0 & \ddots & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & \frac{1}{|R_N|}\end{bmatrix}\end{aligned} \tag{2}$$

In the probability $\theta_xP_{xy}(t)$, P_{xy} represents the probability of guessing sender of the data in set y from data set x . θ_x is a parameter, when data set x is empty, θ_x would be set to 0, or else θ_x would be set to 1. Parameter t represents a specific point in time and is set to 0.

When x data in R_b has transferred to R_a , the probability vector P_{R_α} turns into (3)

$$\begin{aligned}P_{R_a}&=[\theta_aP_{a1},\cdots\theta_aP_{aa},\cdots\theta_aP_{ab},\cdots\theta_aP_{an}]=\\ &\left[0,\cdots\frac{|R_a|}{|R_a|+x}\bullet\frac{1}{|R_a|},\cdots\frac{x}{|R_a|+x}\bullet\frac{1}{|R_b|},\cdots0\right]\end{aligned} \tag{3}$$

But the data set R_b remains the same in (4).

$$\begin{aligned}P_{R_b}&=[\theta_bP_{b1},\cdots\theta_bP_{ba},\cdots\theta_bP_{bb},\cdots\theta_bP_{bn}]\\ &=\left[0,\cdots0,\cdots\frac{1}{|R_b|},\cdots0\right]\end{aligned} \tag{4}$$

When the number of transferred data is $|R_b|$, means all the data in the data set R_b was transferred to R_a. Its probability vector can reach the minimum in (5).

$$\begin{aligned} P_{R_a} &= [\theta_a P_{a1}, \cdots \theta_a P_{aa}, \cdots \theta_a P_{ab}, \cdots \theta_a P_{an}] \\ &= \left[0, \cdots \frac{1}{|R_a|+|R_b|}, \cdots \frac{1}{|R_a|+|R_b|}, \cdots 0 \right] \end{aligned} \tag{5}$$

At this time all the data in c_b has transferred to c_a, so $\theta_b = 0$ in (6).

$$\begin{aligned} P_{R_b} &= [\theta_b P_{b1}, \cdots \theta_b P_{ba}, \cdots \theta_b P_{bb}, \cdots \theta_b P_{bn}] \\ &= [0, \cdots 0, \cdots 0, \cdots 0] \end{aligned} \tag{6}$$

After the data set $R = \{R_1, R_2, \cdots R_y\}$ among y cluster-head nodes $C = \{c_1, c_2, \cdots c_y \mid |c_1| + |c_2| + \cdots |c_y| \geq K\}$ has been mixed. It makes sure certain cluster-head node's data set $R_i (i \in [1, y])$ has at least one data from each one of k sensor nodes. The probability in the attacked matrix $\Lambda(t)$ with the relationship between the data in the mixed data set and its source node reaches the minimum, that is $1/k$. For its probability has already reached a minimum, since then, any data mixed operation between the data set $R = \{R_1, R_2, \cdots R_y\}$ of the y cluster-head nodes and the mixed each data set $R_i (i \in [1, y])$ will not affect its probability.

When a data set can make each probability vector in the probability matrix with k-anonymous privacy requirements, means in $\Lambda(t)$ any xy is satisfied with (7).

$$\theta_x P_{xy} \leq \frac{1}{k} \tag{7}$$

The probability of guessing any data's source sender is not more than $1/k$. This data set meets the k-anonymous condition.

B. Network Segmentation

For the data trasferring between the cluster nodes is still in an open wireless channel. The data transmission process between the cluster-head nodes is vulnerable to be attacked. So it should make sure that the data transmission process between the cluster-head nodes also can meet the k-anonymous requirements. And transmitting the data set which meets the k-anonymity as a token between the cluster-head nodes in order to ensure data's privacy security.

Considering the requirements of life cycle, energy consumption and data delay in BANs, it may take a lot of time to mix data between cluster-head nodes in the whole network. To produce more data tokens also make network operation more complex. Therefore, considering the actual situation demands, the network structure is divided into many smaller networks with k-anonymous condition according to privacy intensity k of user's requirement. It can meet the needs of the anonymous privacy protection, and at the same time can effectively reduce the data transmission delay and the energy consumption which is caused by transmission of many tokens between the cluster-head nodes. When dividing those nodes in the network, the minimal number of sensor nodes is needed to be k. At the same time the distance between the cluster-head nodes should be shortest, so the network transmission cost will be lower, and the data transmission delay will be reduced. For the divided small ring network, the transmission delay will be lower.

The division of network topology is on the basis of the mathematical model of the multiple traveling salesmen problem (MTSP). In our network it can be expressed as many data tokens sent in the ring network with k-anonymous condition. Each data token starts from any cluster-head node, passes by a number of cluster-head nodes, and finally returns to their starting node. At the same time, there is no overlap between the nodes. The transmission process also should make the node distance as short as possible. The network segmentation algorithm is shown in Table I.

TABLE I. NETWORK SEGMENTATION PROCESS

Algorithm 1:Networks division based on MTSP	
Input: network topology of BSN cluster heads $C = \{c_1, c_2, \cdots c_N\}$	
Output: divided network topology loop $\{L_1, L_2, \cdots L_i\}, (L_1 + L_2 \cdots + L_i = C)$	
1.	Initialize the populations, generate random population of possible routes popRoute[popSize]=randperm(n), generate population of possible breaks popBreak[popSize]= rand_breaks().
2.	Generate possible solutions by popRoute and popBreak.
3.	Calculate total nodes number N_i of each population members.
4.	If $N_i \geq k$, select the solutions.
5.	Else eliminate the solutions.
6.	Calculate distance of each population member to evaluate fitness.
7.	Find the best route in the population (select the shortest route).
8.	Generate new random set of possible breaks.
9.	Generate new solutions of possible routes by (Genetic algorithm operators which include Flip, Swap and Slide etc.)
10.	If number of desired iterations numIter<1500 GOTO Step2.
11.	End

The genetic algorithm will be used to calculate the approximate solution of the network division problem. Genetic algorithm finds out the optimal solution of problem by means of natural selection and genetic mechanism. The algorithm finds out the solution to the problem starting from the solution set of the problem and processes the individual solution in multiple groups at the same time so that it is conducive to searching for the global optimal solution. The algorithm is performed by the computer of medical data center. The lower-layer nodes do not need to participate in network segmentation. Firstly, to store the cluster-head nodes in the routing-array after disrupting the order of cluster-head nodes. Then, to generate the breakpoint array randomly. Inserting the nodes in the possible path corresponding to each population of breakpoint can form a possible

solution. Every solution will be measured if it meets the condition $N_i \geq k$ after generating all the solutions. We evaluate the solution and select the solution which includes the shortest path. Next, new solutions will be generated by changing the breakpoint and path again and again until we get the optimal sulution.

C. The Generation of K-anonymous Token

According to instruction in the previous section, the data center divides the network. In the divided small ring network, the data center sends the divided network topologies to the cluster-head nodes in each divided network. After the divided small ring network receives the network topology, the cluster-head nodes began to produce the k-anonymous data token. The generation of k-anonymous token is shown in Table II.

TABLE II. THE GENERATION OF K-ANONYMOUS TOKEN

Algorithm 2:Token Generation based on divided networks
Input: divided network topology loop L_i
Output: Token $\mathrm{T}_i(\mathrm{t\_born})$ in L_i
1. for random cluster head $CH_i \in L_i$ generate initial Token $\mathrm{T}_{ini}(\mathrm{t\_born})$ do
2. if $\lvert T_i \rvert \leq k$
3. if $R_i \neq \varnothing$ then $\mathrm{T}_{ini}(\mathrm{t\_born}) = \mathrm{T}_{ini}(\mathrm{t\_born}) + r_i$ ($r_i \in R_i, i \in [1, \lvert c_i \rvert]$)
4. send $\mathrm{T}_{ini}(\mathrm{t\_born})$ to next $CH_{i+1} \in L_i$
5. wait for t_ack timeout
6. wait for time-limit timeout
7. if t_ack timeout resend $\mathrm{T}_{ini}(\mathrm{t\_born})$
8. else delete $\mathrm{T}_{ini}(\mathrm{t\_born})$ in CH_i
9. end if
10. if time-limit timeout
11. generate a new token $\mathrm{T}_{ini}(\mathrm{t\_born})$
12. end if
13. end if
14. else $\lvert T_i \rvert \geq k$
15. turn to $\mathrm{T}_i(\mathrm{t\_born})$
16. end if
17. end for

As described in the algorithm, in each divided small ring network, there is no data in the k-anonymous token $\mathrm{T}_{ini}(\mathrm{t\_born})$ that is initiated by any cluster-head node $CH_i \in L_i$. Then initiated $\mathrm{T}_{ini}(\mathrm{t\_born})$ could collect the data sent by the sensor nodes in R_i. Next, the cluster-head node sends the token to the next one in the ring network, and waits for *ACK* message to confirm the token has been received. After the next cluster node CH_{i+1} receives the k-anonymous token, it will judge whether the data number reaches k first. If not, it will continue to add the cluster-head's data to the token until the data in the token include at least k different data sent by each sensor nodes. Therefore, the token that meets the k-anonymous condition can be transformed in the network. **A** data storage time-limit $T.storage$ is set. If there is not another token arriving the cluster-head node after forwarding a token over the $T.storage$, it would generate a new token to mix data.

D. Data Mixed Transmission

After generating the k-anonymous data token that can run in the ring network successfully, the network enters into a data security mixed transmission phrase. Each k-anonymous data token in the divided small ring network continues to do mixed anonymous operation with the data received by the cluster-head nodes. The k-anonymous data set token produced by generating algorithm has met the k-anonymous requirements. The probability in the attacking matrix has reached the minimum. Mix operation in any subset within the network with $\mathrm{T}_i(\mathrm{t\_born})$ could not affect the probability in the attacking matrix. When all the data in the data set transfers to $\mathrm{T}_i(\mathrm{t\_born})$, the probability has been reached minimum. The data mixed transmission process is as shown in Fig. 2.

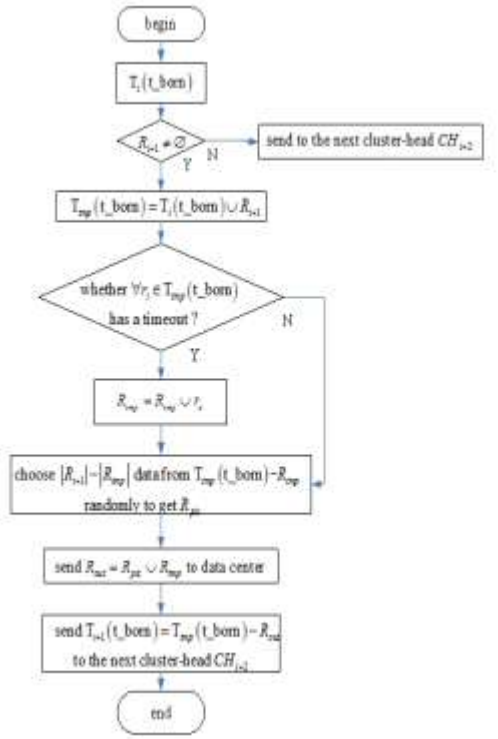


Figure 2. Data mixed transmission process

When the token $\mathrm{T}_i(\mathrm{t\_born})$ arrives the cluster-head node CH_{i+1}, the cluster-head detects whether its cache is empty. If it is null, the token is sent to the next cluster-head node CH_{i+2} in the ring. If not, the data mixed process is started. The cluster-head mixes token $\mathrm{T}_i(\mathrm{t\_born})$ with data R_{i+1} in the cluster node and gets a temporary token. Then it judges all the data $r_i \in \mathrm{T}_{tmp}(\mathrm{t\_born})$ in the temporary token whether its data transmitting time $r_i.transmit$ is longer than the tolerate delay T_{delay}. T_{delay} is set to prevent the physiological data collected by the nodes from not being sent to the medical data center. All the data surpass the tolerate delay will add to the overtime data set $R_{tmp} = R_{tmp} \cup r_x$. When all the

data check is completed, it selects $\left|R_{pic}\right|=\left|\mathrm{T}_{tmp}\left(\mathrm{t\_born}\right)\right|-\left|R_{tmp}\right|-K$ data from the temporary token randomly and get the data set R_{pic}.

Then the node sends the data set $R_{out}=R_{pic}\cup R_{tmp}$ to the data center. The R_{out} meets the k-anonymous requirements through data mix. After mix transmission, the new k-anonymous data token $\mathrm{T}_{i+1}\left(\mathrm{t\_born}\right)=\mathrm{T}_{tmp}\left(\mathrm{t\_born}\right)-R_{out}$ will be sent to the next cluster-head node CH_{i+2} in the ring. And network continues to carry out the operation of security data mix transmission. The pseudo-code of security data mix operation is as Table III.

TABLE III. DATA MIX TRANSMISSION

Algorithm 3:Data mix and transmit based on Token	
Input: Token $\mathrm{T}_i\left(\mathrm{t\_born}\right)$ in L_i	
Output: Data set R_{out} and Token $\mathrm{T}_{i+1}\left(\mathrm{t\_born}\right)$ in L_i	
1.	for cluster head $CH_{i+1}\in L_i$ received Token $\mathrm{T}_i\left(\mathrm{t\_born}\right)$ do
2.	if $R_{i+1}\neq\varnothing$
3.	$\mathrm{T}_{tmp}\left(\mathrm{t\_born}\right)=\mathrm{T}_i\left(\mathrm{t\_born}\right)\cup R_{i+1}$
4.	for x=1 to $k+\left\|R_{i+1}\right\|$
5.	if data $r_x.transmit\geq T_{delay}$
6.	$R_{tmp}=R_{tmp}\cup r_x$
7.	end if
8.	end for
9.	R_{pic} =random pick from $\mathrm{T}_{tmp}\left(\mathrm{t\_born}\right)$, $\left\|R_{pic}\right\|=\left\|\mathrm{T}_{tmp}\left(\mathrm{t\_born}\right)\right\|-\left\|R_{tmp}\right\|-K$
10.	send $R_{out}=R_{pic}\cup R_{tmp}$ to base station
11.	send $\mathrm{T}_{i+1}\left(\mathrm{t\_born}\right)=\mathrm{T}_{tmp}\left(\mathrm{t\_born}\right)-R_{out}$ to cluster head $CH_{i+2}\in L_i$
12.	else send $\mathrm{T}_{i+1}\left(\mathrm{t\_born}\right)=\mathrm{T}_i\left(\mathrm{t\_born}\right)$ to next $CH_{i+2}\in L_i$
13.	wait for t_ack timeout
14.	if t_ack timeout resend $\mathrm{T}_{i+1}\left(\mathrm{t\_born}\right)$
15.	else delete $\mathrm{T}_{i+1}\left(\mathrm{t\_born}\right)$ in CH_{i+1}
16.	end if
17.	end if
18.	end for

V. SIMULATION

A. Simulation Scenario

The algorithm for security data mix transmission based on k-anonymity (SDMT) proposed above is simulated by using the Omnet++. In order to compare the performance of the algorithm conveniently, the following scene is considered:

A certain medical institution deploys the network of BAN. Each ward deploys 20 cluster-head nodes. According to the network segmentation process of the algorithm, the medical data center divides the network into several small ring networks. The deployment of cluster nodes is generated random. The anonymous requirement of users' k is 50. The distribution of nodes and the division of the network is shown in Fig. 3. The FTATM algorithm proposed by Xice is shown and compared to the algorithm proposed by this paper. The network topology of the node distribution of FTATM is shown in Fig. 4.

In this paper, the structure and distribution of the network can be expanded and changed at any time in demand. The number of sensor nodes in each cluster subjects to random distribution [15, 25]. Because the distance between nodes can affect the time of data transmission, the delay of data transmission between cluster-head nodes is considered to subject to random distribution [0.5s-2s] and its value is decided by the size of the two-dimensional space between cluster-head nodes. Because the BAN has requirements of periodicity and real-time of the patients' data collection, the data acquisition cycle of the sensor nodes is assumed to be 0.3s. If the delay of the data is too long in the process of transmission, the useful value of the data will drop. Therefore, the longest delay tolerant time is assumed to be 20s after the data has generated from sensor nodes and data storage time-limit of every cluster-head node is 10s.

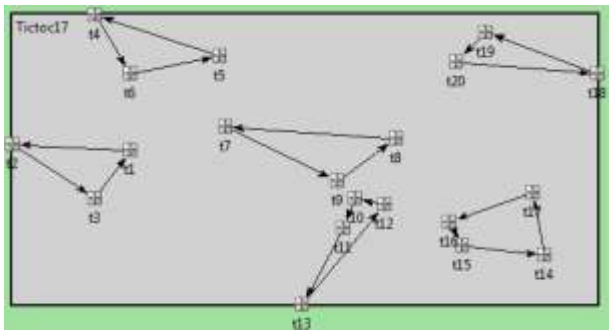


Figure 3. The division of the network

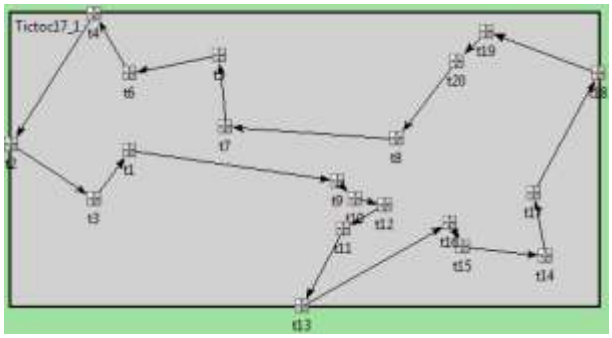


Figure 4. The network topology of FTATM

B. The Contrast of Network Parameters

The SDMT has divided the network topology. This division not only reduces the transmission delay of the token, but also reduces the energy consumption of message transmission and increase the executive efficiency of the network. As shown in Fig. 5, the total communication distance of SDMT between nodes is 18.7081, but the total communication distance of FTATM is 30.1733. SDMT has saved 30% of the communication distance, and also reduced the energy consumption of communication.

As shown in Fig. 6, the token transmission is faster in the divided small ring network of SDMT, so the network has not generated extra token and the number of tokens is stable. However, the number of tokens of FTATM is lower at the beginning, so the network has generated

extra tokens with the increment of the number of data stored in the nodes.

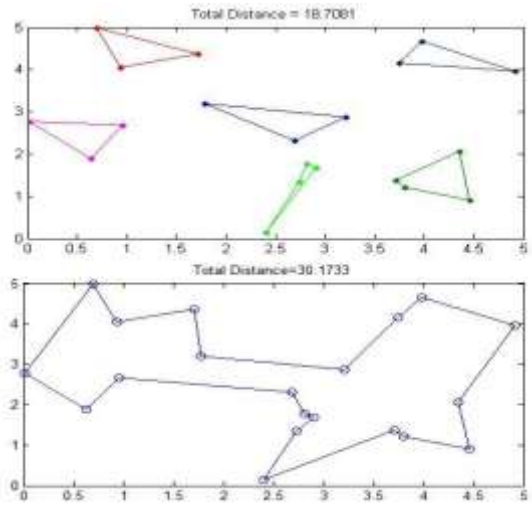


Figure 5. The comparison of the total distance of the communication

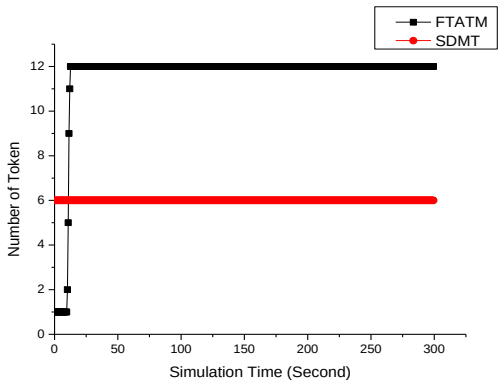


Figure 6. The comparison of the number of tokens

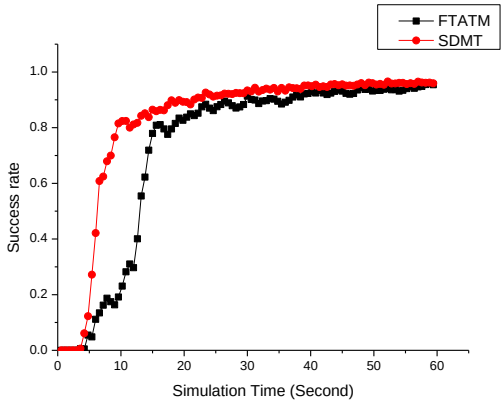


Figure 7. The success rate of data transmission

C. The Success Rate of Data Transmission

The ratio of the number of messages sent successfully to the base station and the number of messages collected by sensor nodes at the same time is defined as the successful transmission rate of the data. As shown in Fig. 7, the success rate of data transmission of FTATM rises slowly, and reaches 100% almost in 60s. The success rate of data transmission of SDMT rises fast to 80% in about 7s and is higher than FTATM later. This is because SDMT has generated 6 tokens according to the divided network. More data has been transmitted successfully. However, FTATM has only one token in the network after the initialization has finished, then generates more tokens gradually when the stored data has time out.

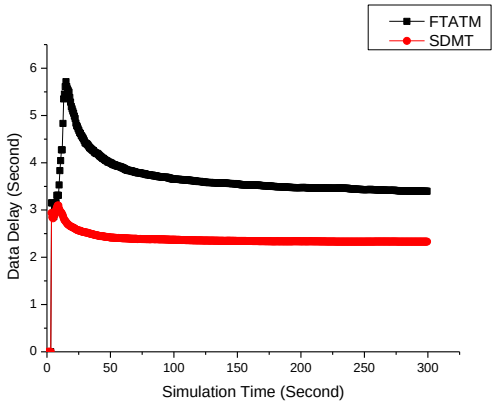


Figure 8. The average arrival delay

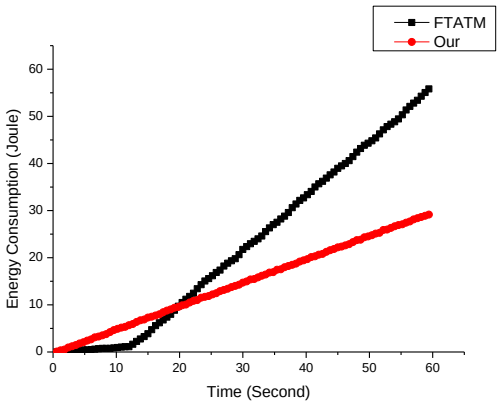


Figure 9. The average energy consumption

D. The Data Delay

The ratio of the sum of all the messages delay and the number of data sent to the base station is defined as the average arrival time. As shown in Fig. 8, both of the two programs have not sent any data to the base station in the first 4s. After 4s, the average arrival time of SDMT is not high. Because the network topology of FTATM is big, the average arrival time rapidly rises. When the network has generated more anonymous data token, the rate decreased gradually but is always higher than SDMT.

E. Energy Consumption

The ratio of the energy consumption of all the cluster-head nodes in the transmission process and the total number of the cluster-head nodes is defined as the average energy consumption of nodes. As shown in Fig. 9, the average energy consumption of SDMT rises gently. However, the average energy consumption of FTATM is low when the number of tokens is small, and with the

increment of the number of tokens, the energy consumption rises faster than SDMT.

VI. Conclusion

This paper has researched the method of protecting the security and privacy of data transmission, which is applied to the structure of BANs under the circumstance of traditional protection of the data content. The technology of privacy protection and typical network structure are analyzed, and the algorithm for security data mix transmission based on k-anonymous privacy protection and mix anonymous communication is proposed. This algorithm aims to protect the privacy of data transmission and prevent adversary acquiring use's other privacy except data content. In this algorithm, the network structure is divided into many smaller networks of meeting k-anonymous condition in order to reduce the data transmission delay and the energy consumption. The simulated results show that the performance of our algorithm is better than FTATM.

Acknowledgment

This work was supported by the National Natural Science Foundation (Grant No. 61309032), Project Supported by Program for Innovation Team Building at Institutions of Higher Education in Chongqing (Grant No. KJTD201310), the Natural Science Foundation of Chongqing (Grant No. cstc2012jjA40053). the Chongqing Medical Research Project (Grant No. 2013-1-049) and the Scientific Research Fund of Chongqing University of Posts and Telecommunications (Grant No. A2012-12).

References

[1] S. L. Chen, H. Y. Lee, C. A. Chen, C. C. Lin and C. H. Luo, "A wireless body sensor network system for healthcare monitoring application," *Biomedical Circuits and Systems Conference*, 2007, pp. 243-246.

[2] C. S. Jang, D. G. Lee and J. W. Han, "A proposal of security framework for wireless body area network," *Security Technology*, 2008, pp. 202-205.

[3] L. Yu, Y. Lu, X. L. Zhu and L. Feng, "Research advances on technology of internet of things in medical domain," *Application Research of Computers*, vol. 29, no. 01, 2012, pp. 1-7.

[4] Saleem, Shahnaz, S. Ullah, and H. S. Yoo, "On the security issues in wireless body area networks," *Digital Content Technol*, 2009, pp. 178-184.

[5] X. C. Sun, "Distributed privacy-preserving techniques for business-driven wireless sensor network," *University of Zhejiang*, Zhejiang, China, 2010.

[6] P. Kamat, W. Y. Xu and W. Trappe, "Enhancing source location privacy in sensor network routing," *Distributed Computing Systems*, 2005, pp. 599-608.

[7] L. Zhang, "A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing," *International Conference on Wireless Communications and Mobile Computing* - IWCMC, 2006, pp. 33-38.

[8] P. Kamat, W. Y. Xu, W. Trappe and Y. Y Zhang, "Temporal privacy in wireless sensor networks: theory and practice," *ACM Transactions on Sensor Networks*, vol. 5, no. 4, 2009, pp. 1-24.

[9] M. Shao, Y. Yang, S. C. Zhu and G. H. Cao, "Towards statistically strong source anonymity for sensor networks," *IEEE INFOCOM*, 2008, pp. 51-55.

[10] K. Mehta, D. G. Liu and M. Wright, "Location privacy in sensor networks against a global eavesdropper," *International Conference on Network Protocols* – ICNP, 2007, pp. 314-323.

[11] R. Doomun, T. Hayajneh, P. Krishnamurthy, and D. Tipper, "Source and destination seclusion using clouds for wireless ad hoc networks," *IEEE Symposium on Computers and Communications*, 2009, pp. 361- 367.

[12] R. V. Boppana and P. Pan, "Source capture time analysis of privacy communication protocols for wireless sensor networks," *Tech. Rep. CS-TR-2010-007*, CS Department, UT San Antonio, Texas, USA, 2010.

[13] Y. Yang, S. C. Zhu, G. H. Cao and T. LaPorta, "An active global attack model for sensor source location privacy: analysis and countermeasures," *Security and Privacy in Communication Networks*, vol. 19, 2009, pp. 373-393.

[14] S. Kokalj-Filipovic, F. Le Fessant, and P. Spasojevic, "The quality of source location protection in globally attacked sensor networks," *Pervasive Computing and Communications Workshops*, 2011, pp. 44-49.

Guangxia Xu earned her Ph.D. degree at Chongqing University in 2011. She is an associate professor of the School of Software Engineering at Chongqing University of Posts and Telecommunications. Her current research interests include dependable computing, distributed systems, security of wireless network and flash memory.

Fuyi Lin Graduate student of Chongqing University of Posts and Telecommunications. His research interests include security of wireless sensor network, internet of things and body sensor network.

Yu Liu Graduate student of Chongqing University of Posts and Telecommunications. His research interests include security of wireless network, internet of things and body sensor network.

Study of Downlink Scheduling Algorithms in LTE Networks

S. Fouziya Sulthana and R. Nakkeeran
Department of Electronics Engineering, School of Engineering and Technology, Pondicherry University, Puducherry-605014, India
Email: fouziya@pec.edu, nakkeeranpu@gmail.com

***Abstract*—Long Term Evolution (LTE) is one of the fastest growing technologies which supports variety of applications like video conferencing, video streaming, VoIP, file transfer, web browsing etc. In order to support multiple applications, Radio Resource Management (RRM) procedure is one of the key design roles for improving the system performance. LTE system effectively utilizes the resources by dynamically scheduling the users in both frequency and time domain. However, scheduling algorithms are not defined in the Third Generation Partnership Project (3GPP) specifications. Therefore, it becomes one of the special interests for service providers. In this paper a study of downlink scheduling algorithms present in the literature is put forth and performance evaluation of four algorithms proposed for LTE downlink is carried out. This paper also discusses the key issues of scheduling algorithms to be considered for future traffic requirements.**

***Index Terms*—LTE; Resource Allocation; Scheduling**

I. Introduction

The emerging applications with different throughput, delay, Packet Loss Rate (PLR) and bandwidth requirements emphasize the need of a network capable of supporting range of services. To fulfil this need Long Term Evolution (LTE) was introduced by Third Generation Partnership Project (3GPP) [1]. The main objective of the LTE network is to enhance the data rate so as to provide the radio resources for variety of highly demanded services, while taking into consideration a satisfied level of Quality-of-Service (QoS) to all active users. For this requirement, LTE system uses Orthogonal Frequency Division Multiple Access (OFDMA) technology in the Downlink (DL) and Single Carrier-Frequency Division Multiple Access (SC-FDMA) in the Uplink (UL). The OFDMA technology divides the available bandwidth into multiple sub-carriers and allocates a group of sub-carriers to a user based on its QoS requirements. Hence, the design of efficient resource allocation algorithm is important for effective use of radio resources to meet the system performance targets.

Packet scheduler at radio base station (evolved Node B (eNB) in LTE specification) is in charge of assigning portions of spectrum shared among users. The performance of the network can differ according to the algorithms used for scheduler. Designing an effective scheduler is therefore an important task in order to differentiate the performance of one wireless system from another. The packet scheduler in LTE aims to maximize the spectral efficiency and makes the negative impact of channel quality drops into negligible [2].

Several packet scheduling algorithms are proposed to support the increasing traffics. In this paper, the key design aspect of LTE scheduling and the performance analysis of four existing algorithms are given. The rest of the paper is organised as follows: In section II, the overview of LTE network is given. Radio Resource Management (RRM) concepts and different scheduling algorithms for LTE downlink is discussed in section III. In section IV, performance analysis of different algorithms is carried out, the future challenges of LTE are given in section V and conclusion is given in section VI.

II. Overview of LTE Network

In order to support wide variety of applications, LTE network is designed with challenging requirements that overtakes the features of 3G networks mainly designed for voice services [1]. LTE network provides spectrum flexibility where the transmission bandwidth can be selected between 1.4 MHz and 20 MHz depending on the available spectrum. The peak data rate, which is the important parameter by which different technologies are usually compared, generally depends on the amount of spectrum used. The allowed peak data rate for the DL and UL is equal to 100 Mbps and 50 Mbps respectively. LTE targets to provide spectral efficiency two to four times better than 3G systems (15 bps/Hz in DL and 3.75 bps/Hz in UL).

LTE is flat, Internet Protocol (IP) based architecture with respect to the previous 3G systems [3]. In previous system, separate Radio Access Network (RAN) that consists of Radio Resource Control (RRC), Radio Link Control (RLC) and Medium Access Control (MAC) protocols is used to interface with User Equipment (UE). But in LTE, eNB takes care of the above mentioned protocol functions. So it requires lesser number of nodes that reduces the system latency and improves overall performance [4]. The network architecture of LTE consists of core network called Evolved Packet Core (EPC) and access network called Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) as shown in Fig. 1.

doi:10.4304/jnw.9.12.3381-3391

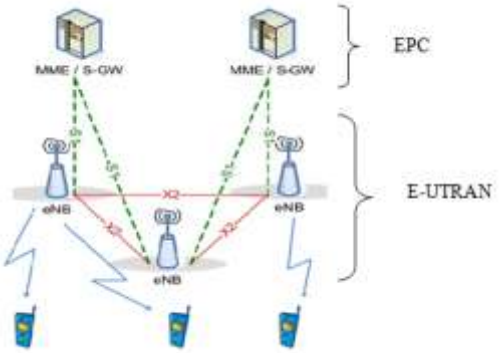


Figure 1. System architecture of E-UTRAN [1]

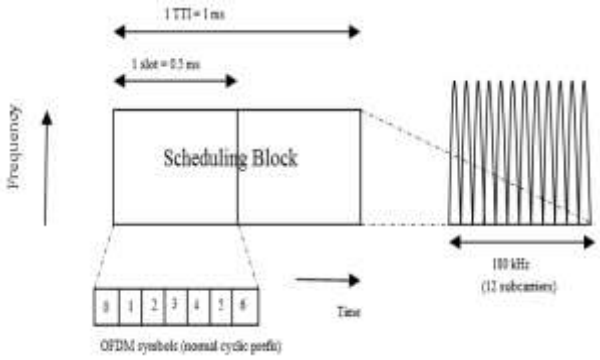


Figure 2. LTE downlink resource block structure

The responsibility of eNB in the access network is to ensure that the necessary QoS for a bearer over the interface is met. Each bearer has an associated QoS Class Identifier (QCI) [5] and each QoS class is characterized by priority, tolerable packet loss, and tolerable delay as shown in Table 1.

Generally bearers can be classified into two categories based on the nature of the QoS they provide: Guaranteed Bit-Rate (GBR) bearers which are real time bearers and non-GBR bearers which are non real time bearers.

At the physical layer, LTE supports both Time Division Duplex (TDD) and Frequency Division Duplex (FDD) modes. OFDMA is chosen as the DL access technology. The available bandwidth is divided into multiple Resource Blocks (RBs) based on time and frequency domains [6]. A RB is the smallest allocation unit in LTE which can be modulated independently. In the frequency domain the RB consists of 12 consecutive subcarriers and in the time domain it is made up of one time slot of 0.5 ms duration and adopts two slots as allocation period. The scheduling period is called as one Transmission Time Interval (TTI) and it lasts for 1 ms duration as shown in Fig. 2.

III. Radio Resource Management in LTE

RRM is the general word used in wireless systems to cover all radio related functions like assignment, management and sharing of radio resources among users. The scheduler which is found in the eNB, controls the assignment of RBs to UEs to avoid intra-cell interference. In general the function of scheduler is to find the optimal allocation of the resource unit (time, frequency, power etc) to UEs such that QoS requirements of users are satisfied.

The radio interface in LTE uses one common shared channel which is shared by all users in the cell. The eNB controls the allocation of RBs both on UL and DL shared channel ie., Physical Uplink Shared Channel (PUSCH) and Physical Downlink Shared Channel (PDSCH), respectively [6]. Both the UL and DL scheduling are carried out at eNB. To indicate the scheduled RBs for a particular UE the Physical Downlink Control Channel (PDCCH) is used. The PDCCH is carried in the first 1-3 OFDM symbols in each TTI.

The scheduler selects the UE to be scheduled and number of RB to be assigned based on two factors: the channel quality and the QoS requirements. In DL, the scheduler can assign any random set of RBs for a particular UE whereas in the UL the RBs allocated have to be adjacent to each other because of single carrier property. To facilitate the channel dependent scheduling on DL, the eNB has to get the channel quality reports from the UE. Each UE calculates the signal-to-noise (SNR) ratio based on its channel condition. It sends the Channel Quality Indicator (CQI) value to eNB based on its calculated SNR to choose the appropriate modulation and coding scheme (MCS).

CQI reporting method is to find balance between channel quality estimation and minimum signalling overhead. Many CQI reporting methods are proposed in [7]. In case of erroneous transmission, eNB performs retransmission by Hybrid Automatic Repeat Request (HARQ) procedure. HARQ is based on well known stop and wait algorithm [8].

A. Dynamic Resource Allocation in LTE

Dynamic resource allocation or Packet Scheduling (PS) takes care of QoS aspects on the access side by employing suitable algorithm for scheduling the data in both UL and DL. The main task of any scheduling algorithm is to maximize the network utilization and provide fairness among users. The PS is an entity of RRM in LTE which is present in the MAC layer of eNB. The MAC layer also provides most important procedures for the LTE radio interface like multiplexing/demultiplexing, random access procedures, scheduling requests etc [9].

In multiuser environment, a good PS scheme makes use of multiuser diversity and channel fading. When many users fade independently, at any time there is a high probability that one of the users will have a good channel. By allowing only that user to transmit, the shared channel resource is used in the most efficient way and the total system throughput is maximized. Thus with increasing number of users the multiuser diversity gain increases [10]. The difficulty lies in the fact that radio resource allocation should also satisfy fairness among UEs. Moreover, in slow fading, multiuser diversity hardly satisfies all QoS parameters at the same time, especially fairness. Ultimately, RRM should follow a combined form of multiuser diversity and fairness scheduling.

The two main entities of PS are Time Domain Packet Scheduling (TDPS) and Frequency Domain Packet

TABLE I. STANDARDIZED QCI FOR LTE [5]

QCI	Resource Type	Priority	Packet Delay Budget [ms]	Packet Loss Rate	Example services
1	GBR	2	100	10^{-2}	Conversational voice
2	GBR	4	150	10^{-3}	Conversational video (live streaming)
3	GBR	5	300	10^{-6}	Non-Conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real time gaming
5	non- GBR	1	100	10^{-6}	IMS signalling
6	non- GBR	7	100	10^{-3}	Voice, video (live streaming), interactive gaming
7	non- GBR	6	300	10^{-6}	Video (buffered streaming)
8	non- GBR	8	300	10^{-6}	TCP based (e.g., WWW, e-mail), chat, FTP, P2P file sharing
9	non- GBR	9	300	10^{-6}	

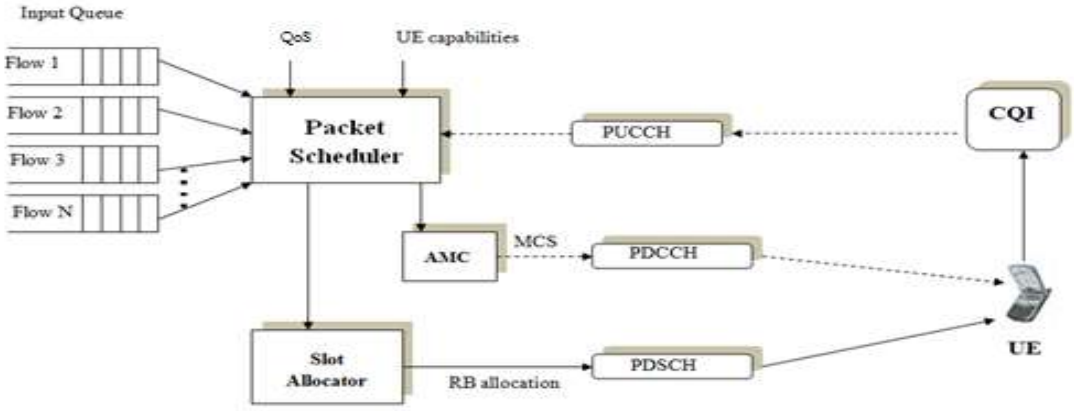


Figure 3. Generalized model of packet scheduler

Scheduling (FDPS). The TDPS selects a subset of schedulable UEs and FDPS determines the transport block size, MCS, Physical Resource Block (PRB) to UE mapping. Resource allocation for any UE is based on the scheduling decision of the algorithm. The factors that need to be considered before designing an algorithm are Qos provisioning, throughput maximization, fairness, complexity and scalability.

In LTE downlink, the QoS aspects depend on number of factors like channel conditions, resource allocation policies, available resources, delay sensitive/insensitive traffic etc. The resource allocation is realized in every TTI, that is exactly every two consecutive RBs. That is, resource allocation is done on a resource block pair basis. Fig. 3 shows the generalised model of a packet scheduler.

Resource allocation for each UE is usually based on the comparison of per-RB metric. This metric can be interpreted as the transmission priority of each UE on a specific RB. The detailed key issues in designing a scheduler are given in [11]. The scheduling strategies of any wireless network can be broadly classified as shown in Fig. 4.

Channel independent scheduling is based on the assumption that channel is time invariant and error-free. The channel independent scheduling is first introduced in wired networks [12]. Examples of channel independent scheduling are First-in-First-out (FIFO), Round Robin (RR), Weighted Fair Queuing (WFQ), Earliest Deadline First (EDF), Largest Weighted Delay First (LWDF) etc. Here some algorithms satisfy the QoS requirements and some simply schedules.

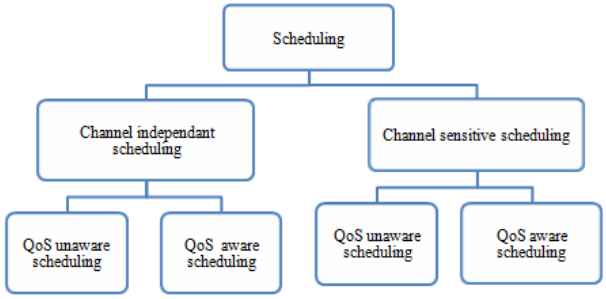


Figure 4. General classification of scheduling

With the help of CQI reports which are periodically sent by UEs to eNB, the scheduler can estimate the channel quality experienced by each UE. The scheduling performed by these schedulers is called channel sensitive scheduling. In this type of scheduling the scheduler may try to maximize the QoS requirements of each UE (QoS aware scheduling) or it may try to provide fairness among UEs (QoS unaware scheduling). Examples of channel sensitive scheduling are Maximum Throughput (MT), Proportional Fairness (PF), Throughput To Average (TTA), Modified- Largest Weighted Delay First (M-LWDF), Exponential Proportional Fairness (EXP/PF), Exponential rule (EXP rule), Logarithmic rule (LOG rule) etc. In LTE only channel sensitive scheduling is done based on the CQI reports from the UE.

B. Channel Sensitive Scheduling

Many scheduling algorithms are proposed based on the channel estimations in LTE network. Some algorithms aim to maximize the throughput (like MT, M-LWDF,

EXP/PF, EXP rule, LOG rule) while some aim to provide fairness among UEs (like PF, TTA). Some of them are discussed here.

Maximum Throughput: This algorithm provides the maximum overall throughput by allocating each RB to the UE which experience the good channel conditions. That is, the UE which experience the good channel quality will always be scheduled. The priority metric used in MT for i^{th} user on k^{th} RB can be expressed as

$$p_i^k = \arg\max_i (d_k^i(t)) ;\ 1 \le i \le N \tag{1}$$

where $d_k^i(t)$ is the expected data rate for i^{th} user at time t on k^{th} RB and N is the number of users in a network. This algorithm maximizes the cell throughput but at the same time it provides unfairness resource sharing among UEs especially, cell edge users.

Proportional Fairness: This algorithm provides balance between spectral efficiency and fairness among UEs. The priority metric used for PF for i^{th} user on k^{th} RB can be expressed as

$$p_i^k = \arg\max_i \left(\frac{d_k^i(t)}{\overline{R_i(t-1)}} \right);\ 1 \le i \le N \tag{2}$$

where $d_k^i(t)$ is the expected data rate for i^{th} user at time t on k^{th} RB, $\overline{R_i(t-1)}$ is the past average throughput up to time slots *t-1* and N is the number of users. The denominator value will be decreased for the users experiencing bad channel conditions, which maximizes the priority metric, so that the poor channel users will also be allocated resources. The past average throughput can be calculated as follows:

$$\overline{R_i(t)} = (1-\frac{1}{T})\overline{R_i(t-1)} + \frac{1}{T} r_i(t) \tag{3}$$

here T is the fairness window would be equal to one TTI. $r_i(t)$ is the data rate achieved by the i^{th} user at time t.

Many algorithms have been proposed in literature with modifications to PF algorithm. A new scheduling approach based on PF algorithm is introduced in [13] which try to balance coverage and cell throughput. In [14], the problem is formulated which aims to maximize the throughput using PF algorithm. The results showed that the performance obtained by using different PF implementation increase with the complexity of the optimization problem.

The Generalized Proportional Fair (GPS) scheduling is developed in [15]. The PF metric is modified by means of two parameters ξ and ψ . The priority metric can be expressed as

$$p_i^k = \arg\max_i \left(\frac{[d_k^i(t)]^{\xi}}{[\overline{R_i(t-1)}]^{\psi}} \right);\ 1 \le i \le N \tag{4}$$

The parameters ξ and ψ act as weighting factor for resource allocation produce on the instantaneous data rate and the past achieved throughput, respectively. Similar to this approach, in [16] and [17] use adaptive approach which can be able to adjust the fairness level depending on the system requirements. In [18], PF scheme is applied to both time and frequency domain. In time domain the scheduler selects a subset of active users in the current TTI and in frequency domain RBs are allocated to each UE.

Throughput to Average: This algorithm can be considered as an intermediate approach between MT and PF. Its priority metric can be expressed as

$$m_i^k = \arg\max_i \left(\frac{d_k^i(t)}{d_i(t)} \right);\ 1 \le i \le N \tag{5}$$

where $d_k^i(t)$ is the expected data rate for i^{th} user at time t on k^{th} RB, $d_i(t)$ is the long term average expected data rate for i^{th} user at time t and N is the number of users. From the metric it is easy to understand that the higher the overall expected throughput of UE lower will be its metric on a single RB.

Modified-Largest Weighted Delay First: It is channel aware extension of LWDF [19] used in wireless networks. In this algorithm non-real time and real time flows are treated differently [20]. The priority metric can be expressed as follows:

$$p_i^k = \arg\max_i \left(\alpha_i D_i \frac{d_k^i(t)}{\overline{R_i(t-1)}} \right);\ 1 \le i \le N \tag{6}$$

where α_i is weight parameter, D_i is the head-of-line packet delay, i.e., delay of the first packet to be transmitted by i^{th} user, $d_k^i(t)$ is the expected data rate for i^{th} user at time t on k^{th} RB, $\overline{R_i(t-1)}$ is the average throughput up to time slots t-1 and N is the number of users. This algorithm tries to guarantee good throughput and acceptable level of fairness. A theoretical analysis of M-LWDF fairness is given in [21]. It is shown that M-LWDF fairness depends on the channel condition, packet's arrival process and the ratio of QoS requirements of different service queues. Based on the theoretical analysis an enhanced M-LWDF algorithm was proposed which improves the fairness compared to M-LWDF algorithm. In [22], a modified version of M-LWDF algorithm based on token mechanism is proposed which gives better performance to real time flows in the DL systems.

Exponential PF: EXP/PF algorithm considers both the characteristics of PF for handling non real time flows and exponential function of the end-to-end delay for real time flows. It is first developed to support multimedia applications in time multiplexed systems [23]. It tries to guarantee the delay bound of real time services and maximizes the throughput with acceptable level of fairness. For real time flows the priority metric is calculated as:

$$p_i^k = \arg\max_i \left(\exp(\frac{\alpha_i D_i - \bar{D}_i}{1+\sqrt{\bar{D}_i}}) \frac{d_k^i(t)}{\overline{R_i}(t-1)} \right); 1 \le i \le N \tag{7}$$

TABLE II. COMPARISON OF DIFFERENT SCHEDULING APPROACHES

Algorithm	Scheduling parameter	Pros	Cons
FIFO	Request time	Simple	Inefficient, Channel conditions not known
RR	Serving time instant	Simple	Inefficient, Channel conditions not known
WFQ	Priority weight	Introduces priority	Channel conditions not known
EDF	Delay threshold	Avoids deadline expiration	Channel conditions not known
LWDF	Acceptable packet loss rate	Provides QoS in terms of delay	Channel conditions not known
MT	Expected data rate	Maximize overall throughput	unfair
PF	Expected data rate, Past average throughput	Provides fairness	Low spectral efficiency
TTA	Expected data rate, Wideband expected data rate	Strong level of fairness	Low spectral efficiency, does not exploit multiuser diversity
M-LWDF	Head-of-line packet delay	Real time and non real time flows are treated differently	Inefficient in overloaded conditions.
EXP/PF	Head-of-line packet delay	Real time and non real time flows are treated differently	complex
EXP rule	Head-of-line packet delay, spectral efficiency of UE	Good scheduling performance	complex
LOG rule	Head-of-line packet delay, spectral efficiency of UE	Good scheduling performance	complex

where

$$\bar{D}_i = \frac{1}{N_{rt}} \sum_{i=1}^{N_{rt}} \alpha_i D_i \quad (8)$$

and N_{rt} is the number of active real time DL flows, α_i is weighting parameter, D_i is the head-of-line delay, $d_k^i(t)$ is the expected data rate for i^{th} user at time t on k^{th} RB, $\overline{R_i(t-1)}$ is the average throughput up to time slots t-1. PF algorithm handles non real time flows.

Exponential rule: This algorithm has been presented in [24]. This algorithm is enhancement of EXP/PF. Its priority metric is given as

$$p_i^k = \arg\max_i \left(b_i \exp\left(\frac{a_i D_i}{c + \sqrt{(1/N_{rt}) \sum_j a_i D_j}}\right) \Gamma_k^i \right) \; 1 \le i, j \le N \quad (9)$$

where a_i , b_i and c are optimal parameter set for the system requirements, and N_{rt} is the number of active real time DL flows, D_i is the head-of-line delay, Γ_k^i is the spectral efficiency of i^{th} user on k^{th} RB and N is the number of users. EXP rule takes into account the overall network status, because that the delay of the considered UE is normalized over the sum of experienced delays of all UEs. In [25] author proposes an interesting procedure based on cooperative game theory that performs resource sharing based on EXP rule with virtual token mechanism.

Logarithmic rule: This algorithm has been also presented in [24]. This algorithm is similar to that of EXP rule but it uses logarithmic function of delay to calculate the scheduling metric.

$$p_i^k = \arg\max_i \left(b_i \log(c + a_i D_i) \Gamma_k^i \right); \; 1 \le i \le N \quad (10)$$

where b_i, c and a_i are tunable parameters, D_i is the head-of-line delay, Γ_k^i is the spectral efficiency of i^{th} user on k^{th} RB and N is the number of users. Optimum throughput and fairness can be achieved by taking suitable values for b_i, c and a_i. In [26], the paper considers the design of multiuser opportunistic packet scheduler for UEs sharing a time-varying wireless channel based on LOG rule. It is concluded that a scheduler optimized for the overall system performance is likely to be more robust to changes in the traffic and channel statistics than the one optimized for the worst case. Table 2 summarizes the comparison of main scheduling algorithms used in wireless networks including LTE.

Apart from above mentioned scheduling algorithms many algorithms are proposed in literature. Some considers buffer status, some considers energy savings and some presents the combinations of algorithms.

Delay based algorithms: In [27], a cross layer algorithm is presented as an optimization problem to minimize the average delay under the constraints of the transmission power and block error rate requirements. In [28], the author associates a delay function to each data packet. That is, longer the delay higher the probability of the packet to be allocated. Delay based prioritized scheduling approach is proposed in [29]. In this paper, the algorithm first orders the users depending on the remaining time before deadline expiration. Once the urgent users were identified the frequency allocation step is performed in order to transmit the head of line packet. Frequency-time scheduling approach with delay constraints is proposed in [30] to handle streaming services like multimedia services. The QoS for this kind of service can be attained at the expense of overall system capacity. The proposed algorithm tries to balance the QoS of service without losing much cell capacity.

Power based algorithms: Transmit power based scheduling algorithm is proposed in [31], where the scheduling metric is based on the ratio of transmit powerper bit and allocates resources. A resource allocation problem is formulated in [32], with constraints on power, rate and delay. The analytical design is used to evaluate the system performance under different network parameters. Imperfect channel state information is considered in problem formulation. Based on the matrix analysis the formulated problem is transformed to optimization problem. The solution obtained was complex and considered as impractical one. So a heuristic

solution is proposed with lower complexity to achieve acceptable system performance.

CQI feedback based algorithms: In LTE, CQI feedback enables the scheduler to achieve multiuser diversity gain by allocating resources to UEs with good channel condition leading to unfairness. A multiuser scheduling method is proposed in [33] which is based on fairness utility function and aims to provide resources to the cell edge users also. A priority based approach is presented in [34] where the priority sets are created based on CQI of each bearer and classified as GBR and non-GBR set. By using FDPS, GBR set is allocated RBs and the remaining RBs are allocated to non-GBR set based on PF algorithm.

Service based algorithms: A QoS aware scheduling algorithm for downlink transmission with emphasis for support in overload state is presented in [35]. In this method multiple real time traffic metrics are processed through array of ranking functions and then they are multiplexed to aggregate ranking function. This ranking function is utilized in scheduling function. A different approach is followed in [36], where authors develop two level framework that guarantees delay to real flows. At upper level, discrete control theory is applied to every frame to calculate the total amount of data of real time flows which is having delay constraints. At lower level PF metric is used to satisfy the non real time flows. It is concluded that this algorithm is suitable for real time video flows.

In a similar manner [37] designed an algorithm which consists of three phases. In frequency domain, a method is developed to utilize the RBs in an effective manner. In time domain, a method is proposed for predicting the packet delays for different applications in the queue. Then with the calculated results, a method is proposed which rearrange the transmission order and discard the packets which do not meet the delay requirements. It is claimed that this method is suitable for real time services. In [38] dynamic scheduler for VoIP is proposed. It facilitates priority during only VoIP can be allocated. For QoS aware packet scheduler, delivering packets within the pre-fixed expiration is the fundamental characteristics. To satisfy the QoS requirements, [39] proposed a method called Token Bucket Scheduler (TBS). TBS utilizes instantaneous DL channel Signal to Interference plus Noise Ratio (SINR) and QoS information while allocating RB to real time services.

Queue based algorithms: A cross layer design approach is presented in [40], which makes use of both users' queue states and channel states in allocation of resources. This method has low computational complexity since it considers users' minimum data rate and target bit error rate as QoS parameters. Similar to this approach the algorithm proposed in [41] allocates resources according to CQI feedback from the physical layer and considers buffer status of user to avoid buffer overflow to guarantee fairness among users.

QoE based Algorithms: In [42] the paper deals with the human perceived quality maximization, when scheduling multimedia traffic. Work has been carried out in two levels. First, the Quality-of-Experience (QoE) aware scheduling problem is formulated as a suitable Markov Decision Process (MDP) model. Then to solve the problem, a simple heuristic rule is designed. This paper claims that QoE experienced by users outperforms most scheduling techniques.

IV. Performance Analysis of Main Scheduling Strategies

From user's point of view, the important characteristic of a network related to its performance is its QoS. QoS is analyzed by means of many parameters like goodput, delay, Packet Loss Ratio (PLR), fairness index etc. In this section, the main scheduling algorithms used in LTE network are analyzed by using an open source simulator, LTEsim [43]. The modules present in LTEsim are explained in [44].

A. Simulation Scenario

For performance analysis, a single cell scenario with fixed eNB is considered where the users are uniformly distributed among the cell. Two user's speed (30 kmph, 120 kmph) are considered for analysis using random mobility model [45]. Each user receives one video flow, one VoIP flow and one Best Effort (BE) flow at the same time. The buffer at the scheduler is considered to be infinite ie., the packet loss is not due to the buffer overflow.

Video service has 128 kbps source rate produced by H.264 coder. For VoIP, G.729 voice flows are used with source rate of 8 kbps. Finally, best effort traffic corresponds to the ideal source that always has packet to send. In real time services, the maximum delay should be in the range of 100-200 ms. Accordingly, the target delay is set to 0.1 s. The main simulation parameters used for analysis is shown in Table.3

TABLE III. Simulation parameters

Parameter	Value
Bandwidth	10 MHz
Carrier frequency	2 GHz
Frame structure	FDD
Channel model	6-ray Typical Urban (TU)
Path loss	128.1 + 37.6 log r (dB)
Penetration loss	20 dB
Mobility model	Random
Speed of UE	3 kmph, 120 kmph
UE application flow	One video, one VoIP, one BE
Maximum delay	0.1 s
Simulation duration	100 s
Traffic model	Video - Trace based (H264) VoIP - G.729 voice flows BE - Infinite buffer

B. Results and Discussion

As a result of simulation, the performance analysis is performed in terms of average goodput, PLR and fairness index by increasing the number of users with the step of ten.A scheduling algorithm should balance its allocation method between fairness and throughput maximization in order to guarantee atleast minimum data rate to the cell edge users. The fairness index for video, VoIP and BE service is shown in Figs 5.

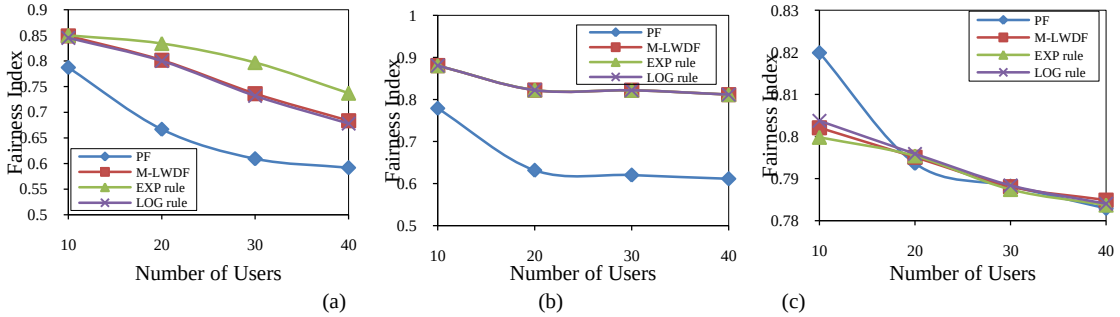


Figure 5. Fairness index for (a) video (b) voice and (c) BE

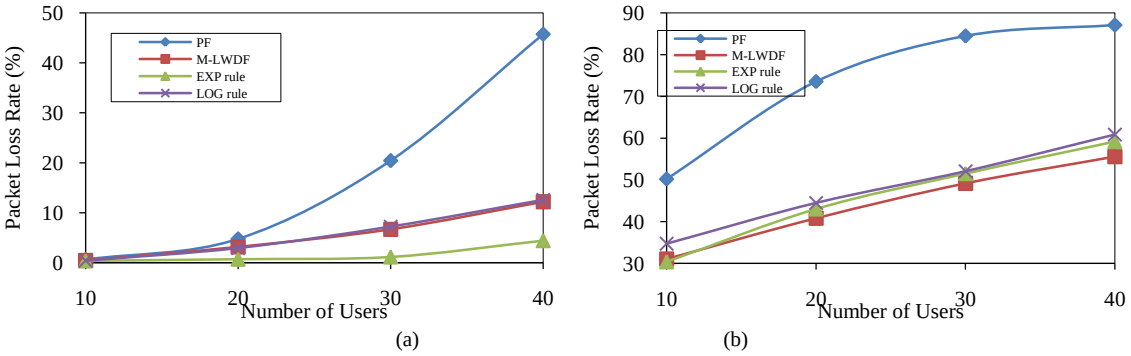


Figure 6. PLR of Video (a) at 3 kmph and (b) at120 kmph

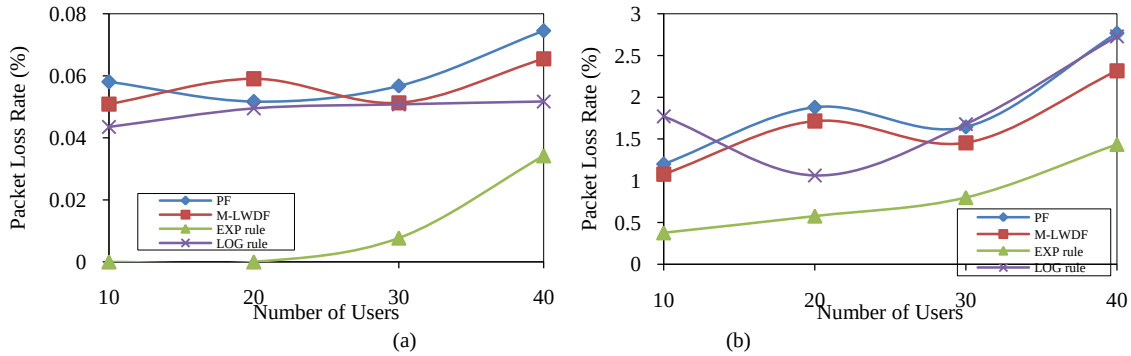


Figure 7. PLR of VoIP (a) at 3 kmph and (b) at120 kmph

For real time flows, it is observed that all the schedulers except PF show comparable level of fairness closer to 0.85 then decrease with increasing users. Since PF algorithm goes on balancing between the data rate and fairness, it shows lower fairness index for real time flows. The fairness index experienced by the non-real time flows is lesser than that of real time flows because of its low priority.

Regarding real time flows PLR is the standard metric used to evaluate the QoS offered by the network. Figs. 6 and 7 show the PLR achieved for video and VoIP flow respectively.

It is observed that VoIP flows experience considerably smaller PLRs than video. This is due to the fact that VoIP flows having a lower source bit rate get higher priority from the schedulers. It is also noted that as the user speed increases, PLR also increases for all investigating algorithms.

For video flows, the PLR is higher for PF algorithm when compared with other algorithms. In low mobility scenario, PLR is about 0.2-1% for lesser number of users and increases with increasing users. PF algorithm drops 40% of forwarded packets and other algorithms used for analysis, drop 5-10% of packets for maximum number of users used in this simulation. When the speed is increased to 120 kmph PF algorithm drops 90% of forwarded packets and other algorithms drops 50-55% of forwarded packets for maximum number of users used in this simulation. For VoIP flows with low mobility EXP rule algorithm gives good performance of 0-0.03% of packet drop and other algorithm achieves 0.04-0.08% of packet drop for maximum number of users used in the simulation. For the speed of 120 kmph EXP rule gives 0.5-1% packet loss and other algorithm achieves 2-3% packet loss for maximum number of users used in this simulation.

The average goodput for video, VoIP and BE flows with two different user speeds are shown in Figs. 8, 9, 10. Average goodput is defined as the rate of useful bits successfully transmitted during the entire simulation.

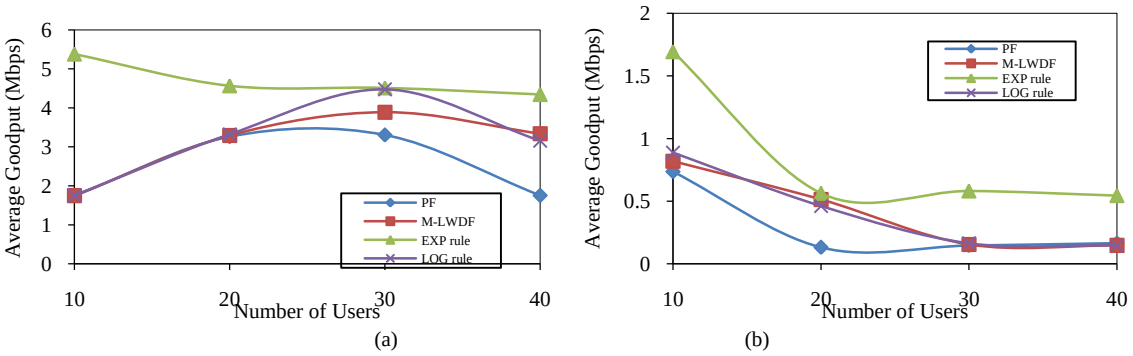


Figure 8. Goodput of video (a) at 3 kmph and (b) at120 kmph

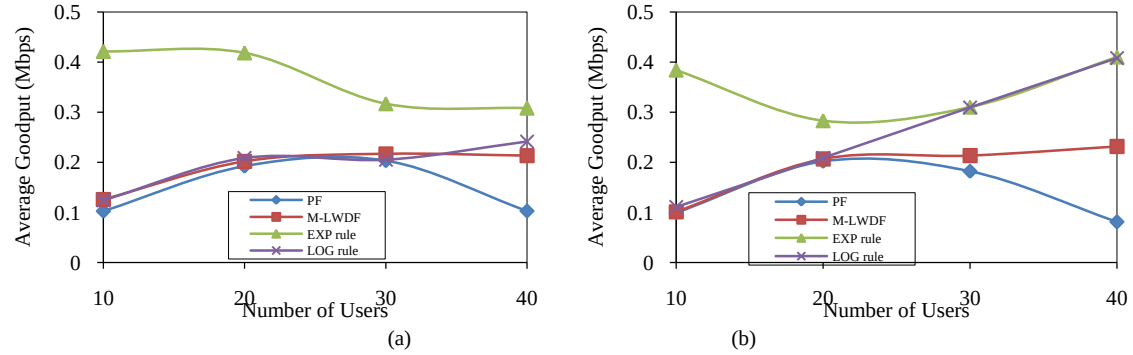


Figure 9. Goodput of VoIP (a) at 3 kmph and (b) at120 kmph

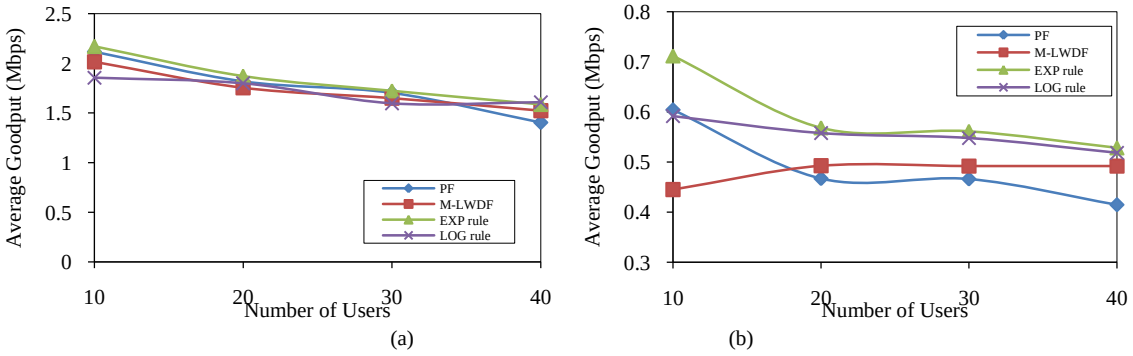


Figure 10. Goodput of BE (a) at 3 kmph and (b) at120 kmph

Average goodput is limited by packet loss and delay. From the figures it is observed that goodput decreases with increasing users. The rate of reduction is higher in case of PF algorithm. In high mobility scenario, users are affected by lower average goodput which affects the service quality for real time services. It is observed that EXP rule algorithm gives better performance when compared with other algorithms for real time services. For non real time services, all algorithms provide similar performance.

V. Future Challenges

Though LTE overcomes the performance of current 3G systems, it is not suitable for future data traffic requirements which have been given in IMT-Advanced [46]. For fulfiling the requirements of IMT-Advanced, LTE-Advanced is introduced by 3GPP. To meet the target requirements LTE-Advanced is standardized by many technologies like carrier aggregation, enhanced multi-antenna support, Coordinated Multi-Point (CoMP) transmission techniques, relaying and Heterogeneous Networks (HetNet) deployment [47].

In order to utilize the wider bandwidth upto 100 MHz and keeping backward compatible with LTE, a carrier aggregation scheme is proposed. Carrier aggregation consists of LTE component carriers (CCs) so that the devices can be able to use a greater amount of bandwidth. A device capable of carrier aggregation has one primary CC and one or more secondary CCs. Carrier aggregation may be of contiguous or non-contiguous. An eNB can use up to 5 adjacent channels of 20 MHz to increase the network capacity [48]. In a scenario where both LTE and LTE-Advanced users are present, the RRM at MAC layer should be able to differentiate among these users. In particular, LTE-Advanced users should be assigned multiple CCs while LTE users should be assigned single carrier. Scheduling for LTE-Advanced users with carrier aggregation can be done in two ways: same carrier scheduling and cross carrier scheduling.

In same carrier scheduling, separate PDCCH is used for each CC and in cross carrier scheduling, common PDCCH is used for multiple CCs. The challenge of designing the scheduler lies in allocating CCs and resources to the users.

CoMP is contemplated as an essential technique to alleviate inter-cell interference and to improve the cell-edge performance in LTE-Advanced networks. It makes use of multiple transmit and receive antennas from multiple eNBs to enhance the signal quality and to decrease the interference. The resource allocation for this technique needs to be synchronized among different eNBs. CoMP in downlink can be classified into two schemes. Coordinated Scheduling and/or Beam-Forming (CS/CB) and Joint Processing (JP). In CS/CB, the signaling and resource allocation to a single user are performed from the serving cell. However the scheduling is dynamically coordinated between the cells. In that manner, the interference between different transmissions can be decreased. The scheduler at eNB makes its decisions independently but additional information about other user's channel condition is needed to perform more optimal scheduling. In JP, signaling and resource allocation to a single user is concurrently performed from multiple transmissions to optimize cell edge performance. This scheme is more challenging because the scheduling decisions must be exchanged over the backhaul. So the scheduling algorithms ensuring eNB synchronization need to be designed [49].

With the introduction of low power eNBs like micro, pico, femto, the demand for different scheduling methods has been increased. Combining macro cells with low power nodes will overcome the problem of coverage holes which improves the capacity in hot spot areas. The low power nodes would be able to serve the limited number of UEs with less coverage area. All the scheduling methods which were previously discussed can be used for heterogeneous networks by taking into account, the interference produced by macro cells [50]. The method of simulating LTE femtocells using open source simulator is presented in [51] which shows that throughput is maximized with the introduction of low power nodes.

To increase the capacity of a cellular network, large number of base stations have to be deployed which is very expensive. For this purpose LTE-Advanced introduced a technique called relaying. eNB can forward the information through relay node to remote user with high data rate, thereby reducing the deployment cost. The source eNB from which the relay node receives the signal is called donor eNB and the link between the donor eNB and relay node is called backhaul link. The link between the relay node and the end user is called access link. Since the control and data transmissions are carried out through backhaul link and then access link, the scheduler in the donor eNB should take into account the additional link delay also. The resource allocation algorithm for relaying may be centralized or distributed. In centralized resource allocation, the donor eNB is in charge of doing resource allocation to both end user and relay node. In distributed resource allocation, relay node is incharge of doing similar resource allocation as done by donor eNB with a constraint that it has limited resources. The combination of OFDMA with relaying techniques provides increased opportunities for cost-effective and high-performance networks. To make use of such opportunities requires intelligent RRM algorithms [52].

VI. Conclusion

The 3GPP LTE standards aim to achieve revolutionary data rate, spectral flexibility with seamless mobility and enhanced QoS over the entire IP network. In this paper, a study of downlink scheduling algorithms for LTE networks has been carried out. The most important RRM task is performed by the packet scheduler who distributes radio resources among UEs in efficient way. This paper identifies the strength and weakness of well known algorithms in the downlink LTE system and the key aspects that should be taken into account when designing a new algorithm. It can be inferred that PF algorithm is more suitable for non real time services because it does not account packet delays during its decision making. On the other hand the other schedulers such as M-LWDF, EXP/PF, EXP rule and LOG rule are better choice for real time services. Combinations of algorithms can also be carried out to find the optimal solution according to the network requirements. These algorithms can also be used to LTE-Advanced with some modifications according to the techniques used.

References

[1] 3GPP, Tech. Specific. Group Radio Access Network-Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN), *3GPP TS* 25. 913.

[2] International Telecommunication Union (ITU), overall network operation, telephone service, *service operation and human factors, ITU-T recommendation E. 800 Annex B*, Aug. 2008.

[3] 3E. Dahlman, S. Parkvall, J. Skold and P. Beming, 3G Evolution HSPA and LTE for mobile Broadband. *Academic Press*, 2008.

[4] Amit Kumar, Jyotsna Sengupta, Yun-fei Liu, "3GPP LTE: The Future of Mobile Broadband" *Wireless Personal Communication*, vol. 62, pp. 671-686, 2012.

[5] 3GPP, Tech. Specific. Group Services and System Aspects – Policy and charging control architecture (Release 9), *3GPP TS* 23. 203.

[6] 3GPP, Tech. Specific. Group Radio Access Network – Physical Channel and Modulation (Release 8), *3GPP TS* 36. 211.

[7] N. Kolehmainen, J. Puttonen, P. Kela, T. Ristaniemi, T. Henttonen, and M. Moisio, "Channel Quality Indication Reporting Schemes for UTRAN Long Term Evolution Downlink," *in Proceedings of IEEE Vehicular Technology Conference*, VTC-Spring, Marina Bay, Singapore, vol. 1, pp. 2522 –2526, May 2008.

[8] T. I. Sesia S. and B. M., "LTE, The UMTS Long Term Evolution: From theory to practice" *John Wiley & Sons*, 2009.

[9] 3GPP, Tech. Specific. Group Radio Access Network – Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Terrestrial Radio Access Network (E-

UTRAN); *Medium Access Control (MAC) protocol specification (Release 9), 3GPP TS* 36. 321.

[10] I. C. Wong, Z. Shen, B. L. Evans and J. G. Andrews, "A Low Complexity Algorithm for Proportional Resource Allocation in OFDMA Systems" *IEEE Workshop on Signal Processing Systems*, USA, vol. 1, pp. 1-6, Oct. 2004.

[11] F. Capozzi, G. Piro, L. A. Grieco, G. Boggia and P. Camarda, "Downlink Packet Scheduling in LTE Cellular Networks: Key Design Issues and a Survey" *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 678-700, 2013.

[12] A. S. Tennenbaum, "modern operating systems", 3rd edition. Prentice Hall Press, 2007.

[13] G. Monghal, K. I. Pedersen, I. Z. Kovacs, P. E. Mongensen," QoS Oriented Time and Frequency Domain Packet Scheduler for the UTRAN Long Term Evolution", *IEEE Vehicular technology Conference*, VTC spring, Singapore, vol. 1, pp. 2532-2536, 2008.

[14] R. Kwan, C. Leung, and J. Zhang, "Proportional Fair Multiuser Scheduling in LTE," *IEEE Signal Process. Letters*, vol. 16, no. 6, pp. 461–464, June 2009.

[15] C. Wengerter, J. Ohlhorst, and A. von Elbwart, "Fairness and Throughput Analysis for Generalized Proportional Fair Frequency Scheduling in OFDMA," in *Proceedings of IEEE Vehicular Technology Conference*, VTC-Spring, Stockholm, Sweden, vol. 3, pp. 1903 – 1907, May 2005.

[16] M. Proebster, C. Mueller, and H. Bakker, "Adaptive Fairness Control for a Proportional Fair LTE Scheduler," in *Proceedings Of IEEE Personal Indoor and Mobile Radio Communication, PIMRC*, Istanbul, Turkey, vol. 1, pp. 1504 –1509, Sep. 2010.

[17] X. Li, B. Li, B. Lan, M. Huang, and G. Yu, "Adaptive PF Scheduling Algorithm in LTE cellular system," in *Proceedings of International Conference on Information and Communication Technology Convergence, ICTC*, Jeju Island, Korea, vol. 1, pp. 501 –504, Nov. 2010.

[18] K. C. Beh, S. Armour, and A. Doufexi, "Joint Time-Frequency Domain Proportional Fair Scheduler with HARQ for 3GPP LTE Systems," *in Proceedings of IEEE Vehicular Technology Conference*, VTC-Fall, Calgary, Alberta, vol. 1, pp. 1–5, Sep. 2008.

[19] A. Stolyar and K. Ramanan, "Largest Weighted Delay First Scheduling: Large Deviations and Optimality," *Annals of Applied Probability*, vol. 11, pp. 1–48, June 2001.

[20] H. Ramli, R. Basukala, K. Sandrasegaran, and R. Patachaianand, "Performance of Well Known Packet Scheduling Algorithms in the Downlink 3GPP LTE System," in *Proceedings of IEEE Malaysia International Conference on Communication, MICC*, Kuala Lumpur, Malaysia, vol. 1, pp. 815 –820, Nov. 2009.

[21] Xian Yon-ju, TIAN Feng-chun, XU Chang-biao, YANG Yue," Analysis of M-LWDF Fairness and an Enhanced M-LWDF Packet Scheduling Mechanism" *Journal of China Universities of Posts and Telecommunications*, vol. 18, no. 4, pp. 82-88, Aug. 2011.

[22] Mauricio Iturralde, Tara ali Yahiya, Anne Wei and Andre-Luc Beylot, "Performance Study of Multimedia Services Using Virtual Token Mechanism for resource Allocation in LTE Networks" *IEEE Vehicular Technology Conference*, vol. 1, pp. 1-5, 2011.

[23] J. -H. Rhee, J. Holtzman, and D. K. Kim, "Scheduling of Real/non-real Time Services: Adaptive EXP/PF Algorithm," in *Proceedings of IEEE Vehicular Technology Conference*, VTC-Spring, Jeju, Korea, vol. 1, pp. 462 – 466, Apr. 2003.

[24] B. Sadiq, R. Madan, and A. Sampath, "Downlink Scheduling for Multiclass Traffic in LTE," *Eurasip Journal of Wireless Communication Networks*, vol. 2, pp. 9–13, Oct. 2009.

[25] M. Iturralde, A. Wei, and A. Beylot, "Resource Allocation for Real Time Services using Cooperative Game Theory and a Virtual Token Mechanism in LTE Networks," in *IEEE Personal Indoor Mobile Radio Communications*, PIMRC, vol. 1, pp. 879-883, Jan. 2012.

[26] Bilal sadiq, Seung Jun Baek, "Delay-Optimal Opportunistic Scheduling and Approximation: The Log Rule" *IEEE/ACM Transactions on Networking*, vol. 19, no. 2, pp. 405-418, April 2011.

[27] H. Fattah and H. Alnuweiri, "A Cross-layer Design for Dynamic Resource Block Allocation in 3G Long Term Evolution System," in *Proceedings of IEEE Mobile Adhoc and Sensor Systems*, MASS, Macau, China, vol. 1, pp. 929 –934, Nov. 2009.

[28] P. Liu, R. Berry, and M. Honig, "Delay-Sensitive Packet Scheduling in Wireless Networks," in *Proceedings of IEEE Wireless Communication and Networking Conference, WCNC*, Atlanta, Geogia, USA, vol. 3, pp. 1627 –1632, Mar. 2003.

[29] K. Sandrasegaran, H. A. Mohd Ramli, and R. Basukala, "Delay-Prioritized Scheduling DPS for Real Time Traffic in 3GPP LTE System," *in IEEE Wireless Communications and Networking Conference* WCNC, vol. 1, pp. 1–6, Apr. 2010.

[30] Mohamed Assaad, "Frequency –Time Scheduling for Streaming Services in OFDMA Systems" *IEEE Conference on Wireless*, vol. 1, pp. 1-5, 2008.

[31] Jungsup Song, Gye-Tae Gil, and Dong-Hoi Kim, "Packet-Scheduling Algorithm by the Ratio of Transmit Power to the Transmission Bits in 3GPP LTE Downlink" *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1-8, 2010.

[32] Seyed Mohamad Alavi, Chi Zhou, Wan Wang Gen, "Efficient Resource Allocation Algorithm for OFDMA Systems with Delay Constraint" *Computer Communications*, vol. 36, pp. 421–430, 2013.

[33] Stefan Schwarz, Christian Mehlfuhrer and Markus Rupp," Throughput Maximizing Multiuser Scheduling with Adjustable Fairness" *Proceedings of ICC*, Kyoto, vol. 1, pp. 1-5, 2011.

[34] Y. Zaki, T. Weerawardane, C. Gorg, and A. Timm-Giel, "Multi-QoS-Aware Fair Scheduling for LTE," in *IEEE 73rd Vehicular Technology Conference* VTC Spring, vol. 1, pp. 1–5, May 2011.

[35] Michael Brehm, Ravi Prakash, "Overload-state Downlink Resource Allocation in LTE MAC Layer", *Wireless Networks*, vol. 19, pp. 913-931, 2013.

[36] G. Piro, L. Grieco, G. Boggia, R. Fortuna, and P. Camarda, "Two-level Downlink Scheduling for Real-Time Multimedia Services in LTE Networks," in *IEEE Transaction on Multimedia*, vol. 13, no. 5, pp. 1052 –1065, Oct. 2011.

[37] Wei Kuang Lai, Chang-Lung Tang, "QoS-aware Downlink Packet Scheduling for LTE Networks" *Computer Networks*, vol. 57, pp. 1689-1698, 2013.

[38] S. Choi, K. Jun, Y. Shin, S. Kang and B. Choi, "MAC Scheduling Scheme for VoIP Traffic Service in 3G LTE" in *proceedings of IEEE vehicular Technology Conference*, VTC-Fall, Baltimore, MD, , USA, vol. 1, pp. 1441-1445, Oct. 2007.

[39] Liqun Zhao, Yang Qin, Maode MA, Xiaoxiong Zhong, Li Li," QoS Gaurenteed Resource Block Allocation Algorithm in LTE Downlink" *IEEE International*

Conference on Communications and Networking, China, vol. 1, pp. 307-312, 2012.
[40] Ioannis G. Fraimis, Stavros A. Kotsopoulos, "Queue-Aware Resource Allocation for Multi-cell OFDMA System with QoS Provisioning" *Wireless Personal Communication*, vol. 71, pp. 3033-3044, 2013.
[41] Yan Lin, Guanxin Yue, "Channel Adapted and Buffer Aware Packet Scheduling in LTE Wireless Communication System", *IEEE Conference on Wireless Communication and Networking*, USA, vol. 1, pp. 1-4, 2008.
[42] Ianire Taboada, Fidel Liberal, Jose Oscar Fajardo, Urtzi Ayesta, "QoE–aware optimization of multimedia flow scheduling" *Computer Communication*, vol. 1, pp 1-6, 2013.
[43] G. Piro, "LTE-Sim - the LTE simulator," [OnLine] Available: http:// telematics. poliba. it/LTE-Sim.
[44] Giuseppe Piro, Luigi Alfredo Grieco, Gennaro Boggia, Francesco Capozzi and Pietro Camarda, "Simulating LTE Cellular Systems: an Open Source Framework" *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 498-513, 2010.
[45] B. Jabbari, G. Mason, Y. Zhou, F. Hillier," Random walk modelling of mobility in wireless networks," *IEEE Vehicular Technology Conference* – VTC 98, vol. 1, pp. 639-643, May 1998.
[46] ITU-R, Requirements Related to Technical Performance for IMT-Advanced Radio Interfaces, Rep. M. 2134, 2008.
[47] S. Parkvall, A. Furuskar, and E. Dahlman, "Evolution of LTE toward IMT-advanced*," IEEE Communication Magazine*, vol. 49, no. 2, pp. 84 –91, Feb. 2011.
[48] K. I. Pedersen, F. Frederiksen, C. Rosa, H. Nguyen, L. Garcia and Y. Wang, "Carrier Aggregation for LTE-advanced: Functionality and Performance Aspects" *IEEE Communication Magazine*, vol. 49, no. 6, pp 89-95, June 2011.
[49] Juho Lee, Younsun Kim, Hyojin Lee, Boon Loong Ng, David Mazzarese, Jianghua Liu, Weimin Xiao, and Yongxing Zhou, "Coordinated Multipoint Transmission and Reception in LTE-Advanced Systems" *IEEE Communications Magazine*, vol. 50, no. 11, pp. 44-50, Nov. 2012.
[50] Beatriz Soret, Hua Wang, Klaus I. Pedersen, Claudio Rosa, "Multicell Cooperation for LTE-Advanced Heterogeneous Network Scenarios" *IEEE Wireless Communications*, vol. 20, no. 1, pp. 27-34, Feb. 2013.
[51] Francesco Capozzi, Giuseppe Piro, Luigi A Grieco, Gennaro Boggia and Pietro Camarda, "On accurate simulations of LTE femtocells using an open source simulator", *EURASIP Journal on Wireless Communications and Networking*, vol. 328, pp. 1-13, 2012.
[52] Mohamed Salem, Abdulkareem Adinoyi, Mahmudur Rahman, Halim Yanikomeroglu, David Falconer, Young-Doo Kim, Eungsun Kim, and Yoon-Chae Cheong, "An Overview of Radio Resource Management in Relay-Enhanced OFDMA-Based Networks" *IEEE Communications Surveys & Tutorials*, vol. 12, no. 3, Third Quarter 2010.

S. Fouziya Sulthana received her B.E degree in Electronics and Communication from Bharadidasan University, Tamilnadu in 2002 and M.Tech degree in electronics and Communication from Pondicherry University, Puducherry in 2008.She is student member of IEEE and IEICE. She worked as Assistant Professor in private engineering college. She is currently a PhD student in Pondicherry University. Her current research focuses on Radio resource Management in broadband networks.

Dr. R. Nakkeeran received B.Sc. degree in Science and B.E degree in Electronics and Communication Engineering from Madras University in 1987 and 1991 respectively and M.E degree in Electronics and Communication Engineering (with diversification in Optical Communication) from Anna University in 1995. He received PhD degree from Pondicherry University in 2004. Since 1991, he has been working in teaching profession. Presently, he is Associate Professor in the Department of Electronics Engineering, School of Engineering and Technology, Pondicherry Central University. He is life member of IETE, ISTE, OSI and fellow of IE (I). Also, he is member of IEEE, OSA, IEICE and SPIE. He has published around 175 papers in National and International Conference Proceedings and Journals. He has co-authored a book, published by PHI. His areas of interest are Optical Communication, Networks, Antennas, Electromagnetic Fields and Wireless Communication.

Delay and Jitter in Networks with IPP Traffic: Theoretical Model

Adnan Huremovic[a], Mesud Hadzialic[b]
[a] Faculty of Electrical Engineering, University of Sarajevo, Sarajevo 71000, Bosnia-Herzegovina
Email: adnan.huremovic@bhtelecom.ba
[b] Faculty of Electrical Engineering, University of Sarajevo, Sarajevo 71000, Bosnia-Herzegovina
Email: mesud.hadzialic@etf.unsa.ba

Abstract— **In this paper we analyze delay and jitter in networks with traffic modelled as Interrupted Poisson process (IPP), and relatively small traffic loads. In one-node analysis, we estimate the probability for delay bounds violation, and we obtain expression for the jitter, with respect to phase probabilities, traffic load, and tagged traffic share in aggregate traffic flow. We also analyze delay and jitter for simple tandem network, where we propose a model for end-to-end jitter. Our research shows how end-to end jitter is conditioned with phase probabilities of the incoming process, and we determine the nature of that correlation. Finally, we estimate the probability for end-to-end delay bounds violation, with respect to the jitter occurring on network nodes. Our propositions lead to some fast-to-compute approximations for the limit cases, which we propose as useful in evaluation of QoS constraints for real IP traffic.**

Index Terms— **delay, jitter, IPP, QoS, IP traffic**

I. Introduction

DELAY and jitter are two crucial QoS parameters for inelastic applications over IP networks. If delay or jitter constraints are not met, quality of experience on user level for inelastic application would degrade to unacceptable. It is of great importance to find a usable theoretical model to predict behaviour of these parameters. The model itself should describe measured traffic with desired accuracy, but also, one should be able to conduct fast reconstruction of the model parameters from the measurement results. If these conditions are fulfilled, we can use the results based on our model for admission purposes, i.e., to enforce QoS bounds for all inelastic applications in the network. In this paper we propose the analytical model for delay and jitter, based on Interrupted Poisson Process (IPP) as incoming traffic. Main motivation for this paper is to analytically describe delay and jitter behaviour for traffic model that is suitable for real IP traffic. Model based on IPP lies between simpler Poisson traffic model, and more suitable models for real IP traffic, such as MMPP with provisional number of phases.

Markov Modulated Poisson Processes (MMPP), and its special case IPP are widely used in traffic modelling, with recapitulation in [1]. Construction of all types of MMPP from sampled traffic is thoroughly described in literature, and, specifically, construction of IPP from sampled traffic can be achieved through techniques described in [2]. Main contribution in our work presented in this paper, compared to earlier works, is that we provide results for delay and jitter in closed form for one node and N-node case, with respect to various ratios of tagged and background traffic, traffic loads, and phase probabilities of incoming traffic. Our results can be further used for relatively fast delay and jitter prediction for real IP traffic.

Paper is organized in six main sections and the conclusion. After a brief insight of previous work, in third section we analyze delay and jitter for one node. We conclude this part with our proposition for probability of QoS violation, as function of traffic parameters (tagged and background traffic intensity, phase probabilities) and node parameters. We also propose a model for one-node jitter, including Poisson traffic model as one special case, which is validated in fourth section. In fifth section we analyze end-to-end jitter for number of consecutive nodes. We propose approximation for queue correlation and a formula for jitter estimation. We also analyze end-to-end delay, and its relation to jitter, and propose limit values for different cases of incoming traffic, which can be used as a rule of thumb for delay and jitter estimation. Numerical evaluation for N-node case is described in sixth section.

II. Related Work

Paper [1] contains basic conclusions related to delay analysis, elaborated more in [2] for IPP, and [3], [4] for MMPP. Detailed analysis of jitter for MMPP arrivals is done in [5], where model of correlation statistics for MMPP/M/1/K system was obtained. Although very useful for our N-node analysis, [5] does note provide exact expression for jitter in closed form. Other analytical models known to the authors for jitter are obtained in [6] and [7], for periodic CBR traffic. Novelty in our work compared to [7]can be noted in the traffic model we used. In [7], authors assume periodic traffic with constant packet size, combined with background traffic. Also, these authors used one approximation for waiting time in GI/GI/1 system, while in third section, we used exact waiting time expression to obtain closed-form expression for the jitter. Results in [7] are applicable for CBR flows and several background flow distributions. Our results apply to any traffic flow, with IPP parameters reconstructed from measured traffic. End-to-end jitter model based on

doi:10.4304/jnw.9.12.3392-3399

Poisson arrivals is described in [8]. This model provides relatively simple, closed form expressions for jitter, and it is also used here as a reference for some limit cases of IPP. In [9], authors conducted jitter analysis of IPP stream with Poisson background traffic and exponential serving on one node. Authors described jitter on one node through percentile of the inter-departure time, and also did a numerical simulation for small tagged flow intensities compared to the background traffic. Jitter for IPP traffic is described in [10], with no delay or loss probability taken into account and some results formulated in [10] are expanded here with additional delay analysis.

Simultaneous analysis of several QoS parameters (multidimensional QoS) became prominent with appearance of large number applications sensitive to different QoS parameters. Reference related to our work is [11], where authors described relations between delay and loss for exponential ON/OFF traffic. Authors did not analyze jitter, and traffic model is more primitive as compared to IPP. Other papers related to subject include bandwidth sharing with delay differentiation in [12], and also valuable for our work, delay and jitter correlation for Poisson flows [13].

III. One Node Analysis

In following we take that during active (ON) phase, total traffic intensity λ is a sum of tagged traffic intensity λ_k and background traffic λ_0. During OFF phase, all sources are inactive. Transition rates from OFF to ON phase and back are denoted as ω_1 and ω_2, respectively. Traffic modelled with IPP is determined with transition matrix $\mathbf{Q}$ and rate matrix Λ_k:

$$\mathbf{Q} = \begin{bmatrix} -\omega_1 & \omega_1 \\ \omega_2 & -\omega_2 \end{bmatrix}, \quad \Lambda_k = \begin{bmatrix} 0 & 0 \\ 0 & \lambda_k \end{bmatrix} \tag{1}$$

We take into account exponential serving intensity on node, and denote it by parameter value μ. We define delay on one node for tagged flow k as:

$$T_{i,k} = r_{i,k} - t_{i,k} \tag{2}$$

where $r_{i,k}$ is departure time of last bit for packet i and flow k, and $t_{i,k}$ is arrival time of first bit for packet i and flow k. Jitter for tagged flow k is defined, according to [14] as:

$$J = E[|T_{i+1,k} - T_{i,k}|] \tag{3}$$

where $T_{i+1,k}$ and $T_{i,k}$ are delays on the node for two consecutive packets of tagged flow. In further analysis we will assume that $T_{i+1,k}$ and $T_{i,k}$ are *iid* random variables. Assumption holds for cases when average intensity of the tagged flow λ_k is relatively small compared to aggregate income traffic λ, and also for all other cases with relatively small load. In other words, we assume that packet leaves the node before other packet of tagged flow arrives (generally for small load), or that two consecutive packets of tagged flow are separated by large number of other packets, so we can neglect correlation of waiting times $T_{i+1,k}$ and $T_{i,k}$. Precisely, for small load case, packet interarrival time τ_k for tagged flow is larger than than sojourn packet time T_{i+1} on node. We provide exact calculations for premises introduced above, but we offer results to approximate delay and jitter behaviour for other cases as well (e.g. case $\lambda_k \gg \lambda_0$ or $\rho \to 1$). Reasoning is as follows. First, in [5], authors claim that correlation values for IPP on node are not significantly affected by phases. Conservative approach would be to assume correlation that corresponds to Poisson arrivals. Additionally, results in [8] for Poisson arrivals show that similar premises for traffic load and tagged traffic weight lead to results applicable to all cases with high accuracy. To conclude, violation of assumptions related to delay correlation in all cases should not be worse than violation made in [8], where simulation confirmed results over all loads and traffic ratios.

A. Delay on One Node

In stationary state (equilibrium), mean node occupancy $\overline{N}$ is:

$$\overline{N} = \mu \overline{T} \tag{4}$$

Random variables T_i and T_{i+1} are described with pdfs:

$$f_{T_{i+1}}(t) = \begin{cases} 0 & t < 0 \\ k_1 r_1 e^{-r_1 t} + k_2 r_2 e^{-r_2 t} & t > 0 \end{cases} \tag{5}$$

$$f_{T_i}(t) = \begin{cases} 0 & t < 0 \\ K(k_1 r_1 e^{-r_1 t} + k_2 r_2 e^{-r_2 t}) & 0 < t < \tau \\ 0 & t > \tau \end{cases} \tag{6}$$

where K is normalization constant:

$$K = \{k_1(1 - e^{r_1 \tau_k}) + k_2(1 - e^{r_2 \tau_k})\}^{-1} \tag{7}$$

Our assumptions (light traffic load or $\lambda_k \ll$) results with large interarival period τ_k (regardless of values of ω_1, and ω_2). In these cases, for the sake of simplicity, we take $K = 1$.

If we accept maximum allowed delay (due to QoS constraints) as T_{max}, we can treat all packets that violate T_{max} as lost (they need to be resent). Using effective bandwidth theory, the probability of delay violation is given with [15], [16], [17]:

$$P_{viol} = P\{N_q > N_{max}\} \approx e^{-\mu T_{max} \delta} \tag{8}$$

where N_q is queue occupancy, N_{max} is maximum allowed queue occupancy, and δ satisfies following condition when $t \to \infty$:

$$\delta = max\{s : A(s) \leq \mu\} \tag{9}$$

where $A(s)$ is limit value of effective bandwidth for IPP flow [18]:

$$A(s) = \lim_{t \to \infty} A(s,t) = \frac{\sqrt{\beta^2 + 4\lambda\omega_1(e^s - 1)} - \beta}{2s} \tag{10}$$

and

$$\beta = \omega_1 + \omega_2 - \lambda\omega_1(e^s - 1) \tag{11}$$

Condition for effective bandwidth (9) with (10) leads to:

$$\frac{\sqrt{\beta^2+4\lambda\omega_1(e^s-1)}-\beta}{2s}\leq\mu \tag{12}$$

arranging (12) and squaring the root, we get:

$$e^s-1\leq\frac{\mu s^2+s(\omega_1+\omega_2)}{\frac{\lambda}{\mu}\omega_1+\lambda s} \tag{13}$$

Expression (13) cannot be solved in closed form, but setting inequality:

$$s+\frac{s^2}{2}<\frac{\mu s^2+s(\omega_1+\omega_2)}{\frac{\lambda}{\mu}\omega_1+\lambda s} \tag{14}$$

we derive conservative estimation for δ:

$$\delta=-\frac{\Phi}{2}+\frac{1}{2}\sqrt{\Phi^2-4\Psi} \tag{15}$$

where $\lambda=\lambda_k+\lambda_0$, and:

$$\Phi=2+\frac{\omega_1}{\mu}-\frac{2\mu}{\lambda} \tag{16}$$

$$\Psi=\frac{2\omega_1}{\mu}-\frac{2(\omega_1+\omega_2)}{\lambda} \tag{17}$$

In (8) and (15) we give connection between traffic parameters $(\lambda,\omega_1,\omega_2)$, node parameter μ, and probability that tagged flow would override maximum allowed delay. If we decide to treat all violated packets as lost, we can use (8) to estimate loss probability.

B. Jitter on One Node

Waiting times on node are described with pdf [1]:

$$f_\eta(t)=k_1r_1e^{-r_1t}+k_2r_2e^{-r_2t} \tag{18}$$

where

$$\eta=\mu-\lambda \tag{19}$$

$$r_1=\frac{1}{2}\left\{\eta+\omega_1+\omega_2+\sqrt{(\eta+\omega_1+\omega_2)^2-4\eta\omega_1}\right\} \tag{20}$$

$$r_2=\frac{1}{2}\left\{\eta+\omega_1+\omega_2-\sqrt{(\eta+\omega_1+\omega_2)^2-4\eta\omega_1}\right\} \tag{21}$$

$$k_1=\frac{\eta-r_2}{r_1-r_2},\quad k_2=1-k_1 \tag{22}$$

The pdf for random variable $\Delta=T_{i+1}-T_i$ can be obtained by:

$$f_\Delta(z)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\delta(z-(x-y))f_{T_{i+1}}(x)f_{T_i}(y)\,dx\,dy \tag{23}$$

Mean jitter value can be found now by:

$$J_k=\overline{|\Delta|}=\int_{-\infty}^{0}(-z)f_\Delta(z)\,dz+\int_0^{\infty}zf_\Delta(z)\,dz \tag{24}$$

After the integration we get:

$$J_k=\frac{K}{r_1r_2(r_1+r_2)}e^{-2(r_1+r_2)\tau_k}\{A+B+D_{12}+D_{21}\} \tag{25}$$

where

$$\begin{aligned}A &= -\left(k_2^2r_1e^{2r_1\tau_k}+k_1^2r_2e^{2r_2\tau_k}\right)(r_1+r_2)\\ &\quad -2k_1k_2\left(r_1^2+r_2^2\right)e^{(r_1+r_2)\tau_k}\end{aligned} \tag{26}$$

$$\begin{aligned}B &= \left(k_2^2r_1+k_1^2r_2\right)(r_1+r_2)e^{2(r_1+r_2)\tau_k}\\ &\quad +2k_1k_2\left(r_1^2+r_2^2\right)e^{2(r_1+r_2)\tau_k}\end{aligned} \tag{27}$$

$$\begin{aligned}D_{ij} &= -e^{(2r_i+r_j)\tau_k}k_j(r_i+r_j)\left[k_jr_ir_j\tau_k\right.\\ &\quad \left.+k_i(r_i-r_j+r_ir_j\tau_k)\right],\\ &\quad (i,j=1,2)\end{aligned} \tag{28}$$

Consider extreme values in (25). For $\omega_2\to0$, arriving process tends to Poisson, and we can easily get:

$$\lim_{\omega_2\to0}J_k=\frac{1}{\eta}\left(1-\eta\tau_ke^{-\eta\tau_k}-e^{2\eta\tau_k}\right) \tag{29}$$

which is identical to jitter expression for Poisson arrivals in [8]. If, on the other hand, we let IPP be sparse to maximum ($\omega_1\to0$, $\pi_{\mathrm{OFF}}=\omega_2/(\omega_1+\omega_2)\to1$), we get:

$$\lim_{\omega_1\to0}J_k=\infty \tag{30}$$

In other words, when ON phase probability tends to 1, our expression for jitter tends to an already known formula given in [8]. Jitter behaviour in this case depends on $\rho=(\lambda_k+\lambda_0)/\mu$, and ratio of intensities λ_k and λ_0 . When input traffic becomes more bursty, jitter growth is mostly conditioned by phase probabilities, and increases as OFF phase probability grows.

Expression (25) deserves to be numerically validated, which we conduct in the following section by comparing our results with the existing results for the Poisson process.

IV. Numerical Evaluation for One-node Case

First we evaluate (25) for IPP with $\pi_{\mathrm{ON}}=\omega_1/(\omega_1+\omega_2)\to1$. In this case IPP degenerates to Poisson process and we will denote this as *degenerated IPP*. We take following parameter values: $\pi_{\mathrm{ON}}=0.95$, $\mu=5000$ and evaluate jitter behavior for $0<\rho<1$.

A. Dominant tagged flow

For dominant tagged flow ($\lambda_k\gg\lambda_0$) results are shown on Fig.1. We get jitter values for degenerated IPP close (but always larger, since ω_2 has some nonzero value) to the jitter calculated for Poisson process using (29) obtained in [8]. More important, we can see that the jitter obtained with (25) has a concave form, and decreases as aggregate load increases, as shown in [8] for Poisson arrivals.

B. Dominant background flow

For dominant background flow ($\lambda_k\ll\lambda_0$) the results are shown on Fig.2. We can see that jitter values calculated by (25) are again very close to the values we obtained using (29). Note that, due to small share of tagged flow, jitter nature is different: as load increases, the jitter tends to infinity. This is also intuitively expected: with given $\lambda_k\ll\lambda_0$, consecutive packets of tagged flow are

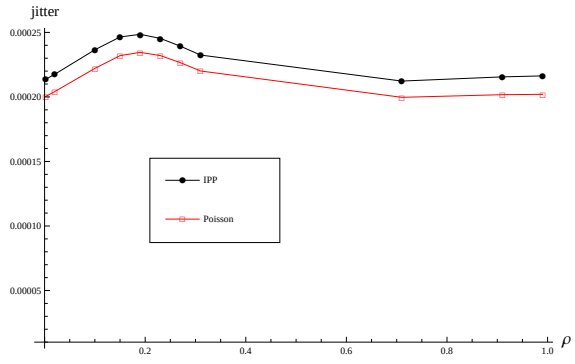


Figure 1. One-node jitter for IPP and Poisson process: $\pi_{\mathrm{ON}} = 0.95$, $\lambda_k \gg \lambda_0$.

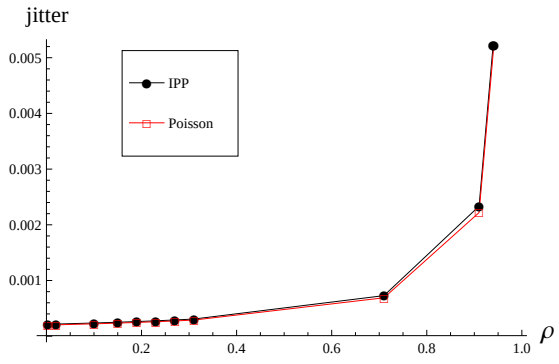


Figure 2. One-node jitter for IPP and Poisson process: $\pi_{\mathrm{ON}} = 0.95$, $\lambda_k \ll \lambda_0$.

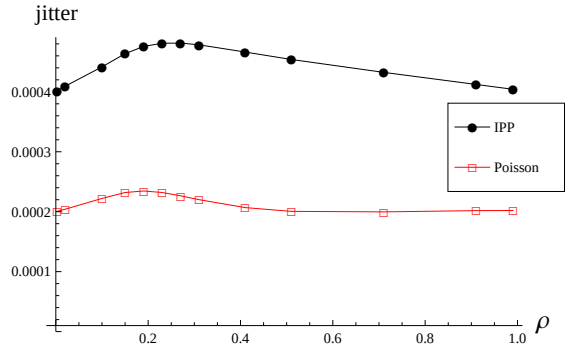


Figure 3. One-node jitter for IPP and Poisson process: $\pi_{\mathrm{ON}} = 0.5$, $\lambda_k \gg \lambda_0$.

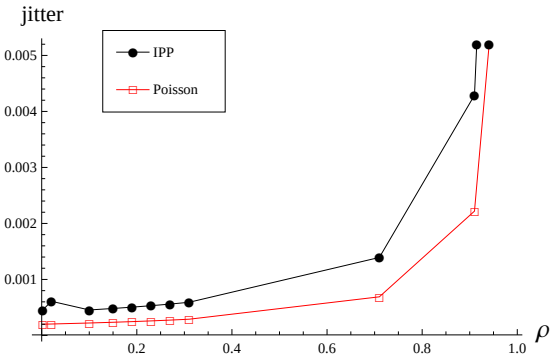


Figure 4. One-node jitter for IPP and Poisson process: $\pi_{\mathrm{ON}} = 0.5$, $\lambda_k \ll \lambda_0$.

increasingly more spaced as aggregate load increases, and jitter increases more with each packet.

C. Non-degenerated IPP

We evaluate (25) for non-degenerated ("pure") IPP, and take $\pi_{\mathrm{ON}} = \pi_{\mathrm{OFF}} = 0.5$. Results for $\lambda_k \gg \lambda_0$ and $\lambda_k \ll \lambda_0$ are shown on Fig.3 and Fig.4, respectively. We see, by comparing jitter behaviour and values on Fig.3 and Fig.1, that decrease of π_{ON} leads to larger jitter values, and that jitter dependence on ρ is similar for both cases. Comparison of Fig.2 and Fig.4 also yields to conclusion that, with smaller π_{ON}, jitter values for IPP are larger, beside the fact that jitter in these cases ($\lambda_k \ll \lambda_0$) diverges when $\rho \to 1$. These results confirm that, for real variable traffic, we can expect larger jitter values than obtained with (29). Furthermore, effect of π_{ON} and ρ are different for $\lambda_k \gg \lambda_0$ and $\lambda_k \ll \lambda_0$, as shown on Fig.5 and Fig.6. For $\lambda_k \gg \lambda_0$, jitter dominantly depends on phase probabilities and grows as π_{OFF} increases. For $\lambda_k \ll \lambda_0$ jitter dominantly depends on aggregate traffic load, and grows as traffic load tends to 1.

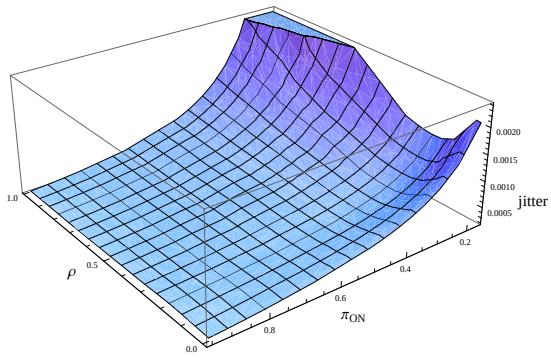


Figure 5. One-node jitter for IPP as function of π_{ON} and ρ with $\lambda_k \gg \lambda_0$.

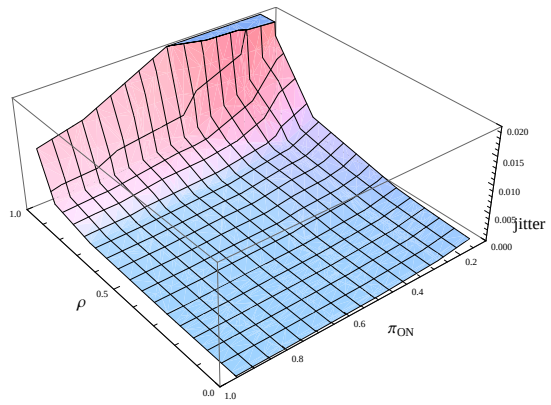


Figure 6. One-node jitter for IPP as function of π_{ON} and ρ with $\lambda_k \ll \lambda_0$.

V. N-Node Analysis

In N-node case, we analyze simple tandem network with N nodes. We assume that there are no losses, so all the traffic (tagged flow λ_k and background flow λ_0) that enters the first node is served and goes to the second node, and so on, until the last node. We denote serving intensity on n-th node as $\mu^{(n)}$. Note that, due to queuing

and jitter on first node, values for $\tau_k^{(n)}$ and $\lambda_k^{(n)}$ change for every node n, and traffic load $\rho^{(n)}$ differs on each node. Precisely, it decreases compared to the traffic load on first node $\rho^{(1)}$. That is the reason why it is necessary to first analyze jitter on each node.

A. Jitter analysis

For jitter estimation in case of IPP traffic and multiple node case, significant problem is to evaluate correlation of waiting times on adjacent nodes. Other papers analyze jitter phenomena for N-node case, where the most relevant for our subject is [5], where authors showed that jitter correlation for adjacent nodes cannot be calculated precisely in closed form, especially for nodes with infinite memory. In [5] authors also presented results for jitter and queue autocorrelation in time domain for CBR flows and finite memory, as special case of MMPP/M/1/K system. In [8], N-node case is analyzed, for Poisson traffic model.

Consider N nodes in tandem. In following, we index tagged flow with subscript k, and all variables corresponding to node n with superscript (n). Resulting jitter for tagged flow is limited with:

$$J_k^{[1\ldots N]} \leq \sum_{n=1}^{N} J_k^{(n)} \tag{31}$$

where $J_k^{(n)}$ is jitter for flow *k*, on node *n*. Equality holds in cases without correlation. For jitter on second node, we must take into consideration delay correlation on the entrance on second node. If this correlation is significant, jitter on second node will be proportionally smaller. Furthermore, due to jitter on first node, mean interarrival time on the entrance on second node would increase by $J_k^{(1)}$. This change will also affect parameter η on second node (even if we take $\mu^{(n)} = \mu$ on every node). If we denote dependence of jitter in (25) on τ_k and η as $f(\tau_k, \eta)$, and delay correlation factor as K_k, we can use following expression for jitter on second node [8]:

$$J_k^{(2)} = K_k^{(2)} f(\tau_k + J_k^{(1)}, \eta^{(2)}) \tag{32}$$

where mean interarrival time for IPP is:

$$\tau_k = \frac{k_1'}{r_1'} + \frac{k_2'}{r_2'} = \frac{\omega_1 + \omega_2}{\lambda_k \omega_1} \tag{33}$$

and

$$r_1' = \frac{1}{2}\left\{\lambda_k + \omega_1 + \omega_2 + \sqrt{(\lambda_k + \omega_1 + \omega_2)^2 - 4\lambda_k\omega_1}\right\} \tag{34}$$

$$r_2' = \frac{1}{2}\left\{\lambda_k + \omega_1 + \omega_2 - \sqrt{(\lambda_k + \omega_1 + \omega_2)^2 - 4\lambda_k\omega_1}\right\} \tag{35}$$

$$k_1' = \frac{\lambda_k - r_2'}{r_1' - r_2'}, \quad k_2' = 1 - k_1' \tag{36}$$

$K_k^{(2)}$ is correlation factor, and problem of N-node jitter reduces to determine $K_k^{(n)}$. We propose $K_k^{(n)}$ as:

$$K_k^{(n)} = 1 - \left|\overline{q_i^{(n)} q_{i+1}^{(n)}}\right| \tag{37}$$

where $\overline{q_i^{(n)} q_{i+1}^{(n)}}$ is autocorrelation function of queue occupancy. For an N-node case, we can take the same expression as in [8]:

$$J_k^{[1\ldots N]} = f(\tau_k, \eta^{(1)}) + \sum_{n=2}^{N} K_k^{(n)}\left(\lambda_k^{(n)}\right) f(\tau_k^{(n)}, \eta^{(n)}) \tag{38}$$

where

$$\eta^{(n)} = \mu - \lambda^{(n)} \tag{39}$$

$$\tau_k^{(n)} = \tau_k + \sum_{i=2}^{n} J_k^{(i-1)} \tag{40}$$

$$\lambda_k^{(n)} = \frac{\omega_1 + \omega_2}{\tau_k^{(n)} \omega_1} \tag{41}$$

$\lambda^{(n)}$ denotes aggregate arrival traffic at the entry of node n. Correlation factor can be determined using [5]:

$$\overline{q_i^{(n)} q_{i+1}^{(n)}} \approx \int_0^\infty {R_q}^{(n)}(\tau) {f_{\zeta_1}}^{(n)}(\tau)\, d\tau \tag{42}$$

where $q_i^{(n)}$ represents number of packets on node n in moment when i^{th} packet arrives, ${R_q}^{(n)}(\tau)$ is queue autocorrelation function for time interval τ on node n, ${f_{\zeta_k}}^{(n)}(\tau)$ is time pdf for k units to arrive on n-th queue, and $k = 1$. Using Chapman-Kolmogorov forward equation we get:

$$f_{\zeta_1}(\tau) = \frac{\omega_1}{\omega_1 + \omega_2} \lambda e^{-(\lambda + \omega_2)\tau} \tag{43}$$

Now we estimate the queue autocorrelation $R_q(\tau)$. For MMPP/M/1 system, and even for final state MMPP/M/1/K, exact calculation of $R_q(\tau)$ is practically infeasible. However, [5] and [19] showed that queue length and its autocorrelation function can relatively fast converge to a steady state, which can be used for estimation of $R_q(\tau)$. Particularly for IPP, due to the smoothing effect of silence period (OFF phase), rough estimation of $R_q(\tau)$ would be to assume that queue autocorrelation function is not appreciably affected by the ON and OFF phases [5]:

$$R_q(\tau) \approx E\{q(t)q(t+\tau) | \text{IPP is ON}\} \tag{44}$$

This assumption reduces the calculation of $R_q(\tau)$ for well-known M/M/1 system. In this paper we use estimation from [20], [21]:

$${R_q}^{(n)}(\tau) = \frac{\frac{1}{2}\left(e^{-A^{(n)}\tau} + e^{-B^{(n)}\tau}\right) R^{(n)} + {L^{(n)}}^2}{R^{(n)} + {L^{(n)}}^2} \tag{45}$$

where

$$A^{(n)} = \frac{\left(1 - \rho^{(n)}\right)^2}{1 + \rho^{(n)} + \sqrt{\rho^{(n)}}} \tag{46}$$

$$B^{(n)} = \frac{\left(1 - \rho^{(n)}\right)^2}{1 + \rho^{(n)} - \sqrt{\rho^{(n)}}} \tag{47}$$

$$L^{(n)} = \frac{\rho^{(n)}}{1 - \rho^{(n)}} \tag{48}$$

$$R^{(n)} = \frac{\rho^{(n)}}{\left(1 - \rho^{(n)}\right)^2} \tag{49}$$

From (42), (43) and (45), we finally get:

$$\overline{q_i^{(n)} q_{i+1}^{(n)}} = \frac{{L^{(n)}}^2}{{L^{(n)}}^2 + {R^{(n)}}^2} \frac{\lambda_k^{(n)} \omega_1}{\omega_1 + \omega_2} \left(\frac{1}{\lambda_k^{(n)} + \omega_2} + \frac{1}{2} \frac{1}{A^{(n)} + \lambda_k^{(n)} + \omega_2} + \frac{1}{2} \frac{1}{B^{(n)} + \lambda_k^{(n)} + \omega_2} \right) \quad (50)$$

Now we are able to calculate end-to-end jitter values for IPP using (37), (38), and (50).

Consider the behaviour of $K_k^{(n)}(\lambda_k^{(n)})$ and end-to-end jitter (38) for some extreme values of ρ and π_{ON}. First, assume that $\pi_{\mathrm{ON}} \to 1$ ($\omega_2 \to 0$). In this case, IPP tends to Poisson process, and it is easy to find:

$$\lim_{\substack{\omega_2 \to 0 \\ \rho^{(n)} \to 0}} K_k^{(n)} \left(\lambda_k^{(n)} \right) = 1 \quad (51)$$

hence, $J_k^{[1 \ldots N]}$ tends to sum of individual jitter values for each node. For large loads:

$$\lim_{\substack{\omega_2 \to 0 \\ \rho^{(n)} \to 1}} K_k^{(n)} \left(\lambda_k^{(n)} \right) = 0 \quad (52)$$

In this case, end-to-end jitter tends to jitter value on the first node. Compare this to the expression for Poisson traffic model obtained in [8]. We get the same limit values:

$$\lim_{\rho^{(n)} \to 0} K_k^{(n)} \left(\lambda_k^{(n)} \right)_{\mathrm{Poisson}} = 1 \quad (53)$$

$$\lim_{\rho^{(n)} \to 1} K_k^{(n)} \left(\lambda_k^{(n)} \right)_{\mathrm{Poisson}} = 0 \quad (54)$$

For sparse IPP ($\omega_1 \to 0$) we get, for both limit values for $\rho^{(n)}$:

$$\lim_{\omega_1 \to 0} K_k^{(n)} \left(\lambda_k^{(n)} \right) = 1 \quad (55)$$

We conclude that, regardless of the load, end-to-end jitter tends to the sum of individual jitter values on each node. We summarize these limit values in Table I.

TABLE I.
LIMIT VALUES FOR $J_k^{[1 \ldots N]}$.

	$\rho^{(n)} \to 0$	$\rho^{(n)} \to 1$
$\pi_{\mathrm{ON}} \to 0$	$\sum_{n=1}^{N} J_k^{(n)}$	$\sum_{n=1}^{N} J_k^{(n)}$
$\pi_{\mathrm{ON}} \to 1$	$\sum_{n=1}^{N} J_k^{(n)}$	$J_k^{(1)}$

B. Delay analysis

Mean n-th node occupancy in equilibrium is:

$$\overline{N^{(n)}} = \mu^{(n)} \overline{T^{(n)}} \quad (56)$$

Denote maximum allowed end to end delay as $T_{max}^{[1..N]}$. Violation occurs for

$$\sum_{n=1}^{N} T^{(n)} > T_{max}^{[1..N]} \quad (57)$$

Violation probability is:

$$P_{viol}^{[1..N]} = P(T^{(1)} + \ldots + T^{(N)} > T_{max}^{[1..N]}) \quad (58)$$

First we determine conservative bound for delays on each node. Violation will not occur if, for every i holds:

$$T^{(i)} \leq \frac{T_{max}^{[1..N]}}{N} \quad (59)$$

Violation probability is then:

$$P_{viol}^{[1..N]} = 1 - P\left\{ \left(T^{(1)} \leq \frac{T_{max}^{[1..N]}}{N} \right) \& \ldots \& \left(T^{(N)} \leq \frac{T_{max}^{[1..N]}}{N} \right) \right\} \quad (60)$$

Using (8) we get:

$$P_{viol}^{[1..N]} = 1 - \prod_{n=1}^{N} (1 - e^{-\mu^{(n)} \frac{T_{max}^{[1..N]}}{N} \delta^{(n)}}) \quad (61)$$

where

$$\delta^{(n)} = -\frac{\Phi^{(n)}}{2} + \frac{1}{2} \sqrt{\Phi^{(n)2} - 4\Psi^{(n)}} \quad (62)$$

$$\Phi^{(n)} = 2 + \frac{\omega_1}{\mu^{(n)}} - \frac{2\mu^{(n)}}{\lambda^{(n)}} \quad (63)$$

$$\Psi^{(n)} = \frac{2\omega_1}{\mu^{(n)}} - \frac{2(\omega_1 + \omega_2)}{\lambda^{(n)}} \quad (64)$$

and $\lambda^{(n)} = \lambda_k^{(n)} + \lambda_0^{(n)}$, with jitter influence on $\lambda_k^{(n)}$ taken into account by (41). For this value of $\delta^{(n)}$, we can determine upper bound for $P_{viol}^{[1..N]}$, but we need to analyze traffic on each node. However, we can reduce (61) for cases when background traffic is constant on each node: $\lambda_0^{(n)} = \lambda_0$, or the ratio between tagged traffic and background traffic is constant. In these cases, load on first node is largest, since $\lambda_k^{(n)}$ decreases as n grows, due to jitter effect shown in (41). Violation is not going to occur if largest delay (on first node) is not larger than $\frac{T_{max}^{[1..N]}}{N}$. Probability (61) reduces to:

$$P_{viol}^{[1..N]} = e^{-\mu^{(1)} \frac{T_{max}^{[1..N]}}{N} \delta^{(1)}} \quad (65)$$

Last expression requires only calculation for first node case, and simplifies estimation of violation probability for N-node case.

VI. NUMERICAL EVALUATION FOR N-NODE CASE

In following numerical results, we take simple tandem network with N=5 successive nodes. We assume that there are no losses, so all traffic (tagged flow λ_k and background flow λ_0) lead to first node is served and goes to the second node, and so on, until the last node. We take that every node has same serving intensity μ. Note that, due to queuing and jitter on first node, as well as values for $\tau_k^{(n)}$ (40) and $\lambda_k^{(n)}$ (41), traffic load $\rho^{(n)}$ differs on each node. Precisely, it decreases compared to the traffic load on first node $\rho^{(1)}$. We calculate jitter value on each node according to corresponding $\rho^{(n)}$.

First we evaluate approximation for degenerated IPP: $\pi_{\mathrm{ON}} = 0.95$, $\mu = 5000$ and evaluate jitter values for $\rho^{(1)} \in (0, 1)$. Results for both cases correspond well to the conclusions summarized in Table I, and already known jitter for Poisson process.

A. Dominant tagged flow

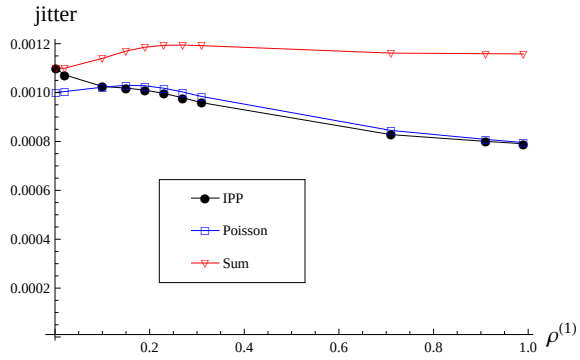


Figure 7. End-to-end jitter: $\pi_{\mathrm{ON}} = 0.95$, $\lambda_k \gg \lambda_0$.

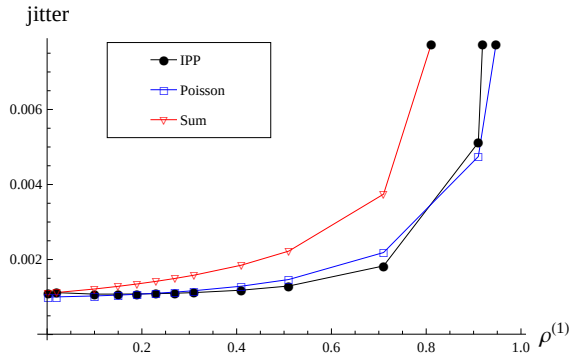


Figure 8. End-to-end jitter: $\pi_{\mathrm{ON}} = 0.95$, $\lambda_k \ll \lambda_0$.

For dominant tagged flow ($\lambda_k \gg \lambda_0$) results are shown on Fig. 7. As expected, obtained jitter values for degenerated IPP are close to the jitter calculated for Poisson process. End-to end jitter decreases when $\rho^{(1)} \to 1$.

B. Dominant background flow

For dominant background flow ($\lambda_k \ll \lambda_0$) results are shown on Fig. 8. End-to-end jitter in this case increases with $\rho^{(1)} \to 1$. Also, jitter for IPP takes close values to Poisson process.

C. Non-degenerated IPP

We evaluate (38) for non-degenerated IPP, and we take $\pi_{\mathrm{ON}} = 0.67$. On Fig.9 and Fig.10 we show results for $\lambda_k \gg \lambda_0$ and $\lambda_k \ll \lambda_0$, respectively.

Increasing π_{OFF} leads to jitter values larger than ones from Poisson process, but still smaller than sum of individual jitter for $\lambda_k \gg \lambda_0$ (Fig. 9). Difference is even more significant for $\lambda_k \ll \lambda_0$ (Fig. 10). On Fig.11 and Fig.12 we show jitter behaviour for wide range of π_{ON} and $\rho^{(1)}$. Jitter heavily depends on phase probabilities for $\lambda_k \gg \lambda_0$. In this case, jitter grows with increase of π_{OFF}, similar as in one-node case. For $\lambda_k \ll \lambda_0$, jitter grows as π_{ON} and $\rho^{(1)}$ grow.

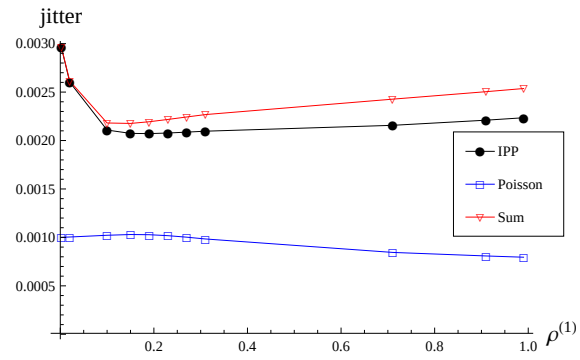


Figure 9. End-to-end jitter: $\pi_{\mathrm{ON}} = 0.67$, $\lambda_k \gg \lambda_0$.

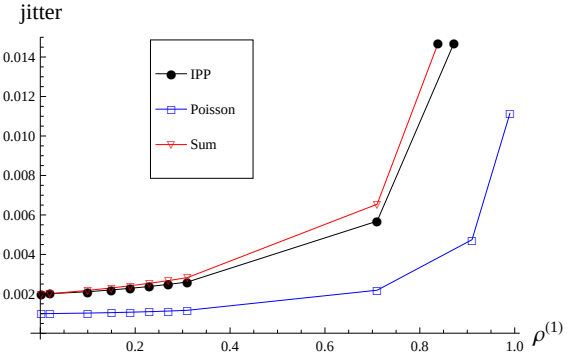


Figure 10. End-to-end jitter: $\pi_{\mathrm{ON}} = 0.67$, $\lambda_k \ll \lambda_0$.

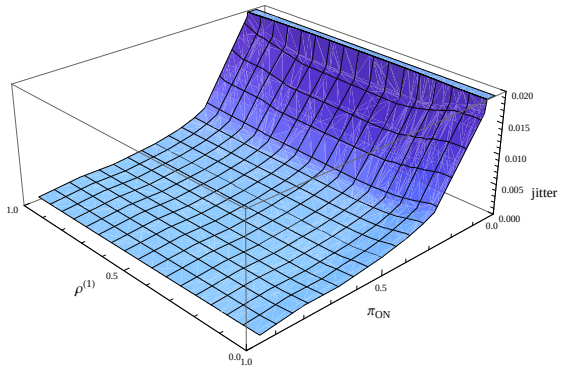


Figure 11. End-to-end jitter for IPP as function of π_{ON} and $\rho^{(1)}$ with $\lambda_k \gg \lambda_0$.

VII. Conclusion

In this paper we proposed a theoretical model for delay and jitter for small load and IPP traffic. We estimate probability of delay QoS bound violation for one node, as well as end-to-end case, based on theory of effective bandwidths. In one node analysis we show how delay violation probability depends on incoming process phase

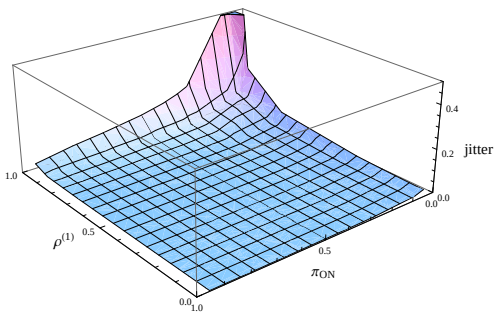


Figure 12. End-to-end jitter for IPP as function of π_{ON} and $\rho^{(1)}$ with $\lambda_k \ll \lambda_0$.

probabilities and traffic load. In our jitter analysis, we describe jitter dependence on phase probabilities, traffic load, and ratio of tagged and background traffic. On the basis of previous work, we propose our theoretical results even for cases with significant traffic loads, and tagged traffic share. For dominant tagged flow, phase probabilities heavily affect jitter behaviour compared to effect of traffic load. In these cases, concave nature of the jitter due to load intensity is inferior compared to the effects of phase probabilities, and jitter grows with increase of OFF phase probability (burstiness of traffic). In cases with dominant background traffic, effects of load are more expressed, and jitter grows as load increases.

In N-node analysis, we propose formula for end-to end jitter estimation. Numerical results show that jitter values on consecutive nodes for very small ON phase probabilities, as well as in cases with very small loads, do not have significant correlation, and can be approximated as sum of individual jitter values on each node. In case of large load and relatively smooth traffic, total jitter can be approximated with jitter value on first node. We also show that jitter for Poisson arrivals can be obtained as a special case of our model. We show that jitter for real time traffic (which is more similar to IPP compared to Poisson process) is larger than one obtained using the Poisson model. Finally, in our delay analysis, we propose expression for end-to-end delay violation probability, but also give approximation for cases with constant background traffic, and constant ratio of tagged and background traffic. For further considerations, similar analysis with loss effects included would result in more accurate results. Obtained equations and their limit cases give simple rule-of-thumb relations useful for fast jitter and delay estimation in real networks.

ACKNOWLEDGMENT

The authors are grateful to Kenan Suruliz for valuable discussion and suggestions to improve the presentation of this paper.

REFERENCES

[1] W. Fischer and K. S. Meier-Hellstern, "The Markov-Modulated Poisson Process (MMPP) Cookbook," *Perform. Eval.*, vol. 18, no. 2, pp. 149–171, 1993.

[2] I. Ide, "Superposition of interrupted poisson processes and its application to packetized voice multiplexers," in *Twelveth International Teletraffic Congress*, 1988, p. 3.

[3] L. Gün, *"An Algorithmic Analysis of the MMPP/G/1 Queue"*, ser. Technical research report. Systems Research Center, University of Maryland, 1988.

[4] H. Heffes and D. Lucantoni, "A Markov Modulated Characterization of Packetized Voice and Data Traffic and Related Statistical Multiplexer Performance," *IEEE J.Sel. A. Commun.*, vol. 4, no. 6, pp. 856–868, Sept. 1986.

[5] C. A. Fulton and S. qi Li, "Delay jitter first-order and second-order statistical functions of general traffic on high-speed multimedia networks," *IEEE/ACM Trans. Netw.*, vol. 6, no. 2, pp. 150–163, 1998.

[6] K. Sohraby and A. Privalov, "End-to-end jitter analyisis in networks of periodic flows," in *INFOCOM*, 1999, pp. 575–583.

[7] O. Brun, C. Bockstal, and J.-M. Garcia, "Analytic approximation of the jitter incurred by CBR traffics in IP networks," *Telecommunication Systems*, vol. 33, no. 1-3, pp. 23–45, 2006.

[8] H. Dahmouni, A. Girard, and B. Sansò, "An analytical model for jitter in IP networks," *Annales des Télécommunications*, vol. 67, no. 1-2, pp. 81–90, 2012.

[9] G. Geleji and H. Perros, "Jitter analysis of an IPP tagged traffic stream in an {IPP,M}/M/1 queue," *Annals of Telecommunications*, pp. 1–12, 2013.

[10] A. Huremovic, M. Hadzialic, and F. Skaka, "Analytical model for jitter in networks with IPP traffic," in *5th International Workshop on TRaffic Analysis and Characterization, TRAC 2014 (IWCMC 2014 - TRAC Workshop)*, Nicosia, Cyprus, Aug. 2014.

[11] N. X. Liu and J. S. Baras, "Modelling Multi-dimensional QoS: Some Fundamental Constraints," *Int. J. Commun. Syst.*, vol. 17, no. 3, pp. 193–215, Apr. 2004.

[12] X. Zhou, D. Ippoliti, and L. Zhang, "Fair bandwidth sharing and delay differentiation: Joint packet scheduling with buffer management," *Comput. Commun.*, vol. 31, no. 17, pp. 4072–4080, Nov. 2008.

[13] H. Dahmouni, A. Girard, M. Ouzineb, and B. Sansò, "The impact of jitter on traffic flow optimization in communication networks," *IEEE Transactions on Network and Service Management*, vol. 9, no. 3, pp. 279–292, 2012.

[14] C. Demichelis and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)," RFC 3393 (Proposed Standard), Internet Engineering Task Force, November 2002.

[15] F. P. Kelly, S. Zachary, and I. Ziedins, Eds., *Notes on Effective Bandwidth*. Oxford University Press, 1996, pp. 141–168.

[16] C.-S. Chang and J. A. Thomas, "Effective bandwidth in high-speed digital networks," *IEEE J.Sel. A. Commun.*, vol. 13, no. 6, pp. 1091–1100, Sept. 2006.

[17] X. Yu, I. L.-J. Thng, and Y. Jiang, "Measurement-based effective bandwidth estimation for long range dependent traffic," in *TENCON 2001. Proc. of IEEE Region 10 Internat. Conf. on Electrical and Electronic Technology*, vol. 1, 2001, pp. 359–365 vol.1.

[18] A. Berger and W. Whitt, "Effective bandwidths with priorities," *Networking, IEEE/ACM Transactions on*, vol. 6, no. 4, Aug 1998.

[19] L. A. Kulkarni and S. qi Li, "Transient behaviour of queueing systems with correlated traffic," *Perform. Eval.*, vol. 27/28, no. 4, pp. 117–145, 1996.

[20] W. W. J. Abate, "The Correlation Functions od RBM and M/M/1," *Communications in Statistics*, 1998.

[21] M. Roughan, "A Comparison of Poisson and Uniform Sampling for Active Measurements," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 12, pp. 2299–2312, 2006.

Adnan Huremovic received the B.Sc. and M.Sc. degree in Electical Engineering from the University of Sarajevo, Bosnia-Herzegovina, in 2003, and 2007 respectively. He is currently working towards his Ph.D. degree in QoS issues at University of Sarajevo, Bosnia-Herzegovina. His major interests are teletraffic engineering, network management, and quality of service.

Mesud Hadzialic received the B.Sc., M.Sc., and Ph.D. degree in Electrical Engineering from University of Sarajevo, Bosnia-Herzegovina, in 1978, 1987, and 2001, respectively. He is an associate professor at the Faculty of Electrical Engineering, University of Sarajevo, Bosnia-Herzegovina. His research interests include simulation of the telecommunication networks and channels, wireless networks and fading simulators, traffic models, and EMC issues.

A Novel Method to Improve the Accuracy of the RSSI Techniques Based on RSSI-D

Xiaofeng Li [1, 2], Liangfeng Chen [1, 2*], Jianping Wang [3], Zhong Chu [4], and Bing Liu [5]
1. University of Science and Technology of China, Hefei 230026, China
2. Institute of Intelligent Machines, Chinese Academy of Sciences, Hefei 230031, China
3. Hefei University of Technology, Hefei 230009, China
4. Hefei University, Hefei 230601, China
5. Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, China
*Corresponding Author Email: quinear@gmail.com

***Abstract*—In this paper, a novel method is proposed to estimate the distance between sensor nodes based on a statistical model of GMM, which is established with the offline RSSI values, called RSSI-D. In order to estimate the arguments of RSSI-D with unobserved latent variables, EM is used to calculate the arguments of RSSI-D as accurately as possible in this paper. After RSSI-D established, the probability of sub models of RSSI-D that the online RSSI values obey can be calculated by the posterior probability in Bayesian statistics. Based on the probability of sub models corresponding to the distance segment, the distance between sensor nodes can be estimated by the weighted value of distance segments. In the simulation, the accuracy is improved obviously by RSSI-D and the arguments such as K and N are provided by the simulation results.**

***Index Terms*—RSSI; GMM; EM; Posterior Probability**

I. INTRODUCTION

Recently, Wireless Sensor Networks (WSN), which consists of a lot of small devices deployed in a physical environment called sensor nodes which have special capabilities, such as communicating with their neighbors, sensing and recording data and processing, has been widely used in many areas [1], such as object detection, target tracking, security surveillance, and environmental monitoring etc. Most of these applications require the knowledge of the position of sensor nodes in WSN [2].The current localization algorithms can be classified into two categories: the range-based method and the range-free scheme [3]. Most range-based algorithms have been studied to improve the position accuracy, because this scheme offers better accuracy than the range-free method generally. The range-based localization depends on the assumption that sensor nodes have the ability to estimate the distance or angle to other nodes by means of one or more of the following measurements: angle of arrival (AoA), time of arrival (ToA), time difference of arrival (TDoA), and received signal strength indicator (RSSI) [4].Most of the measurements need additional costly hardware support except RSSI. So, RSSI range-based localization systems [5]-[8] are much more popular since most of radio transceiver chips for WSN provide the RSSI circuitry by themselves. However, the distance estimated by RSSI is usually inaccurate and unreliable [5], because the wireless signals are more likely to suffer from multipath interference, reflection, refraction, obstruction interference, etc.A key point to improve the accuracy of the sensor nodes' position is raising the measurement accuracy of the RSSI technique based on the original RSSI data with noise.

A number of methods have been proposed recently to improve the accuracy of the RSSI techniques. Some have focused on obtaining good RSSI values based on eliminating noise, such as Kalman Filter (KF) [9], Extended Kalman Filter (EKF) [10] and Particle Filter (PF) [11]. These methods that can get more smooth RSSI values than the original data but need to establish the accurate mathematical system models are hard to be used in the reality due to their complex. Other approaches have been studied on the statistical property which represents the relationship between RSSI and the distance between sensor nodes. These methods based on establishing the injective function between the RSSI values and the distance have been proposed in the [12]-[14]. However, the injective function above can't be established accurately as one RSSI value can be measured at different distance between sensor nodes because of the multipath interference or the reflection.

It's easier to find the relationship between RSSI and the distance than to establish an accurate mathematical system, so based on the statistical property of the test data, a novel method in this paper is proposed to improve the accuracy of the RSSI techniques. In this paper, a Gaussian Mixture Model (GMM) that describes the relationship between the RSSI values and the distance is established with the offline RSSI values measured by anchor sensor nodes, which is called the RSSI-D model. And then, the EM algorithm that is an iterative method for finding maximum likelihood or maximum a posteriori (MAP) estimate of parameters in statistical models where the model depends on unobserved latent variables, is used to estimate the arguments of RSSI-D with a few of the offline RSSI values. Based on the established RSSI-D model with the estimating arguments, the probability of each sub model of RSSI-D, which the online RSSI value belongs to, can be calculated by the posterior probability

doi:10.4304/jnw.9.12.3400-3406

in Bayesian statistics. Finally, the distance between sensor nodes is estimated by the weighted corresponding distance to each sub model, since the probability that the online RSSI value belongs to the sub model is larger than the set threshold and regarded as the weight of each corresponding distance.

The rest of the paper is organized as follows: the RSSI-D model that is established based on the offline RSSI data and its arguments estimated by EM are introduced in Section II. Based on RSSI-D, the distance between sensor nodes can be estimated in Section III. Simulation results with comparison of the performances of RSSI-D and Log-D are presented in Section IV where the influence of the number of simple points on accuracy of RSSI is discussed. The conclusion of the paper is shown in Section V.

II. RSSI-DMODEL

The Path Loss (PL) model that means the relationship between received power and distance is formed as:

$$\mathrm{PL}(d) = \mathrm{PL}(d_0) + 10n\log_{10}(d/d_0) + X_\sigma \quad (1)$$

where n = [2,5], n=2 for free space. The $\mathrm{PL}(d_0)$is the received power from the transmitter at a known distance $d_0$that is usually set to one meter andX_σ denotes a zero mean Gaussian random variable that reflects the interference from indoor environment [15].

As described in (1), the injective function from the RSSI value to the distance can't be established because of the random variableX_σ. In order to improve the accuracy of RSSI, we study on the statistical property of the RSSI values firstly and try to establish a most accurate model.

A. The Test Scenario

The model is established based on the offline RSSI values that were collected by the sensor nodes deployed in the iron mine. As a special application scenario, the special features of the topology structure of WSN are described as follows:

1) Straight or Cross Path

The road in the mine is always straight as a beeline though having a cross. The length of the road may be several hundred meters or even more, but the width is always smaller than 4 meters and the height of the road space is about 3 meters only. In the scenario, the distance between sensor nodes can be equal to the distance in X-Direction.

2) Independent of Network Connectivity

The anchor sensor nodes whose locations are known and accurate are deployed to cover the areas which the un-anchor sensor nodes may reside in. Meanwhile, the method proposed in this paper does not need depending on neighboring sensor nodes communication.

3) Having the Moving Un-Anchor Sensor Nodes

The un-anchor sensor nodes located in the mine can be classified into two categories, as the moving sensor nodes and the static nodes. The static nodes are usually used to collect the arguments of the circumstances of the mine, and the moving nodes that are wore on the workers or the harvesters are used to get the location information. In the mine, the maximum speed of the moving sensor nodes wore on the workers is lower than three meters per second, and that of the harvesters is smaller than eight meters per second.

In order to collect more RSSI data and avoid the local optimization problem because the sample capacity of the RSSI values are small, we collected the RSSI data of moving sensor nodes in two scenarios described in details in next section.

B. TheTest System

1) The Information of the Sensor Nodes

a) Seven anchor nodes are located with known coordinates manually at a segment of a crossroad in the mine, of which the width is 3.8 meters, the height is 3.0 meters, the length in X-Direction is 500 meters and the length in Y-Direction is 200 meters. All anchor nodes are located at a fixed height as 2.5 meters, and the un-anchor sensor nodes are distributed randomly. The scenario above is shown as Fig. 1.

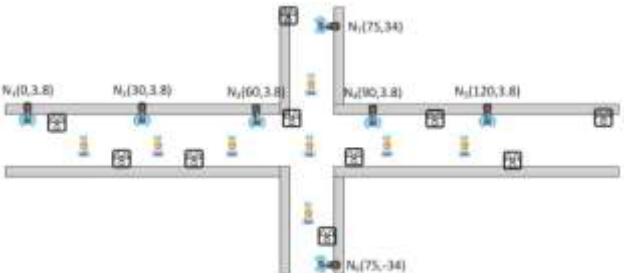


Figure 1. The locations of sensor nodes

b) All sensor nodes are composed by the same hardware, such as ZigBeeCC2430 in this paper, and equipped with omni-directional antennas and RF transceivers with built-in RSSI circuitry. In addition, as in the case of some other schemes, anchors are assumed to have a larger communication range than un-sensor nodes so that their beacons can reach all wireless nodes in the network.

c) For simplicity and ease of presentation, we limited that all moving sensor nodes wore on the workers were at the height of one meter.

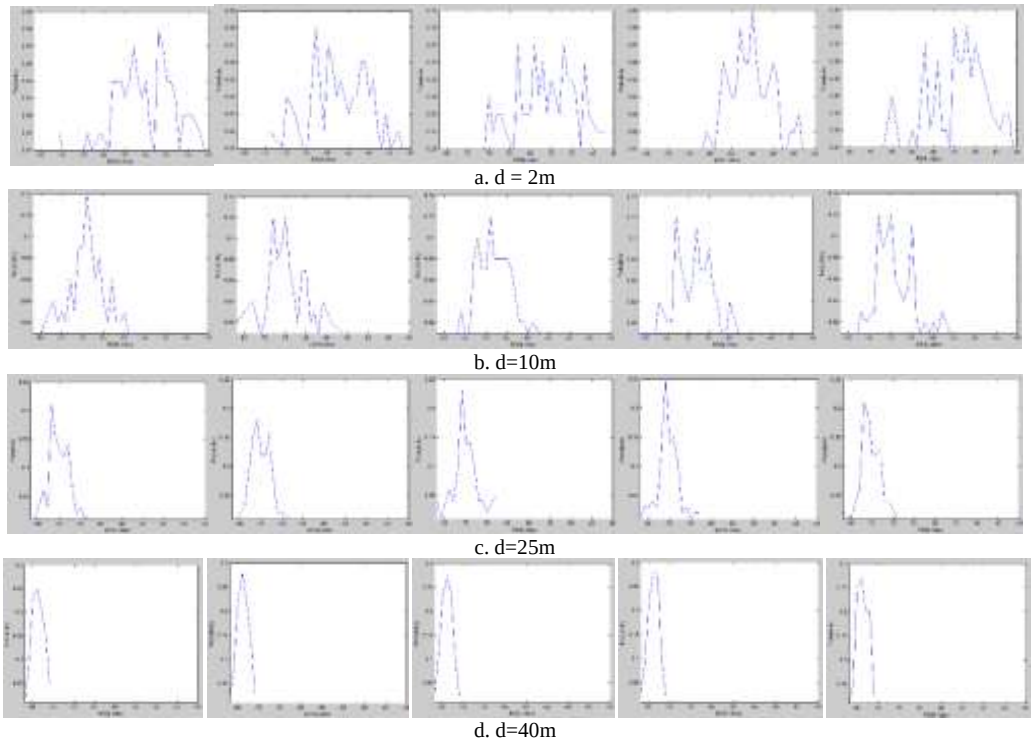
2) The Testing Ways

a) A scenario is that the moving sensor nodes move far from or close to anchor nodes with a fixed step each time such as one meter a step, meanwhile, the moving nodes remain stationary with a long time at each place of the moving paths.

b) Another scenario is that the moving sensor nodes make a round trip to the areas where RSSI of moving nodes can be measured by the anchor nodes at a random speed.

3) Analyzing the RSSI Data

All RSSI values of the moving sensor nodes measured in the scenarios above by the anchor nodes are recorded and sent to the central computer by the network. The results analyzed in many ways by the Mat lab software are described as follows:



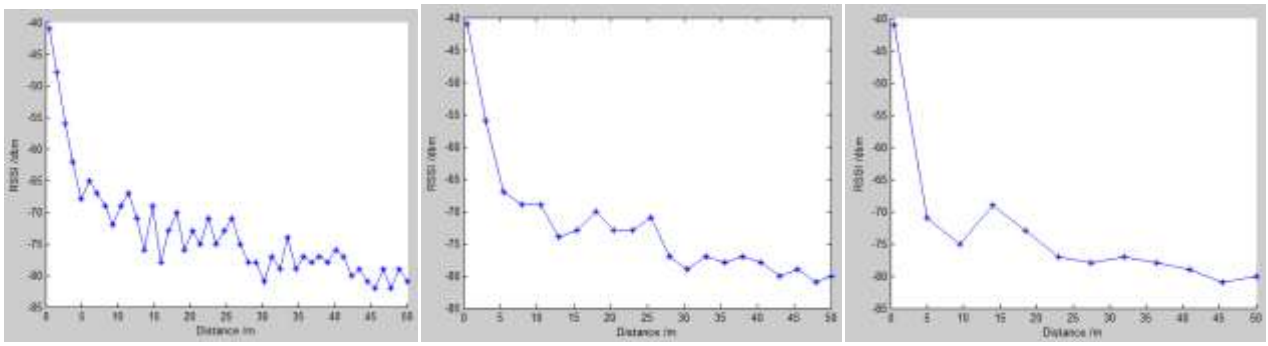
a. d = 2m

b. d=10m

c. d=25m

d. d=40m

Figure 2. The RSSI values at different places.



a. v=1.1m/s b. v=2.5m/s c. v=5.5m/s

Figure 3. The relationship between RSSI of the moving sensor node moving at the different fixed speed and the distance

a) We gathered 500 RSSI values of the moving sensor nodes that kept static one minute at least at each place on the path. The RSSI data with noises are shown in Fig. 2.

Based on Fig. 2, some conclusions can be proposed as follows:

The RSSI values are variable because of the noises so as that the injective function from RSSI to the distance can't be established in reality as well. Hence, the distance calculated by (1)is very unreliable.

The smaller is the distance between anchor sensor nodes and the moving sensor nodes, the more the RSSI values will change. On the contrary, the larger is the distance, the more stationary are the RSSI values.

The probability distribution of the RSSI values with different distances between the anchor sensor nodes and the moving sensor nodes is the Gauss distribution with different mean values and variances as well. Meanwhile, the mean values and the variance are becoming smaller with the distance decreasing.

The conclusions discussed above are suitable to any anchor node though it may measure the different RSSI values at the same scenario.

b) We selected the RSSI values of one moving sensor node, which made round trips to the areas at the different fixed speed, measured by one anchor node to observe the influence of the speed of moving nodes on the relationship between RSSI and the distance. After filtering the very large and very small RSSI values, the relationship between the average values of the remainder RSSI values and the distance between the moving sensor nodes and the anchor nodes is shown as Fig. 3.

The conclusion that can be proposed is that the phenomenon that the RSSI values decrease with the distance increasing is always perfect though the moving sensor node moves at the different speed.

Based on the conclusions discussed above, the model that describesthe relationship between the RSSI values of moving or static sensor nodes measured by any anchor node and the distance can be established.

C. RSSI-D

1) RSSI-D—one GMM

The model that describes the relationship between RSSI and the distance is shown as follows:

$$\mathrm{P}(\mathrm{RSSI}|\theta) = \sum_{k=1}^{K} \alpha_k \phi(\mathrm{RSSI}|\theta_k) \quad (2)$$

where the coefficient $\alpha_k \geq 0$ and $\sum_{k=1}^{K} \alpha_k = 1$; the function $\phi(\mathrm{RSSI}|\theta_k)$ that is the Gauss distribution function is described as:

$$\phi(\mathrm{RSSI}|\theta_k) = \frac{1}{\sqrt{2\pi}\sigma_k} e^{\frac{-(\mathrm{RSSI}-\mu_k)^2}{2\sigma_k^2}} \quad (3)$$

where $\theta_k = (\mu_k, \sigma_k^2)$ is the arguments of the kth model $\phi(\mathrm{RSSI}|\theta_k)$; $\mu k$and σ_k^2 are the mean value and variance of the kth model; k=1,…,K, K is the total number of the Gauss distribution functions.

As the conclusions mentioned in Section II.B, the K value of RSSI-D is decided by the segmented distance mode. For example, when a moving sensor node moved with the speed one meter per second, the distance segment is R divided by one, while R is the anchor node's communication distance. So, the more are the distance segments, the larger is the K and the better is the model because of the degree of the distance subdivision, however, the more complex is the model to calculate.

So, the key point establishing the model is how to estimate the arguments expect K as accurately as possible with a few of sample data.

2) Calculating the Arguments of RSSI-D

In this paper, the RSSI-Darguments are estimated by the expectation maximization (EM) algorithm that is an iterative method for finding maximum likelihood or maximum a posteriori (MAP) estimates of parameters in statistical models, where the model depends on unobserved latent variables.

In order to describe the holonomic data by the few sample points, the unobserved latent RSSI variables are recorded as γ_{jk}:

$$\gamma_{jk} = \begin{cases} 1, \text{the oberved value obeys the kth model} \\ 0, \text{others} \end{cases} \quad (4)$$

while the holonomic data can be described as: $(\mathrm{RSSI}_j, \gamma_{jk})$, where j=1,…,N and k=1,…,K; N is the total number of the observed RSSI values.

So, the maximum likelihood of the holonomic data is described as:

$$\mathrm{P}(\mathrm{RSSI}, \gamma|\theta) = \prod_{j=1}^{N} P\left(\mathrm{RSSI}_j, \gamma_{j1}, \ldots, \gamma_{jK}|\theta\right) = \prod_{k=1}^{K}\prod_{j=1}^{N}[\alpha_k \phi(\mathrm{RSSI}_j|\theta_k)]^{\gamma_{jk}} \quad (5)$$

Algorithm 1EM is used to estimate the arguments of RSSI-D

Inputs: the offline RSSI values collected by the anchor nodes are recorded as: RSSI1, RSSI2,…, RSSIN, and the RSSI-D model.

Outputs: the arguments of RSSI-D.

The steps calculating the maximum likelihood of the model above in algorithm 1 are described as follows:

a) The values of α_k,θ_k and K are initialized by the statistic result of the RSSI values by the method discussed above.

b) Expectation step (E step): Calculate the expected value of the γjk[13], with respecting to the conditional distribution of γ_{jk} given RSSI under the current estimate of the parameters θ_k:

$$\hat{\gamma}_{jk} = \mathrm{E}(\gamma_{jk}|\mathrm{RSSI}, \theta) = \frac{\alpha_k \phi(\mathrm{RSSI}_j|\theta_k)}{\sum_{k=1}^{K} \alpha_k \phi(\mathrm{RSSI}_j|\theta_k)} \quad (6)$$

c) Maximization step (M step): Calculate the parameters that maximize the quantity above:

$$\hat{\mu}_k = \frac{\sum_{j=1}^{N} \hat{\gamma}_{jk}\,\mathrm{RSSI}_j}{\sum_{j=1}^{N} \hat{\gamma}_{jk}} \quad (7)$$

$$\hat{\sigma}_k^2 = \frac{\sum_{j=1}^{N} \hat{\gamma}_{jk}\,(\mathrm{RSSI}_j - \hat{\mu}_k)^2}{\sum_{j=1}^{N} \hat{\gamma}_{jk}} \quad (8)$$

$$\hat{\alpha}_k = \frac{\sum_{j=1}^{N} \hat{\gamma}_{jk}}{N} \quad (9)$$

where $k = 1,2,\ldots,K$.

d) Iterate steps b) and c) until convergence.

In order to estimate the arguments of RSSI-D rapidly and accurately, the initial values ofθ are assigned by the statistic values of 500 RSSI data that was collected at each distance segment that a moving sensor node moved far from an anchor node at the one meter per step, while K=50 as R=50 meters , $\alpha_k = 1/50$.

III. CALCULATING THE DISTANCE

After RSSI-D established accurately, the distance corresponding to the RSSI value can be estimated by the kth model with the maximum probability calculated by (2), because the kth model is established based on the RSSI values that are measured at the distance segment k*R/K, where the result of R/K means that the moving node moves at a fixed step at once. So, based on the kth model that the online RSSI may obey in the maximum possibility, the distance between the sensor nodes can be estimated with RSSI finally.

This procession can be described by the posterior probability in Bayesian statistics, and the probability of each sub model that the online RSSI values may obey can be calculated by (10):

$$\mathrm{P}(\theta_k|\mathrm{RSSI}) = \frac{\alpha_k \phi(\mathrm{RSSI}|\theta_k)}{\sum_{k=1}^{K} \alpha_k \phi(\mathrm{RSSI}|\theta_k)} \quad (10)$$

So, the kth model that RSSI obeys can be selected by (11):

$$\mathrm{RSSI} \in \theta_k,\ \mathrm{P}(\theta_k|\mathrm{RSSI}) = \max_{1 \leq k \leq K} \mathrm{P}(\theta_k|\mathrm{RSSI}) \quad (11)$$

Though, the distance estimated by (11) may be not exact because that the $\mathrm{P}(\theta_k|\mathrm{RSSI})$ value may be a good approximation to its neighbors, such as $\mathrm{P}(\theta_k|\mathrm{RSSI})$ or $\mathrm{P}(\theta_{k-1}|\mathrm{RSSI})$, especially the RSSI values are very low or K is large, based on the conclusions discussed in Section II.B. So, a threshold of possibility values is set here to select proper models to calculate the distance between sensor nodes with different weight that is equal to the probability of the model that RSSI obeys.

Based on the established RSSI-D and combining the posterior probability in Bayesian statistics, the distance between sensor nodes can be estimated by (12) shown as follows:

$$d = \frac{\sum_{k=1}^{M} P(\theta_k|RSSI)d_k}{\sum_{k=1}^{M} P(\theta_k|RSSI)} \quad (12)$$

where: d_k is the distance that corresponds to the kth model; M is the number of the selected models whose probability is larger than the threshold; K is the total number of the models.

IV. SIMULATION

As the conditions of the test have been described in the section II.A, the simulation with the collected test data is described in three manners.

a) The accuracy of the RSSI techniques by RSSI-D is compared to that by Log-D that is a typical curve smoothly fitting method.

b) The influence of K on the measure accuracy.

c) The influence of N on the measure accuracy.

A. Errors

By default, the number of the RSSI values of a moving senor node collected at each distance segment is 500; Meanwhile, K value is equal to 50 that means that the moving sensor node is far from the anchor node whose communication range is 50 meters at one meter per step. That means K=50 and N=25000. In order to decrease the influence of the noise on the measure accuracy of RSSI, the very large or small RSSI values of each measurement are filtered and the average value of the remainder RSSI is used to estimate the distance. The analyzing result is shown as follows:

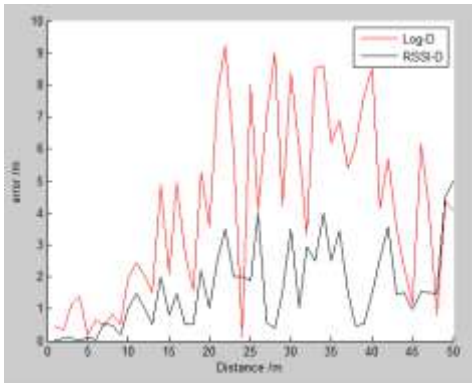


Figure 4. RSSI-D vs Log-D in accuracy

The conclusions based on the Fig.4 are proposed as follows:

a) RSSI-D has a better performance on the accuracy of RSSI than Log-D, and the minimum errors and the average of the errors of RSSI-D are lower obviously.

b) The smaller is the distance between sensor nodes, especially it is smaller than 10 meters, and the better is the accuracy by both methods. Because that when the distance is smaller, the RSSI values measured by the anchor node are less affected by ambient noise and more reliable.

c) When the distance between the moving sensor node and the anchor node is very large, such as that it's lager than 40 meters, the difference of the RSSI values of the moving sensor node at different distance segment is very little, and the RSSI values measured at one place may be the same as those measured at other place. So, the error may increase by both methods because the same RSSI value is corresponding to the different distance in large probability.

d) The accuracy of RSSI estimated by RSSI-D is much better than that of Log-D when the distance between the moving sensor node and the anchor node is in the range [10, 40]. The reason is that the pattern of the RSSI values can be described more accurate by RSSI-D than by Log-D that is only a curve.

B. K values vs.Errors

As mentioned above, K is decided by the number of the distance segments that is equal to the anchor's communication distance divided by the sampling interval. In order to analyze the influence of K on the errors, we set the sampling interval, which means the distance that the moving sensor node moves one step, as 0.5m, 1m and 2m. Meanwhile, keeping N always equal to 25000 in each test scenario. That's to say, K is 100, 50 and 25 corresponding to the intervals. The error between the estimated distance and the reality distance is shown in Fig. 5 and Table I.

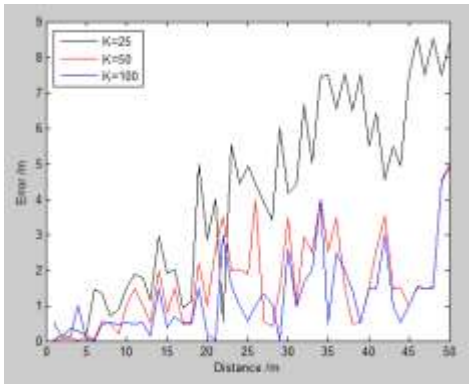


Figure 5. K values vs. errors

TABLE I. K VALUES VS. ERRORS

K	K=25	K=50	K=100
Max error	8.56	5	4.92
Min error	0.11	0	0
Average error	4.09	1.61	1.2

The conclusions can be proposed as follows:

a) The larger is K that means the number of the distance segments and also means the number of the sub models of RSSI-D, and the smaller are the errors that include max errors, min errors and average errors. However, the calculating complexity increases with K in a power.

b) The errors have little difference though the K values are striking difference when the distance between the moving sensor node and the anchor node is larger than 30 meters. The reason is same to what has been concluded in previous section.

C. N values vs.Errors

In general, the larger is the number of sample points, and the more accurately is the distance estimated by RSSI-D, however the more complex is the calculating. Meanwhile, N is large so that RSSI-D is hard to update and to be used in reality. In order to estimate a proper value of N, we set N as different values such as5000, 15000, 25000 and 30000with a proper K, which can be assigned to 50 based on the result analyzed above, to compare the accuracy each other. The result is shown in Fig. 6 and Table II as follows:

The conclusion is that the arguments of RSSI-D that are estimated by EM have good accuracy when N is larger than 15000.

TABLE II. THE N VALUES VS. ERRORS

Num(N/50)	Num=100	Num=300	Num=500	Num=600
Max error	4.95	4.49	5	4.8
Min error	0.12	0.01	0	0
Average error	1.91	1.75	1.61	1.57

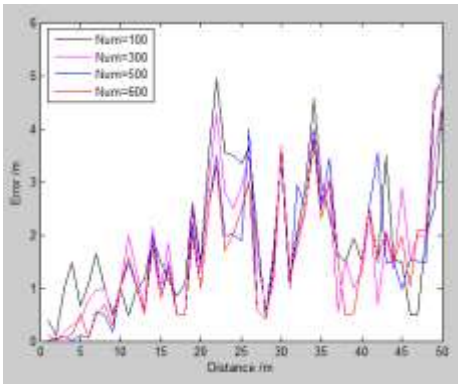


Figure 6. The N values vs. errors

V. CONCLUSION

The contributions of this paper are concluded here:

a) A novel method that is used to increase the accuracy of RSSI techniques is proposed in this paper based on RSSI-D that is a type of GMM and established with the offline RSSI values and their statistic patterns.

b) It's impossible to collect all offline RSSI values, so the EM algorithm is used to estimate the arguments of RSSI-Din this paper, where the model depends on unobserved latent variables.

c) Based on the accurate RSSI-D model, the distance between sensor nodes can be estimated in two steps. Firstly, sub models of RSSI-D that the RSSI values obey in large probability, which is calculated by the posterior probability in Bayesian statistics and larger than a threshold set by test are selected; secondly, the distance between sensor nodes is equal to the weighted value ofthe distance segments corresponding to the sub models of RSSI-D, whose weight is equal to the probability above.

d) In simulation, the accuracy of RSSI estimated by RSSI-D is better than that of Log-D obviously. Meanwhile, K and N are analyzed in the simulation and set properly to have a good accuracy and decrease the calculating complexity as much as possible.

How to increase the sensor node's position accuracy based on the method proposed in this paper is our next work.

ACKNOWLEDGMENT

This work was supported by the Key Program for Natural Science Foundation of Anhui Province Education Development under Grant (GrantNo.KJ2013A225), and "Twelfth Five Year Plan" of Anhui province science and technology projects(GrantNo.11010402183).

REFERENCE

[1] Y. S. E. C. I.F. Akyildiz, W. Su, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks. *John Wiley & Sons*, 2005.

[3] S. Meguerdichian, S. Slijepcevic, V. Karayan, and M. Potkonjak, "Localized algorithms in wireless ad-hoc networks: location discovery and sensor exposure, in," *in Proceedings of the Second ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobi-Hoc*? 2001, 2001, pp. 106–116.

[4] G. Blumrosen, B. Hod, T. Anker, D. Dolev, and B. Rubinsky, "Enhanced calibration technique for rssi-based ranging in body area networks," *Ad Hoc Networks*, vol. 11, no. 1, pp. 555 – 569, 2013.

[5] Z. J. Qiao Gangzhu, "An improved rssi localization method suitable for dynamic environments," *Journal of Computer Research and Development*, vol. 47, no. z2, pp. 111–114, 2010.

[6] H. Miura, K. Hirano, N. Matsuda, H. Taki, N. Abe, and S. Hori, "Indoor localization for mobile node based on rssi," *in Knowledge-Based Intelligent Information and Engineering Systems, ser. Lecture Notes in Computer Science*, B. Apolloni, R. Howlett, and L. Jain, Eds. Springer Berlin Heidelberg, 2007, vol. 4694, pp. 1065–1072.

[7] S. Tian, X. Zhang, P. Liu, P. Sun, and X. Wang, "A rssi based dv-hop algorithm for wireless sensor networks," *in Wireless Communications, Networking and Mobile Computing*, 2007. WiCom 2007. International Conference on, Sept 2007, pp. 2555–2558.

[8] Z. Shan and T.-S. Yum, "Precise localization with smart antennas in ad-hoc networks," *in Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, Nov 2007, pp. 1053–1057.

[9] J. Yim, J. Joo, and C. Park, "A kalman filter updating method for the indoor moving object database," *Expert Syst. Appl.*, vol. 38, no. 12, pp. 15 075–15 083, Nov. 2011.

[10] H. Chen, D. Ping, Y. Xu, and X. Li, "A novel localization scheme based on rss data for wireless sensor networks," in Advanced Web and Network Technologies, and Applications, ser. Lecture Notes in Computer Science, H. Shen, J. Li, M. Li, J. Ni, and W. Wang, Eds. Springer Berlin Heidelberg, 2006, vol. 3842, pp. 315–320.

[11] F. Caballero, L. Merino, I. Maza, and A. Ollero, "A particle filtering method for wireless sensor network localization with an aerial robot beacon," *in Robotics and Automation, 2008. ICRA 2008. IEEE International Conference on*, May 2008, pp. 596–601.

[12] C. X.-h. ZHAO Zhao, "An improved localization algorithm based on rssi in wsn," *Chinese Journal of Sensors and Actuators*, vol. 22, no. 3, pp. 391–394, 2009.
[13] A. Awad, T. Frunzke, and F. Dressler, "Adaptive distance estimation and localization in wsn using rssi measures," in Digital System Design Architectures, Methods and Tools, 2007. DSD 2007. 10th Euromicro Conference on, Aug 2007, pp. 471–478.
[14] L. D.-d. e. a. SUN Pei-gang, ZHAO Hai, "Research on rssi-based location in smart space," *Acta Electronica Sinica*, vol. 35, no. 7, pp. 1240–1245, 2007.
[15] J. Andersen, T. Rappaport, and S. Yoshida, "Propagation measurements and models for wireless communications channels," *Communications Magazine, IEEE*, vol. 33, no. 1, pp. 42–49, Jan 1995.
[16] L. Hang, Statistical learning method. *Tsinghua University Press*, 2005.

Liangfeng Chen (Anhui, Hefei, 1986.03) He is currently working towards his Ph.D. degree in WSN at University of Science and Technology of China, and also a student in Institute of Intelligent Machines, Chinese Academy of Sciences. His current research interest includes wireless sensor network position, security and applied cryptography.

An Adaptative Energy Efficient Routing Protocol for MANET

Anil Singh
Medi-caps Institute of Technology and Management/Computer Science, Indore, India
Email: itanilmits@yahoo.co.in

Shashikala Tapaswi
ABV-Indian Institute of Technology and Management/Information Technology, Gwalior, India
Email: stapaswi@hotmail.com

***Abstract*—The dynamic nature of Mobile ad hoc network has several constraints like scalability, robust connectivity and limited power constraints. So an efficient routing protocol is required. It should be adaptable and able to maintain stable routes in spite of the dynamic network connectivity. This paper proposes a hybrid protocol, called Poly-Meshed routing protocol (PMRP). It is a cluster-based routing protocol. It deploys the concept of mesh tree. It minimized the control overhead while maintaining robust connectivity and scalability. PMRP uniquely addresses the issues of dynamic adaptation. It has a feature that enables an enhanced connectivity through a hierarchical cluster-based approach. It deploys virtual identifiers. The main advantage of PMRP over the various other MANET protocols lies in simplicity and low message complexity. The simulation results show that the PMRP perform better in terms of Packet Delivery Ratio, Routing Overhead, End to End delay, Effects of Non-Optimality, Configurability and Energy Consumption when compared with AODV (Ad hoc On demand Distance Vector) protocol.**

***Index Terms*—Clustering; MANET; AODV; Hybrid Routing; Non-optimality; Meshed Routing**

I. INTRODUCTION

The network technology is improving rapidly, and there is an increased adoption of non-centralized and adaptive networks. The adoption increases the demand of large scale ad hoc networks. The large-scale ad-hoc networks find applications in several areas which include consumer-owned networks, tactical military networks, natural disaster discovery services and vehicular networks. Ad hoc networks are resource constraint systems. When size of the network increases several types of challenges, like scalable routing, bandwidth, and battery power occurs.

The prevalent ad-hoc routing protocols such as DSDV (Destination-Sequenced-Distance-Vector), OSLR (Optimized Link State Routing), AODV and DSR (Dynamic Source Routing) only scaled to a limit of dozens or sometimes hundreds of nodes. But as the networks grow larger there is always a need for a routing protocol that performs efficiently so as to scale to larger networks.

Clustering is a solution for scalability. The process of dividing the network into interconnected substructures called clustering, and the interconnected substructures are called clusters. Clusterhead (CH) control the aggregation of nodes into clusters and provides a convenient framework for the development of important features such as channel access, routing and bandwidth allocation.

The paper proposes a hybrid protocol called Poly-Meshed Routing Protocol (PMRP). It is a cluster-based routing protocol, which utilizes the concept of mesh tree and aims at minimizing the control overhead while maintaining the robust connectivity and scalability. The traditional network requires multiple hops due to wireless range limitations. PMRP networks take care of this need. The node in PMRP act as host as well as routers and thus it uses an efficient routing protocol.

The primary focus of this work is on implementation of cluster-based routing protocol for large-scale networks and understand the protocol structure with their advantages. Simulation shows comparison of PMRP and prevalent mobile ad-hoc network protocol AODV. The performance of PMRP exhibit more resilient connectivity due to redundant routes, particularly for larger sized systems.

Rest of the paper is organized as follows, Section II describes related work in the area of hybrid routing, clustering and robust route connectivity in MANET. Section III describes in detail the PMRP with its working procedure. Section IV provides the simulation details, discusses performance and a comparison of the proposed protocol with AODV. Section V gives the conclusions.

II. RELATED WORK

The paper relates to routing and clustering algorithms for mobile ad hoc networks. The significance in this solution lies in the tightly integrated operations of routing and clustering. Following are the related studies.

M. Rezaee and Yagmaee [8] proposed a cluster-based routing protocol for ad hoc network. This approach is used on weight group for increasing cluster formation speed and provides more accessible network services. Recreating of clusters is rarely executed, and when two clusters are located in the same range, one of them

doi:10.4304/jnw.9.12.3407-3414

becomes the gateway of another. Gateways prevent cluster reconstructions. The routing is also done quickly because it depends on the address of CH. Route breaks are managed by CH. When any node in the route fails, CH may use another node to forward packets.

Srungaram and Prasad [1] proposed Enhanced CBRP (Cluster-based routing protocol). Enhanced CBRP improves the cluster stability and improves the functioning of traditional cluster-based routing protocol (CBRP). Weighted clustering algorithm enables better clustering approach and manages several routing challenges.

Saha and Chaki [4] proposed a Cluster-based Mobility Considered Routing Protocol for MANET. Load balance and mobility are critical parameters of this approach. Load balance plays a role in between CH. Mobility of node is used to form clusters. Nodes are placed in the corresponding cluster according to their mobility.

Aparna and Reza [2] proposed MODIFIED-AODV an improvement over the existing AODV protocol. The key idea is finding a robust route by making use of a metric called the Robust Route Index (RRI). RRI is computed as the weighted sum of path hop-length and average speed between the individual nodes with nodal delay identifiers such as congestion identifiers. In the algorithm, the node with highest RRI forwards the RREQ packet among multiple RREQ packets received. Unlike in AODV, here each node waits for a predefined amount of time in order to collect several RREQ packets and then selects the one that provides the highest robustness level while offering the shortest route among all such received RREQ packets.

Shenoy and Pam [10] proposed Multi Meshed Tree (MMT) routing algorithm. MMT used proactive routing scheme for high route robustness with a quick and simple forwarding approach based on virtual IDs (VID), by using the combined features of a tree and a mesh. The scheme support multi hop mobile nodes in a limited area with limited wireless hops from an Internet-connected gateway.

Nordstrom and Gunningberg [3] proposed robust and flexible MANET-INTERNET integration approach using AODV routing protocol. Indirection approach is integrated using tunnels with the AODV routing protocol. Default route forwarding is also integrated to compare the two approaches. Similar gateway discovery and route setup mechanism is used for both default route and tunneling. Proxy RREP solution is used for routing. The scheme uses RREQ to determine the route in the MANET as a normal process. A gateway replies by RREP to determine the locality of destination. The address locality check at gateway is implemented through a prefix check or using a visitor list. Flag G is used to mark gateways to indicate backup tunnels for faster hand off and I flag to distinguish internet host entry from normal MANET route entry.

Zhou and Gerla [7] proposed cluster-based inter-domain routing (CIDR) protocol. The clusters are formed depending on the geography, motion, or task. The CH acts as a local Domain Name System (DNS) for own cluster and its neighbor clusters. The advertising protocol acts as the Border Gateway (BG) protocol. The protocol routes the packets to remote nodes and to the local destinations through CH advertised routes and the local routing algorithm respectively. It provides efficient communication and scalability in large networks.

Chan and Wong [11] proposed IDRM (Inter-Domain routing protocol for MANETs). IDRM supports opaque interoperation among multiple domains of MANETs. It needs special nodes as gateways, whose role is to handle inter-domain routing and to bridge any technical stream that exists between MANETs at physical, MAC and network layers.

Chunhua and Cheng [9] proposed a protocol called KHCBRP (K-hop cluster-based routing protocol). It expands the range of electives CH to K-hops in which the concept of constraints degree is introduced to keep the CH election. KHCBRP also improves the routing by integrating the inter-cluster on-demand routing and the intra cluster table driven routing, which solve blindly "Broadcast" problem in cluster-based routing protocol (CBRP) and reduce redundant information and routing overhead in the networks.

Imm and Seah [6] proposed a variant of AODV, namely MobDHop-AODV, is introduced to work better than a stable, two-tier cluster structure formed by the MobDHop clustering algorithm. It makes use of the collection of the topology information stored at every CH. This prevents the need to flood the network with route request (RREQ) packets in the search for respective destinations.

III. METHODOLOGY

PMRP addresses the scalability in large wireless ad hoc networks using the hierarchical address structure and hybrid routing with proactive and reactive routing components which helps in reducing routing overheads. The algorithm is performed in two parts:

- Cluster Formation
- Routing

A. Cluster Formation: In this process mobile nodes organize themselves into clumps with an elected CH. The flow chart of the process is shown in Figure 1 and algorithm is as follows:

Step 1: A node joins the network with a unique identification number known as UID.

Step 2: The network Nodes then broadcast hello message in its transmission range to maintain their neighborhood.

Step 3: The CH election algorithm elects the CH based on the highest degree of neighbors. Once CH is elected, it continues for a predefined period or till it is disabled or dies.

Step 4: The CH sets the following parameters-

i. MAX Number of nodes in Cluster= MAX_CLUSTER_SIZE
ii. MAX Number of level in Cluster=MAX_HOP
iii. VID of CH= UID of CH
iv. Advertising Node= CH

Step 5: The Advertising node advertises its VID in its neighborhood.

Step 6: Neighbors of Advertising node hears the advertisement. If any of the neighbors wants to join the cluster, it sends a joining request to CH via Advertising node.

Step 7: CH receives joining request of a node and accepts the requesting node as a clusterclient(CC) if and only if

i. MAX_CLUSTER_SIZE<Total Number of nodes in Cluster.
ii. MAX_HOP<Level of requesting node.

Step 8: If requesting node satisfy step 7 then CH accepts a node as a CC and allocates a VID. The structure of CC VID is Advertising node VID appended with a single digit integer.

Step 9: CH registered CC and updates its routing table. If CC has more than one VIDs of different cluster then it is marked as Border or Gateway node.

Step 10: CH change the advertising node as a newly registered CC. If CC has more than one VIDs of same cluster then it advertises smallest length VID.

Step 11: Repeat Step 5 until the cluster has reached its maximum configurable size.

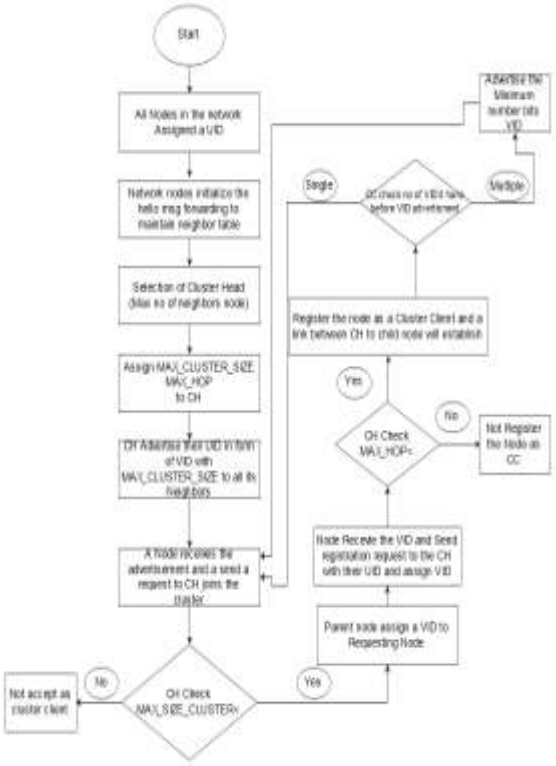


Figure 1. Cluster formation process

In cluster formulation process when a node joins the network, a UID (Unique Identifier) is assigned to the node and after that the nodes broadcast the hello messages to maintain the neighbor table. Then after node having the highest number of neighbors is elected as the CH. Once a CH is elected it continues for a predefined period or till it is disabled or dies and set cluster re-configurability parameters.

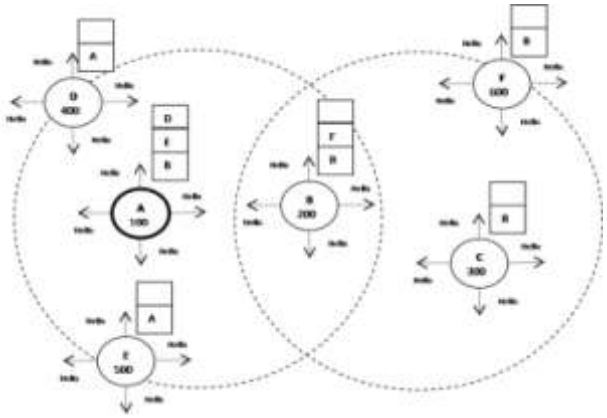


Figure 2. Clusterhead(CH) Election

Figure 2 shows Node A, B, C, D, E and F which join the network. The respective UIDs are 100, 200, 300, 400, 500 and 600. Each node then acquires number of its neighbor nodes by interactively exchanging HELLO MESSAGE. Node 'A' having highest number of neighbors is elected as CH. Node 'A' sets following cluster configurability parameters-

i. MAX Number of nodes in Cluster= MAX_CLUSTER_SIZE='n'
ii. MAX Number of level in cluster=MAX_HOP='m'
iii. VID of CH= UID of CH ='100'
iv. Advertising Node= CH =Node 'A'

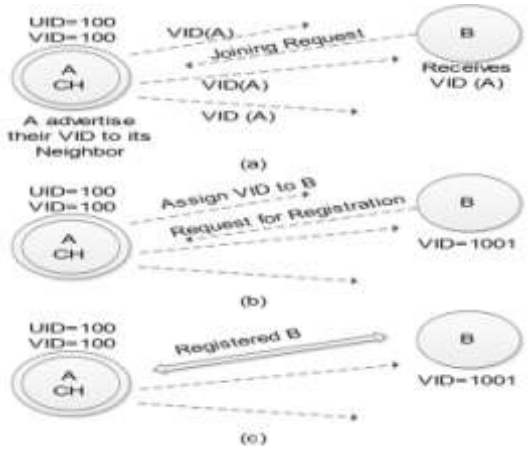


Figure 3. First-hop cluster formation

Figure 3 shows first hop cluster formation. CH 'A' (VID=100) as an advertising node advertises its VID in its neighborhood. Node B hears this advertisement and sends a request to CH 'A'. CH 'A' checks the following parameters MAX_CLUSTER_SIZE and MAX_HOP and node B satisfies both conditions. CH 'A' registers node B as a CC and allocate a VID (1001) that is advertising node VID appends with a single digit integer. If other nodes wants to join as a first hop client of CH 'A', it will be given a VID 1002; the following one will be given a VID 1003 and so on. After that registered CC works as an advertising node to form a multi-hop cluster i.e. Advertising node=Node B.

Figure 4 shows the Multi-hop cluster formation. CC 'B' (VID=1001) as an advertising node advertise its VID in

its neighborhood. If node B has more than one VID then, it will forward only the smallest length VID for advertisement. Node C hears this advertisement and sends a request to CH 'A' via advertising node. CH 'A' checks the following parameters MAX_CLUSTER_SIZE and MAX_HOP and node C satisfies both conditions. CH 'A' registers node C as a CC and allocate a VID (10011) that is advertising node VID is appended with a single digit integer. When other nodes want to join as a second hop client of CH 'A', it will be allocated a VID 10012, the succeeding next will be VID 10013 and so on. After that newly registered CC works as an advertising node till the cluster has reached its maximum configurable size.

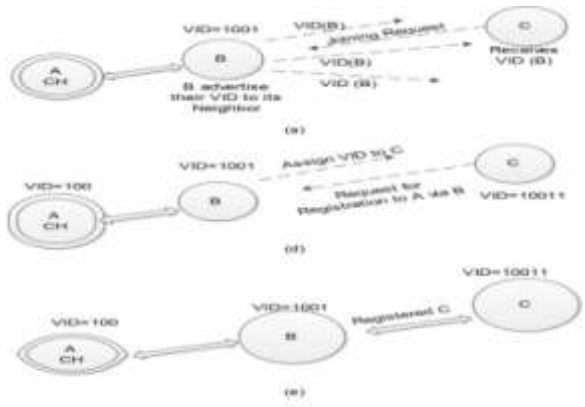


Figure 4. Multi-hop cluster formation

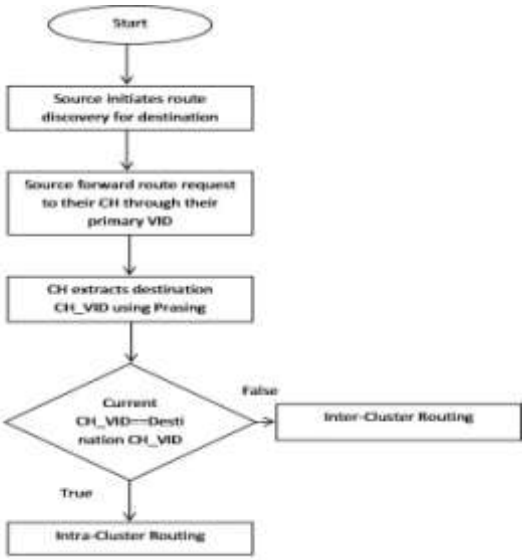


Figure 5. Routing process

B. Routing:

A hybrid approach of routing is used for communication in cluster-based network after cluster conceptualization. Figure 5 shows flowchart of routing algorithm. The source CC initiates route discovery process to a destination CC. Source CC send a route request to its CH using its primary VID. The VID carries route information from CC to CH. Every CC has one or multiple numbers of VID. A CC has single VID means it has a single route towards its CH. If CC has multiple VIDs then the concept of secondary VIDs is originated. Nodes that have more than one VIDs, classify their VIDs into primary VID (that has the least digits, and hence the shortest hops to reach the CH), and the remaining as secondary VIDs. The secondary VIDs were acquired by these nodes by overhearing the advertisements from their neighbors and joining as their children. The multiple VIDs thus result in various routes (also known as multiple branches). The dynamic multiple proactive route establishments provide robust connectivity with low overhead.

CH receives the route request of source CC and extracts the destination CH, VID using parsing technique. The technique is as follows-

```
TEMP_VID= Destination_VID;
Length_of_VID ( TEMP_VID)=N;
Length_of_VID ( CH_VID)=M;// Fixed for Network
VID  Parsing (TEMP_VID, N)
{
    if(N==M)
        Return TEMP_VID;
   Else
        Return  Forward_Parsing(TEMP_VID, N-1);
        }
```

CH then compares destination CH, VID to itself. If condition is true that means source and destination belong to same cluster else different clusters. Due to this belongingness the routing procedure is split in two sections-

1) Intra-Cluster Proactive Routing:

Algorithm for routing packets within a cluster. It is a proactive algorithm in which CH regularly checks and updates its routing table.

Figure 6 shows the multiple proactive route establishment process. The first hop children of CH 'A' for example B gets a VID = 1003, C gets a VID = 1001, D gets VID = 1002. The second hop children are K, G, H and J, which have respectively VIDs 10012, 10031, 10043 and 10053, which have been inferred from their parents namely C, B, F and E respectively.

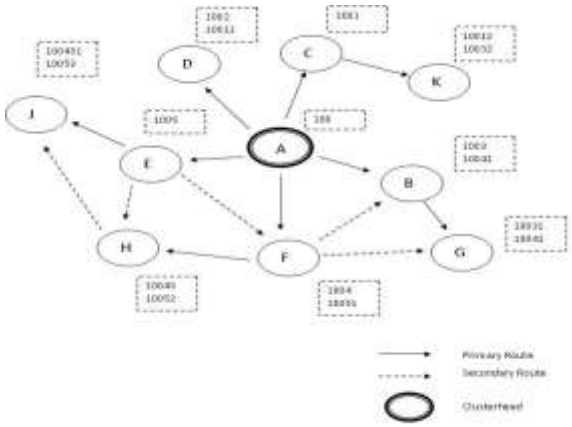


Figure 6. Multiple route establishment process

Let node I(10053) is the source and K(10012) is a destination node. Source node forwards a route request to

its CH ‘A’ through its primary VID (10053). CH ‘A’ extracts destination CH VID (100) using parsing technique. CH ‘A’ compares its own VID (100) with destination CH VID (100). Both are same then Intra-cluster routing initiates. CH ‘A’ checks their routing table as shown in Table 1 for establishing a path (I ->E ->A ->C ->K) towards destination K.

TABLE I. ROUTING TABLE OF CH ‘A’ (VID=100)

UID	First-Hop (VID)	Second-Hop (VID)	Third-Hop(VID)
B	1003	10031	-----
C	1001	10012	-----
D	1002	-----	-----
E	1005	10053,10052,10051	-----
F	1004	10041,10042,10043	100431

2) Inter-Cluster Reactive Routing:

Algorithm for routing packets across clusters. It is a reactive algorithm which kicks in only when a CH acknowledges that the destination is not within its cluster. To further improve route robustness in the scheme, the clusters are allowed to overlap i.e. CC member under different clusters. These nodes are known as border nodes. The border work as a gateway between two clusters. When a CH registers a node that have different cluster VIDs, it set this node as a border node. When reactive route search is initiated, the requesting CH broadcast their request to their border nodes and border node forward it to another linked CH. This maintains a low overhead inter-cluster-based reactive routing.

Figure 7 shows two clusters, one with A as the CH and another with L as the CH. The client VIDs under A start with 100, whereas the clients VIDs under L start with 200, the CH portion in the VID is shown underlined. Nodes B, K and G with a double circle are members of both clusters as they have VIDs that start with 100 and 200.

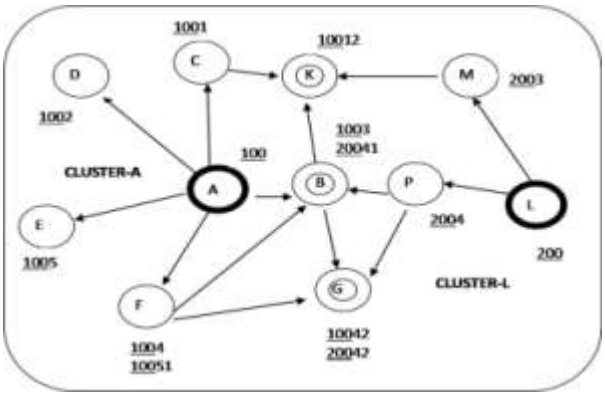


Figure 7. Inter cluster Routing

Let node E (1005) is the source and M (2003) is a destination node. Source node forwards a route request to its CH ‘A’ through its primary VID (1005). CH ‘A’ extracts destination CH VID (200) using parsing method. CH ‘A’ compares its own VID (100) with destination CH VID (200). Both are different then Inter-cluster routing initiates. CH ‘A’ forward route request to their border node B and border node B forward it to their linked CH ‘L’. CH ‘L’ again extracts destination CH VID (200) using parsing technique. CH ‘L’ compares its own VID (200) with destination CH VID (200). Both are same then CH ‘L’ checks their routing table for establishing a path (E ->A ->B ->P ->L ->M) towards destination.

IV. SIMULATION & RESULTS

For simulation NS2 version, 2.35 has been used on core i3 environment. The simulator parameters considered are as given in Table 2.

TABLE II. SIMULATION PARAMETERS

Parameter	Values
No. of Nodes	100
Maximum Speed	5 m/s
Minimum Speed	0 m/s
Node Flows	10
Simulation time	300s
Packet Size	512
Traffic Type	CBR
Dimension of Space	750 x750
Pause Time	10 s
MAC	802_11
Routing Protocol	AODV, PMRP
Clusterhead(CH)	5
Agent	UDP

Packet Delivery Ratio: The packet delivery ratio is the proportion between the number of packets originated by the application layer Constant Bit Rate (CBR) sources and the number of packets received by the CBR sink at the final destination. The numbers of packets sent to the number of packets received are calculated as the Packet delivery ratio. This is diagrammed as a role of the optimal number of hops taken from the root to the destination.

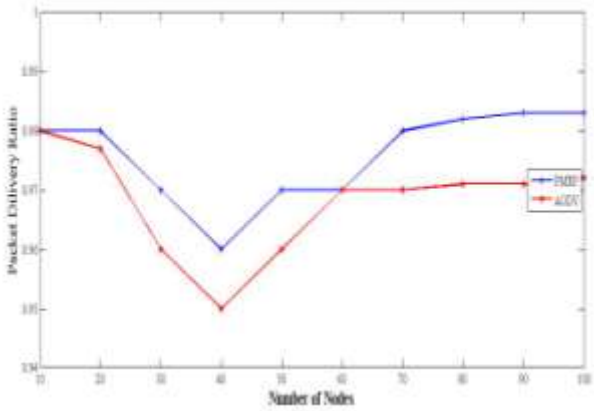


Figure 8. Packet delivery ratio

Figure 8 shows the packet delivery ratio of PMRP and AODV with respect to network size. Initially, PMRP performance is not better then AODV because it forms clusters. As the system size increases the performance of PMRP improves in comparison to AODV. This performance gain is attributed to the cluster-based routing.

Routing Overhead: Routing overhead is a metric for comparing protocols. As it measures the scalability of the protocol, the degree to which it will function in congested or low bandwidth environments, and its efficiency in terms of consuming node battery power. It is calculated as the total number of routing packets transmitted during

the simulation. For packets sent over multiple hops, each transmission of the packet (each hop) counts is taken as one transmission. Protocols that send large numbers of routing packets can also increase the probability of packet collisions and may delay data packets in network interface transmission queues.

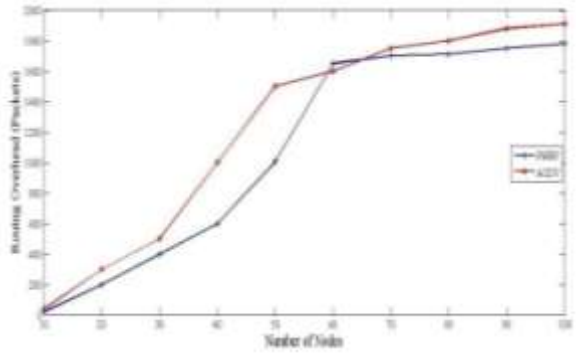


Figure 9. Routing overhead

Figure 9 shows the routing overhead of PMRP and AODV with respect to network size. As the network size increases, the difference of routing overhead increases in PMRP and AODV. The PMRP outperforms the AODV as the network becomes large. PMRP has lower overhead because it generates lesser control traffic. PMRP handles maximum traffic at cluster level (Local traffic management). This confirms both the robustness and the scalability of PMRP.

End to End Delay: End-to-end delay is the time taken for a packet to be transferred across a network from source to destination. It includes transmission delays, propagation delays as well as processing delays. The numbers of hops were varied between the source node and destination and then average end-to-end delay over all packets transmitted is calculated.

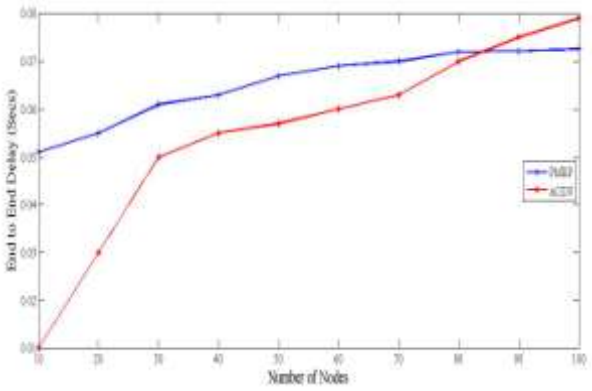


Figure 10. End to End delay

Figure 10 shows the End to End delay with respect to increase in network size. As network size increases the network require more resources. Initially, PMRP delay increases due to control traffic of cluster formation. With respect to network size, PMRP performs better because more than 60% traffic is controlled within the cluster at local level. This confirms optimization of network resources like bandwidth and energy.

Effects of Non-Optimality: The PMRP protocol is extremely rich in nature, provides multiple routes, and has comparatively low operating cost compared to proactive protocols, there is an important component of non-optimality which must be seen. Data transmission is not along the shortest path since all traffic must go through the CH. The effect of non-optimality is one of the factors, which increase the delay in data transfer. We experiment to determine the effects of Route non-optimality by comparing the number of hops needed for data to reach from the source to destination by PMRP versus AODV as a benchmark.

Figure 11 show the divergence from AODV is larger for a shorter number of hops and tends to lessen as the number of hops increases. This is expected, as for a small number of hops, the Intra-cluster proactive protocol is predominant and all traffic must pass through the CH. This limitation leads to longer routes and the effect of this would depend on the size of the cluster.

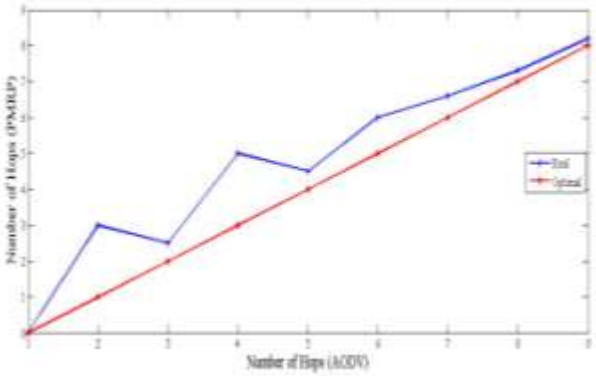


Figure 11. Effects of non-Optimality

Configurability: A key feature of the PMRP Protocol is its configurability, which includes controlling the size of the cluster. Here we explain the effects of changing the cluster size of the routing overhead. This is managed by controlling the Maximum number of hops from the CH at which the client can connect that particular cluster. We have considered a 40, 60, 80 node network with 5 data sources transmitting packets through a Constant-Bit-Rate generator. To accommodate all nodes, CHs were added as the cluster size reduced.

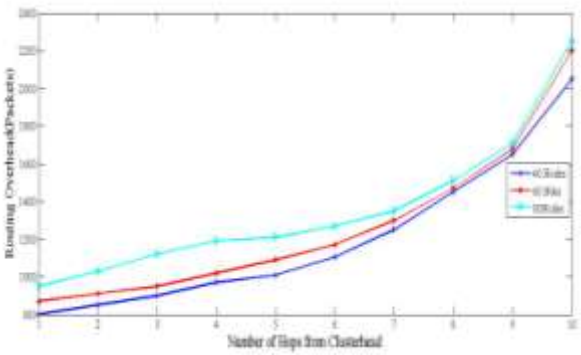


Figure 12. Configurability

Figure 12 show increase in routing overhead is exponential with respect to increasing cluster size. This is

attributed to an increase in proactive routing traffic within the cluster.

Energy Consumption: The energy consumption associated with each packet at a node is represented as the total of incremental cost' proportional to the packet size and a fixed cost 'b' associated with channel acquisition [12]:

$$Energy_{Consumption} = m \times size + b$$

Thus, the energy consumption of a broadcast packet will be of the form

$$Energy_{Broadcast} = m_{send} \times size + b_{send} + \sum_{n \in S} m_{recv} \times size + b_{recv}$$

where

$S = Set\ of\ nodes\ with\ in\ transmission\ range\ of\ the\ transmitting\ node.$

$m_{send}, b_{send} = increental\ and\ fixed\ cost\ for\ the\ sending\ the\ broadcast\ packet.$

$m_{recv}, b_{recv} = increental\ and\ fixed\ cost\ for\ the\ receving\ the\ broadcast\ packet.$

The cost of the unicast packet will be of the form

$$Energy_{unicas\ t_{sender}} = b_{sentclt} + b_{recvclt} + m_{sent} \times size + b_{sent} + b_{recvclt}$$

$$Energy_{unicast\ \_receiver} = b_{recvclt} + b_{sentclt} + m_{recv} \times size + b_{recv} + b_{sentclt}$$

where

$m_{sendclt} = fixed\ cost\ for\ the\ sending\ a\ control\ \ packet.$

$m_{recvclt} = fixed\ cost\ for\ the\ recieving\ a\ control\ \ packet.$

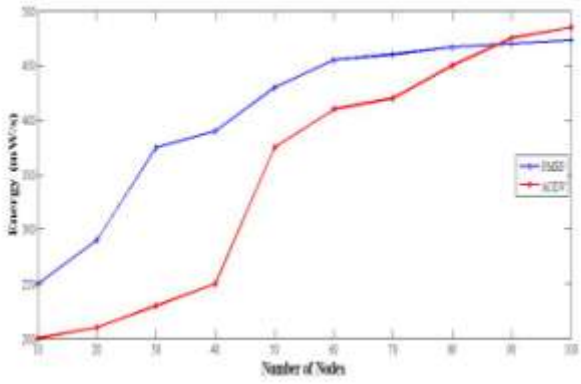


Figure 13. Energy consumption

Figure 13 show energy consumption of PMRP is initially higher than AODV, but when the number of hops increases, the gain in the consumption is more stable as compared to AODV.

V. Conclusion

It has been the focus of this paper to explore the current challenges that MANET routing protocols face, and propose a novel algorithm to address some of these challenges. We explained the detailed operation of the Poly-Meshed Tree based Routing protocol and discussed its main characteristics and how it attempts to solve the issues associated with dynamic environments through redundant routes and reduced route dependency. The unique aspects of the algorithm is it uses a single algorithm to perform clustering and proactive routing, reactive routes are a concatenation of the proactive routes. Reactive routes use a loose source routing concept and are impacted by only the local changes in a cluster, (which are resolved local to the cluster) and do not depend on the dynamics of all the nodes that are forwarding. The scheme supports the maintenance of multiple proactive routes, which is uncommon in proactive routing as the algorithms used until now determine and maintain one best route and on the failure of this route (which is known through topology dissemination), recalculate another. Unification of tree and mesh topologies is new and helps leverage the advantages of the two Multi hop multiple overlapped cluster formation is achieved in a simple way with low overhead. Proactive routes are setup as clusters are formed i.e. both functions are achieved in one operation. Cluster nodes do not maintain routing tables and states, except when communicating with clients outside their cluster. No complex algorithms are involved the simple VID scheme is novel as it facilitates all the above. Through simulation results and comparative analysis with AODV protocol, certain advantages of the Poly-Meshed tree routing protocol have been demonstrated such as its low overhead and robust connectivity.

Refrences

[1] K. Srungaram and M. K. Prasad, "Enhanced Cluster Based Routing Protocol for MANET," in *Advances in Computer Science and Information Technology. Networks and Communications. Second International Conference, CCSIT*, Bangalore, India, 2012, pp. 231-239.

[2] M. Aparna, M. Reza, P. Sahu, and S. Das, "An Efficient Approach towards Robust Routing in MANET," in *Communication Systems and Network Technologies (CSNT), 2012 International Conference on IEEE*, Rajkot, 2012, pp. 388-391.

[3] E. Nordström, P. Gunningberg, and C. Tschudin, "Robust and flexible Internet connectivity for mobile ad hoc networks," *Journal Ad Hoc Networks, Elsevier Science Publishers B. V. Amsterdam, The Netherlands, The Netherlands*, vol. 9, no. 1, pp. 1-15, Jan. 2011.

[4] S. Saha and R. Chaki, "Cluster Based Mobility Considered Routing Protocol for Mobile Ad Hoc Network," in *First International Conference on Computer Science and Information Technology, CCSIT* , Bangalore, India, 2011, pp. 33-42.

[5] S. Mangai and A. Tamilarasi, "A new approach to geographic routing for location aided cluster based MANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 18, no. 1, pp. 1-10, Jun. 2011.

[6] E. Inn, N. Lion, and S. Winston, "Adaptive Cluster-based Approach for Reducing Routing Overheads in MANETs," in *16 Asia-Pacific Conference on Communications*, Crown, 2010, pp. 316-321.

[7] B. Zhou, Z. Cao, and M. Gerla, "Cluster-based inter-domain routing (CIDR) protocol for MANETs," in *WONS'09 Proceedings of the Sixth international conference on Wireless On-Demand Network Systems and*

Services, IEEE Press Piscataway, NJ, USA, 2009, pp. 17-24.
[8] M. Rezaee and M. Yaghmaee, "Cluster based Routing Protocol for Mobile Ad Hoc Networks," *INFOCOM, Journal of Computer Science*, vol. 8, no. 1, pp. 30-36, Mar. 2009.
[9] Z. Chunhua and T. Cheng, "A Multi-Hop Cluster Based Routing Protocol for MANET," in *Information Science and Engineering (ICISE),IEEE*, Nanjing, 2009, pp. 2465-2468.
[10] N. Shenoy, Y. Pan, D. Narayan, D. Ross, and C. Lutzer, "Route Robustness of a Multi-Meshed Tree Routing Scheme for Internet MANETs," in *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE (Volume:6).*, St. Louis, MO, 2005, pp. 6-3351.
[11] C. Chi-Kin, C. Jon, L. Kang-Won, and W. Starsky, "IDRM: Inter-Domain Routing Protocol for Mobile Ad Hoc Networks," University of Cambridge Technical UCAM-CL-TR-708, 2008.
[12] G. Allard, P. Minet, D.-Q. Nguyen, and N. Shrestha, "Evaluation of the Energy Consumption in MANET," INRIA, France, Technical Report ISSN 0249-6399, 2006.

Anil Singh obtained the Master's degree in Computer Science and Engineering from RGPV, Bhopal. He is presently pursuing Ph.D. from RGPV, Bhopal, Madhya Pradesh, in Ad Hoc Wireless Networks. He is currently working as an Associate Professor in the Department of Computer Science and Engineering in Medi-Caps institute of Technology and Management, affiliated to RGPV University, Bhopal and has 10 years of teaching experience. His specializations include Computer Networks, Operating Systems and Theory of Computations.

ShashikalaTapaswi is a Professor in Information Technology at of Atal Bihari Vajpayee—Indian Institute of Information Technology and Management, Gwalior (M.P.) India. She has done Ph.D. (Computer Engineering) from Indian Institute of Technology, Roorkee, M.Tech. (Computer Science) from University of Delhi, and B.E. (Electronics Engineering) from Jiwaji University, Gwalior, India. Her primary research areas of interest are Artificial Intelligence, Neural Network, Fuzzy Logic, Digital Image Processing, Computer Networks, Mobile Adhoc Networks, Network Security, Cloud Computing and Cloud Security.

SIP-Based QoS in IP Telephony

Muhammad Yeasir Arafat, Muhammad Morshed Alam, and Feroz Ahmed
Department of Electrical and Electronic Engineering, School of Engineering and Computer Science, Independent University, Bangladesh
Email: yeasir08@yahoo.com,morshed380@yahoo.com, fahmediub@gmail.com

***Abstract*—In this paper, the authors analyze the factors resulting to the degradation of the quality of service in voice over IP (VoIP) telephony. SIP protocol is used to explore the QoS characteristics of different Codec. The system is designed for an IP telephony service provider with other GSM operator network cloud. A soft IP PBX maintains the dial pattern, SIP proxies are used in order to implement call control and to allow the distributing of the gateways' lines. The system is executed in a test bed where QoS factors likes delay, packet loss, forward and reverse jitter, MOS and delta measured. A Popular simulation software Wireshark is used to simulate and analysis the transmission characteristics of packetized voice over the IP network channel. The results are graphically shown, which reveal the effects of packet size on QoS. Packet sizes from 10 to 60 bytes are used for a G.729 Codec in 11.2-24 Kbps channel bandwidths are studied. A 20 byte packet size at 24 Kbps channel bandwidth is seen to show the best result in terms of jitter, delay and delta. The results of studies conducted by also shown that G.729 codec shown high MOS value and low mean forward and reverse jitter for simultaneous call compare with other codecs.**

***Index Terms*—VoIP; SIP; QoS; RTP; UDP; MOS**

I. INTRODUCTION

Generally voice over internet protocol (VOIP) system uses the internet protocol (IP) to transmit voice as packets over an IP network. By using VOIP protocols, voice communications can be achieved on any IP network regardless it is internet, intranets or local area networks (LAN). In a VOIP allowed network, the voice signal becomes digitized, compressed and converted to IP packets and transmitted over the IP network. VOIP signaling protocols are used to set up and tear down calls, transmit data required to find users and negotiate capabilities.

While the evolution of internet telephony is experiencing significant development due to its low-price for long distance calls also experiencing major challenge such as good response quality, delay, jitter, packet loss, bandwidth and other parameters known as the quality of service (QoS) [1]. A VoIP system consists of three vital apparatus - codec, packetize and play out buffer. Service quality of VoIP is to make sure that voice packets are not delayed, lost or dropped during the transmission over the network since VoIP functions are sensitive to delay and packet loss. QoS measures the degree of user satisfactions, the higher the service value, the higher degree of user satisfaction.

The issue is how to guarantee that packet traffic for a voice or other time sensitive media will not be delayed or dropped due to interference from other lower priority traffic in the network.

Quality of service for voice over IP network is a critical matter since it is real time and delay sensitive application. Session initiation protocol (SIP) is the internet engineering task force (IETF) standard for establishing voice connection. SIP is an application layer protocol (according to OSI Layer) for creating, modifying and terminating multimedia sessions with one or more participants. Borrowing from internet protocols, like as hyper text transfer protocol (HTTP), SIP is text-encoded and very extensible [2] [19]. SIP uses the real time transport protocol (RTP) for transmitting audio and time sensitive data and uses the session description protocol (SDP) for describing multimedia session steps. RTP is utilized over UDP to transmit audio and video data. Real-time transport control protocol (RTCP) is used along with RTP, to supply some QoS information. For a point-to-point case the RTCP information can provide delay, jitter and loss information in each path to both participants. Since SIP targets time-sensitive applications, several delays can be considered to assess the quality of service of this protocol. In this paper QoS has been approximated from the edge of end user and performance parameters have been analyzed, i.e. mean packet loss rate and mean jitter, maintained stable values and acceptable QoS levels. In VoIP there are also exclusive causes of degradation including codec compression, packet loss, discarded packets, bit errors, frame erasures and various compression schemes. Voice quality measurement considers the extent of all of these factors, whether they occur in the network or outside it, and determines the overall impact of quality in the opinion of the customer, a measurement known as a Mean Opinion Score (MOS). The major justification for this selection is such that the study focuses on the performance of VoIP communication over different networking conditions and environment, and hence the time and reliability would be the major concerns for evaluation.

The remainder of this paper is organized as follows. We first discuss related study of SIP in Section 2. Then, described the VOIP codec in Section 3. In Section 4, we described the common QoS parameters in VOIP communications. In Section 5, we evaluated codec quality in our designed test bed. Finally, conclusions are presented in Section 6.

doi:10.4304/jnw.9.12.3415-3426

II. BACKGROUND STUDY ON SIP

There are four logical types of units participate in SIP-based VOIP calls: user agents (client 'UAC' or server 'UAS'), registrars, proxy and redirect servers. The user agents commence requests and they are also the final destination. Registrars maintain track of users within their assigned network domain (e.g., all users with identifiers x@ipphone.dhakacom.com register with the registrar in the ipphone.dhakacom.com domain). Proxy servers are works as an application-layer routers they forward SIP requests and responses. Redirect servers works for receive requests and then return the location of another SIP user agent or server where the user might be found. It is quite common to find proxy, redirect, and registrar servers implemented within the same program in a same server. In a classic SIP session, SIP messages originating at a user agent negotiate one or more SIP proxy servers and then reach one or more SIP user agents. While, SIP user agents can also communicate directly with each other. In fact, it is widespread that only the first request exchange activities along a chain of proxies, with all subsequent requests exchanged directly between the two user agents.

A user agent is a terminal participating in SIP communications (this can be hardware or software). Users can register their current location (i.e. IP-address) with the registrar of their domain. This enables mobility: A location server is used by a registrar to store the location of users (the binding of a SIP-URI with a current IP-address). The location server provides a directory for other SIP entities to look up the current location for a given SIP-URI [3].

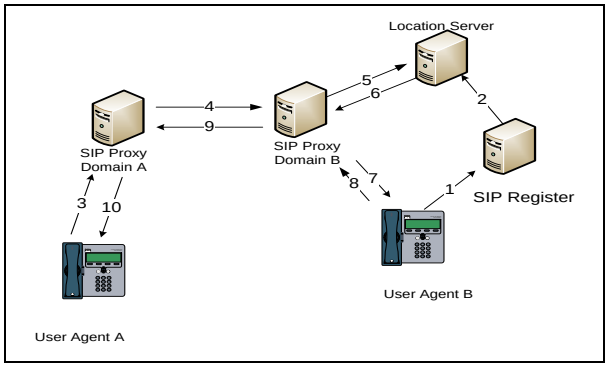


Figure 1. Setting a phone calls with SIP

The establishment of a voice connection between two users is illustrated in Figure 1. In this Figure 1, user agent A and B are in different domains and have registered with different proxies. Initial, the caller (user agent B) needs to register with its local registrar server (1) to be able to receive calls. The registrar stores the location information at a location server (2). When user agent A wants to call user agent B, it sends an INVITE-request to its local SIP-proxy (3) which passes on the request (after a DNS lookup) to the proxy of user B's domain (4). The proxy in domain B needs lo look up the IP-address of user agent B at the location server (5, 6) before it can send the request to user agent B (7). The answer message for user agent A can take the same route path back (8, 9, and 10).

Session Description Protocol (SDP) is used to choose factors (such as the codec and media type) for the transmission. After a session has been established with SIP, the actual media transfer is transmitted with the Real-time Transport Protocol (RTP) [3]. Because SIP is applied to set up a session, any protected connection that can be established in a SIP session can further be used to negotiate secrets for a secure RTP stream. Therefore, SIP security is of high significance for IP Telephony security. SIP is a client-server protocol which is similar to HTTP. Signaling is support on text messages: A message consists of a header and an optional body. A message is contain either requests or responses. If a SIP entity obtains a request, it performs the resultant action and sends back a response to the originator of the request. Responses are three-digit status codes. Table 1 list SIP requests; table 2 lists classes for SIP response codes.

TABLE I. SIP REQUESTS

SIP Request	Description
INVITE	Initiates a call signaling sequence
BYE	Terminates a session
ACK	Acknowledge
OPTIONS	Queries a server about its capabilities
CANCEL	Used to cancel a request in progress
REGISTER	Used to register location information at a registrar

TABLE II. SIP RESPONSE

SIP Response Codes
1xx – Informational
2xx – ok
3xx – Redirection
4xx – Client error
5xx – Server error
6xx – Global failure

III. VOIP CODES

There are several factors that control codec choice. Most important are bandwidth availability and required quality. Toll quality can be achieved with 64 kb/s G.711 which is also used in integrated services digital network (ISDN). SIP supports various codecs likes: G.711, G.722, G.728, G.729 and G.723.1 [4].

TABLE III. VOICE CODEC OVERVIEW

Codec	Bandwidth Requirements	Frame Size
G.711	64 kb/s	1ms
G.722	64 kb/s	1 ms
G.728	16 kb/s	2.5 ms
G.729 A	8 kb/s	10 ms
G. 723.1	5.3, 6.4 kb/s	30 ms

Table 3 show that codecs use different frame sizes. If we choose to use G.711, we would pack 20 frames in one voice packet. Setting the right length for a voice packet is very important. Packet length order ratio between the information part of the packet and an overhead that is introduced by underlying protocols. Let us describe "exploit" ratio with Qe = voice data / overhead.

If we select to be traditional to SIP recommendation and use G.711, IP packet will consist of 40-byte header (IP, UDP, and RTP headers) and 160 bytes of voice data. That demands bandwidth of 80 kb/s and provides $Qe_{G:711}$=160/4 =4. If we choose to use codec that can work with lower bandwidth, the ratio may change radically. With G.728 we form 20 ms with only 8 voice frames (Tab. 3), 5 bytes each, which results in 40-byte header and 40 bytes of voice data. If we suppose usage of public IP infrastructure, without QoS provision, packets can take different paths to peers destination. They can reach your destination in random order or get lost on their way. For voice packets usage of user datagram protocol (UDP) is expected. It is unreliable, connection-less protocol for applications that do not desire transmission control protocol (TCP's) flow control.

In public network, like Internet is used for the transport of VoIP packets, packets reach to their destination at irregular time gaps. This is called jitter and introduces another barrier in VoIP communication. At present jitter is solved with the use of special buffers - jitter buffers. They are introducing additional delay in the range of 100ms. Various researches established that delay of 200 ms is acceptable even for business use, but delays greater than 200 ms showed to be unacceptable. In table 4 shows presents sources of delay on voice packet path [5].

TABLE IV. END-TO-END IP TELEPHONY PACKET LATENCY AND DELAY

Latency Delay Source	Typical Delay
Recording	10-40 ms
Encoding	5-10 ms
Compression (Speech Coder)	5-10 ms
Internet Delivery	70-120 ms
Jitter Buffer	50-200 ms
Decompression(Speech Coder)	5-10 ms
Decoding (Codec)	5-10 ms
Average	150-400ms

IV. COMMON PARAMETERS IN QUALITY OF SERVICE (QOS) IN IP TELEPHONY

The basic routing idea on the Internet is "best-effort." This approach serves most users suitably but it is not sufficient for the time-sensitive, continuous stream transmission required for IP telephony. QoS refers to the ability of a network to give better, more unsurprising service to selected network traffic over various underlying technologies, including IP-routed networks [5-6]. QoS features can be implemented in network routers by:

- Supporting dedicated bandwidth;
- Improving loss characteristics;
- Avoiding and managing network congestion;
- Shaping network traffic; and
- Setting traffic priorities across the network.

Voice applications have unusual characteristics and supplies from those of traditional data applications. Because they are naturally real-time, voice applications accept minimal delay in delivery of their packets. Moreover, they are fanatical of packet loss, out-of-order packets, and jitter. To efficiently transport voice traffic over IP, mechanisms are required that ensure reliable transport of packets with low and controlled latency.

There are another approach utilizes resource reservation protocol (RSVP) [5] which is a relatively new protocol developed to enable the internet to support QoS. Using RSVP, a VoIP application can reserve resources along a route from source to destination. RSVP-enabled routers will then schedule and prioritize packets to fulfill the QoS. RSVP is part of the internet integrated service (IIS) model, ensuring best-effort service, real-time service, and controlled link sharing. While QoS is an addition to IPv4- the current version of IP-IPv6 will naturally support QoS. However, IPv6 also has a much larger packet header, so it is possible that while QoS will improve much of the jitter and congestion voice packets presently suffer, it could come at the cost of increased latency. IPv6 headers necessitate 40 bytes, compared with 20- byte IPv4 headers, thus doubling the overhead. This may create trouble for vocoders that only succeed with little packets. Nevertheless, this larger packet overhead can be partially offset if IPv6 provides for efficient compression schemes for the header.

A. Voice Traffic Characterise

VoIP traffic is a particular type of data traffic. For this reason it is very sensitive to underlying network performance, Users complain about bad quality [7]. Voice traffic characterize are likes as

- Very consistent traffic flows
- High PPS
- Small packets
- Different codecs present more or less of the above
- Always real-time traffic
- No re-transmissions
- Delay and delay variance (jitter) affect the quality of the call

In the network major concerns for voice are

- Queuing delays
- Congestion
- Serialization delays
- Packet drops and performance on third party links (ISP, Carrier links, etc.)
- Over subscription of bandwidth
- High latency and or jitter

B. Packet Loss

UDP will not supply a pledge that packets will be delivered at all, much less in order. Packets may be dropped under peak loads and during periods of congestion. Due to time sensitivity of voice transmissions, the normal TCP based retransmission schemes are not suitable. Approaches used to recompense for packet loss include interpolation of speech by replaying the last packet and sending redundant information. Packet losses more than 10 percent are normally intolerable, unless the encoding scheme supplies extraordinary strength [8]. Some reasons for packet drop in IP network are given below:

- If there is not enough bandwidth on a link for the presented load, some traffic will be dropped

- May be due to interface congestion
- May be due to polices enforcing service parameters
- Bad physical layer can cause lost / corrupt packets

C. Jitter

IP networks will not guarantee the delivery time of data packets, the data will arrive at very inconsistent rates. The disparity in inter-packet arrival rate is jitter, which is presented by variable transmission delays over the network. Eliminating jitter to allow an equable stream needs assembling packets and saving them long enough to allow the slowest packets to reach in time to be performed in the correct sequence. The jitter buffer is used to eliminate the packet delay difference that each packet runs into transiting the network. Each jitter buffer adds to the overall delay. Some real fact on Jitter are given below

- Jitter is variance in inter-packet arrival times
- Variable delay
- Latency itself does not garble voice traffic. Jitter does normally caused by serialization delays
- Small packet gets caught waiting for a large packet to transmit or multiple traffic forwarding paths for the same flows resulting in packets taking different paths

D. Latency and Delay

Latency [9] is the time delay acquired in speech by the IP telephony system. One-way latency is the amount of time measured from the moment the speaker utters a sound until the listener hears it. Round trip latency is the sum of the two one-way latency figures that compile the user's call. In an IP Telephony implementation used to reduce costs, studies recommend that users will tolerate one-way latency of up to 200 ms. The 1996 ITU Recommendation G.114 for one-way end-to-end transmission time limit is [6]:

- Under 150 ms: acceptable for most user applications;
- 150 to 400 ms: acceptable provided administrators know of the transmission time impact on the quality of user applications;
- Over 400 ms: unacceptable for general network planning purposes.

Two difficulties are echo and talker overlap that result from a high end-to end delay in a voice network. Echo wherein the speaker's voice is reflected back-becomes a problem when the round-trip delay is more than 50ms. Since echo is supposed as a major quality barrier, the VoIP system must address the need for echo control by implementing echo cancellation. Talker overlap-the problem of one caller stepping on the other talker's speech-is made worse when the one-way delay is greater than 250ms. The end-to-end delay allowance, therefore, is the major limitation and powerful prerequisite for reducing latency through a packet network. Latency source are given below

- Codec delay
- Processing delay
- Serialization delay
- Queuing delay
- Propagation delay
- Jitter buffer delay

Transmission time includes delay due to codec processing as well as propagation delay. Delay variation, occasionally called jitter, is furthermore important.

E. Transport

Usually Internet applications use TCP/IP, where VoIP uses RTP/UDP/IP. While IP is a connectionless best effort network communications protocol, TCP is a reliable transport protocol that uses acknowledgments and retransmission to ensure packet receipt. TCP has a rate adjustment characteristic that increases the transmission rate when the network is uncongested, but quickly decreases the transmission rate when the originating host does not receive positive acknowledgments from the destination host. TCP/IP is not appropriate for real-time communications, such as speech transmission, because the acknowledgment/retransmission feature would lead to unnecessary delays. UDP gives unreliable connectionless delivery service using IP to transport messages between end points in an internet. RTP, used in conjunction with UDP, provides end-to-end network transport functions for applications transmitting real-time data, such as audio and video, over unicast and multicast network services [10]. RTP does not support reserve resources and does not assurance quality of service. A companion protocol RTCP does allow monitoring of a link, but most VoIP applications offer a continuous stream of RTP/UDP/IP packet without regard to packet loss or delay in reaching the receiver.

Voice quality can be sustained while using silence suppression if the receiving codec inserts a carefully planned comfort noise during each silence period. For example, Annex B of ITU-T Recommendation G.729 defines a robust voice activity detector that measures the changes over time of the background noise and sends, at a low rate, enough information to the receiver to generate comfort noise that has the perceptual characteristics of the background noise at the sending telephone. Coding and packetization result in delays greater than users typically experience in terrestrial switched circuit networks. As, standard speech codecs are available for output coding rates in the approximate range of 64 to 5 kb/s. Packet design engages a tradeoffs between payload effectiveness (payload/total packet size) and packetization delay (the time required to fill the packet).

For IPv4, the RTP/UDP/IP header is 40 bytes. A payload of 40 bytes would mean 50% payload efficiency. At 64 kb/s, it only takes 5 ms to accumulate 40 bytes, but at 8 kb/s it takes 40 ms to accumulate 40 bytes. A packetization delay of 40 ms is important, and many VoIP schemes use 20-ms packets despite the low payload efficiency when using low-bit-rate codecs. For continuous speech, the call transmission capacity requirement BW (in kb/s) is related to the header size H

TABLE V. BANDWIDTH CALCULATIONS TABLE

Codec Information				Bandwidth Calculations					
Codec & Bit rate (Kbps)	Codec & Sample size (Bytes)	Codec & Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload size (Bytes)	Voice Payload size (ms)	Packets per Seconds (PPS)	Bandwidth MP or FRF12 (kbps)	Bandwidth wc/R TPMP or FRF12 (kbps)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80 Bytes	10 ms	4.1	160Bytes	20 ms	50	82.8 Kbps	67.6 Kbps	87.2 Kbps
G.729 (8 Kbps)	10 Bytes	10 ms	3.92	20 Bytes	20 ms	50	26.8 Kbps	11.6 Kbps	31.2 Kbps
G.723.1 (6.3 Kbps)	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	18.9 Kbps	8.8 Kbps	21.9 Kbps
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	17.9 Kbps	7.7 Kbps	20.8 Kbps
G.726 (32 Kbps)	20 Bytes	5 ms	3.85	80 Bytes	20 ms	50	50.8 Kbps	35.6 Kbps	55.2 Kbps
G.726 (24 Kbps)	15 Bytes	5 ms		60 Bytes	20 ms	50	42.8 Kbps	27.6 Kbps	47.2 Kbps
G.728 (16 Kbps)	10 Bytes	5 ms	3.61	60 Bytes	30 ms	33.3	28.5 Kbps	18.4 Kbps	31.5 Kbps
G722_64k(64 Kbps)	80 Bytes	10 ms	4.13	160Bytes	20 ms	50	82.8 Kbps	67.6Kbps	87.2 Kbps
ilbc_mode_20(13.33Kbps)	38 Bytes	20 ms	NA	38 Bytes	20 ms	50	34 Kbps	18.8Kbps	38.4 Kbps
ilbc_mode_30(13.33Kbps)	50 Bytes	30 ms	NA	50 Bytes	30 ms	33.3	25.867Kbps	15.73Kbps	28.8 Kbps

(in bits), the codec output rate (in kb/s) and the payload sample size *S* (in milliseconds) as $BW = R + H/S$

V. VOICE QUALITY AND CODECS

Many factors determine voice quality, encompassing the choice of codec, echo control, packet loss, delay, delay variation (jitter), and the design of the network. Packet loss grounds voice clipping and skips. Some codec algorithms can correct for some lost voice packets. If the end-to-end delay becomes too long, the conversation begins to sound like two parties talking on a people band radio. A buffer in the obtaining tool always recompense for jitter (delay variation). If the delay variation exceeds the size of the jitter buffer, there will be buffer overruns at the receiving end, with the same effect as packet loss anywhere else in the transmission path. Telephones or gateways engaged in setting up a call will be able to adept which codec to use from among a small working set of codecs that they support [11].

A. Codec

There are various codecs available for digitizing speech. The quality of a voice call through a codec is often measured by subjective testing under controlled conditions using a large number of listeners to determine an MOS. Several characteristics can be considered by varying the test conditions. Important characteristics include the effect of environmental noise, the effect of channel degradation (such as packet loss), and the effect of cycle encoding/decoding when interworking with other wireless and global transport networks. The last feature is especially important since VoIP networks will have to interwork with switched circuit networks and wireless networks using different codecs. The general order of the fixed-rate codecs listed in the table, from best to worst performance in cycle, is G.711, G.726, G.729, G.728, and G.723.1. Since voice quality suffers when placing low-bit-rate codecs in cycle in the transmission path, the network design should attempt to keep away from cycle codecs whenever and wherever possible [12].

A. Per Call Bandwidth

These protocol header assumptions are used for the calculations [12]:

- 40 bytes for IP (20 bytes) / UDP) (8 bytes) / RTP) (12 bytes) headers.
- Compressed Real-Time Protocol (cRTP) reduces the IP/UDP/RTP headers to 2or 4bytes (cRTP is not available over Ethernet).
- 6 bytes for Multilink Point-to-Point Protocol (MP) or Frame Relay Forum (FRF).L2 Layer 2 (L2) headers.
- 1 byte for the end-of-frame flag on MP and Frame Relay frames.
- 18 bytes for Ethernet L2 headers, including 4 bytes of Frame Check Sequence (FCS) or Cyclic Redundancy Check (CRC).

B. Bandwidth Calculation Formula

These calculations are used:

- Total packet size = (L2 header: MP or FRF.12 or Ethernet) + (IP/UDP/RTP header) + (voice payload size)
- PPS = (codec bit rate) / (voice payload size)
- Bandwidth = total packet size * PPS

PPS: PPS comprises the number of packets that need to be transmitted every second in arrange to deliver the codec bit rate. For example, for G.729 call with voice payload size per packet of 20 bytes (160 bits), 50 packets need to be transmitted every second [50 pps = (8 Kbps) / (160 bits per packet)]

Voice Payload Size (ms): The voice payload size represented in terms of the codec samples. For example, a G.729 voice payload size of 20 ms (two 10 ms codec samples) represents a voice payload of 20 bytes [(20 bytes * 8) / (20 ms) = 8 Kbps]

Voice Payload Size (Bytes): The voice payload size represents the number of bytes (or bits) that are filled into a packet. The voice payload size should be a multiple of the codec sample size. For example, G.729 packets can use 10, 20, 30, 40, 50, or 60 bytes of voice payload size.

MOS: Speech quality has always been a concern for VoIP calls. It is a subjective listening test where the user rates the speech quality during the call. MOS tests can also be present in two variations as: absolute category rating (ACR) and degradation category rating (DCR). The DCR test is used in several incidents to get the degradation MOS (DMOS) scores [8]. The best packet

network conceive codes the speech once beside the speaker and decodes it once beside the listener. Concatenation of low-bit-rate speech codecs, as well as the trans coding of speech in the middle of the transmission path, degrades speech quality. An MOS of 5 is excellent, 4 is good, 3 is fair, 2 is poor, and 1 is very bad. It is a new objective model proposed by ITU-T and it takes into account all the drawbacks of PESQ. It is a non-intrusive process of calculating the voice quality. E-model takes into account various factors that affect the speech quality and calculates a Rating factor (R-factor) that ranges between 0 -100. The *R*-factor can also be converted into a MOS rating to give the MOS score. The *R*-factor is calculated as [13]:

R_{obj} = R0 - Is - Id - Ie + A

where:

R0: Signal to noise ratio (S/N) at 0 dBR point

Is: Various speech impairments (e.g. Quantization noise, side tone level)

Id: Impairments that occur due to delay (e.g. absolute delay, echo)

Ie: Impairments caused by the equipment (e.g. codec's, jitter, packet loss)

A: Advantage factor (A is 0 for wire line and A is 5 for wireless

ITU G.107 provides an equation to convert the R-factor value in MOS score:

For R < 0: MOS =1

For 0 < R < 100: 6 MOS=1+ 0.035R +R (R- 60)(100-R)7.10^-6

For R > 100: MOS = 4.5

Based on ITU G.107 recommendation, the R- factor equation can be simplified as:

R-factor = 93.2 – Id – Ie – A

where *A* is the advantage factor; 0 for wire line and 5 for wireless networks. The value of *Ie*, which is codec dependent impairment, is calculated as:

Ie = a + b ln (1+ cP/100)

where, *P* is percentage packet loss and *a*, *b* and *c* are codec fitting parameters. The value of *Id*, which is impairment due to delay is calculated as:

Id = 0.024d + 0.11 (d – 177.3) H(d – 177.3)

where *d* is the total one way delay (includes serialization delay, processing delay and propagation delay) in milliseconds. *H(x)* is a step function defined as: *H(x) = 0* , *x<0* and *H(x) = 1* otherwise.

The drawback of E-model is that the MOS scores calculated by E-model do not correlate very well with the subjective MOS scores. Also E-model does not calculate the packet loss and delay accurately during handovers, when a VoIP call moves from one network to another.

C. Sample Calculation

The required bandwidth for a G.729 call (8 Kbps codec bit rate) with cRTP [9], MP and the default 20 bytes of voice payload are:

- Total packet size (bytes) = (MP header of 6 bytes) + (compressed IP/UDP/RTP header of 2 bytes) + (voice payload of 20 bytes) = 28 bytes
- Total packet size (bits) = (28 bytes) * 8 bits per byte = 224 bits
- PPS = (8 Kbps codec bit rate) / (160 bits) = 50 pps

Note: 160 bits = 20 bytes (default voice payload) * 8 bits per byte

- Bandwidth per call = voice packet size (224 bits) * 50 pps = 11.2 Kbps

D. Impact of Changing Voice Payload Sizes

The number of codec samples per packet is another factor that settle on the bandwidth and delay of a VoIP call [14 -15]. The codec defines the size of the sample, but the total number of samples placed in a packet influences how many packets are sent per second. When you increase the voice payload size the bandwidth will reduces and the overall delay increases. The following example illustrates this:

- G.729 call with voice payload size of 20 bytes (20 ms): (40 bytes of IP/UDP/RTP headers + 20 bytes voice payload)* 8 bits per byte * 50 pps = 24 Kbps
- G.729 call with voice payload size of 40 bytes (40 ms): (40 bytes of IP/UDP/RTP headers + 40 bytes voice payload) * 8 bits per byte * 25 pps = 16 Kbps

Layer 2 (L2) headers are not considered in this calculation. **2.** The calculations showed, while the payload size is doubled, the number of packets per second required is subsequently cut in half. **3.** As defined in the international telecommunication union telecommunication standardization sector (ITU-T) G.114 specifications, the recommended one-way overall delay for voice is 150 ms. For a private network, 200 ms is a reasonable goal, and 250 ms must be the maximum.

E. Jitter Calculation

A protocol analyzer free tool Wireshark calculates jitter according to RFC3550 (RTP). If Si is the RTP timestamp from packet *i*, and *Ri* is the time of arrival in RTP timestamp units for packet *i*, then for two packets *i* and *j*, *D* may be expressed as

D (i,j) = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si)

The inter coming jitter should be calculated continuously as each data packet i is received from source SSRC_n, using this difference *D* for that packet and the previous packet *i-1* in order of arrival (not necessarily in sequence), according to the formula *J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16*

RTP timestamp is stranded on the sampling frequency of the codec, 8000 in most audio sample codecs. As the sampling frequency must be known to correctly calculate jitter it is difficult to calculate jitter for dynamic payload types as the codec and its sampling frequency must be known which involves that the setup information for the session must be in the trace and the codec used must be known to the program.

Developers with time to spend could change the current implementation to also record the sampling frequency in the SDP data and add that to the RTP conversation data and use that in the RTP analysis. This is what we have in the packets and what we will use in the formula [10]:

R0 = frame 356: frame.time = August 10, 2013 12:56:25.348411000

S0 = frame 356: rtp.timestamp = 1240

R1 = frame 357: frame.time = August 10, 2013 12:56:25.418358000

S1 = frame 357: rtp.timestamp = 1400

R2 = frame 358: frame.time = August 10, 2013 12:56:25.421891000

S2 = frame 358: rtp.timestamp = 1560

We also have rtp.p_type = ITU-T G.711 PCMA (8) and thus we know sampling clock is 8000Hz and thus the unit of rtp.timestamp is 1/8000 sec = 0.000125 sec. Calculation are given below

Frame 356:

J(0) = 0

Frame 357:

D(0,1) = (R1 - R0) - (S1 - S0)

= [in seconds] (.418358000 sec - .348411000 sec) - (1400 * 0.000125 sec - 1240 * 0.000125 sec) = 0.049947

J(1) = J(0) + (|D(0,1)| - J(0))/16

= [in seconds] 0 + (|0.049947| - 0)/16 = 0.0031216875

Frame 358:

D(1,2) = (R2 - R1) - (S2 - S1)

= [in seconds] (.421891000 sec - .418358000 sec) - (1560 * 0.000125 sec - 1400 * 0.000125 sec) = -0.016467

J(2) = J(1) + (|D(1,2)| - J(1))/16

= [in seconds] 0.0031216875 + (|-0.016467| 0.0031216875)/16 = 0.00395576953125

VI. System Implementation and Codec Appraisal

The purpose of this experiment is to investigate which codecs would give better performance using SIP in an internet telephony service provider (IPTSP) to other mobile operator network. In Figure 2 shows a test bed experiment diagram. Here, media gateway is connected with interconnection exchange (ICX) network through SS7 signaling [16]. An IP-PBX server is connected with SIP proxy by SIP trunk. SIP Phone is connected in LAN. We delivered the call from IPTSP operator SIP Phone to a Mobile operator phone number. In the same way mobile operator also connected with ICX.

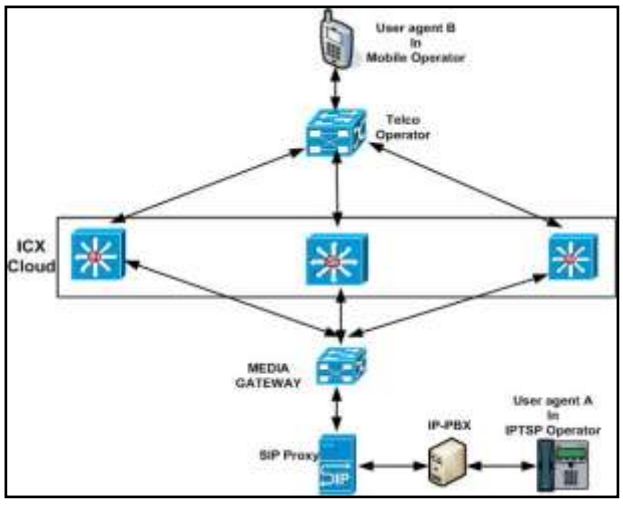


Figure 2. Network configuration for Experiment

The analysis tool that was used in this research is relatively simple and most of the used software is freeware known as Wireshark.

A. Call Test on G.729 Codec

G.729 is commonly used codec used in VoIP. In figure 3 we have shown call flow duration from SIP Phone to Mobile using G.729 codec.

The performance metrics are the transfer time and packet loss. Both of these metrics could be collected using the Wireshark application. Transfer time could be divided into 2 types namely the estimated transfer time and exact transfer time [12]. The estimated transfer time is defined as the time duration when a SIP REFER request had been sent and when the new conversation between the corresponding node (CN) and the target device is established (i.e. when the first Real Time Protocol (RTP) packet is sent or received).

The exact transfer time is the time between the terminations of initial call acknowledged by the last RTP packet received/sent and the establishment of the new RTP session where the first RTP packet is send/received. By monitoring the packets captured by Wireshark, the session transfer time between the devices can be determined [11].

From the figure 3 total duration to establish call is (92.721-84.036)s=8.685s.

The Graph Analysis dialog shows the SIP messages sent by the various parties. The first message in Figure 3 is an INVITE message, which is the first step in setting up a call. In this case, the IP phone is asking the PBX to place a call to a SIP address of sip:01755518856@202.4.96.20, which is a mobile operator number. The response to this is a request for authentication, which is acknowledged. The phone tries again and is given a status of "Trying" by the PBX. The PBX then proceeds to INVITE the remote endpoint by contacting fwd.pulver.com. Several more messages are exchanged before the call is set up properly. The estimated transfer time is computed as the difference between the time stamps when the REFER request is sent out and the first RTP packet in the transferred call is received as shown in Figure 3.

Figure 3. Call flow diagram

One of SIP's jobs is to set up the RTP stream between two endpoints. It does this through the Session Description Protocol (SDP), which carries the information about codecs, IP addresses and port numbers that is necessary for VoIP to work. The RTP streams are unidirectional, so a full duplex conversation requires a separate RTP stream to be set up in each direction, using two separate SDP messages. This SDP message will contain the IP address, UDP port and codec that the remote end is to use to talk to the local IP phone. SDP messages are tagged with SDP in the Graph Analysis window. In figure 4 illustrate the different QoS parameters which have to be considered. We will measure the time since the INVITE message is sent by the origin until it arrives to the destination phone. We calculate call arrivals follow a Poisson distribution with different values. Call duration has been modeled with a normal distribution of 180 sec. average. The comment column has protocol dependent information.

From the packet analyzer software, RTP packets from both the forward and reverse directions are filtered. VOIP networks are very sensitive to packet losses which affect QoS. In figure 4 shown RTP streaming analyses from LAN IP 172.16.1.127 to SIP server IP 202.4.96.20.
From the Figure 4 we find the delta value(ms), jitter value, number of RTP packets and bandwidth per packet for G.729 Codec.

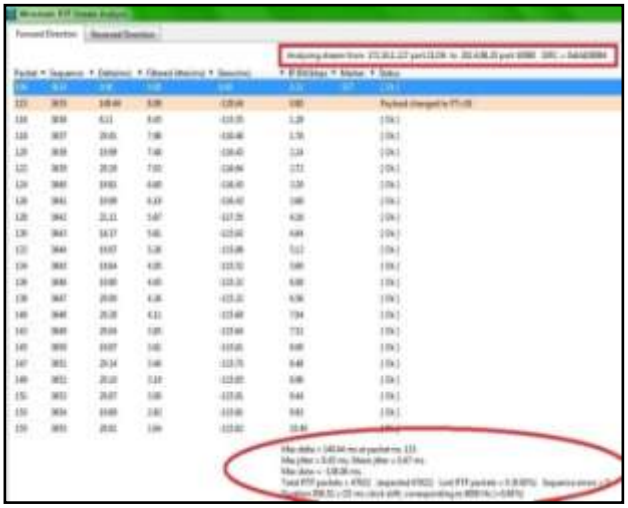


Figure 4. RTP Stream analysis during the call

Maximum Jitter = 8.45 ms,
Mean Jitter = 0.47 ms,
Total RTP = 47922
Lost RTP =0, Secuence Error =0
Total call duration = 958.51 s

The Max Delta (latency) was 149.44ms and average delta was 19ms for that stream. The Max Jitter was also good at 8.45ms (150ms of one-way latency and 20ms of jitter are the limits of what is considered acceptable). However, nearly 0% packet loss was encountered, which is extraordinary. This screen, shown in Figure 4, also displays helpful statistics, such as the current bandwidth, latency and jitter.

We have test for simultanious call and mean forward and reverse jitter are shown in figure 5. For this experiments simultaniouly 7 calls test from IPTSP operator to mobile operator and found lowest mean jitter for both forward and reverse jitter in G.729 codec.

Avearage mean forward jitter was 0.32ms to 0.37ms and means reverse jitter was 0.88ms to 1.0 ms. Averatge RTP packets /sec = 50.00

In the Figure 5 graph is representing the mean forward and reverse jitter. The IP network can induce varying delays to the received packets that is known as jitter. To control Jitter, RTP and RTCP provide information, such as time stamps and inter arrival jitter values that real-time communications applications can use to compensate for jitter during a session. An application's jitter buffers use the time stamps and the inter arrival jitter values to make adjustments so that a smooth, even flow of packets is received.

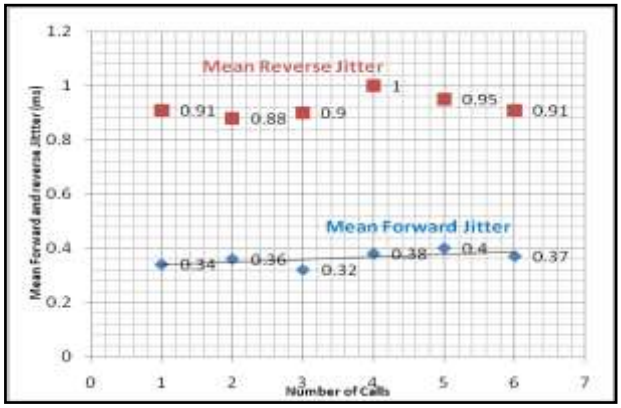


Figure 5. Mean forward and reverse jitter for G.729 calls

MOS [13] Score (objective) for G.729: E-model calculations for G.729 without handover:

Delay delta=19ms

Total delay *d*= delta + packetization delay + processing delay; = 19 + 20 + 5 = 44ms

Id=0.024 *d + 0.11(d-177.3) H (d-177.3) = 1.056

Ie is 0 for G.729

R=Ro-Id-Ie = 93.2-1.056-0= 92.144

Therefore MOS = 4.38

E-model Calculation for G.729 with handover

Avg one way delay =19ms

d=19+5+20 = 44ms

Therefore *Id* = 0.024*d = 1.056

Packet loss *(P)* for G.729 was 0.0%

Therefore, *Ie = a + bln(1+cP/100)*

= 0+30 ln(1+0.0*15/100) =0.0

R factor = 93.2-1.056 – 0.0 = 92.144

*MOS (emodel) = 1 + 0.035*R + R(R-60)(100-R)7*10^-6*

MOS (emodel) = 4.4

The RTP receiver keeps a reserve of samples in order to absorb the network jitter, instead of playing out all the samples as soon as they arrive. This reserve is known as a jitter buffer. The bigger the jitter buffer, the more jitter it can absorb, but this also introduces bigger delay. If jitter buffer size is too small, then many late packets may be

considered as lost and thus lowers the voice quality and lowers the overall QoS. In figure 6 there are 6 graphs. Graph 1 means Forward jitter from 202.4.96.20 to 172.16.1.127. Graph 2 Forward difference from 202.4.96.20 to 172.16.1.127, Graph 3 Forward delta from 202.4.96.20 to 172.16.1.127, Graph 4 means reverse jitter from 172.16.1.127 to 202.4.96.20. Graph 5 reverse differences from 172.16.1.127 to 202.4.96.20, Graph 6 reverse delta from 172.16.1.127 to 202.4.96.20.

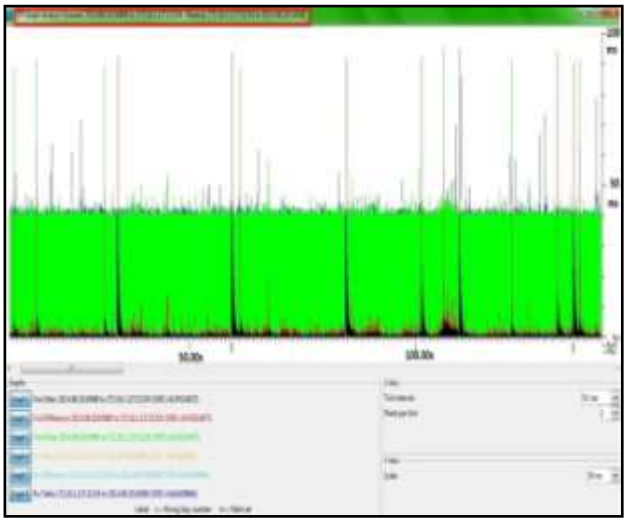


Figure 6. Graph of forward and reverse jitter and delta during the call

B. Call Test on G.711A Codec

G.711 is an ITU –T standard and is primarily referred to as telephony codec. Formal name for G.711 is Pulse Code Modulation (PCM) and it represents speech sampled at 8000 samples/second. G.711 uses two main logarithmic algorithms: A- law and the μ – law. A – law is suitable for lower level signals.

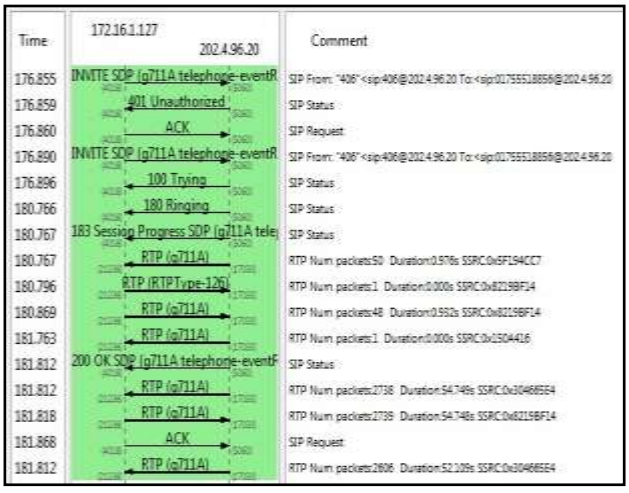


Figure 7. Call flow diagram

In Figure 7 we have shown call flow duration from SIP Phone to Mobile using G.711a codec.

From the figure 7 total duration to establish call is (181.812-176.855)s=4.957s.

From the Figure 8 we find the delta value(ms), jitter value, number of RTP packets and bandwidth per packet for G.711a Codec.

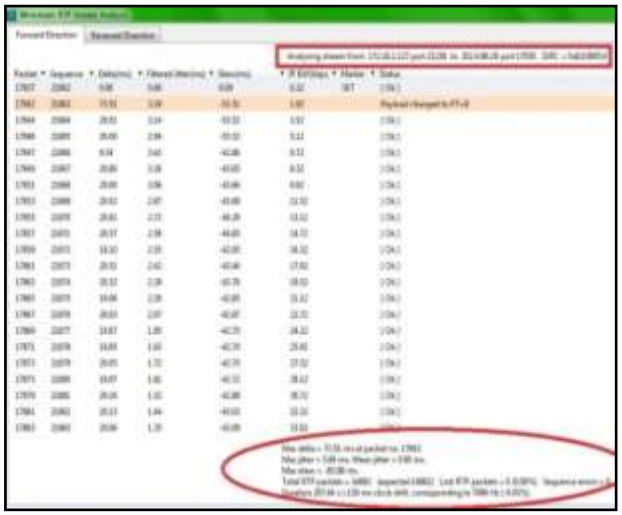


Figure 8. Overview of RTP Stream during the call

Maximum Jitter = 5.60 ms,
Mean Jitter = 0.60 ms
Total RTP = 14882
Lost RTP = 0, Sequences Error =0
Total call duration = 297.64 s

The Max Delta (latency) was 73.51ms and average delta was 20.5ms for that stream. The Max Jitter was also good at 5.60ms (150ms of one-way latency and 20ms of jitter are the limits of what is considered acceptable). However, nearly 0% packet loss was encountered, which is extraordinary. This screen, shown in Figure 8, also displays helpful statistics, such as the current bandwidth, latency and jitter.

We have anlysis result on simultanious call. In the Figure 9 a graph is representing the forward and reverse delta value and jitter for Codec G.711a. Avearage mean forward jitter was 0.60ms to 0.66ms and means reverse jitter was 1.15ms to 1.26 ms. Averatge RTP packets /sec = 50.00

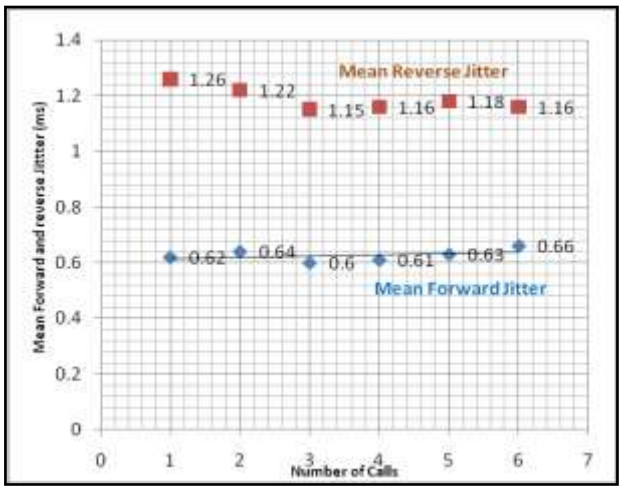


Figure 9. Mean forward and reverse jitter for G711a calls

MOS Score (objective) for G.711a: E-model calculations for G.711a without handover:

Delay delta=19ms

Total delay *d*= delta + packetization delay + processing delay; = 20.5 + 20 + 5 = 45.5ms

Id=0.024 *d + 0.11(d-177.3) H (d-177.3) = 1.092

Ie is 0 for G.711

R=Ro-Id-Ie = 93.2-1.092-0= 92.108

Therefore MOS = 4.37

E-model Calculation for G.711a with handover

Avg one way delay =19ms

d=20.5+5+20 = 45.5ms

Therefore *Id* = 0.024*d = 1.092

Packet loss *(P)* for G.711 was 0.0%

Therefore, *Ie = a + bln(1+cP/100)*

= 0+30 ln(1+0.0*15/100) =0.0

R factor = 93.2-1.092 – 0.0 = 92.108

*MOS (emodel) = 1 + 0.035*R + R(R-60)(100-R)7*10^-6*

MOS (emodel) = 4.38

In the figure 10 shows reverse and forward delta and jitter during the call.

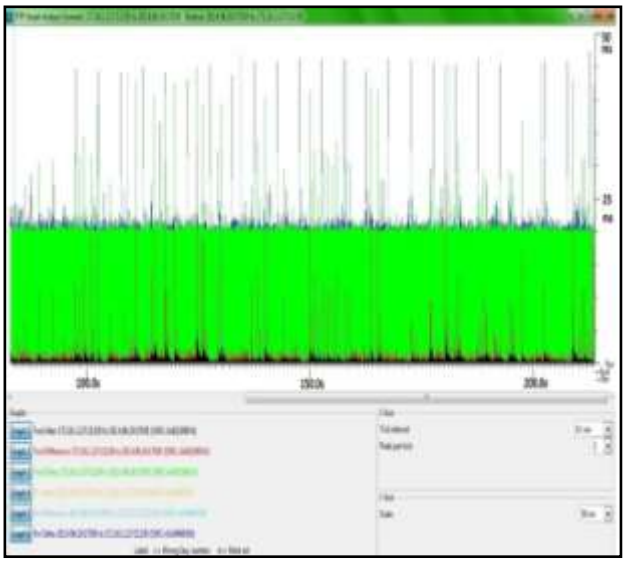


Figure 10. Graph of forward and reverse jitter and delta during the call

C. Call Test on G.711U Code

G.711 is an ITU-T standard for audio companding. Known as Pulse Code Modulation (PCM), is a very commonly used waveform codec [17-18]. The μ – law is more suitable for higher level signals. In Figure 11 we have shown call flow duration from SIP Phone to Mobile using G.711u codec. From the figure 11 total duration to establish call is (87.343-82.090)s=5.253s.

From the Figure 12 we find the delta value(ms), jitter value, number of RTP packets and bandwidth per packet for G.711u Codec.

From the Figure 12 we alalysis RTP analysis where we find Maximum delta = 135.67, Maximum Jitter= 7.23 ms,

Mean Jitter= 0.67 ms,

Total RTP= 39523, Lost RTP= 0, Sequences Error=0,

Total call duration= 790.56 s

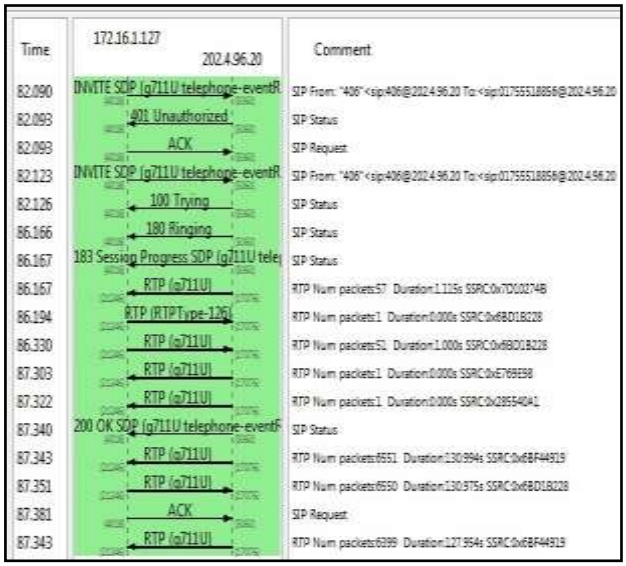


Figure 11. Call flow diagram

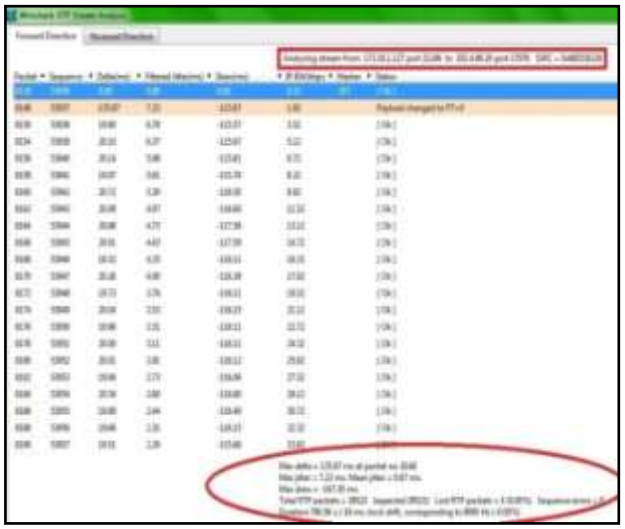


Figure 12. Overview of RTP Stream during the call

MOS Score (objective) for G.711u: E-model calculations for G.711u without handover:

Delay delta=19.5ms

Total delay *d*= delta + packetization delay + processing delay; = 19.5 + 20 + 5 = 44.5ms

Id=0.024 *d + 0.11(d-177.3) H (d-177.3) = 1.068

Ie is 0 for G.711

R=Ro-Id-Ie = 93.2-1.068-0= 92.132

Therefore MOS = 4.37

E-model Calculation for G.711u with handover

Avg one way delay =19ms

d=19.5+5+20 = 44.5ms

Therefore *Id* = 0.024*d = 1.068

Packet loss *(P)* for G.711u was 0.0%

Therefore, *Ie = a + bln(1+cP/100)*

= 0+30 ln(1+0.0*15/100) =0.0

R factor = 93.2-1.068– 0.0 = 92.132

MOS (emodel) = 1 + 0.035*R + R(R-60)(100-R)7*10^-6

MOS (emodel) = 4.39

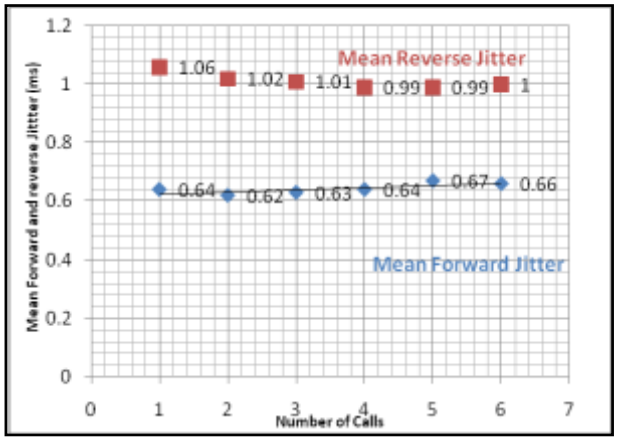


Figure 13. Mean forward and reverse jitter for G711u calls

From the RTP alaysis we have shown mean jitter in figure 13. The Max Delta (latency) was 135.67ms and average delta was 19.5ms. Avearage mean forward jitter was 0.62ms to 0.67ms and means reverse jitter was 1.0ms to 1.06 ms. Averatge RTP packets /sec = 50.00

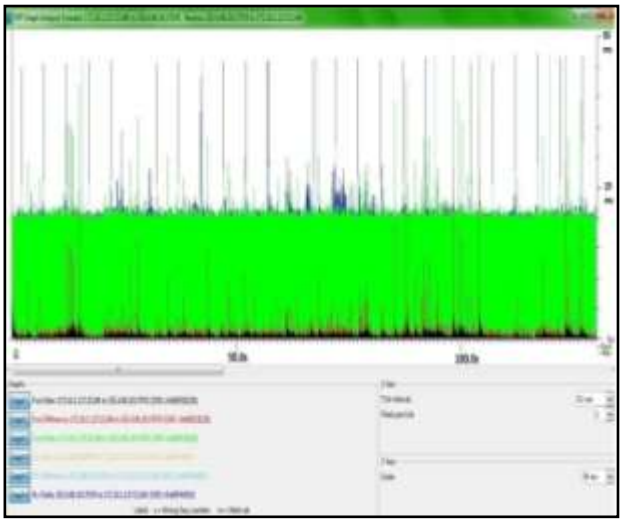


Figure 14. Graph of forward and reverse jitter and delta during the call

In the Figure 14 a graph is representing the forward and reverse delta and jitter for Codec G.711u.

VII. Conclusion

In this paper, we have analyzed several important critical qualities of service parameters of VoIP such as average one way delay, average forward and reverse Jitter, MOS and packet loss for different VoIP codecs like G.711u, G.711a, and G.729 with respect to number of VoIP call flows in this wired network. Simulation results show that G.729 codec performs better than G.711u and G.711a codec under heavy load in respect of delay, Jitter, MOS and packet loss in wired network. It is shown that G.729 gives the best performance in terms of jitter buffer variation on LAN environment. Other fact has been found that the increasing number of jitter buffer size is not linear to the decreasing of packet drop percentage. As there is a less bandwidth requirement for G.729 codec, therefore this codec is mostly used in VoIP applications where bandwidth must be conserved.

Acknowledgment

The authors would like to thanks Department of Electrical and Electronic Engineering, School of Engineering and Computer Science, Independent University, Bangladesh.

References

[1] Akbar Ali, Nehal Ahmad, Mohd Sharique Akhtar, Aditya Srivastava, “Session Initiation Protocol,” International Journal of Scientific and Engineering Research, Vol. 4, No.1, pp.1 -6, 2013.

[2] Stephan Massner, Chris Richter,Uwe Hautzendorfer, “SIP Trunking — General Requirements for Interconnecting Enterprise Networks,” Journal Of Networks, Vol. 8, No. 10, pp.2195-2212, 2013.

[3] Muhammad Yeasir Arafat, Feroz Ahmed, M Abdus Sobhan, ‘‘SIP Security in IP Telephony,” Elastix world 2013, Mexico, 2013

[4] Hira Sathu, Mohib A. Shah, “Performance Comparison of VoIP Codecs on Multiple Operating Systems using IPv4 and IPv6,” International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 2, No. 2, pp.122 -125, 2012

[5] Sk.Nagulmeera, V.T.Venkateswarlu, “Quality of Service (QoS) Improvement in VOIP over WLANs,” Int. J. of Advances in Computer, Electrical & Electronics Engineering, Vol. 2, No. Sp. Issue of NCIPA, pp.86-89, 2012

[6] F. Javier Rivas, Almudena D áz, Pedro Merino, “Obtaining More Realistic Cross-Layer QoS Measurements: A VoIP over LTE Use Case,” Journal of Computer Networks and Communications, Vol. 2013, No. 10, pp.48 -55, 2013

[7] M. Voznak, J. Rozhon, “Approach to stress tests in SIP environment based on marginal analysis,” Springer Telecommunication Systems, vol. 10, No. 10, pp.1243-1257, 2011.

[8] F. Alvarez-Vaquero, J. Sanz-Gonzalez, “Network VoIP for corporative environment design,” In Proc. 7th WSEAS International Conference on Telecommunications and Informatics, Turkey, pp. 194-198, 2008

[9] Xianhui Che, Lee J. Cobley, “VoIP Performance over Different Interior Gateway Protocols,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 1, pp. 34-41, 2009.

[10] M. Voznak, J. Rozhon, “SIP infrastructure performance testing,” 9th WSEAS International Conference on Telecommunications and Informatics, Catania, pp. 153-158, 2010

[11] Said El Brak, Mohammed Bouhorma, Mohamed El Brak, Anouar Bohdhir, “Speech Quality Evaluation Based Codec for VoIP Over 802.11P,” International Journal of Wireless & Mobile Networks (IJWMN), Vol. 5, No. 2, pp. 75-87, 2013

[12] Priyanka Luthra, Manju Sharma, “Performance Evaluation of Audio Codecs using VoIP Traffic in Wireless LAN using RSVP,” International Journal of Computer Applications, Vol. 40, No.7, pp.88 – 97, 2012

[13] A. Kovac, M. Halas, M. Orgon, M. Voznak, “E-model MOS Estimate Improvement through Jitter Buffer Packet Loss Modelling,” In Advances in Electrical and Electronic Engineering, Vol. 9, No. 5, pp. 233-242, 2011

[14] M. N. Ismail, "Analysis of Secure Real Time Transport Protocol on VoIP over Wireless LAN in Campus Environment," International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 02, pp.898-902, 2010
[15] Nasreddine Hajlaoui, Issam Jabri, Maher Ben Jemaa, "Experimental Performance Evaluation and Frame Aggregation Enhancement in IEEE 802.11n," International Journal of Communication Networks and Information Security (IJCNIS) Vol. 5, No. 1, pp 48-58, 2013
[16] Muhammad Imran Tariq, Muhammad Ajmal Azad, Syed Khurram Rizvi, "Effect of Mobility Patterns on VoIP QoS in Mobile WiMAX," International Journal of Computer Science and Telecommunications, Vol. 4, No. 1, pp.1-7, 2013
[17] Rajesh Kumar1, Sandip Chauhan, Survey, "Analysis of Media Keying Techniques in Session Initiation Protocol (SIP)," Journal of Computer Science and Information Technology, Vol. 2, No. 5, pp.289 – 301, 2013
[18] Salma RATTAL, Abdelmajid BADRI, Mohammed MOUGHIT, "Performance Analysis of Hybrid Codecs G.711 and G.729 over Signaling Protocols H.323 and SIP," International Journal of Computer Applications, Vol. 72, No.3, pp.30-33,2013
[19] Mohamed Khedr, Onsy Abd El Aleem, Mohamed Mahmoued Selim, " Evulation of SIP-based VOIP in Heterogeneous Netwroks," International Conference on Computer Engineering and Systems, pp. 184-89, ICCES,2007

Muhammad Yeasir Arafat received the B.Sc. degree in Electronic and Telecommunications engineering from Independent University, Bangladesh, in 2012, the M.Sc. degree in Computer Network and Communications engineering from Independent University, Bangladesh, in 2014. He worked as a System Engineer at Dhakacom Limited. His research interests include Computer networks, Network architecture, Network planning, design and Network security, communication protocols: SIP, H.323, Linux and UNIX, Open source VoIP system, Asterisk, VoIP development, integration, VoIP Security, Quality of Service and Universal radio peripheral (USRP) Software. He has published over 4 papers in different peer reviewed international journals and 4 papers on national and international conferences. Mr. Yeasir is a member of the Institute of Electrical and Electronic Engineers (IEEE).

Muhammad Morshed Alam received the B.Sc. degree in Electrical and Electronic engineering from Independent University, Bangladesh, in 2013. He worked as a System Engineer at Link3 Technology, Dhaka. His research interests include Computer networks, Network architecture, Network planning, design and Network security, communication protocols: SIP, H.323, Linux and UNIX, Open source VoIP system, Asterisk, VoIP development, integration, VoIP Security, Quality of Service and Universal radio peripheral (USRP) Software. He has published over 2 papers in different peer reviewed international journals.

Feroz Ahmed received the B.Sc. degree in electrical and electronic engineering from Rajshahi University of Engineering and Technology, Bangladesh, in 1995, the M.Sc. degree in electrical engineering from University Technology Malaysia, Malaysia, in 1998, and the Ph.D. degree in communication engineering from the University of Electro-Communications, Tokyo, Japan in 2002. From 2002 to 2005, he worked as a postdoctoral research fellow at Gunma University, Gunma, and the University of Electro-Communication, Tokyo, Japan. In 2005, he was appointed as an Assistant Professor in the school of engineering and computer science at the Independent University, Bangladesh and became an Associate Professor in 2011. His research interests include optical fiber communications, wireless communications, and network security. He has published over 55 papers in different peer reviewed international journals and conferences. Dr. Ahmed is a member of the Institute of Electrical and Electronic Engineers (IEEE).

A Resource-Efficient System for Detection and Verification of Anomalies Using Mobile Agents in Wireless Sensor Networks

Muhammad Usman, Vallipuram Muthukkumarasamy, and Xin-Wen Wu
School of Information and Communication Technology, Griffith University,
Gold Coast Campus, Queensland 4222, Australia
Email: muhammad.usman3@griffithuni.edu.au, v.muthu@griffith.edu.au, x.wu@griffith.edu.au

Abstract— **Sensor readings are vulnerable to in situ and in transit anomalies. A well designed anomaly detection system should be able to identify the source of anomalies through in situ verification of suspicious behavior of sensor nodes. One approach for in situ verification is physical diagnosis of sensor nodes, which is a cumbersome and time-consuming task in medium-to-large-scale networks. Therefore, we propose a novel method for in situ verification of malicious sensor nodes using mobile agents. We employ Coordinated Resource Management mechanism-based observations to detect first-order anomalies and perform in situ verification. Since mobile agents cannot be frequently transmitted over the resource constrained Wireless Sensor Networks (WSN) due to the expensive nature of the communication operation as compared to the processing operation, we propose a method which exploits the historical information of anomalous behavior of the sensor node to optimize mobile agent transmission. The performance of the proposed system is investigated via simulations, experiments on MICAz mote, and comparative study. The results and analysis demonstrate the effectiveness and efficiency of the proposed system, in comparison with other existing schemes.**

Index Terms— **Agent transmission optimization, Anomaly detection system, First-order anomalies, In situ verification, Anomaly agent, Wireless sensor networks**

I. Introduction

THE emergence of innovative networking frameworks such as Internet of Things and Shared Sensor Networks has increased the deployment of the Wireless Sensor Networks (WSN) for a number of application domains such as wireless smart home sensor networks, built infrastructure monitoring, smart cities, and health monitoring [1]. The built infrastructure monitoring is one of the promising WSN applications, which monitors water, electricity, and gas consumption, and carbon dioxide (CO_2) emission in the built environments [2]. The performance of such data-centric applications is highly dependent on the accuracy of the received sensed data. However, sensor nodes and their sensor readings are vulnerable to *in situ* and *in transit* anomalies due to several factors such as faults, errors, and attacks. An anomaly detection system can be deployed to detect such anomalies in order to mitigate them. Effective mitigation can only be performed after correct identification of the source of anomalies. Existing anomaly detection schemes, however, focus only on detection of anomalies rather than the identification of the source of anomalies [3]-[7]. This limits the effectiveness of the existing schemes.

A robust anomaly detection system should be able to identify the source of anomalies, after their timely detection. This may be accomplished through in situ verification of malicious sensor nodes. Typically, in situ verification of a sensor node can be performed through physical diagnosis. However, it may not always be possible to gain frequent physical access to sensor nodes, particularly when they are deployed on difficult terrains or within the vicinity of private built infrastructure (such as houses). Over the years, the research community has proposed several software mobile agent-based anomaly detection schemes, which have employed mobile agents for different roles such as transmission of control messages among different entities and random sampling of sensed data over the sensor network [3]-[7]. However, these schemes have not considered mobile agents for in situ verification of sensor node in pursuit of identification of the source of anomalies.

In this study, we propose a method that enables mobile agents to use Coordinated Resource Management (CRM) mechanism-based information to perform in situ diagnosis of the sensor nodes. The CRM mechanism enables sensor nodes to share their resource status with corresponding cluster heads or the base station for network resource management. The TinyOS facilitates CRM mechanism through low-level interfaces to share and manage the hardware state of the node over the network [8], [9]. In addition to the traditional network resource management, our hypothesis is to employ CRM-based information to detect several types of first-order anomalies and to perform an in situ verification process. To the best of our knowledge, this is the first study to employ CRM mechanism for both these purposes.

In the proposed system, we exploit the statistical association among different features of the CRM-based observations to define first-order joins over their underlying dis-

Manuscript received June 8, 2014; revised October 24, 2014.
Correspondence e-mails: manilasani@yahoo.com, muhammad.usman3@griffithuni.edu.au
A preliminary version containing initial work of this study has appeared in the proceedings of the 9th International Conference on Ubiquitous Intelligence and Computing, and 9th International Conference on Autonomic and Trusted Computing, pp. 322-329, September 2012.

doi:10.4304/jnw.9.12.3427-3444

tributions. This enables our proposed Anomaly Detection System (ADS) to detect a range of first-order anomalies, which are caused by denial of sleep attack, battery exhaustion attack, and sensor node faults. The ADS further uses information received from CRM-based observations to verify the source of anomalies using mobile agents. However, mobile agents cannot be frequently transmitted due to the expensive nature of communication overhead in terms of energy consumption [10]. To address this research challenge, we propose a method that optimizes mobile agent transmission by taking into account the weighted sum of anomalous instances of historical and current observations. This approach assists the system administrator in controlling the transmissions of mobile agents, which prolongs the network lifetime as compared to the existing approaches [3]-[7].

In summary, the main contributions of this paper are as stated below:

- The proposed mobile agent-based anomaly detection and verification system with internal structure and algorithms, which is not only capable of detecting a range of first-order anomalies, but also performs in situ verification of the cluster member sensor nodes using information gathered through the CRM mechanism.
- A mobile agent transmission optimization method is proposed that incorporates the past and current behaviors of the sensor node to optimize the agent transmission process in order to prolong the network lifetime.
- The proposed algorithms are implemented on a real sensor node to assess the feasibility of the proposed methods on the low-resource sensor nodes. We also carried out a thorough analysis of the proposed model through a simulation study, to estimate the detection rate of anomalies and energy consumption.

The remainder of this paper is organized as follows: Section II provides a brief overview of the related work. The architecture of the proposed anomaly detection system is explained in Section III. Algorithms of the proposed system are presented in Section IV. Section V provides analysis of the results obtained through implementation, simulation, and comparative study. Section VI concludes the paper.

II. Related Works

The use of anomaly detection in communication and networking systems to discover outliers, exceptions, or contaminants caused by in situ or in transit errors, faults, or attacks was started as early as in 1987 with the pioneer work carried out by Denning [11]. Her hypothesis advocates the use of abnormal pattern in the audit record to detect anomalies in the system. Her proposition later on served as a base to develop several real-time anomaly detection systems in various network types and applications. On the basis of the position of the anomaly detection component within the WSN, the existing anomaly detection schemes can be classified into three categories, namely, centralized, semi-centralized, and distributed [12]. The central authority, a base station, is responsible for carrying out the anomaly detection process in the centralized class of schemes. The cluster heads are responsible for detection in the semi-centralized schemes. The distributed schemes have a cooperative nature of working among cluster heads and cluster members nodes to accomplish the anomaly detection task. Based on this taxonomy, the research community has proposed several notable anomaly detection schemes for WSNs over the last decade [13]-[16]. However, none of these centralized, semi-centralized, or distributed schemes have focused on the identification of the source of anomalies, which is an important service to effectively rectify the causes of anomalies.

Over the years, several attempts have been made to use the mobile agent technology for anomaly detection in addition to other tasks such as localization, parallelism, and distributed data fusion [3]-[7]. One of the initial studies which advocates the use of mobile agent technology for anomaly detection was undertaken by Krugel et al. [3]. Their work suggests the dispatch of mobile agents as guards to roam among different nodes to accomplish random sampling. The comprehensive detection is initiated after the identification of the anomalous activities. Although this proposal reduces dispatch and arrival costs of the mobile agents, nodes are vulnerable to attacks in the absence of guards.

Ketel suggested the use of several static and mobile agents for distributed anomaly detection application in WSNs [4]. In his work, Static Agents (SA) are located at each cluster head and transmit the anomaly report to the Mobile Agent Server (MAS) after observing anomalous activities. In response, MAS triggers a mobile agent to the respective monitoring node. The mobile agents are further divided into thick and thin agents associated with rich and low resource nodes, respectively. The Victim Node List (VNL) is responsible for generating the itinerary of MA. However, the author has offered no explanation about the internal details of the MAS repository and working of the VNL. In another study, Pugliese and colleagues proposed a rule-based method to detect network-layer anomalies by using mobile agents [5]. The formalism based on Weak Process Models (WPM), a non-parametric version of Hidden Markov Model, is employed to reduce the rules of reachability. The threat model is classified into low and high types of attacks. However, the authors have only reported the early implementation results. The thorough performance analysis of the proposed method is required to establish its effectiveness for low resource WSNs.

Eludiora et al. investigated the use of mobile agents for a distributed intrusion detection application in which sensor nodes directly communicate with the base station instead of the cluster heads [6]. The mobile agents are employed to communicate among different base stations. This model is based on two algorithms. The first algorithm detects DoS attacks and consequently updates the status of the sensor node to the base station. The second algorithm

calculates the probability of the failure of the base station to discover anomalies. The major drawback of this study is its heavy reliance on the non-realistic assumption of one hop distance among sensor nodes and the base station. Khanum et al. presented an architecture of mobile agent based hierarchical IDS for WSN [7]. Their work employs three agents for anomaly detection: Analyzer Agent, Management Agent, and Coordinating Agent. The detection module is installed at each cluster head. Then anomalies are detected at two levels: node and network. Nevertheless, in their work no attempt has been made to quantify the proposed architecture through experimental or analytical study.

The analysis of the above-mentioned studies provides the evidence that none of the existing schemes is specifically designed for the CRM-based observations. Similarly, no scheme has considered the verification of source of anomalies that is desired to effectively counter them. Furthermore, existing mobile agent-based anomaly detection schemes have not considered space and transmission costs of mobile agents. Therefore, these schemes have overlooked an important aspect that the mobile agents cannot be freely used and transmitted over the network because of the memory and energy restrictions of WSNs. To overcome these issues, this study presents a detailed mobile agent-based anomaly detection system after due consideration of space and transmission costs. We have exploited association among the CRM-based normal profile features to detect several types of first-order anomalies. We have also proposed a method which employs mobile agents to perform the in situ verification in order to confirm the source of anomalies. Furthermore, the transmissions of the mobile agents are optimized by taking into account the anomalous instances of the historical and current observations. Unlike existing schemes, we have also performed the thorough theoretical and empirical analyses to investigate the efficiency and effectiveness of the proposed system.

III. Anomaly Detection and Verification Architecture

In this section, we describe the network model and explain the role of the components of the anomaly detection module in the proposed system.

A. Network Model

We consider a network region with a large number of low resource MICAz sensor nodes. The network region is virtually segmented into several clusters which are governed by the resource rich Cluster Head (CH) nodes. The cluster member nodes (SN) periodically sense their ambient environment and transmit data to their respective CHs. The CH nodes keep track of the resource status of the SNs through the CRM-mechanism [9]. The CH nodes are also aware of the actions performed by the SNs such as sensing from the ambient environment and going into sleep and wake up modes. The CH nodes detect anomalies and take appropriate actions after filtering incoming data packets that are received from the SNs. The mobile agents are positioned at CH nodes that can transmit them for in situ verification of the SN, in addition to other traditional operations such as code and data dissemination, localization, and distributed data fusion. A resource rich node, that is, a personal digital assistant or laptop class device, acts as a Base Station (BS). The BS manages the overall network through a user application. The BS is a main decision-making authority, whereas CH nodes act as regional chiefs. The generalized structure of the mobile agent-based network model is depicted in Figure 1.

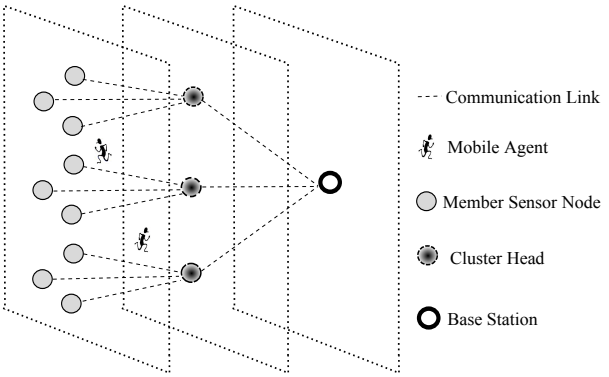


Figure 1. Mobile agent-based network model

The overall course of the main events in the network model can be formally described as given below:

- $<E_0,\ SN_R>$: In the event E_0, the sensor reading R is collected by the sensor node SN from its ambient environment.
- $<E_1, R>/<E_1, R^{'}>$: In the event E_1, the normal reading R or the anomalous reading $R^{'}$ is sent to the cluster head CH.
- $<E_2, Anly>$: In the event E_2, the CH performs analysis on $<E_1, R>/<E_1, R^{'}>$.
- $<E_3, Anm_Agnt>$: In the event E_3, the anomaly agent Anm_Agnt is transmitted to the SN for in situ verification.
- $<E_4, Ins_V>$: In the event E_4, the Anm_Agnt performs in situ verification of the SN.
- $<E_5, Ins_R>$: In the event E_5, the SN transmits results of in situ verification to the CH.
- $<E_6, Agg_R>/<E_6, Anm>$: In event E_6, the aggregated data or anomaly report is forwarded to the BS.
- $<E_7, Dec_P>$: In the event E_7, the BS makes a decision on $<E_6, Agg_R>/<E_6, Anm>$.
- $<E_8, Dec_R>$: In the event E_8, the report of $<E_7, Dec_P>$ is sent to the CH.
- $<E_9, Act>$: In the event E_9, the CH takes an action on the sensor node.

Note that the order of the aforementioned events is only for the first cycle of the system at the time of deployment. During normal operation of the system, event E_8 may not occur. However, if BS wishes to update CH regarding the anomaly detection process, then event E_8 may take place. To have a better picture of the working of the overall system, the above-mentioned course of events can

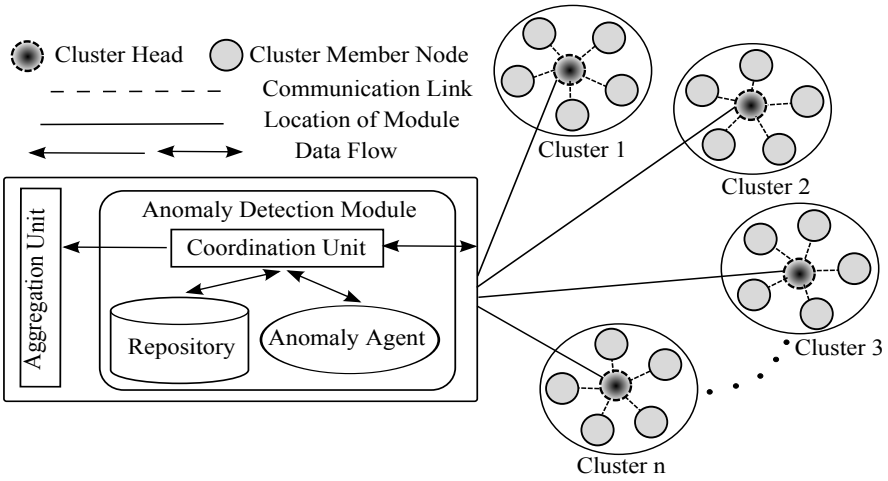


Figure 2. Anomaly detection module deployed on cluster heads

be formally defined as illustrated below:

$S \in SN, CH \ \& \ BS$

$S_0 \in SN$

$\sum = \{<E_0, SN_R>, \ <E_1, R>/<E_1, R^{'}> \ <E_2, Anly>, <E_3, Anm\_Agnt>, <E_4, Ins_V>, <E_5, Ins_R>, <E_6, Agg_R>/<E_6, Anm>, <E_7, Dec_P>, <E_8, Dec_R>, <E_9, Act>\}$

$\wedge \in 0, 1$

$T : S \times \sum \rightarrow S = \{(SN \times <E_0, SN_R> \rightarrow SN), (SN \times <E_1, R> \rightarrow CH), (SN \times <E_1^{'}, R^{'}> \rightarrow CH), (CH \times <E_2, Anly> \rightarrow CH), (CH \times <E_3, Anm\_Agnt> \rightarrow SN), (SN \times <E_4, Ins_V> \rightarrow SN), (SN \times <E_5, Ins_R> \rightarrow CH), (CH \times <E_6, Agg_R> \rightarrow BS), (BS \times <E_7, Dec_P> \rightarrow BS), (BS \times <E_8, Dec_R> \rightarrow CH), (CH \times <E_9, Ac> \rightarrow SN) \}$

$G : S \rightarrow \wedge = \{ (SN \rightarrow 0, 1), (CH \rightarrow 0, 1), (BS \rightarrow 0, 1) \}$

In the above definition, "0" and "1" denote normal and anomalous states, respectively. Note that we have assumed CH and BS as secure, however, they are prone to faults, thus they can have values of either 0 or 1.

B. Anomaly Detection Module

Each cluster head is equipped with an Anomaly Detection Module (ADM). The ADM performs several key jobs including first-order anomaly detection, in situ verification using mobile agents, and agent transmission optimization. The ADM is composed of three components: Coordination Unit, Anomaly Agent, and Repository. Figure 2 illustrates the structure of the ADMs positioned on the different CH nodes.

1) Coordination Unit: The Coordination Unit (CU) is a core element of the ADM. It performs intra-ADM components coordination and anomaly detection related communication with other entities of the network such as BS. The CU extracts values of "features of interest" from incoming network traffic to perform anomaly detection as per anomaly detection criteria. The process of anomaly detection is described in Section IV-B. The normal sensor reading is forwarded to the Aggregation Unit (AU) after the anomaly detection process. The AU is a logical unit within the cluster head that aggregates sensor readings and forwards them to the BS after a pre-defined period of time. On the other hand, if received observation is found anomalous, then the CU may take the following action(s) against the anomalous node: (a) trigger anomaly agent for in situ verification, (b) generate alarm to the BS, (c) announce node as malicious or faulty to other nodes in the cluster, and (d) minimize communication with suspicious node.

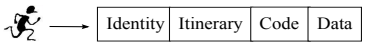


Figure 3. Internal structure of the anomaly agent

2) Anomaly Agent: The anomaly agent (a software mobile agent) is composed of four parts, viz., identity, itinerary, code, and data. Each anomaly agent has a unique identity which links it with target cluster member sensor node. The itinerary of the agent contains the address of the destination node. The code segment is made up of the code for in situ verification process and data portion consists of the values of the historical observations that are used for in situ verification of anomalous sensor node. Figure 3 depicts the internal structure of the anomaly agent.

The CU may trigger an anomaly agent for the in situ verification of the suspicious sensor node after detecting anomalies in received observations. One of three situations may arise after transmission of an anomaly agent: (a) the successful execution of the anomaly agent on the suspicious sensor node and transmission of the in situ verification result to the CH, (b) the suspicious node may defend the investigation of the anomaly agent and as a consequence does not send any result to the CH, and (c) migration of the anomaly agent to the suspicious sensor node is vulnerable to the agent execution manipulation attack. In case (a), the anomaly agent will send the desired result to the CH. In case (b), if the suspicious

node defends the investigation of the anomaly agent and does not send any result to the cluster head, this will confirm its anomalous status, which is the ultimate goal of sending the anomaly agent. In case (c), the agent execution integrity protection mechanism can be employed to avoid the execution manipulation attack [17]. Note that case (c) is only applicable to those situations where SNs are vulnerable to more sophisticated attacks and the adversary takes complete control of the node. The agent execution integrity protection mechanism is not required for anomalies caused by faults or other types of attacks. The algorithm for the in situ verification of SN using anomaly agent is elucidated in Section IV-C.

C. Repository

The repository, Rep, stores normal profile features and other related data to perform anomaly detection and mobile agent transmission processes in the form of five tuples. The structure of the repository is an extension to the initial idea reported in [11]. The tuples of the proposed system can be expressed as shown below.

$$Rep = \langle N_{id}, Res_{st}, Fet_{set}, Anm_{obs}, Act_{set} \rangle \quad (1)$$

In the above equation, N_{id} is a column vector which stores identities of the cluster member SNs. The tuple Res_{st} denotes resource status of SNs. Each SN has multiple resources such as battery and memory, which are stored as $m \times n$ matrix, where m denotes a number of SNs in the cluster and n represents their resources. The Fet_{set} tuple is based on "features of interest" which are used for anomaly detection. By default, the sensor nodes with a similar role in the network have single Fet_{set} in order to optimize the overall memory consumption of the cluster head. However, different values of Fet_{set} of similar nodes can also be accommodated depending on the security requirements and available memory space. The basic structure of the Fet_{set} is given below.

$$Fet_{set} = \langle \lambda, T, \varphi, \upsilon, F \rangle \quad (2)$$

In the above equation, λ defines minimum to maximum bounds on sensor reading values. For example, during summer daytime, feature λ can hold values between $15\,^{\circ}\mathrm{C}$ - $35\,^{\circ}\mathrm{C}$ to define the normal behavior of the SN. The feature T denotes the time interval to monitor the activities of the SN for a certain period of time. This feature keeps track of the normal behavior of the SN with respect to other features such as resource status and sensor reading. The feature φ stores values for entitled actions performed by the SN such as sensing, sleeping, wake-up, and transmission of observations. The features υ and F denote the status of the resources of the SN and received packet count, respectively.

The tuple Anm_{obs} is $w \times n$ matrix which stores w number of historical anomalous observations to facilitate the computation of threshold values to optimize anomaly agent transmission. The agent transmission optimization method is described in Section IV-D.

TABLE I.
κ ACTIONS DEFINITIONS

State	Description
A	Perform anomaly detection using first-order joins.
B	Forward aggregated data to the aggregation unit.
C	Cluster head checks behavior of the sensor node for anomaly agent transmission optimization.
D	Transmit anomaly agent to the sensor node for the in situ verification process.
E	Minimize the communication with the sensor node.
F	Announce faulty node status to other cluster heads.
G	Generate an alarm to the base station about the malicious sensor node.

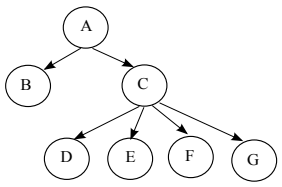


Figure 4. κ actions states flow

The structure of Anm_{obs} can be expressed as stated below.

$$Anm_{obs} = Fet'_{set} \quad (3)$$

The Fet'_{set} holds values for λ', T', φ', υ', and F', where λ' represents anomalous sensor reading values which lie outside the normal bounds, T' denotes anomalous activities of the SN with respect to time, φ' represents unauthorized actions performed by the SN, and F' denotes the abnormal frequency of received packets.

The tuple Act_{set} defines the set of actions which facilitates functionality of the anomaly detection system. It is composed of two types of actions, namely, κ and τ.

$$Act_{set} = \langle \kappa, \tau \rangle \quad (4)$$

In the above equation, κ denotes the anomaly detection action, which performs the anomaly detection after arrival of each observation. After the anomaly detection process, the anomaly detection module forwards the normal sensor reading to the aggregation unit. If an anomalous observation is received, the anomaly detection module would transmit the anomaly agent to the SN or take different actions such as generating an alarms to the BS, announcing the SN as malicious or faulty to other nodes in the cluster, and minimizing communication with the suspicious node for those observations that lie in the tolerance zone. The tuple τ represents tuning actions such as updates in first-order join bounds, and also in normal, tolerated, and anomalous zones for the Fet_{set} of the SNs. It is submitted that the action κ is executed automatically by the ADM on the CH after arrival of each observation, whereas the action τ is initiated by the network administrator from the BS. Tables I and II represent definitions of sample set of actions. Accordingly, Figures 4 and 5 show flows of these actions.

TABLE II.
τ ACTIONS DEFINITIONS

State	Description
H	Update normal zone bounds for the Fet_{set}.
I	Update tolerance zone bounds for the Fet_{set}.
J	Update first-order join bounds for the λ and T features.
K	Update first-order join bounds for the T and υ features.
L	Update first-order join bounds for the φ and υ features.
M	Update first-order join bounds for the φ and T features.
N	Update first-order join bounds for the F and T features.

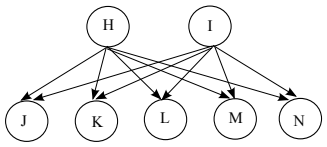


Figure 5. τ actions states flow

IV. ALGORITHMS AND ANALYSIS

The workflow of the proposed anomaly detection system consists of four processes, namely, features collection, anomaly detection, in situ verification, and anomaly agent transmission optimization. The notations used for the pseudocodes of the proposed algorithms and their analysis are listed in Table III.

A. Features Collection on Sensor Node

At time t_1, the g_{th} sensor node, SN_g, in the q_{th} cluster, collects values of the features $f_i \in Fet_{set(1)}$. The $Fet_{set(1)} = \{\lambda, \varphi, \nu\}$, $Fet_{set(2)} = \{T, F\}$, and $Fet_{set} = Fet_{set(1)} \cup Fet_{set(2)}$, where f_i denotes the value of each individual feature and λ, φ, υ, T, and F denote sensor reading, resource status, entitled action, time interval, and packet count, respectively, as described in Section III-C. The $Fet_{set(1)}$ is stored by the SN_g in its stack memory and transmitted to the cluster head, CH_q, as observation Obs_j. The values of $Fet_{set(1)}$ are used by the anomaly agent for the in situ verification process. The previous values of the features of $Fet_{set(2)}$ are computed on the CH_q after arrival of the Obs_j and used for detection of the first-order anomalies along with the received values of the $Fet_{set(1)}$. The pseudocode for the features collection process on the SN_g is illustrated in Algorithm 1.

Algorithm 1 Features, $Fet_{set(1)} = \{\lambda, \varphi, \nu\}$, collection on SN_g

1: At time t_1
2: **while** $j < m$ **do**
3: SN_g collects $f_i \in Fet_{set(1)}$
4: $PUSH$ f_i in $stck$ of SN_g
5: $Obs_j \leftarrow Obs_j + f_i$
6: $j \leftarrow j + 1$
7: **end while**
8: $TRNSMT$ Obs_j to CH_g

TABLE III.
NOTATIONS

Notation	Definition
$Aggr\_Unt$	Aggregation unit
$Agnt\_Opt(Fet_{set})$	Agent transmission optimization function
$Agnt\_stck$	Anomaly agent stack
Anm_Agnt	Anomaly agent
Anm_Beh	Anomalous behavior
Beh	Behavior of sensor node
Beh_Tol	Tolerated behavior
CH_q	q_{th} cluster head
$(CHKAnm_{1\_ord})$	Anomaly detection function
$(CHKBeh\_Anm)$	Function to check tolerated behavior Tol_η
$(CHKBeh\_Tol_\gamma)$	Function to check tolerated behavior Tol_γ
$(CHKBeh\_Tol_\zeta)$	Function to check tolerated behavior Tol_ζ
CU	Control Unit
Fet_{set}t	Features set
f_i	i_{th} single or joined feature(s)
$Fet_{set(1)}$	Features λ, φ, and υ
$Fet_{set(2)}$	Feature T and F
h	Number of stored historical tolerated and anomalous observations for agent transmission optimization
$Norm\_Beh$	Normal behavior
Obs_j	j_{th} observation
SN_g	g_{th} member sensor node in the cluster
S_{SN_g}	SN_g's historical observations score
$S_{MA_{trn}}$	Agent transmission score
SN_g_Beh	SN_g's behavior
SN_g_stck	SN_g's stack memory
SR	Sensor reading
SN_g_susp	Suspicious SN_g
$SN_g\_vrf\_rst$	In situ verification result for SN_g
$TRNSMT$	Transmit
u	f_i's tolerated current instance
v	f_i's anomalous current instance
α_1, α_2	Weighting factors for the tolerated and anomalous instances of the historical observations
β_1, β_2	Weighting factors for the tolerated and anomalous instances of the current observation
Ω_{ij}	Number of f_i's instances in the tolerated and anomalous zones from the historical observations
$\psi, -1\sigma, 1\sigma, -2\sigma, 2\sigma$	Agent transmission optimization thresholds

B. Anomaly Detection on Cluster Head

One of the objectives of the proposed anomaly detection system is to maximize the use of received CRM-based observation, Obs_j, values and computed information of $Fet_{set(2)} = \{T, F\}$ for the anomaly detection process, where $Obs_j = Fet_{set(1)} = \{\lambda, \varphi, \nu\}$. To this end, we exploit the statistical association among features of interest, $Fet_{set} = \{\lambda, \varphi, \nu, T, F\}$, to detect certain types of group anomalies, which are caused by in situ fault or attack, resource exhaustion attack, denial of sleep attack, and faults on node. We define the first-order join as a two-dimensional association among two features by defining bounds on each feature to compute normal region. On the basis of this definition, we establish a first-order join between λ and T features to detect anomalies caused by in situ fault or attack. The symptom of such anomalies on the CH_q is the receipt of the erroneous values of the sensor readings with respect to the time intervals. The combined normal region for λ and T features can be computed from the following equation.

TABLE IV.
FIRST-ORDER JOINS, CORRESPONDING ANOMALIES, AND THEIR DESCRIPTION

First-order joins	Anomalies	Description
$N(\lambda, T)$	In situ fault or attack	Out of normal bounds sensor readings with respect to time
$N(T, \nu)$	Resource exhaustion attack	The unexpected surge in battery usage with respect to time
$N(\varphi, \nu)$	Faulty node, attack on node's resources	The excessive battery usage while performing routine tasks
$N(\varphi, T)$	Faulty node	The unauthorized actions performed by the sensor node with respect to time
$N(F, T)$	Denial of sleep attack, faulty node	The repetitive transmission of data packets with respect to time

$$N(\lambda, T) = \int_{\lambda_i}^{\lambda_f} \int_{T_i}^{T_f} f(\lambda, T)\, dT\, d\lambda \tag{5}$$

In the above equation, letter N denotes the normal region with respect to the features λ and T, and subscripts i indicates the initial and f represents the final limit of the respective feature. The next first-order join is set up by joining the features T and ν to detect anomalies caused by the resource exhaustion attack. The symptom of such anomalies is an unexpected surge in the resource usage with respect to the time interval. The normal region for the resource exhaustion attack can be computed from the equation (6).

$$N(T, \nu) = \int_{T_i}^{T_f} \int_{\nu_i}^{\nu_f} f(T, \nu)\, d\nu\, dT \tag{6}$$

The next two first-order joins are (φ, ν) and (φ, T). These first-order joins detect anomalies which occurred due to faulty node and attack on the node's resources. In these cases, the symptoms are unusual resource usage while performing routine tasks and unauthorized actions performed by the sensor node with respect to time. The normal regions for the first-order joins (φ, ν) and (φ, T) can be derived from the following equations.

$$N(\varphi, \nu) = \sum_{\varphi_i}^{\varphi_f} \int_{\nu_i}^{\nu_f} f(\varphi, \nu)\, d\nu \tag{7}$$

$$N(\varphi, T) = \sum_{\varphi_i}^{\varphi_f} \int_{T_i}^{T_f} f(\varphi, T)\, dT \tag{8}$$

Finally, the first-order join is established among the features F and T to detect the anomalies caused by the faulty node and denial of sleep attack. The symptom for such anomalies at the cluster head is the exceeding number of packet count. The normal region for this first-order join can be calculated from the equation (9).

$$N(F, T) = \sum_{F_i}^{F_f} \int_{T_i}^{T_f} f(F, T)\, dT \tag{9}$$

The first-order joins of the feature set, corresponding anomalies, and their description are summarized in Table IV.

To detect the above mentioned anomalies, the CH_q receives the Obs_j from the SN_g. Then the coordination unit extracts the values of the $Fet_{set(1)} = \{\lambda, \varphi, \nu\}$ from the received Obs_j to perform the anomaly detection process using first-order joins. If the SN_g is found normal on the basis of received Obs_j, then the sensor reading is forwarded to the aggregation unit. On the other hand, if the SN_g is found anomalous, then the anomaly detection algorithm invokes the agent transmission optimization procedure (Phase 2 of Algorithm 4) that returns the SN_g's behavior as anomalous (Beh_Anm), tolerated category 1 (Beh_Tol_η), tolerated category 2 (Beh_Tol_γ), or tolerated category 3 (Beh_Tol_ζ). For anomalous behavior, the anomaly detection module transmits the anomaly agent to the SN_g to perform the in situ verification. On the other hand, for tolerated categories 1, 2, and 3, the anomaly detection module announces the SN_g as anomalous to the other cluster member nodes and cluster head nodes, minimizes the communication with the SN_g, and generates an alarm to the base station, respectively. The pseudocode for the anomaly detection process is given in Algorithm 2.

Algorithm 2 Anomaly detection on CH_q

CH_q receives Obs_j from SN_g
CU extract $Fet_{set(1)} = \{\lambda, \varphi, \nu\}$ from Obs_j
Compute $Fet_{set(2)}$ = { T, F }
CHK (Anm_{1_ord}) = $\int_{\lambda_i}^{\lambda_f} \int_{T_i}^{T_f} f(\lambda, T)\, dT\, d\lambda$
AND $N(T, \nu) = \int_{T_i}^{T_f} \int_{\nu_i}^{\nu_f} f(T, \nu)\, d\nu\, dT$
AND $N(\varphi, \nu)$ = $\sum_{\varphi_i}^{\varphi_f} \int_{\nu_i}^{\nu_f} f(\varphi, \nu)\, d\nu$
AND $N(\varphi, T) = \sum_{\varphi_i}^{\varphi_f} \int_{T_i}^{T_f} f(\varphi, T)\, dT$
AND $N(F, T)$ = $\sum_{F_i}^{F_f} \int_{T_i}^{T_f} f(F, T)\, dT$
if CHK (Anm_{1_ord}) == $TRUE$ **then**
  Fwd (Agg) // sensor reading is forwarded to the aggregation unit
else
  CALL $Beh = Agnt\_Opt(Fet_{set})$ // invoke Algorithm 4 Phase 2
  if CHK ($Beh = Beh\_Anm$) == $TRUE$ **then**
    TRNSMT Anm_Agnt to SN_g
  else if CHK ($Beh = Beh\_Tol_\eta$) == $TRUE$ **then**
    $Aggr\_Unt$ store SR AND CU announce the SN_g as anomalous to the cluster member nodes and other CHs
  else if CHK (Beh = Beh_Tol_γ) == $TRUE$ **then**
    $Aggr\_Unt$ store SR AND CU minimizes the communication with the SN_g
  else if CHK ($Beh = Beh\_Tol_\zeta$) == $TRUE$ **then**
    $Aggr\_Unt$ store SR AND CU generates an alarm to the BS
  end if
end if

C. Suspicious Node Verification

The sensor node, SN_g, receives the anomaly agent and stores it in its memory portion which is specified for the anomaly agent. The memory portion has a dedicated stack memory segment that is used to store the data which is brought by the anomaly agent for the in situ verification process. The length of the stack memory portion is customizable. The low memory sensor nodes may store the values of only few observations as compared to the rich memory nodes. However, the minimum size of the stack memory should be large enough to accommodate the anomaly agent arrival and comparison of values for the in situ verification process. The arrival of the anomaly agent is dependent on two factors: time taken by the cluster head for the anomaly detection and the anomaly agent trip time from the cluster head to the SN_g. The anomaly agent brings values of three features (i.e., sensor reading, resource status, and actions performed) for the in situ verification of the SN_g. After the arrival of the anomaly agent, the comparison between the values of the SN_g stack and anomaly agent data is performed. If all values are matched, then the sensor node is considered as normal and result "0" is transmitted to the cluster head. Otherwise, in the case of anomaly, result "1" is sent to the corresponding cluster head. Algorithm 3 describes the pseudocode for the in situ verification process.

Algorithm 3 In situ Verification

1: SN_g receive Anm_Agnt from CH_q
2: $PUSH\ Anm\_Agnt$ in $Agnt\_stck$
3: **while** $Stck\_SN_g\ != \varepsilon$ **do**
4: $CMP(Stck\_SN_g[i], Agnt\_stck[k])$
5: **if** CMP is $TRUE$ **then**
6: COUNT $Stck\_SN_g[i] by 1$
7: **else**
8: $Vrf\_rs\_SN_g \leftarrow 1$
9: Break
10: **end if**
11: $Vrf\_rs\_SN_g \leftarrow 0$
12: **end while**
13: $TRNSMT\ Vrf\_rs\_SN_g$

D. Anomaly Agent Transmission Optimization

The anomaly detection module may tolerate the anomalous behavior of the sensor node, SN_g, to some extent to optimize anomaly agent transmission for the in situ verification process. A relatively naive approach for agent transmission optimization can be to perform the examination of each feature, f_i, for its presence in the normal (i.e., $-1\sigma \leq f_i \leq 1\sigma$), tolerated (i.e., $1\sigma < f_i \leq 2\sigma\ OR\ -1\sigma > f_i \geq -2\sigma$), or anomalous (i.e., $f_i > 2\sigma\ OR\ f_i < -2\sigma$) zones. Then, the anomaly agent transmission can be curtailed for the tolerance zone and triggered only for the anomalous zone [26], [27]. However, this approach does not consider the past behavior of the sensor node and transmitting the anomaly agent merely based on the presence of the current anomalous observation, may cause excessive transmission of the anomaly agent. Therefore, we optimize the anomaly agent transmission by taking into account the weighted sum of the instances of the historical and current observations.

We define the SN_g's historical observations score, S_{SN_g}, as stated below.

$$S_{SN_g} = \alpha_1(\frac{\Omega_{i1}}{h}) + \alpha_2(\frac{\Omega_{i2}}{h}) \tag{10}$$

In the above equation, α_1 and α_2 are the weighting factors for the tolerated and anomalous instances of f_i, respectively. The weighting factors $\alpha_1+\alpha_2 = 1$ and $\alpha_2 > \alpha_1$. The weighting factor α_2 is assigned a higher value due to the fact that it is associated with anomalous instances of the f_i.

In the equation (10), the S_{SN_g} has value in the unit interval $[0, 1]$ and is evaluated as a function of the two main parameters:

- Ω_{i1}: The number of f_i instances from h number of historical observations which satisfy the inequality condition $1\sigma < f_i \leq 2\sigma\ OR - 1\ \sigma > f_i \geq -2\sigma$.
- Ω_{i2}: The number of f_i instances from h number of historical observations which satisfy the inequality condition $f_i > 2\sigma\ OR\ f_i < -2\sigma$.

By the above definitions, it is clear that the parameters $\Omega_{i1} + \Omega_{i2} = h$. In order to optimize the values of the weighting factors parameters α_1 and α_2, the equality $\alpha_1+\alpha_2 = 1$ may be rearranged as $\alpha_2 = 1-\alpha_1$, h may be fixed as constant c, and $\Omega_{i1} + \Omega_{i2} = h$ may be rearranged as $\Omega_{i2} = c - \Omega_{i1}$. As a consequence, the equation 10 can be rewritten as given below.

$$S_{SN_g} = \alpha_1(\frac{\Omega_{i1}}{c}) + \alpha_2(\frac{c - \Omega_{i1}}{c}) \tag{11}$$

Since $\alpha_1 + \alpha_2 = 1$ and $\alpha_2 > \alpha_1$, thus $\alpha_1 \in [0, 0.5)$. In the following discussion, to simplify the procedure we fix the window size of the historical observations, i.e., h as c, where $c = 10$, but the procedure is straightforward to generalize. This implies $\Omega_{i1} \in [1, 10]$, where $\Omega_{i1} = 1$ means there exists only a single observation in h that lies in the tolerance zone. On the other hand, $\Omega_{i1} = 10$ shows that there exists all historical observations in the tolerance zone and no observation in the anomalous zone.

For optimization of the weighting parameters, we choose the $mean$ values of the objective functions and identify the corresponding mean value of the first parameters: α_1 and β_1, which are associated with the tolerated instances of f_i. The maximum value of the first parameters are not chosen due to the fact that the second parameters: α_2 and β_2 have high priority due to their association with the anomalous instances of f_i.

To optimize the parameters α_1 and α_2 such that the S_{SN_g} achieves the mean value, we define the following objective function, which is derived from the equation (11), where w and x represents α_1 and Ω_{i1}, respectively.

$$f(w, x) = (1 - w) + (2w - 1)\frac{x}{10} \tag{12}$$

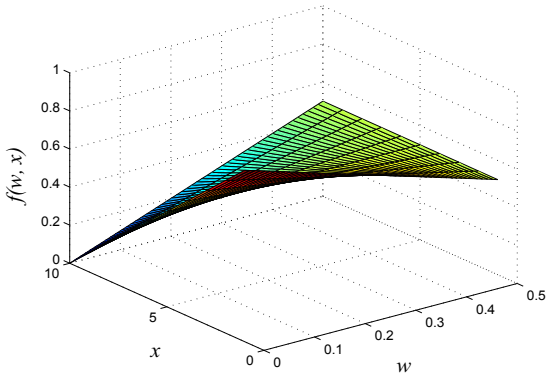


Figure 6. Visualization of the objective function $f(w, x)$

Let $w \in [0, 0.5)$ and $x \in [1, 10]$ based on the facts that $\alpha_1 \in [0, 0.5)$ and $\Omega_{i1} \in [1, 10]$ correspondingly. This gives the mean value of the objective function $f(w, x) = 0.47$. The corresponding values of w that yields the mean value of the objective function $f(w, x)$ lies in the interval $[0.35, 0.47]$ with 0.005 deviation on the both sides of the mean value. The mean of the interval yields $0.415 \approx 0.42$, which we take as the optimum value for w for the above stated scenario. Figure 6 depicts the three-dimensional view of the objective function $f(w, x)$.

From the above mathematical procedure, we obtained the optimized value of $\alpha_1 = 0.42$. By the implication of the relation $\alpha_2 = 1 - \alpha_1$, the value for the parameter α_2 can be deduced as 0.58.

The final score for the anomaly agent transmission can be derived from the following equation.

$$S_{MA_{trn}} = \frac{S_{SN_g}}{2} + \beta_1 u + \beta_2 v \tag{13}$$

In the above equation, the parameters β_1 and β_2 are the weighting factors for the current observation which lies in $1\sigma < f_i \leq 2\sigma \ OR \ -1\sigma > f_i \geq -2\sigma$, and $f_i > 2\sigma \ OR \ f_i < -2\sigma$ zones, respectively. Note that the weighting factors sets $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ are independent of each other. The weighting factors $\beta_1 + \beta_2 = 1$ and $\beta_2 > \beta_1$. The weighting factor β_2 holds the higher value because it is associated with the current anomalous instance of the f_i.

In the equation (13), the $S_{MA_{trn}}$ has value in the unit interval $[0, 1]$ and is estimated as a function of three parameters, namely, S_{SN_g}, u, and v. The S_{SN_g} is obtained from the equation 10, whereas u and v are defined below.

- $u = 1$, if and only if current f_i's instance satisfy the inequality condition $1\sigma < f_i \leq 2\sigma \ OR \ -1\sigma > f_i \geq -2 \ \sigma$, otherwise $u = 0$.
- $v = 1$, if and only if current f_i's instance satisfy the inequality condition $f_i > 2\sigma \ OR \ f_i < -2\sigma$, otherwise $v = 0$.

The relation between parameters u and v is defined as $v = 1 - u$. The weighting factors equality $\beta_1 + \beta_2 = 1$ may be rearranged as $\beta_2 = 1 - \beta_1$. As a consequence, the equation 13 can be rewritten as shown below.

$$S_{MA_{trn}} = \frac{S_{SN_g}}{2} + 1 + 2\beta_1 u - \beta_1 - u \tag{14}$$

Since $\beta_1 + \beta_2 = 1$ and $\beta_2 > \beta_1$, thus $\beta_1 \in [0, 0.5)$ and $S_{SN_g} \in [0, 1]$.

In order to optimize the parameters β_1 and β_2 such that $S_{MA_{trn}}$ achieves the mean value, we define the following objective function, which is obtained from the equation (14), where y and z represent β_1 and $S_{MA_{trn}}$, respectively.

$$f(y, z) = \begin{cases} \frac{z}{2} + 1 - y, & u = 0, \\ \frac{z}{2} + y, & u = 1. \end{cases} \tag{15}$$

To compute the mean value of the objective function $f(y, z)$, let $y \in [0, 0.5)$ and $z \in [0, 1)$ analogous to $\beta_1 \in [0, 0.5)$ and $S_{SN_g} \in [0, 1]$, respectively. The objective function $f(y, z)$ has two cases, viz., case 1: $u = 0$ and case 2: $u = 1$. In case 1, the min, max, and mean values are 1, 1.01, and 1.0049, respectively. On the other hand, in case 2, the min, max and mean values are 0, 0.99, and 0.5048, respectively. The corresponding value for the parameter y for both cases lies in the interval $[0.2401, 0.2499]$. The mean of the interval yields $0.245 \approx 0.25$, which we consider as an optimum value for the parameter y.

Based on the computation on the objective function $f(y, z)$, we estimated the optimized value of parameter $\beta_1 = 0.25$. Again by the implication of the relation $\beta_2 = 1 - \beta_1$, the value for the parameter β_2 is obtained as 0.75.

The derived anomaly agent transmission score should be greater than a pre-defined threshold ψ to transmit an anomaly agent and $\psi \in (0, 1)$. Note that we set the upper bound clipping level of the overall anomaly agent transmission score, i.e., $S_{MA_{trn}}$, as 1. This will, however, not affect the anomaly agent transmission decision, since any value above ψ is deemed as suitable for anomaly agent transmission. Furthermore, if the anomaly agent transmission score is lower than ψ, then the anomaly detection module will take other routine actions such as making an announcement of SN_g as anomalous to the cluster member nodes and other cluster head nodes, minimizing communication with the SN_g, and generating an alarm to the base station for tolerated categories 1, 2, and 3, respectively (as described in Section IV-B). This approach causes less frequent transmissions of the anomaly agents which reduces energy consumption and increases overall network lifetime. The pseudocode for the anomaly agent transmission optimization method is illustrated in Algorithm 4. Note that Phase 1 in Algorithm 4 is computed only at the time of the system deployment and whenever tuning action τ is performed by the system administrator, whereas Phase 2 is executed by the anomaly detection module for each received anomalous observation.

Algorithm 4 Zone Computation and Anomaly Agent Transmission Optimization

Phase 1: Compute zones (Fet_{set})
1: At t_k time
2: **for** each f_i from Fet_{set} **do**
3: Compute $-1\sigma, 1\sigma, -2\sigma, 2\sigma$ // threshold values
4: Update $(Nor_{zone}) = -1\sigma \leq f_i \leq 1\sigma$
5: Update $(Tol_{zone}) = 1\sigma < f_i \leq 2\sigma AND - 1\sigma > f_i \geq -2\sigma$
6: Update $(Anm_{zone}) = f_i > 2\sigma AND f_i < -2\sigma$
7: **end for**

Phase 2: Transmission optimization ($Beh = Agnt\_Opt(Fet_{set})$)
1: **for** each f_i from Fet_{set} **do**
2: Compute $S_{SN_g} = \alpha_1(\frac{\Omega_{i1}}{w}) + \alpha_2(\frac{\Omega_{i2}}{w})$
3: Compute $S_{MA_{trn}} = \frac{S_{SN_g}}{2} + \beta_1 y + \beta_2 z$
4: **if** $S_{MA_{trn}} \geq \psi$ **then**
5: $Beh \leftarrow Beh\_Anm$
6: break
7: **else if** $S_{MA_{trn}} < \psi AND \geq \zeta$ **then**
8: $Beh \leftarrow Beh\_Tol_{\zeta}$
9: break
10: **else if** $S_{MA_{trn}} < \zeta \ AND \geq \gamma$ **then**
11: $Beh \leftarrow Beh\_Tol_{\gamma}$
12: break
13: **else if** $S_{MA_{trn}} < \gamma AND \geq \eta$ **then**
14: $Beh \leftarrow Beh\_Tol_{\eta}$
15: break
16: **else if** $S_{MA_{trn}} < \eta$ **then**
17: $Beh \leftarrow Beh_{Nrm}$
18: **else**
19: f_i++
20: **end if**
21: **end for**
22: return Beh to

E. Space and time complexities

Theorem 1: (a) The space complexity for the features collection process on SN_g is bounded from above by $l[m]$, (b) for anomaly detection process on CH_q it is $C_n + l[n]$, (c) for in situ verification process of SN_g, space complexity is $l[y]$, and (d) for agent optimization process on CH_q, space complexity is constant C_v.

Proof: (a). Let $Fet_{set(1)} = \{\lambda, \varphi, \upsilon\}$ denote the values of the features of interest which are computed on the SN_g and later on used by the Anm_Agnt for the in situ verification process. Let $l[m]$ denote the length of the stack memory to store the values of m number of features and $SN_g[x]$ represent the total stack memory of the node, where $l[m] < SN_g[x]$. Considering m as the number of maximum features values that are accumulated by the SN_g, the space complexity of the features collection process is bounded from above by $l[m]$.

(b). Let $Fet_{set(2)} = \{T, F\}$ be the values that are computed on the CH_q after receiving observation Obs_j, where Obs_j has values of $Fet_{set(1)}$. Thus, $Fet_{set} = Fet_{set(1)} \cup Fet_{set(2)} = \{\lambda, \varphi, \upsilon, T, F\}$. The $Fet_{set(2)}$ takes $l[j]$ space in the memory. Therefore, the total memory space taken by the n number of features of Fet_{set} becomes $l[n] = l[m] \cup l[j]$, where $l[m] > l[j]$. The CH_q takes constant memory spaces C_1, C_2, and C_3 to store threshold values for the first-order joins, aggregated value, and result of agent optimization process, respectively. The anomaly agent consumes C_4 and C_5 memory spaces to store the code and data of the anomaly agent, respectively. Thus, the total memory space taken by the anomaly detection process is $\cup_{n=1}^{5} C_n + l[n]$.

(c). Let $SN_g[y]$ be the length of the stack memory of the SN_g to accommodate the in situ verification process. The $SN_g[y]$ should satisfy the two conditions: (i) $l[n] < SN_g[y]$ and (ii) $C_6 < SN_g[y]$, where $C_6 = C_4 \cup C_5$. This means that the total memory of the SN_g should accommodate the collected values of the $Fet_{set(1)}$ and the code and data of the anomaly agent for the in situ verification process. Considering l[y] as the upper bound for the collective memory of $Fet_{set(1)}$ for both $l[n]$ and C_6, the space complexity for the in situ verification of the suspicious SN_g is $l[y]$.

(d). The CH_q takes constant memory spaces C_7, C_8, C_9, and C_{10} to store the values of the weighting factors α_1, α_2, β_1, and β_2, respectively. The memory spaces C_{11} and C_{12} are used by the CH_q to store the values of the instances of f_i from w number of historical tolerated and anomalous observations. Similarly, the CH_q takes C_{13} space in the memory to store the value of the tolerated or anomalous instance of the current received observation. The memory spaces C_{14}, C_{15}, C_{16}, and C_{17} are taken by the CH_q to store the historical observations score of the SN_g, the agent transmission score, the agent transmission threshold value, and the behavior status of the SN_g, respectively. Considering $C_v = \cup_{v=7}^{17} C_v$, the space complexity of the agent transmission process is constant C_v. ■

Theorem 2: (a) The time complexity for the features collection process on the SN_g is $O(m)$, (b) the anomaly detection process on the CH_q runs in a constant time D for normal observations and has time complexity of $O(n)$ for anomalous observations, (c) the time complexity for the in situ verification process of the SN_g is $O(x)$, and (d) for the anomaly agent transmission optimization process on the CH_q is $O(y)$.

Proof: (a) The time complexity for the features collection process is mainly based on three features of the $Fet_{set(1)} = \{\lambda, \varphi, \upsilon\}$, whereas the $Fet_{set(2)} = \{T, F\}$ is computed on the CH_q after receiving values of $Fet_{set(1)}$ from the SN_g. Let us assume that the SN_g consumes m time to collect $Fet_{set(1)}$ from its ambient environment and to store in its memory. The SN_g takes constant time D_1 to transmit the m number of features to the CH_q. Considering the upper bound case, the complexity of the features collection process is $O(m)$.

(b). The CH_q consumes constant time D_2 to receive the observation from the SN_g, D_3 time to retrieve $Fet_{set(1)}$ values, and D_4 time to compute the $Fet_{set(2)}$ values. To

aggregate the sensor reading, the SN_g consumes D_5 time to transmit the result to the BS for analysis. The CH_q takes D_6 time to perform the anomaly detection process using first-order joins and assigning relevant behavior to the SN_g, which is retrieved after the computation performed by the agent transmission optimization process, where $D_6 > D_5$. The CH_q takes D_7 time for the anomaly agent transmission to the SN_g, where the SN_g is anomalous in this case. Thus, considering $D = \sum_{i=2}^{7} D_i$, the algorithm for the anomaly detection process runs in a constant time D. Moreover, Algorithm 2 calls agent transmission optimization phase for anomalous observations which has $O(n)$ time complexity (as shown in the proof of Theorem 2(d)).

(c). The SN_g receives the anomaly agent and returns the in situ verification result to the CH_q in D_8 and D_9 times, respectively. The SN_g consumes the x time to perform comparison operation between the values of $Agnt\_stck$ and SN_g_Stck. Therefore, by considering the upper bound on the time taken by the comparison process, the time complexity for the in situ verification algorithm is $O(x)$.

(d). The CH_q takes y time for the examination of different zones for the values of n number of features to classify them as normal, tolerated, or anomalous to perform the agent transmission optimization process. By considering the upper bound case, the running time for the agent transmission optimization process becomes $O(y)$. ■

Note that the above proofs should satisfy the relation $O(y) < O(m) < O(x) < O(n)$ due to the fact that Algorithms 2 and 3 involve the transmission, receiving, and processing of anomaly agent, whereas Algorithms 1 and 4 merely include processing on the Fet_{set}.

V. Performance Evaluation

The performance of the proposed system is examined through simulation study, implementation of the proposed algorithms on MICAz mote, and comparison with the competing schemes.

A. Simulation Study

In order to evaluate the performance of the proposed system, we developed simulation scenarios in the object-oriented and discrete event environment, which simulates events in the chronological order [24]. The simulation environment is based on the following models and procedures.

- *Network model:* The simulation plane is based on the $Wd \times Lg$ square meter area. The k number of nodes are randomly deployed in the different simulation scenarios. The base station is placed at (a, b) position in the simulation field.
- *Node model:* The resource capability of the MICAz mote is used as a node model [18]. The program, the SRAM, and the flash data logger memories of the sensor nodes are set as M_P, M_{SRAM}, M_{FLASH}, respectively. At the time of deployment, the total energy of the node is considered as N_E. The energy consumed by the sensor node during sleep mode is assumed as N_{Eslp}.
- *Node Categorization:* In order to investigate the energy consumption, we considered the wireless smart home sensor network scenario. We categorized the sensor nodes as security and non-security devices. The security related sensors may include motion detector, door sensor, and light detector. On the other hand, humidity, temperature, and pressure detectors are a few examples of the non-security sensors. On the basis of this classification, we set a tight bound, σ, for the security nodes. On the other hand, we set a relatively loose bound on the non-security devices, which is 2σ [25].
- *Communication energy dissipation model:* We used a well-known model for the radio hardware energy consumption [19]. The reason for using simplified model is highly stochastic nature of radio wave propagation, which makes it hard to model. The following formulas are used to estimate the energy dissipation by the radio hardware to transmit l-bits over the distance d.

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) \quad (16)$$

$$P_U(u) = \begin{cases} lE_{elec} + l\epsilon_{fs}d^2 & d < d_0, \\ lE_{elec} + l\epsilon_{mp}d^4 & d \geq d_0. \end{cases} \quad (17)$$

Similarly, to receive l-bits, the energy dissipation is estimated from the following equation.

$$E_{Rx}(l) = E_{Rx-elec}(l) + lE_{elec} \quad (18)$$

In the above equations, the E_{elec} illustrates the electronic energy dissipation based on multiple factors such as filtering, modulation, digital coding, and signal spreading. Similarly, $\epsilon_{fs}d^2$ and $\epsilon_{mp}d^4$ are the amplifier energies, which are based on several factors such as acceptable bit-error rate and distance between sender and receiver. Note that the E_{elec} is equivalent to ($E_{Tx} + E_{DA}$) for cluster heads and E_{Tx} for other nodes for transmission, where E_{Tx} denotes the transmission energy and E_{DA} represents the data aggregation energy. On the other hand, the value of the E_{elec} is equivalent to E_{Rx} for cluster heads and other nodes while receiving data packets.
- *Network lifetime:* We employed the "first node die" approach for our experiments [22].
- *Propagation model:* The free space (d^2 power loss) and multipath fading (d^4 power loss) channel models are used for the propagation [20]. These models are based on the distance between the sender and the receiver. If the distance between the sender and the receiver is less than that of the threshold, d_0, then the free space, f_s, otherwise the multipath, mp, channel model is used.

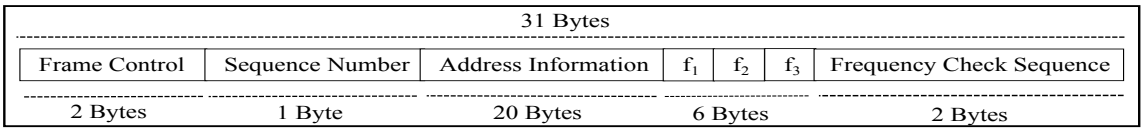


Figure 7. Normal data packet

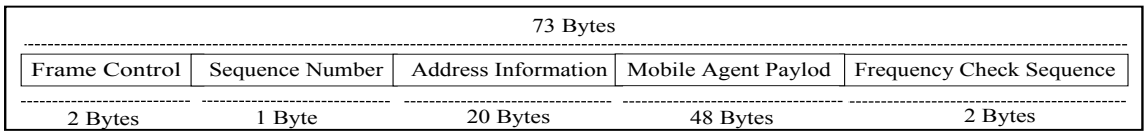


Figure 8. Anomaly agent data packets (except last packet)

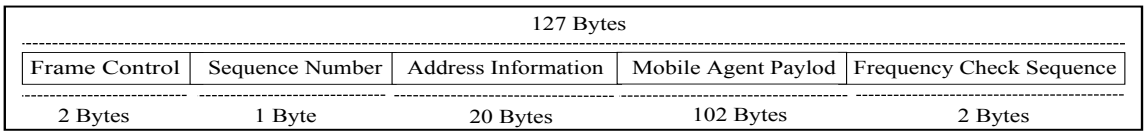


Figure 9. Anomaly agent last data packet

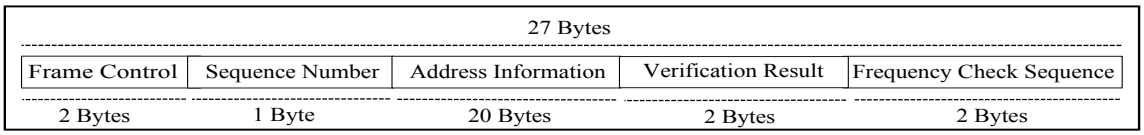


Figure 10. In situ verification result data packet

- *Traffic model:* The nodes are characterized to transmit the periodic data packets. The sensor nodes transmits the data packets after every t seconds on average. Each transmitted data packet has Pkt size including header and payload. The payload of the normal data packet, as depicted in Figure 7, is based on the values of $Fet_{set(1)}$, which are transmitted by the cluster member nodes. In our experiments, we consider features λ, υ, and T as continuous, whereas φ and F as discrete random variables.
- *Cluster formation:* The clusters are formed through the Low-Energy Adaptive Clustering Hierarchy (LEACH) algorithm [19]. LEACH is one of the most commonly used cluster formation algorithms for WSNs. Our scenarios are based on heterogeneous nodes and LEACH supports such nodes to form the cluster-based network topology.
- *Anomaly Agent:* The size of the developed anomaly agent is 762 bytes (including identity, itinerary, code, and data). The anomaly agent cannot travel in one message due to its large size. Therefore, we segment the anomaly agent into multiple frames as per 802.15.4 specifications [21]. According to the 802.15.4 specifications, the maximum permitted frame size is 127 bytes (i.e., payload = 102 bytes and header = 25 bytes). Therefore, we segment the anomaly agent into 8 packets. The header size is 8 $\times$ 25 = 200 bytes. The payload size for the first 7 packets is 7 $\times$ 102 = 714 bytes and for the last packet 1 $\times$ 48 = 48 bytes. The total size of the first 7 packets, on the basis of the formula ((*number of packets* $\times$ *payload size*) + (*number of packet* $\times$ *header size*)), is (7 $\times$ 102) + (7 $\times$ 25) = 714 + 175 = 889 bytes. Similarly, the size of the last packet is (1 $\times$ 48) + (1 $\times$ 25) = 48 + 25 = 73 bytes. Thus, the total anomaly agent size after segmentation is 962 bytes. The size of the packet which carries the result of the in situ verification process is 27 bytes (i.e., 25 bytes header and 2 bytes payload), because this message just sends the result of the verification process in the form of either "1" or "0" representing "anomalous" or "normal" status, respectively. The data packet structure of the anomaly agent and the verification process is illustrated in Figure 8 to Figure 10.
- *Anomalous traffic:* We randomly generated 25% anomalous traffic by anomalous sensor nodes in the simulation plane. The normal and the anomalous data traffics are collected and subsequently used for building the anomaly detection rules.
- *Agent optimization thresholds:* The threshold values for -2σ, -1σ, 1σ, and 2σ are based on six sigma rule to optimize anomaly agent transmission [25]. The values for the weighting factors are set as α_1, α_2, β_1, and β_2. The threshold for the anomaly agent transmission is fixed as ψ, whereas the tolerance zones are defined as Tol_η, Tol_γ and Tol_ζ.
- Number of iterations: The results given in the next subsection are average of the 30 simulated experiments.

Following seeds are used to build the simulation scenarios: Wd = 100, Lg = 100, k = 30 − 150, a = 50, b = 50, E_{Tx} = 50 × 10^{-9} Joules, E_{RX} = 50 × 10^{-9} Joules, ϵ_{fs} = 10 × 10^{-12} $Joules/bit/m^2$, ϵ_{mp} = 1.3 × 10^{-3} × $10^{-12} Joules/bit/m^4$, E_{DA} = 5 × $10^{-9} Joules/bit/signal$, M_p = 128 kb, M_{SRAM} = 4 kb, M_{flash} = 512 kb, N_E = $1e^4$ nJ, t = 0.1, Pkt = 31 bytes, N_{Eslp} = 1 nJ/t, -1σ to 1σ = 0.68, -2σ to 2σ = 0.95, λ = 12 °C to 38 °C, T = 0-1, 2-3, 4-5 seconds, , φ = 1 for entitled action performed and 0 for non-entitled action performed, υ = 100% (full battery) → 0% (empty battery), F = 1 for each timely received and 0 for every delayed received packet, h = 10, α_1 = 0.42, α_2 = 0.58, β_1 = 0.25, β_2 = 0.75, ψ = 0.55, η = 0.50, γ = 0.45, and ζ = 0.40.

1) Results and Analysis: We measured the comprehensive performance of the proposed anomaly detection and verification system in terms of following performance statistics:

- *Anomaly detection rate*: This statistic gives the percentage of the anomalies detected from the total number of anomalies.
- *Energy dissipation estimation*: The energy dissipation is estimated for the network traffic which is comprises of both anomalous and normal data packets (observations). This allows to estimate the impact of using mobile agents for in situ verification on the energy budget of resource constrained WSN.
- *Number of anomaly agents transmitted*: This statistic facilitates measuring the numbers of anomaly agents transmitted with and without employing anomaly agent transmission optimization algorithm.

We performed the first set of experiments to estimate the detection rate of the first-order anomalies which are caused by the in situ faults (refer to the first first-order join $N(\lambda, T)$, as discussed in Section IV-B). In this set of experiments, cluster member nodes continuously transmitted sensed $Fet_{set(1)}$ values instead of periodic transmissions to the respective cluster heads. We generated network traffic based on 5000 data packets, which were transmitted by 30 cluster member nodes to the corresponding cluster heads. In this case, the anomaly detection module detected 99% of the anomalies. For the network traffic comprised of 7000, 9000, 11000, and 13000 observations transmitted by 60, 90, 120, and 150 cluster member nodes, the anomaly detection rates were 98.80%, 98.40%, 98.20%, and 98%, respectively. The experiments results show that the detection rate of the first-order anomalies caused by the in situ faults was in the range of 98% to 99%.

The second and third first-order anomalies are related to the resource consumption by the cluster member nodes. We enforced a resource exhaustion attack, in which cluster member nodes transmitted low battery status instead of expected values of the residual battery status (refer to the second first-order join $N(T, \upsilon)$, as discussed in Section IV-B). The overall detection rate of the anomalies caused by the resource exhaustion attack varied between

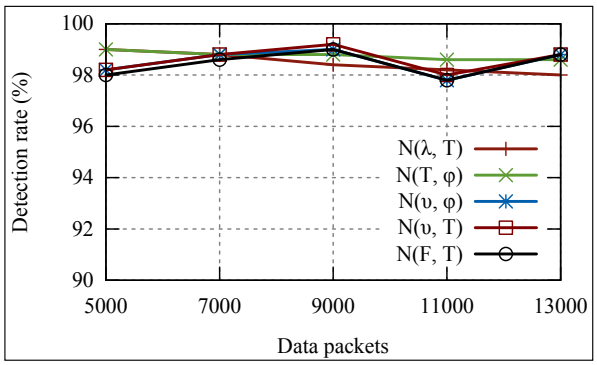


Figure 11. Detection rate for first-order joins

98.60% and 99%. The detection rates for 5000, 7000, 9000, 11000, and 13000 observations were 99%, 98.80%, 98.80%, 98.60%, and 98.60%, respectively. Next, the anomaly detection modules on the cluster heads were enabled to detect the anomalies caused by the faulty nodes (refer to the third first-order join $N(\varphi, \upsilon)$, as discussed in Section IV-B). In these experiments, the energy budget of the faulty cluster member nodes dissipated quickly due to the unauthorized actions performed by them. As a consequence, the nodes transmitted low battery status instead of expected values to the corresponding cluster heads. In these experiments, the detection rates were 98.2%, 98.80%, 99%, 97.80%, and 98.80% for 5000, 7000, 9000, 11000, and 13000 observations, respectively.

Next, we experimented with the scenario of the faulty nodes (refer to the fourth first-order join $N(\varphi, T)$, as discussed in Section IV-B), in which faulty cluster member nodes transmitted anomalous values of the entitled actions with respect to the duration of time. In these cases, the anomaly detection modules, installed on each cluster head, detected 98.2%, 98.80%, 99.2%, 98%, and 98.80% of first-order anomalies for 5000, 7000, 9000, 11000, and 13000 numbers of observations, respectively. Finally, we induced the denial of sleep attack scenarios (refer to the fifth first-order join $N(F, T)$, as discussed in Section IV-B). In these scenarios, cluster member nodes continuously transmitted the sensed observations instead of periodic transmissions. In this set of experiments, the detection rates for 5000, 7000, 9000, 11000, and 13000 observations were 98%, 98.60%, 99%, 97.80%, and 98.80%, respectively. In all of the above cases, anomaly agents were capable of identifying the source of anomalies that have occurred in situ or in transit. The graph shown in Figure 11 summarizes the anomaly detection results. It can be observed that the overall detection accuracy is high for all first-order joins as it varies between 97.80% to 99.20%.

We now analyze the energy dissipation cost of both situations, when normal and anomalous data packets are transmitted in varying node density scenarios. The normal data traffic comprises of data packets that are transmitted from cluster member sensor nodes to their corresponding cluster heads. On the other hand, the anomalous data

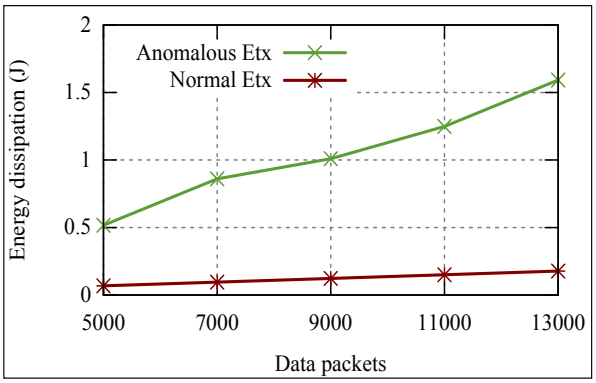


Figure 12. Packet transmission energy dissipation

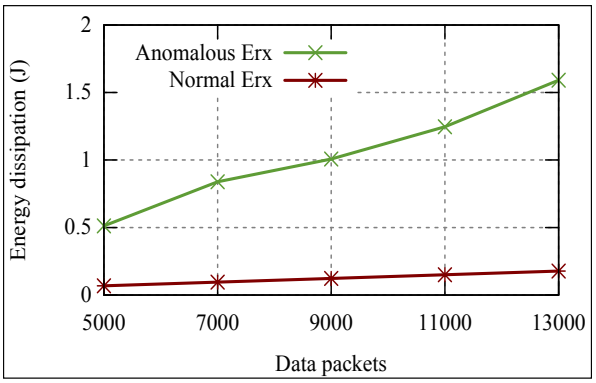


Figure 13. Packet receiving energy dissipation

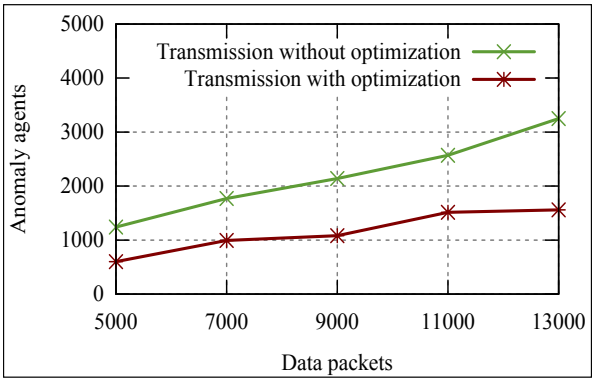


Figure 14. Anomaly agent transmission optimization

traffic includes data packets of the anomaly agents that are transmitted from the cluster heads to the suspicious member nodes for in situ verification and results of in situ verification process that are transmitted back to the cluster heads. It is evident from Figure 12 that the line which denotes the energy dissipation by transmission of 5000, 7000, 9000, 11000, and 13000, normal data packets that are transmitted by 30, 60, 90, 120, and 150 cluster member nodes to their respective cluster heads has a steady growth in the positive direction along the x-axis. This shows the gradual increase in the energy dissipation as numbers of packets increase in the network traffic. On the contrary, the energy dissipation by the anomalous network traffic that is based on the anomaly agents and in situ verification data packets tend to variate and has a relatively non-steady growth. This is due to the variations in the detection accuracy of the corresponding cluster heads and also randomness involved in the generation of underlying anomalous traffic.

Next, we analyze the packet reception cost in terms of energy dissipation. Figure 13 depicts the energy dissipation results for the reception of both normal and anomalous data packets. The energy dissipation caused by receiving data packets follows the same trend as shown by data packets transmission with a slightly lower cost. The data traffic based on 5000 to 7000 data packets caused the dissipation of 0.0686 to 0.177 J energy for transmission and 0.0682 to 0.176 J energy for receiving normal traffic. Similarly, for transmitting and receiving anomalous traffic, the network dissipated 0.517 to 1.592 J energy and 0.51215 to 1.591 J energy, respectively. The relatively low energy dissipation while receiving data traffic is due to the fact that the transmission operation also involves the distance factor in addition to the fixed amount of energy consumed by the transceiver circuitry for data communication. Another key fact which is evident from Figure 12 and 13 is the difference in the magnitude of the energy dissipation by normal data traffic with that of anomalous data traffic. This difference of energy dissipation magnitude is because of the extra traffic transmitted over the network in the form of anomaly agents and in situ verification result data packets for the case of anomalous traffic. The resource rich cluster heads can easily mange this overhead. However, resource low cluster member nodes can quickly drain out their energy, which advocates the use of our proposed anomaly agent transmission optimization method to save the energy budget of the low resource cluster member nodes.

The anomaly detection modules installed on the cluster heads transmitted 1240, 1770, 2140, 2570, and 3249 anomaly agents after detection of similar numbers of anomalies without employing anomaly agent transmission optimization method in the above scenarios. As discussed above, this quickly dissipated the energy budget of the low resource cluster member nodes. Therefore, we employed our proposed anomaly agent transmission optimization method (i.e., Algorithm 4) and as a consequence the numbers of anomaly agent transmissions were reduced to 600, 993, 1080, 1513, and 1560 in data traffic comprised of 5000, 7000, 9000, 11000, and 13000 data packets, respectively, as shown in Figure 14. This reduced the energy dissipation by both transmission and reception of anomalous data traffic over the network down to 42%-52%, as shown in Figure 15 and 16, respectively.

The simulation results and analysis show that the proposed anomaly detection and verification system is not only capable of detecting a range of first-order anomalies at high detection rate, but also capable of successfully performing in situ verification of suspicious nodes. Furthermore, the anomaly agent transmission optimization method, which considers both the current and historical

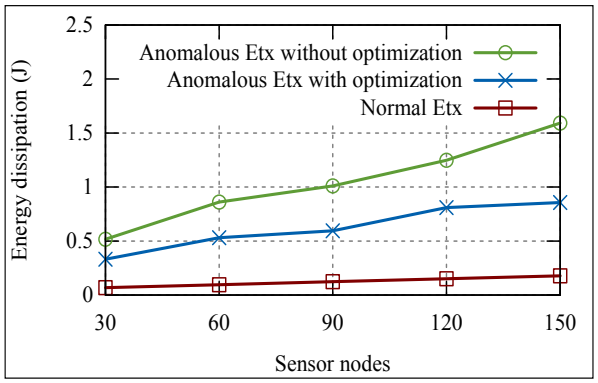


Figure 15. Anomaly agent transmission energy dissipation

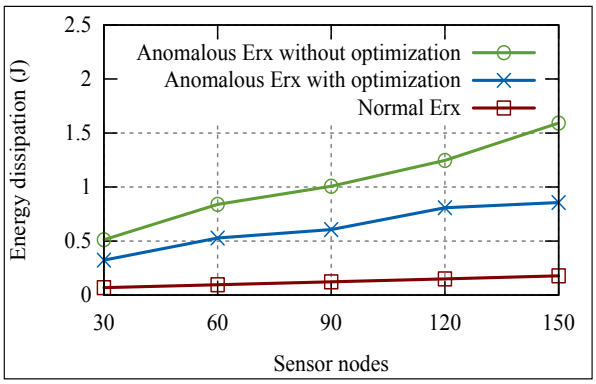


Figure 16. Anomaly agent receiving energy dissipation

observations to optimize the agent transmission, can prolong the network life time by as much as around 50%.

B. Implementation

In order to measure the impact of the proposed scheme on the low resource real sensor nodes, we implemented algorithms on the MICAz mote, running TinyOS 2.1.1 [8]. The MICAz mote consists of a microprocessor (ATmega128L) [18]. The program flash memory, the configuration EEPROM, and the flash data logger memories of MICAz sensor nodes have 128, 4, and 512 kb storage spaces, respectively. The proposed algorithms are programmed using network embedded systems C (nesC) [23], a component-based event-driven programming language, used for building applications in the TinyOS. The objective of the implementation is an estimation of memory and energy dissipation along with processing time taken by the proposed algorithms. Note that we executed the worst case scenarios (i.e., all conditions were executed) to estimate the impact of the proposed algorithms on the resources of MICAz mote.

1) Memory consumption: The programming language nesC generates a memory consumption report of programs during their compilation stage. This report indicates the status of ROM, RAM, .data, .bss, and .text segments of the MICAz mote's memory in terms of bytes. The total memory consumption (i.e., RAM and ROM together) by the proposed Algorithms 1, 2, 3, and 4 are 1567, 2559, 3130, and 1206 bytes, respectively. This result indicates that the memory consumption of Algorithms 2, and 3, is higher than that of the Algorithms 1 and 4 due to the fact that these Algorithms involve processing and transmission of an anomaly agent. The proposed Algorithms 2 and 4 are executed on resource rich cluster head nodes. Therefore, high memory consumption can easily be managed by these nodes. The executions of Algorithms 1 and 3 on the non-cluster head sensor nodes consume 1567 and 3130 bytes of memory, respectively, which can be easily managed by the memory subsystem of the MICAz sensor node family. Furthermore, the execution of Algorithm 3 is not very frequent. It executes only when a suspicious sensor node is found in a cluster and the cluster head triggers the anomaly agent for the in situ verification of the suspicious sensor node after due consideration of the agent transmission optimization method. It should be noted that the anomaly agent occupies the memory space only for a short period of time. As such, the anomaly agent is killed and clears the occupied memory space as soon as it transmits the in situ verification result to the cluster head. Therefore, the impact of the anomaly agent on the cluster member node's memory is rather short term.

2) Processing time: We now examine the processing time taken by the proposed algorithms, as this is an important performance metric for the anomaly detection application. The processing times for the Algorithms 1, 2, 3, and 4 are 6.93, 37.28, 7.65, and 4.13 ms, respectively. Algorithms 2 and 3 perform the jobs of the anomaly detection and in situ verification processes and their combined elapsed time is 44.93 ms. Algorithms 2 and 3 consume high processing time as compared to Algorithms 1 and 4 due to the involvement of the processing of an anomaly agent. This outcome of the processing time is consistent with the theoretical results reported in Section IV-D. Furthermore, if the cluster head also executes the agent transmission optimization process, then the whole procedure takes 49.06 ms time, which is quite efficient.

3) Energy consumption: The process of features collection by the sensor node consumes 55.60 J of energy in each epoch. Algorithms 2 and 4 consume 4039.91 J and 40.02 J of energy, respectively. These algorithms are executed on the resource rich cluster head nodes which can easily manage this amount of energy consumption. The energy consumption by Algorithm 3 is 1570.96 J. However, this energy is only consumed by the suspicious cluster member node for the in situ verification process. The summary of processing time, memory, and energy consumption by the proposed algorithms is given in Table V.

C. Comparative study and discussion

The proposed scheme is compared with three recent related schemes proposed by Ketel [4], Eludiora et al. [6], and Khanum et al. [7]. The comparison is based on the following five aspects: (a) role of mobile agent, (b) nature

TABLE V.
IMPLEMENTATION RESULTS

Algorithm	RAM (bytes)	Rom (bytes)	$\cdot data$ (bytes)	$\cdot bss$ (bytes)	$\cdot text$ (bytes)	Processing Time (ms)	Energy Consumption (μJ)
1	29	1538	9	1932	27	6.93	55.60
2	50	2509	15	2993	31	37.25	4039.91
3	59	3071	23	3048	36	7.65	1570.96
4	24	1182	5	1672	25	4.13	40.02

TABLE VI.
COMPARISON SUMMARY

Scheme	Role of Mobile Agent	Anomalies	Number of agents per node	Detection complexity	Agent transmission optimization
Ketel [4]	Anomaly information collection	Node anomalies through neighbor monitoring	3	Not applicable	No
Eludiora et al. [6]	Inter-BS control communication	Anomalies caused by DoS attack	1	$O(n^2)$	No
Khanum et al. [7]	local anomaly	Sensor reading anomalies	3	$O(n)$	No
Proposed Scheme	In situ node verification	Denial of sleep attack, resource exhaustion attack, and node faults	1	$O(n)$	Yes

of anomalies, (c) number of agents per node, (d) detection time complexity, and (e) agent transmission optimization. In the proposed scheme, the nature of the agent is mobile and only one agent per node is triggered for the in situ verification of the suspicious behavior of the sensor node, using its resources. On the other hand, Ketel's scheme employs three agents for the process of the anomaly detection, namely, static, mobile, and nodal agents [4]. Furthermore, the scheme presented by Eludiora et al. uses a mobile agent for the inter-base station control communication [6]. Also, the proposal by Khanum et al. uses two static agents: coordination and management, and a mobile agent to carry out the anomaly detection process [7]. Both Ketel and Khanum et al. employed three agents for the process of anomaly detection [4], [7]. The use of several agents not only increases the computational cost, it also requires additional computation for inter-mobile agent communication. The use of the multiple agents also increases the communication and processing load of the network.

Another important difference between the proposed and other related schemes is the transmission of the mobile agent by the particular type of the node. In our proposed scheme, the mobile agent is only triggered by the resource rich nodes (i.e., by the cluster heads) and received by the cluster member nodes as compared to other schemes, in which agents are transmitted by all sensor nodes. This approach of existing schemes can quickly dissipate the energy resources of the cluster member nodes. On the other hand, in the proposed scheme, the cluster member nodes receive the mobile agent only for the in situ verification process (i.e., not very often). This approach puts the least burden on the resource limited nodes. Furthermore, our scheme does not support the inter-cluster member nodes mobile agent movement (i.e., between non-cluster head nodes within or outside the cluster). This strategy effectively uses overall WSN resources without negating the role of the mobile agent in the proposed anomaly detection system.

The nature of the anomalies detected in the work presented by Ketel and Eludiora et al. are node and DoS attack based anomalies, respectively [4], [6]. The scheme presented by Khanum et al. only detects sensor reading anomalies [7]. On the other hand, our proposed scheme has the ability to detect several types of first-order anomalies which are caused by attacks such as denial of sleep attack, battery exhaustion attack, and so forth. The detection complexity of the scheme presented by Ketel cannot be estimated, as it is an architectural level scheme and no actual details of the anomaly detection process are provided [4]. The anomaly detection complexity of Eludiora's et al. scheme is $O(n^2)$ [6]. Both, Khanum et al. [7] and the proposed scheme detects anomalies in $O(n)$ time.

Furthermore, none of the existing schemes has considered the optimization of mobile agent transmission [4], [6]-[7]. The proposed scheme optimizes mobile agent transmission by considering historical and current instances of the anomalous observations. This comparative study shows that the proposed scheme is efficient and effective in various aspects as compared to the several existing schemes. A summary of the comparative study is stated in Table VI.

VI. CONCLUSIONS

This study has proposed a mobile agent-based anomaly detection and in situ verification system for cluster-based WSNs. In the proposed system, the mobile agent uses the resources of the victim node to verify if the node is compromised. This approach offers an additional service to the network administrator to confirm the source of the anomaly, before initiating appropriate action against the anomalous node. The proposed system is designed in a way that the majority of the processing is performed by the resource rich cluster head nodes. Furthermore, the itinerary of the mobile agent has only a single node, that

is, from cluster head to cluster member nodes. This design consideration saves the resources of the cluster member nodes, which are consumed in the case of multi-node itinerary. This study has also successfully employed the CRM mechanism to detect different types of first-order anomalies caused by in situ faults, denial of sleep attacks, and resource exhaustion attacks. Further, we have proposed a mobile agent transmission optimization method which prolongs the network lifetime. The results obtained through the detailed performance evaluation advocate the efficiency and effectiveness of the proposed system for resource constrained wireless sensor networks.

In future work, we intend to extend our investigation to examine the effectiveness of the proposed system in large-scale multi-hop sensor networks against complex nature of anomalies.

ACKNOWLEDGMENT

The authors are thankful to the anonymous reviewers for their constructive feedback and suggestions to improve the presentation of this paper.

REFERENCES

[1] L. Atzoria, A. Ierab, and G. Morabitoc, "The internet of things: a survey," *Computer Networks*," vol. 54, no. 15, pp. 2787-2805, 2010.

[2] E. I. Gaura, J. Brusey, R. Wilins, and J. Barnham, "Wireless sensing for the built environment: enabling innovation towards greener, healthier homes," *in proceedings of the Clean Technology,* United Kingdom, pp. 6, 2011.

[3] C. Krugel and T. Toth, "Applying Mobile Agent Technology to Intrusion Detection," *in Proceedings of the ICSE Workshop on Software Engineering and Mobility,* Ontario, Canada, pp. 5, 2001.

[4] M. Ketel, "Applying the mobile agent paradigm to distributed intrusion detection in wireless sensor networks," *in Proceedings of the 40th IEEE Southeastern Symposium on System Theory,* New Orleans, USA, pp. 74-78, 2008.

[5] M. Pugliese, A. Giani, and F. Santucci, "Weak process models for attack detection in a clustered sensor network using mobile agents," *Sensor Systems and Software, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,* vol. 24, no. 1, pp. 33-50, 2010.

[6] S. I. Eludiora, O. O. Abiona, A. O. Oluwatope, S. A. Bello, M. L. Sanni, D. O. Ayanda, C. E. Onime, E. R. Adagunodo, and L. O. Kehinde, "A distributed intrusion detection scheme for wireless sensor networks," *in Proceedings of the IEEE International Conference on Electro/Information Technology,* USA, pp. 1-5, 2011.

[7] S. Khanum, M. Usman, and A. Alwabel, "Mobile agent based hierarchical intrusion detection system in wireless sensor networks," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 1, pp. 101-108, 2012.

[8] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, "TinyOS: An Operating System for Sensor Networks," *in Ambient Intelligence,* Springer-Verlag, USA, 2004.

[9] J. Waterman, G. W. Challen, and M. Welsh, "Peloton: Coordinated resource management for sensor networks," *in proceedings of the 12th Workshop on Hot Topics in Operating Systems,* Switzerland, pp. 5, 2009.

[10] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE communications Surveys,* vol. 8, no. 2, pp. 2-23, 2006.

[11] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on software engineering,* Vol. SE-13, no. 2, pp. 222-232, 1987.

[12] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: A survey," *Journal of Network and Computer Applications,* vol. 34, no. 4, pp. 1302-1325, 2011.

[13] W. Wu, X. Cheng, M. Ding, K. Xing, F. Liu, and P. Deng, "Localized outlying and boundary data Detection in sensor networks," *IEEE Transaction on Knowledge Data Engineering,* vol. 19, no. 8, pp. 1145-1157, 2007.

[14] E. Karapistoli and A. A. Economides, "ADLU: A novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks," *Journal on Information Security,* vol. 2014, no.3, 1-12, 2014.

[15] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. Bezdek, "Quarter sphere-based distributed anomaly detection in wireless sensor networks," *in Proceedings of IEEE International Conference on Communication (ICC)*, Glasgow, United Kingdom, pp. 3864-3869, 2007.

[16] Y. Y. Zhang, W. C. Yang, K. B. Kim, and M. S. Park, "Inside attacker detection in hierarchical wireless sensor network," *in Proceedings of IEEE International Conference on Innovative Computing information and control,* China, pp. 594, 2008.

[17] O. Esparza, J. L. Munoz, J. Tomas-Builart, and M. Soriano, "An infrastructure for detecting and punishing malicious hosts using mobile agent watermarking," *Wireless Communications and Mobile Computing,* vol. 11, no. 11, pp. 1446-1462, 2011.

[18] Crossbow, http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf, as of June 2014.

[19] W. B. Hinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications,* vol. 1, no. 4, pp. 660-670, 2002.

[20] T. Rappaport, "Wireless Communications: Principles & Practice," *Englewood Cliffs, NJ, Prentice-Hall,* 1996.

[21] Part 15.4: Wireless Medium Access (MAC) and Physical Layer (PHY) specifications for low-rate wireless Personal Area Network (LR-WPANs), IEEE Std. 802.15.4, 2006.

[22] J. C. Dagher, M. W. Marcellin, and M. A. Neifeld, "A theory for maximizing the lifetime of sensor networks," *IEEE Transactions on Communications,* vol. 55, no. 2, pp. 323-332, 2007.

[23] D. Gay, P. Levis, R. V. Behren, M. Welsh, E. Brewer, and D. Culler, "The nesC Language: A holistic approach to networked embedded systems," *in Proceedings of the Programming Language Design and Implementation (PLDI),* USA, pp. 1-11, 2003.

[24] A. Varga, "The Omnet++ Discrete Event Simulation System," *in Proceedings of the European Simulation Multiconference,* Czech Republic, pp. 7, 2001.

[25] D. H. Stamatis, "Six Sigma and Beyond: Statistics and Probability," *Taylor & Francis Ltd, Vol. III,* 2002.

[26] M. Usman, Vallipuram Muthukkumarasamy, Xin-Wen Wu, and S. Khanum, "Wireless Smart Home Sensor Networks: Mobile Agent Based Anomaly Detection," *in the proceedings of the 9th IEEE International Conference on Ubiquitous Intelligence and Computing, and 9th International Conference on Autonomic and Trusted Computing,* Fukuoka, Japan, pp. 322-329, September 2012.

[27] M. Usman, "Agent-enabled Anomaly Detection in Resource Constrained Wireless Sensor Networks," *in Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, (PhD Forum WoWMoM 2014),* Sydney, Australia, pp. 1-2, June 2014.

Muhammad Usman received the M. Science (M. Phil) in Computer Science from the PMAS-AAUR Pakistan. He is currently associated with the School of Information and Communication Technology, Griffith University, Gold Coast, Australia, where he is working towards his PhD degree. Prior to joining the Griffith University, he served as a Lecturer at the King Khalid University, Saudi Arabia, and a Project Manager and Lecturer at the University of Central Punjab, Pakistan. He also worked as a System Administrator and Lecturer at the Pakistan Air Force Fazaia College, Pakistan. His current research interests include investigation of research issues in mobile agent-enabled distributed systems, formal modeling and verification of communication protocols, anomaly detection, and design and analysis of cross layer protocols.

Vallipuram Muthukkumarasamy obtained the BScEng with 1st Class Hons from the University of Peradeniya, Sri Lanka and obtained the PhD from the Cambridge University, England. He is currently attached to the School of Information and Communications Technology, Griffith University, Australia as a Senior Lecturer. His current research areas include investigation of security issues in wireless networks, sensor networks, trust management in MANETs, key establishment protocols and medical sensor networks. He is currently leading the Network Security research Group at the Institute for Integrated and Intelligent Systems at the Griffith University. He has also received a number of best teacher awards.

Xin-Wen Wu received the Ph.D. degree from the Chinese Academy of Sciences. He was with the Chinese Academy of Sciences, the University of California, San Diego (as a postdoctoral researcher), and the University of Melbourne (as a research fellow). He was affiliated with the School of Information Technology and Mathematical Science, University of Ballarat, Australia. In April 2010, he joined the Griffith University, Australia, as a faculty member of the School of Information and Communication Technology; and he is currently a Senior Lecturer. His research interests include cyber and data security, coding techniques, and information theory and its applications.

Simulation and Performance Analysis of the IEEE1588 PTP with Kalman Filtering in Multi-hop Wireless Sensor Networks

Baoqiang Lv [1], Yiwen Huang [1], Taihua Li [1*], Xuewu Dai[1], Muxi He[1], Wuxiong Zhang [2], and Yang Yang [2]
1. School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China
2. Shanghai Research Center for Wireless Communications, ShanghaiTech University, Shanghai, 201210, China
*Corresponding author, Email: {jietelv8, piaoyao, catalyst, daixuewu, hemuxi}@swu.edu.cn, {wuxiong.zhang, yang.yang}@wico.sh

***Abstract*—As the wireless sensor networks (WSNs) find wider and wider applications, time synchronization has emerged as a key technology to improve network performance and enable WSNs in time-sensitive applications. The recently proposed IEEE 1588 Precision Time Synchronization Protocol (PTP) has shown its capability for the wired Ethernet, but its performance in multi-hop WSNs is still an open question. This is because of the non-negligible asymmetric delays caused by the wireless media access control protocol, low-cost crystal oscillators and time-stamping uncertainties due to limited resources in WSNs nodes. This paper studies the performance of the IEEE 1588 in a multi-hop WSNs by state-space modeling and realistic simulation. Furthermore, the Kalman filter is introduced to improve the offset and skew estimation. The realistic simulator was developed on the OMNeT++ discrete event simulation platform and the simulation results show that the proposed Kalman filtering improves the performance of time synchronization in multi-hop WSNs in terms of offset and skew estimation.**

***Index Terms*—Time Synchronization; IEEE 1588 PTP; WSNs; Kalman Filter; OMNeT++**

I. INTRODUCTION

Many applications of Wireless Sensor Networks (WSNs) need to maintain time synchronization, such as, event detection, localization, data fusion, Time Division Multiple Access (TDMA) scheduling, remote health monitoring. Generally, the node clocks of WSNs are implemented through crystal oscillator and interrupt mechanism. Furthermore, the precision of the WSN's clock is greatly affected by manufacturing imperfections, temperature variation and the interrupt latency [1]; Moreover, the wireless sensors whose resources are limited is cheap, and are significantly constrained in computing resources, and computational capacity [2]. Therefore, one of the main challenges in WSNs time synchronization is how to achieve high-precision time synchronization while requiring less overhead and consuming less communication bandwidth and CPU sources.

Time synchronization has emerged as a hot research field in distributed systems. The Network Time Protocol (NTP) [3] has been widely used in the Internet; however, in the ideal condition, the accuracy of NTP is within few milliseconds in WSNs, which is not enough for the application requires high time accuracy, such as TDMA scheduling and some industrial wireless networks. In recent years, more and more researchers pay attention to time synchronization protocols and lots of time synchronization protocols have been proposed, such as Flooding Time Synchronization Protocol (FTSP) [4], Timing-sync protocol for sensor networks (TPSN) [5], Reference Broadcast Synchronization (RBS) [6], Delay Measurement Time Synchronization (DMTS) [7], however, these protocols are used in wireless networks with nearly zero propagation delay between nodes, and failed to achieve optimization on energy efficiency and accuracy[8]. Therefore, the new design of time synchronization protocol in WSNs is needed. As a recently proposed time synchronization standard for Ethernet in industrial data acquisition and control applications, the IEEE 1588 Precision Time Synchronization Protocol (PTP) has shown it capability to achieve high synchronization accuracy. The PTP standard and associated techniques are thoroughly examined by J. C. Eidson [9]. The PTP Time synchronization indeed is a process that estimates the local drifting clock's offset and skews by exchanging timing information so that the local clock tracks the reference time as accurately as possible. The PTP time synchronization accuracy is claimed to be in microsecond range, which is much better than the time synchronization accuracy of NTP and FTSP, etc. However, although the PTP has shown it capability for wired Ethernet, its performance in multi-hop WSNs is still an open question due to the non-negligible asymmetric delays and time-stamping uncertainties caused by the wireless media access control protocol and limited resources in WSNs nodes. This motivates us study the IEEE 1588's performance in multi-hop WSNs.

However, in real networks, in order to save the energy on radio transmission, multi-hop communications are widely used in wireless sensor networks. In multi-hop WSNs, a node may work as combination of both sensor node and relay node. Furthermore, large populations of

doi:10.4304/jnw.9.12.3445-3453

sensor nodes will collaborate in order to complete the measuring data at the same time, data gathering, data fusion and localization. In the wireless sensor network with large scale of energy limited nodes, multi hop time synchronization is necessarily applied. Therefore, more and more researchers pay attention to time synchronization in multi-hop WSNs and lots of multi-hop time synchronization algorithms have been proposed over the years. K. Y. Cheng et al proposed Pairwise Broadcast Synchronization (PBS) in multi-hop WSNs [10]. V. Kaseva et al proposed a delay-based time synchronization protocol that is based on calculating delays as packets traverse from node to node for application packets in multi-hop WSNs [11]. A multi-hop time synchronization scheme is proposed for underwater acoustic networks [12]. Haitao Xiao et al proposed a multi-hop low cost time synchronization algorithm for wireless sensor network in bridge health diagnosis system with the purpose of reducing energy consumption and lengthening whole WSN' life [13]. Zhehan Ding et al proposed an improvement of energy efficient multi-hop time synchronization algorithm in wireless sensor network, which consumes less energy than RBS and can decrease overhead [14]. Compare to most existing time synchronization protocols, one of promising features of the PTP is its less demanding on communication bandwidth and computation costs, while keeping the similar level of time accuracy [15]. With small communication bandwidth, the PTP occupies relatively fewer network resources. The PTP has simple operation, small computational and memory requirement, lower hardware requirements, and is easy to maintain. As a result, a well optimization on energy efficiency and accuracy can be achieved by using the PTP in multi-hop WSNs.

In this paper, the IEEE 1588 PTP is adopted in multi-hop WSNs, and the state-space modeling is used to describe the process of time synchronization. The clock offset between master clock and slave clock is estimated and adjusted by IEEE 1588 PTP, but the accuracy of estimated value for skew and offset is not high enough. So an open source simulator for IEEE1588 time synchronization over 802.11 networks has been proposed to evaluate PTP's performance by realistic simulation [16]. Ling Ye et al proposed the Kalman filter for precision time synchronization in wireless sensor networks to improve PTP's performance [17]. Moon et al proposed a linear programming-based algorithm to estimate the clock skew [18]. Xu Bao proposed time synchronization algorithm for WSNs based on cluster [19]. Since the Kalman filter can effectively eliminate noise to avoid influence of the measurement values, it has been intensively studied in time synchronization [20]. In this paper, we study the application of Kalman filter to the PTP's offset and skew estimation in multi-hop WSNs.

A simulator has been developed to evaluate the performance of the proposed IEEE 1588 PTP with Kalman filter for multi-hop WSNs. Due to its capability of simulating the real wireless channel, the OMNeT++ discrete event simulator (DES) is selected as the simulation platform. The OMNeT++ is an open source object-oriented modular discrete event network simulator. Its model consists of hierarchically nested modules; modules communicate with each other by exchanging timing messages, which can contain arbitrarily complex data structures. Our simulator is a further development of x-simulator [21] and new relay nodes are developed, which combine both the IEEE 1588 PTP master node and slave node into one relay node.

The rest of this paper is organized as follows: the clock model is described in section II. The PTP model is presented in Section III. Section IV describes the simulator development for multi-hop time synchronization. We introduced noises in IEEE 1588 offset calculation in section V. Kalman filtering for multi-hop time synchronization is proposed by section VI and section VII presents the performance evaluation.

II. CLOCK MODEL

In practical applications, it is impossible to obtain the crystal oscillator with exactly the same properties of clocks, which were generated by the different rate of counter. In order to understand the clock bias caused by instantaneous phase variations and frequency deviation of the crystal oscillator from its normal value, clock needs to be modeled.

A. Master Node's Ideal Clock

Let t and $M(t)$ represent the *reference time* (or termed as *global time*) and the clock of the master node at time t, respectively, it is common to assume the clock of the master node is accurate. That is:

$$M(t) = t \tag{1}$$

Therefore, synchronizing the slave clock to the master clock is equal to synchronizing to the *reference time t.*

B. Slave Node's Drifting Clock

Let $\theta(t)$ represent the slave node's offset at reference time t, the offset $\theta(t)$ is defined as the time difference between the master clock t and the slave clock $C(t)$.

$$\theta(t) = C(t) - t \tag{2}$$

Skew, represented by $\gamma(t)$, is the deviation of the local clock frequency from the reference clock frequency and can be expressed as:

$$\gamma(t) = \frac{dC(t)}{dt} - 1 \tag{3}$$

Skew is always expressed by the dimensionless unit of *Parts Per Million* (PPM), and $dC(t)/dt$ is the clock's change rate used to describe the local clock frequency. In our simulator, the slave clock is modeled by a "*simple skew model*" (SKM) as shown in reference [22]. In this model, the variations of both the offset and skew are regarded as random processes, and the dynamics of both offset and skew can be written as follows.

$$\theta(k+1) = \theta(k) + \gamma(k)\tau + \omega(k) \tag{4}$$

$$\gamma(k+1) = \gamma(k) + \omega_{\gamma}(k) \quad (5)$$

where k represents the *k-th* physical clock update, τ is a small time interval (referred to as clock update interval) determining how frequently the clock model is updated. $\omega_{\theta}(k)$ *and* $\omega_{\gamma}(k)$ are two independent random processes representing the phase noise (referred to as offset noise) and frequency drifting (referred to as skew noise), respectively. Similar to the treatment in [23], $\omega_{\theta}(k)$ *and* $\omega_{\gamma}(k)$ are considered as two uncorrelated white Gaussian random processes with variances δ_{θ}^2 and δ_{γ}^2 respectively.

III. MATHEMATICAL MODE OF PTP

In this section, the PTP is described as a state-space modeling though two measurement equations so that Kalman filtering is used to improve the performance of PTP time synchronization between the master node and slave node.

A. Clock Offset Estimation by PTP

A typical process of the PTP time synchronization between the master node and its slave nodes is based on a delay request-response mechanism, as demonstrated in Fig. 1. Four types of time-stamped packets are defined in the IEEE 1588 standards [15], They are *Sync* packet, *Follow_Up* packet, *Delay_Req* packet and *Delay_Resp* packet. The *Follow_UP* packet is used to transport the timestamp of the preceding *Sync* packet if there are uncertainties on the master clock. In our simulator, we assume the master node has enough resources and is able to process the time-stamped packet quickly and there is no need to use the *Follow_Up* packet.

The time synchronization is carried out in a series of packet exchange procedures which is repeated periodically and each procedure of packet exchange involves a sequence of packet transmission. Let n denote the *n-th* procedure of packet exchange, at the beginning of the *n-th* time synchronization procedure, a *Sync* packet is sent from the master node to the slave node at time t_1. When the *Sync* packet is received by the slave, the receiving time t_2 provided by the slave's drifting clock is recorded. Let *dms* denote the propagation delay of a *Sync* packet traveling from the master node to the slave node, and let θ denote the clock offset between the master node and the slave node at the *n-th* synchronization procedure. The following relationship holds:

$$t_1(n) + \theta(n) + d_{ms}(n) = t_2(n) \quad (6)$$

Since equation (6) has two unknown variables, offset and master-slave propagation delay, one more equation is needed to measure the propagation delay so that the offset can be solved. Propagation delay measurement is initiated by the slave clock. Firstly, a *Delay_Req* packet from the slave node is sent to the master node at time t_3, and the master node receives the packet and records its receiving time t_4. A *Delay_Resp* packet embedding time t_4 from master node is then sent to the slave node as soon as possible. Let *dsm* denote propagation delay of packet traveling from the slave node and master node. The following relationship holds:

$$t_3(n) + \theta(n) + d_{ms}(n) = t_4(n) \quad (7)$$

The clock offset θ between the master node and slave node can be regarded as an unknown quantity. Consequently, the offset can be calculated by equations (6) and (7):

$$\theta(n) = \frac{(t_2(n) - t_1(n)) - (t_4(n) - t_3(n))}{2} + \frac{d_{sm}(n) - d_{ms}(n)}{2} \quad (8)$$

where equation (8) is called clock offset measurement equation, which describes the relationship among the clock offset and the time stamps during the process of IEEE 1588 packet exchange. Under the condition of propagation delay symmetry, i.e, $d_{sm}=d_{ms}$, the offset can be calculated as:

$$\theta(n) = \frac{(t_2(n) - t_1(n)) - (t_4(n) - t_3(n))}{2} \quad (9)$$

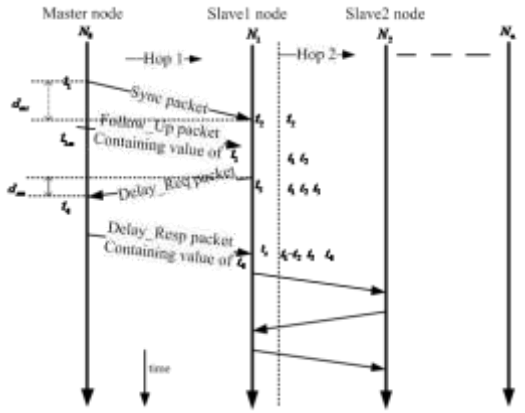


Figure 1. The PTP time-stamping packet exchange

For example, if the *Master* node starts a round of time synchronization by sending the *Sync* packet at t_1=0.1 second (measured at master accurate clock) and the *Sync* packet arrives at *Slave1* at t_2= 0.100015 second (measured at *Slave1*'s drifting clock). *Slave1* node sends back a *Delay_Req* at t_3= 0.100019 second (measured at *Slave1*'s drifting clock) and the *Master* node receives *Delay_Req* at t_4= 0.100029 second (measured at *Master*'s accurate clock). Once the *Delay_Resp* arrives at *Slave1*, the offset between *Slave1*'s clock and *Master*'s clock can be calculated by equation (9). Once the first hop *Master-Slave1* synchronization is done, *Slave1* will work as a master in the second hop (*Slave1-Slave2*). A similar process is carried out between *Slave1* and *Slave2*.

B. Clock Skew Estimation by PTP

Although the IEEE 1588 standard does not define the skew estimation, for a better synchronization between the slave clock and the master clock, it is good to estimate both the clock offset and skew. The measured value of clock offset is acquired by equation (8). Then, the value of the clock skew $\gamma(n)$ can be acquired by sending consecutive *Sync* message. In our simulator, the clock offset θ is assumed as constant in the process of PTP synchronization packet exchange. A simple measured

value of the clock skew $\gamma(n)$ can be obtained by the offset measured values:

$$\gamma_M(n) = \frac{\theta(n) - \theta(n-1)}{\Delta T} \quad (10)$$

IV. Simulator Development for Multi-hop Time Synchronization

In order to study the performance of IEEE 1588 PTP time synchronization in multi-hop WSNs, we developed a realistic simulator on the OMNeT++ platform. The proposed simulator is a further development of the x-simulator [21] and it supports three types of nodes, namely *Master*, *S1M2* and *Slave2*. Fig. 2 illustrates a simple two-hop network topology for the purpose of demonstration. It is worth noting that node *S1M2* works as a slave node in its first hop to *Master* on the left and as a master node in its second hop to *Slave2* on the right.

Figure 2. Multi-hop synchronization simulation

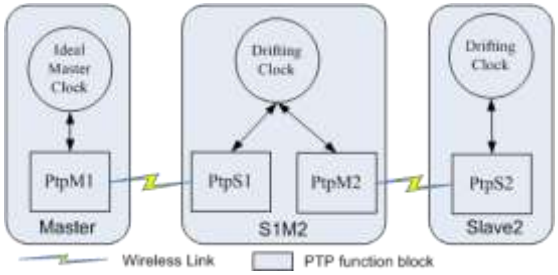


Figure 3. Implementation of each node in Multi-hop WSNs

As shown in Fig. 3, the main blocks of *Master* node are (1) an ideal clock representing the reference time *t* and (2) a *PtpM1* block implementing the functions of PTP master specified by the IEEE 1588 standard. Similarly, the main blocks of *Slave2* node are: (1) a *Drifting Clock* that will be synchronized to the master clock $M(t)=t$; (2) a *PtpS2* block implementing the functions of PTP slave specified by the IEEE 1588 standard. These two types of nodes are the standard master/slave nodes defined by the IEEE 1588 standard. They are implemented in a similar manner as the master/slave node in the x-simulator [21].

The unique feature of the proposed simulator is the *S1M2* node which enables us to simulate multi-hop time synchronization. The *S1M2* node integrates functions of both the PTP master and PTP slave into one node. As shown in Figure 3, the *SIM2* node has three main blocks: (1) a *Drifting Clock*; (2) *PtpS1* block is similar to the *PtpS2* block in *Slave2* node but works as a PTP slave in the first hop to the *Master*'s *PtpM1* block; (3) *PtpM2* block is the additional block working as a PTP master in the second hop to the *Slave2*'s *PtpS2* block.

The process of time-stamped PTP packet exchange among these nodes and the time-stamping procedure within the *S1M2* and *Slave2* nodes are described next. In the following description, unless otherwise specified, packet represents the time-stamped PTP packet between two nodes and message represents the information exchange within a node.

A. PTP Packet Exchange in the First Hop

The process of time-stamped PTP packet exchange among the *Master* node and *S1M2* node in the first hop and the time-stamping procedure within the *S1M2* node are described as follows:

Firstly, the *Master*'s *PtpM1* sends a *Sync* packet periodically at an interval ΔT to the *PtpS1* in the *S1M2* node of the first hop. The *Sync* contains the time t_1, which is the *Sync*'s sending time measured by the master clock.

The *Sync* first arrives at the input gate of the *S1M2*, and then received by the *PtpS1*. The *PtpS1* records t_1, and instantly sends a *Syn_Time_Req* message back to its *Drifting Clock* for the time stamp of t_2. Once receiving the time request message *Syn_Time_Req*, the *Drifting Clock* retrieves the time of drifting clock as t_2 and then sends a *Time-Res* message containing t_2 back to the *PtpS1*. As a result, the *PtpS1* obtains the receiving time stamp t_2 of the PTP packet *Sync*.

Once the *PtpS1* has obtained and recorded the time stamp t_2, it waits for a short period of time delay (to simulate the delays caused by clock interrupt processing and CPU scheduling). Then, *PtpS1* sends a *Dreq Time_Req* message again to the *Drifting Clock* to obtain the time stamp of t_3. Once receiving the *Dreq_Time_Req*, the *Drifting Clock* retrieves its local clock time t_3 and replies with a *Time_Res* message containing t_3.

When *PtpS1* receives the *Time_Res* containing t_3, it records t_3 and immediately sends a *Delay_Req* packet to the *Master*.

When *Master* receives the *Delay_Req* packet it records its arrival time t_4 and encapsulates t_4 into a *Delay_Resp* packet containing t_4. The *Delay_Resp* packet is then sent back to the *S1M2*.

When the *PtpS1* of *S1M2* node receives the *Delay_Resp*, it retrieves the time-stamp t_4.

Once the above packet and message exchange procedures are completed, *PtpS1* of *S1M2* node acquire all the four time stamps (t_1, t_2, t_3, t_4). Then the *PtpS1* is able to calculate the offset between the *Master*'s *Ideal Clock* and the *S1M2*'s *Drifting Clock* by the offset estimation equation (8).

B. PTP Packet Exchange in the Second Hop

The process of time-stamped PTP packet exchange among the *S1M2* node and *Slave2* node in the second hop and the time-stamping procedure within the *Slave2* node are described as follows.

The *PtpM2* sends a *Sync2_time_req* message to the *S1M2*'s *Drifting Clock* periodically at an interval ΔT. The *Drifting Clock* receives the *Sync2_time_req*, and obtains its arrival time t_1, then, sends a *Time_Res* message containing t_1 to the *PtpM2*.

Once receiving the *Time_Res* message from the *S1M2*'s *Drifting Clock*, time t_1 is encapsulated into a *Sync* packet and *PtpM2* sends the *Sync* packet immediately to

the *PtpS2* in the *Slave2* of the second hop. The *Sync* contains the time t_1, which is the *Sync*'s sending time.

When the *Sync* first arrives at the input gate of *Slave2*, it is processed by *Slave2*'s *PtpS2* block. From now on, the reset of PTP packet exchange in the second hop is the same as that in the first hop, as shown in step (2)-(6) in previous subsection. The only difference from the first hop is that the PTP packet exchange in the second hop is between *PtpM2* and *PtpS2*.

Remark: Compared to the time-stamping of *Sync* in *Master* node, the time-stamping of *Sync* in *S1M2* node is provided by the *Drifting Clock*, rather than the reference clock. It worth pointing that, before sending out the *Sync* packet to *Slave2*, *S1M2*'s *PtpM2* first acquires the time of the drifting clock by sending a *Sync2_time_req* message to the *S1M2*'s *Drifting Clock* and then, encapsulate the time-stamping into the *Sync* packet.

V. NOISES IN IEEE 1588 OFFSET CALCULATION

In the IEEE1588 PTP standard, we generally assume that propagation delay is equivalent, namely $d_{sm}=d_{ms}$; however, in the real networks, due to wireless media sharing, conflict avoidance and other factors, the propagation delay is assumed to be asymmetry between the master node and slave node, that is $d_{ms}\neq d_{ms}$. In this paper, the propagation delay asymmetry is described as delay jitter, so the propagation delay d_{sm} and d_{ms} are considered as Gaussian random process $N(d,\delta_d)$ with mean d and variance δ^2_d. Let $\Delta d=(d_{sm}- d_{ms})/2$, equation(8) can be expressed as:

$$\theta_M(n)=\frac{[(t_2(n)-t_1(n))-(t_4(n)-t_3(n))]}{2}+\Delta d \quad (11)$$

where Δd is considered as Gaussian random variable with zero-mean and variance $1/2*\delta_d^2$. In embedded systems, timestamp uncertainty is significantly affected by several different factors such as interrupt latency, timing jitter and scheduling, so the measurement value t_i (i=1, 2, 3, 4) of both the master clock and slave clock have also time stamp uncertainty Δt_i. Both Δt_1 and Δt_2 correspond to the timestamp uncertainty of the master clock, both Δt_3 and Δt_4 correspond to the timestamp uncertainty of the slave clock. Therefore, the measurement equation of clock offset θ_M can be written in the following form:

$$\theta_M(n)=\frac{[(t_2(n)-t_1(n))-(t_4(n)-t_3(n))]}{2}+v_{\theta_M} \quad (12)$$

where corresponds to measurement noise of the clock offset θ_M, which is defined as follows.

$$v_{\theta_M}(n)=\frac{\Delta t_2+\Delta t_3}{2}-\frac{\Delta t_1+\Delta t_4}{2}+\Delta d \quad (13)$$

Measurement noise is sum of timestamp uncertainty Δt_i (i = 1, 2, 3, 4) and propagation delay asymmetry Δd. Assuming that these timestamp uncertainties are independent random variables with zero means, the variance of both Δt_1 and Δt_2 are finite variances δ^2_{MTS} and the variance of both Δt_3 and Δt_4 are finite variances δ^2_{STS}. The variance is the sum of variances of each independent random variables. It is defined as follows.

$$\delta^2_{\theta_M}=\frac{1}{2}(\delta^2_{MTS}+\delta^2_{STS}+\delta^2_d) \quad (14)$$

We assume that timestamp uncertainty for the master node can be disregarded, so δ^2_{MTS} is equal to zero; likewise, δ_d^2 can be initially ignored, unless the uncertainty on propagation delay is specifically assumed to be symmetry in the study. Thus, the skew uncertainty is obtained from

$$\delta^2_{\gamma_M}=2\left(\frac{\delta_{\theta_M}}{\Delta T}\right)^2 \quad (15)$$

It is worth pointing out that the skew $\gamma_M(n)$ is obtained by the measurement value of the offset θ_M, and the measurement noise and are correlated, so their covariance is.

$$Cov(v_{\gamma_M},v_{\theta_M})=Cov(v_{\theta_M},v_{\gamma_M})=\sqrt{2}\frac{\delta^2_{\theta_M}}{\Delta T} \quad (16)$$

VI. KALMAN FILTERING FOR MULTI-HOP TIME SYNCHRONIZATION

In order to adopt the Kalman filter to improve the performance of offset and skew estimation as described by the IEEE 1588 standard, the clock's state equations (4) and (5) have to be written slightly to fit the state space model. Generally, time synchronization occurs periodically at a fixed time synchronization interval ΔT. In addition, considering the facts that the time-stamped PTP packet exchange can be completed in a short time and the variation of a physical clock in such a short period is slow, it is reasonable to assume the clock offset and skew are constant between two time synchronization interval ΔT. As a result, the clock's state equations (4) and (5) are written as:

$$\theta(n+1)=\theta(n)+\gamma(n)\Delta T+\omega_\theta(n) \quad (17)$$

$$\gamma(n+1)=\gamma(n)+\omega_\gamma(n) \quad (18)$$

where n represents the *n-th* time synchronization procedure, the $\theta(n)$ and $\gamma(n)$ represent the offset and the skew between the master node and slave node at the *n-th* time synchronization procedure, respectively. Both the $\omega_\theta(n)$ and $\omega_\gamma(n)$ correspond to the phase noise on $\theta(n)$ and the frequency noise on $\gamma(n)$, respectively.

In order to implement time synchronization between the slave clock and the master clock, the inputs corrections $\mu_\theta(n)$ and $\mu_\gamma(n)$ are calculated at the *n-th* synchronization procedure and applied to adjust the offset and skew, respectively. Therefore, the current value of both offset and skew calculated in equations (17) and (18) at the *n-th* synchronization procedure can be written as recursive relationship:

$$\theta(n+1)=\theta(n)+\mu_\theta(n)+[\gamma(n)-\mu_\gamma(n)]\Delta T+\omega_\theta(n) \quad (19)$$

$$\gamma(n+1) = \gamma(n) - \mu_\gamma(n) + \omega_\gamma(n) \quad (20)$$

where $\theta(n)$ represents the current value of offset at the *n-th* synchronization procedure, $\gamma(n)$ represents the current value of skew at the *n-th* synchronization procedure.

Ideally, if the timestamp information is sufficiently accurate, measurement value of both the clock offset and skew can be directly applied as corrections to the slave clock, that is:

$$\begin{aligned} \mu_\theta(n) &= \theta_M(n) \\ \mu_\gamma(n) &= \gamma_M(n) \end{aligned} \quad (21)$$

In real networks, timestamp information is occasionally inaccurate and it is necessary to be preprocessed by some filters. We can know by analyzing the previous sections, it becomes almost natural to consider Kalman filtering can be used to achieve recursive estimator, consequently the clock state equations (19) and (20) can be expressed as matrix form:

$$\tilde{x}(n) = A\tilde{x}(n) + B\mu(n-1) + \omega(n-1) \quad (22)$$

where $\boldsymbol{\mu}(n)=[\mu_\theta(n),\ \mu_\gamma(n)]^T$ and $\tilde{x}(n)=[\theta(n),\ \gamma(n)]^T$ are input control vector and the state vector at the *n-th* synchronization, respectively. $\boldsymbol{\omega}(n)=[\omega_\theta(n),\omega_\gamma(n)]^T$ is the process noise subjects to Gaussian random process $N(0, \boldsymbol{Q})$, both $\boldsymbol{A}$=[1 ΔT;0 1] and $\boldsymbol{B}$=[-1 -ΔT; 0 -1] represent state transition matrix and input control matrix, respectively.

Likewise, both equations (8) and (10) correspond to the measurement equation of offset $\theta_M(n)$ and skew $\gamma_M(n)$, respectively, can be expressed as the vector matrix measurement equation by defining the clock measurement vector $\boldsymbol{y}(n)=[\theta_M(n),\ \gamma_M(n)]^T$

$$y(n) = H\tilde{x}(n) + v(n) \quad (23)$$

where $\boldsymbol{H}$=[1 0;0 1] is an identity matrix of measurement systems and $\boldsymbol{v}(n)$ represents measurement noise of a Gaussian random process $N(0, \boldsymbol{R})$.

The Kalman filter for recursive equations are written in the following.

$$\tilde{x}(n|n-1) = Ax(n-1) \quad (24)$$

$$P(n|n-1) = AP(n-1)A^T + Q \quad (25)$$

where the matrix $\boldsymbol{Q}$ corresponds to the process noise covariance matrix. Since the random processes $\theta(n)$ and $\gamma(n)$ are independent, $\boldsymbol{Q}$ is a 2×2 diagonal matrix which is reported:

$$Q = \begin{bmatrix} \delta_\theta^2 & 0 \\ 0 & \delta_\gamma^2 \end{bmatrix} \quad (26)$$

If these parameters are known, initialization of the matrix $\boldsymbol{P}(n|n-1)$ is $\boldsymbol{P}(1|0) = \boldsymbol{Q}$.

The general expression for the Kalman gain $\boldsymbol{K}(n)$ is expressed as:

$$K(n) = P(n|n-1)H^T[HP(n|n-1)H^T + R]^{-1} \quad (27)$$

where $\boldsymbol{R}$ corresponds to the measurement noise covariance matrix, which must be set with the measurement uncertainties calculated in equations (14) and (15) .

$$R = \delta_{\theta_M}^2 \begin{bmatrix} 1 & \frac{\sqrt{2}}{\Delta T} \\ \frac{\sqrt{2}}{\Delta T} & \frac{2}{(\Delta T)^2} \end{bmatrix} \quad (28)$$

It worth pointing out that $\boldsymbol{H}$ is an identity, as a consequence, the correction equations is given by the following expression.

$$\tilde{\boldsymbol{x}}(n) = \tilde{\boldsymbol{x}}(n|n-1) + \boldsymbol{K}(n)[\boldsymbol{y}(n) - \tilde{\boldsymbol{x}}(n|n-1)] \quad (29)$$

$$\boldsymbol{P}(n) = [1 - \boldsymbol{K}(n)]\boldsymbol{P}(n|n-1) \quad (30)$$

The state estimate is obtained by equation (29) which is designed to give a better and accurate estimate of the local clock's offset and skew. Once the offset and skew is estimated, a clock correction is carried out to modify the drifting clock's offset and skew accordingly and the time synchronization between the master node and slave node can be achieved.

VII. Performance Evaluation

In this section, we introduce the development of our multi-hop simulator and describe the implementation of PTP packet exchange in multi-hop WSNs. Then, the performance of the proposed Kalman filtering for PTP was analyzed through several simulations. The simulation and performance analysis are done at various scenarios by changing the standard deviation of offset and skew of the slave's local clock.

A. Development of the Multi-Hop Simulator

In order to simulate the clock model based on Kalman filter, a multi-hop network is constructed on OMNeT++ network simulator. In our simulator, three types of PTP time packets are defined according to the PTP standards. Namely, they are *Sync*, *Delay_req* and *Delay_Resp*. The topology of the multi-hop network is shown in Fig.4, where the *Master1* is the master node for the first hop time synchronization and all the slave nodes are to keep their clocks synchronized with *Master1*'s perfect clock. *S1M2* node works as the PTP slave in the first hop and as the master node for the second hop. *Salve2* is a slave node working as the PTP slave in the second hop.

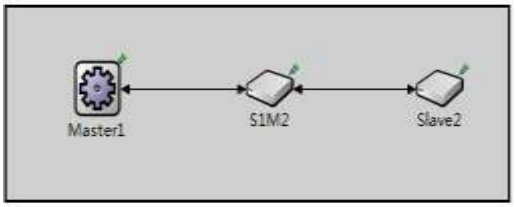


Figure 4. The topology of the two-hop network

The implementation of the *S1M2* node is shown in Fig. 5. It can be seen that the *S1M2* node consists of six

simple module, namely *PtpS1*, *Clock*, *PtpM2*, *Bufferrx*, *Buffertx*, and *Manager*, among which the *PtpS1* is the main module of *S1M2*, and it is employed to achieve the function of the PTP slave node, receives and sends cyclic and acyclic messages; the *PtpM2* is used to achieve the function of the PTP master node specified by the IEEE 1588 standard; the *Bufferrx* and *Buffertx* are realizations of the buffer block, which is used to simulate the behaviour of a first in first-out (FIFO) transmission queue; the *manager* is responsible for generating cyclic or acyclic traffic row. In addition, it worth pointing out that the *Slave2* has a similar structure with the *S1M2*, but the *Slave2* has not the *PtpM2* which is used to implement the functions of the PTP master node.

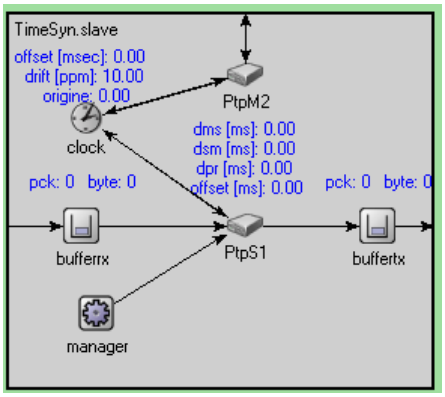


Figure 5. Implementation of the S1M2 node

In our simulator, the time synchronization interval ΔT for the first hop and second hop are the same. When the first hop time synchronization starts, the second hop time synchronization also starts. The implementation of the PTP packets exchange in multi-hop time synchronization is described as follows.

A time synchronization timer in *Master1* is triggered at an interval ΔT. When the timer fires, the first hop time synchronization is initiated and *Master1* sends a *Sync* message to *S1M2*. From now on, the packet exchange in the first hop is the same as the PTP packet exchange in the first hop, as shown in step (1)-(6) in subsection *A* of section IV. Since *Master1* is the master node in the first hop, *S1M2* is to keep time synchronized with *Master1*.

Another time synchronization timer in *PtpM2* is also triggered at a synchronization interval ΔT. When the timer fires, *PtpM2* sends a *Sync2_time_req* message to its *Clock* module to acquire the time value of the drifting local clock. From now on, the packet exchange in the second hop is the same as the PTP packet exchange as shown in step (1)-(3) in subsection *B* of section IV. Please note that *S1M2* is the master node in the second hop time synchronization and *Slave2* is to keep time synchronized with *S1M2*.

B. Simulation Results

In the first simulation experiment, the initial values of the offset and skew of the drifting clocks of S1M2 and Slave2 are 0s and 10ppm, respectively. The update interval of the slave clocks is 0.1ms, which is much smaller than the synchronization interval ΔT (ΔT=0.1s). Please note that ΔT is also the interval of recursive Kalman filtering algorithm. Different levels of time-stamping uncertainties are simulated by using different measurement noises. This is done by setting the standard deviation (δ^2_{STS}) to a value in the range of [10^{-2}~10^{-8}]. A small δ^2_{STS} corresponds to the accurate hardware-assisted time stamping and a larger δ^2_{STS} represents the fluctuating software time stamping.

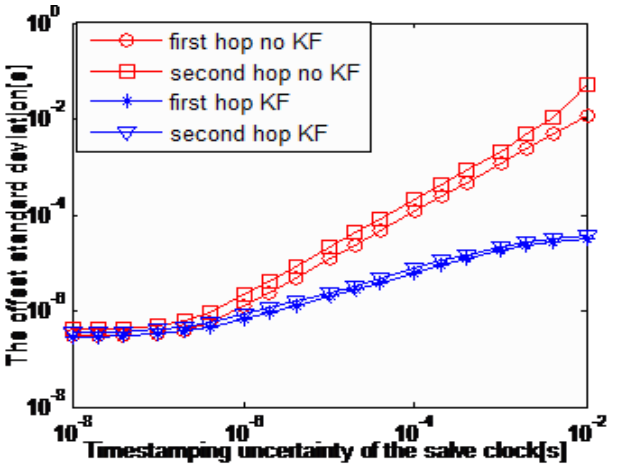


Figure 6. Offset standard deviation against timestamp uncertainty (δ_{STS})

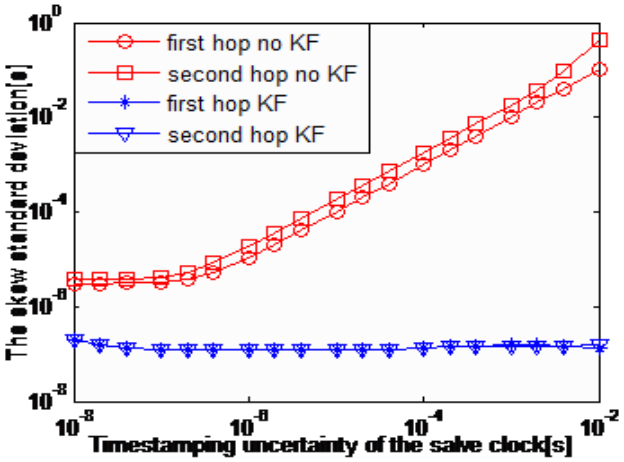


Figure 7. Skew standard deviation against timestamp uncertainty(δ_{STS})

The simulation results are shown in Fig. 6 and 7, where two different time synchronization approaches are compared. One uses the standard IEEE 1588 PTP alone without Kalman filtering and another one is the proposed PTP scheme with Kalman filtering.

Fig. 6 shows that, in both the first and second hop, the standard deviation of clock offset given by the proposed PTP with Kalman filtering are significantly smaller than the case without Kalman filtering. This verifies the performance improvement of the proposed algorithm.

Furthermore, it can be seen that the offset standard deviation of the second hop is larger than the offset standard deviation in the first hop. This applies to both the standard PTP without Kalman filtering and the improved PTP with Kalman filtering. This means that the accumulation of offset and skew errors appears in multi-hop time synchronization network.

Third, it can be seen that, in the standard PTP without Kalman filtering, when $\delta_{STS}>10^{-5}$ with the timestamps uncertainty increasing, the offset standard deviation have a steady increment, This suggests that, the timestamp uncertainty is the main factor which affects the clock stability. Meanwhile, in the standard PTP without Kalman filtering, the offset standard deviation of the second hop is significantly larger than that of the first hop. On the other hand, in the proposed PTP with Kalman filtering, the offset standard deviation of the second hop is almost the same as the value of the first hop and the offset standard deviation has almost no change and is basically stable at a fixed value.

Fig. 7 shows that the skew standard deviation without Kalman filtering increases as the timestamp uncertainty is increasing. In the standard PTP without Kalman filtering, when $\delta_{STS}>10^{-5}$, with the timestamps uncertainty increasing, the offset standard deviation will have a gradual increment. However, in the proposed PTP with Kalman filtering, the skew standard deviation is not only significantly smaller than the case without Kalman filtering, but also maintains a comparatively stable trend. Meanwhile, in the standard PTP without Kalman filtering, the skew standard deviation of the second hop is significantly larger than that of the first hop. In the proposed PTP with Kalman filtering, the skew standard deviation of the second hop is almost the same as the first hop.

Based on the analysis of Fig 6 and 7, we can make a conclusion that the accumulation of synchronization error in the proposed PTP with Kalman filtering is smaller compared with the standard PTP without Kalman filtering. Furthermore, the PTP with Kalman filtering can achieve better time synchronization performance and stability compared with the standard PTP without Kalman filter in multi-hop WSNs. This mean that Kalman filter can eliminate noise and reduce the accumulation of synchronization error and results in the better adaptability in multi-hop time synchronization networks.

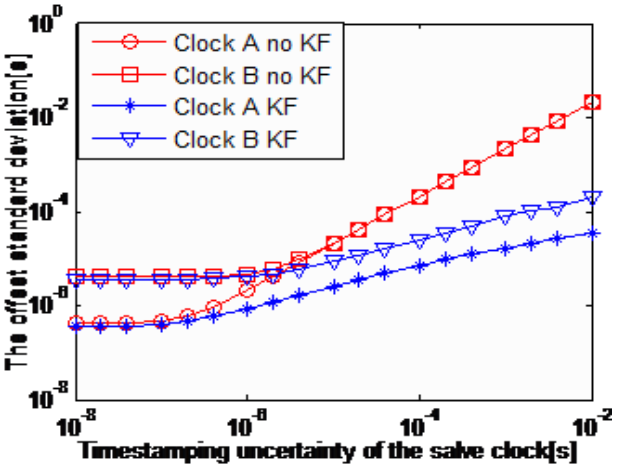


Figure 8. The offset standard deviation against timestamp uncertainty(δ_{STS})for clock A and clock B

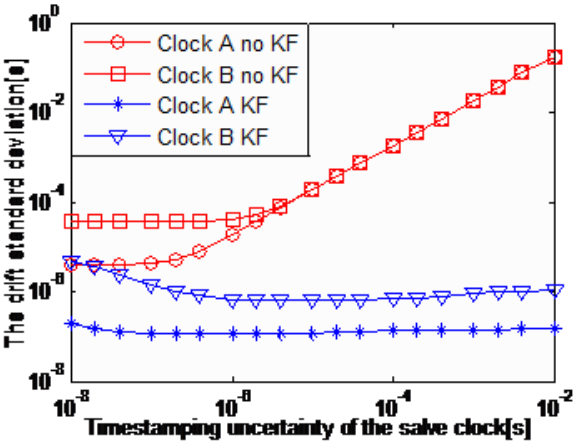


Figure 9. The skew standard deviation against timestamp uncertainty(δ_{STS}) for clock A and clock B

In the second simulation experiment, we compared the performance of the proposed multi-hop time synchronization at two different clocks. Clock A is a relatively stable clock with $\delta^2_{\square\ \square}=10^{-18}$ and $\delta^2_{\theta}=10^{-14}$ [24]. Another clock is a relatively unstable clock B with $\delta^2_{\square\ \square}=10^{-16}$ and $\delta^2_{\theta}=10^{-12}$[25]. The results of the standard PTP without Kalman filtering and the proposed one with Kalman filtering for different clocks are compared in Fig. 8 and Fig. 9. Both figures show the results of the slave clock in the second hop.

Fig. 8 shows that, for both Clock A and B, in the all range of timestamp uncertainty, the offset standard deviation with Kalman filtering is smaller than the case without Kalman filtering. In the standard PTP without Kalman filtering, the offset standard deviation of clock A and clock B show a gradual increment as the timestamps uncertainty increasing. When the time stamping uncertainties are large ($\delta_{STS} > 10^{-5}$), it dominates the synchronization errors and the offset standard deviation of Clock A is almost equal to the offset standard deviation of Clock B. While, in the proposed PTP with Kalman filtering, the offset standard deviation of clock A is significant smaller than that of clock B, even the time stamping uncertainties are large. Meanwhile, we can find that the offset standard deviation of clock B with Kalman filtering is smaller than that of clock A without Kalman filtering.

Similarly, Fig. 9 shows the propose PTP with Kalman filtering performs better than the standard PTP without Kalman filtering in terms of skew estimation. In the standard PTP, the skew standard deviation shows a significant increasing trend as a larger measurement noise occurs. However, with Kalman filter, the skew standard deviation maintain relatively stable and is significantly smaller than that of the PTP without Kalman filtering. This applies to both clock A and clock B. Furthermore, the skew standard deviation of clock A is significant smaller than that of clock B.

From Fig. 8 and 9, we can conclude that the multi-hop time synchronization performance can be improved significantly by adapting the Kalman filtering techniques. In particular, for inaccurate clock (like Clock B in the simulation), the performance improvement is more

obvious, which is a good benefit for low-cost WSNs, as the clocks of the WSN nodes are mostly inaccurate because of the low price and varying working conditions.

VIII. CONCLUSION

In this paper, we proposed a Kalman filtering to improve the IEEE 1588 PTP time synchronization performance in multi-hop wireless sensor networks. The performance of the proposed algorithm is validated by our developed multi-hop WSNS simulator on the OMNet++ platform. The result shows that, compared with the PTP without Kalman filtering, the proposed PTP with Kalman filtering is able to achieve higher precision and stability in multi-hop wireless time synchronization.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (NSFC) under grant 61101135, the Fundamental Research Funds for the Central Universities (XDJK2012C065, XDJK2014C167) and Science and Technology Commission of Shanghai Municipality under grant 13XD1403400.

REFERENCES

[1] J. Phillips, K. Kundert, "Noise in mixers, oscillators, samplers, and logic: An introduction to cyclo stationary noise," *Proc. IEEE CICC*, pp. 431–438, 2000

[2] F. J. Shang, "An Energy-Efficient Communication Protocol for Wireless Sensor Networks," *Journal of Networks* , vol. 6, no. 7, pp. 999-1008, 2011

[3] B. Sundararaman, U. Buy, A. D. Kshemkalyani, "Clock synchronization for wireless sensor networks: a survey," *Ad Hoc Networks*, pp. 281-323, 2005.

[4] M. Maroti, B. Kusy, G. Simon, and A. Ledeczi, "The flooding time synchronization protocol," *Proceedings of the Second International ACM Conference on Embedded Networked Sensor Systems*, pp. 39-49, 2004.

[5] S. Ganeriwal, R. Kumar, and M. B. Srivastava, "Timing-sync protocol for sensor networks," *Proceedings of the First International ACM Conference on Embedded Networked Sensor Systems*, pp. 138-149, 2003.

[6] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," *SIGOPS Oper. Syst.* Rev, vol. 36, no. SI, pp. 147–163, 2002.

[7] S. Ping, "Delay measurement time synchronization for wire sensor networks," *IEEE Micro*, pp.12-24, 2002.

[8] Y. Zeng, B. Hu, "Vector kalman filter using multiple parents for time synchronization in multi-hop sensor networks," *Proc. of the IEEE SECON*, pp. 413–421, 2008.

[9] J. C. Eidson "Measurement, control, and communication using IEEE 1588," London, pp. 35-58, 2006.

[10] K. Y. Cheng, K. S. Lui, Y. S. Wu and V. Tam "A Distributed Multihop Time Synchronization Protocol for Wireless Sensor Networks using Pairwise Broadcast Synchronization," *IEEE transactions on wireless communications*, vol. 8, no. 4, pp. 1764-1772, 2009

[11] V. Kaseva, T. D. Hämäläinen, "Time Synchronization for Resource-Constrained Multi-Hop Wireless Sensor Networks based on Hop Delay Estimation," *The Fifth International Conference on Sensor Technologies and Applications*, pp. 79-84, 2011

[12] C. Sun, F. Yang, L. Ding, "Multi-hop time synchronization for underwater acoustic networks," *IEEE Conference Publications*. pp.1-7, 2012

[13] H. Xiao, C. Lu, H. Ogai, "a multi-hop low cost time synchronization algorithm for wireless sensor network in bridge health diagnosis system," *Embedded and Real-Time Computing Systems and Applications* (RTCSA), pp. 392-395, 2012.

[14] Z. Ding, N. Yamauchi "an improvement of energy efficient multi-hop time synchronization algorithm in wireless sensor network," *Wireless Communications, Networking and Information Security* (WCNIS). pp. 116-120, 2010

[15] IEEE "Standard for a precision clock synchronization protocol for networked measurement and control systems," IEC 61588:2009(E) , vol., no., pp.C1,274, 2009

[16] Y. Huang, Y. Yang, T. Li, X. Dai, "An Open Source Simulator for IEEE1588 Time Synchronization over 802.11 Networks," *Modelling Symposium* (EMS), pp.560-565, 2013

[17] L.Ye, T. Li, X. Dai. "Kalman filtering for precision time synchronization in wireless sensor networks," *Caai Transactions On Intelligent Systems*, pp. 518-524, 2012.

[18] S. B. Moon, P. Skelly, D. Towsley, "Estimation and removal of clock skew from network delay measurements," *Proc. 18th Annu. Joint Conf, IEEE Comput, Cummun*, pp. 227-234, 1999.

[19] Xu Bao, "Time Synchronization for Heterogeneous WSNs Based on Cluster," *Journal of Networks*, vol. 8, no. 12, pp. 2915-2921, 2013

[20] A. Bletsas, "Evaluation of Kalman filtering for networktime keeping," *IEEE Trans. Ultrasonics, Ferroelectrics* and *Frequency Control*, pp. 1452–1460, 2005.

[21] G. Giorgi., C. Narduzzi. "Modelling and Simulation Analysis of PTP Clock Servo. In: IEEE Symposium on Precision Clock Synchronization for Measurement," *Control and Communication ISPCS07*, pp. 155-161, 2007

[22] G. Giorgi, C. Narduzzi, "Performance Analysis of Kalman Filter Based Clock Synchronization in IEEE 1588 Networks," *IEEE Trans-actions on Instrumentation and Measurement*, vol. 60, no. 8, 2011.

[23] J. Rutman, F. L. Walls, "Characterization of frequency stability in precision frequency sources," *Proc. IEEE*, vol. 79, no. 7, pp. 952-960, 1991.

[24] H. Abubakari and S. Sastra, "IEEE 1588 Style Synchronization Over Wireless Link," *Proc. IEEE ISPCS.*, pp. 127–130, 2008

[25] N. Barendt, K. Correll and M. Branicky. "Servo design considerations for software-only implementations of the Precision Time Protocol," *ISPCS*, pp. 10–12, 2005

Enhancing Channel Coordination Scheme Caused by Corrupted Nakagami Signal and Mobility Models on the IEEE 1609.4 Standard

Doan Perdana and Riri Fitri Sari
Department of Electrical Engineering, Faculty of Engineering, University of Indonesia, Depok, Indonesia Kampus Baru UI,
Email : {doan.perdana, riri}@ui.ac.id

***Abstract*—Ensuring high saturated throughput of SCHs and reducing the transmission delay of service packets on CCHs are one of the most challenging issues in multichannel operations IEEE 1609.4 standard. Moreover, multiple issues due to its highly dynamic topology, the high mobility, the change trajectory, and Nakagami propagation channel caused by Additive White Gaussian Noise (AWGN) are challenges in assuring the Quality of Service (QoS) in multichannel operations IEEE 1609.4 standard.**

In this paper, we propose a coordination scheme based on the multichannel operations IEEE 1609.4 standard, in terms to enhance the Quality of Service (QoS) caused by different dynamic topology, high mobility, change trajectory, and Nakagami propagation channel caused by Additive White Gaussian Noise (AWGN). The propose scheme is enhancement of the previous scheme, i.e. *Variable CCH Interval* (VCI). We use ns 3.18 and Matlab tools for the simulation and evaluation of the performance.

From the simulation, we found that the proposed scheme enhance the saturated throughput and reduces the transmission delay of service packets compared the previous scheme. This paper also evaluates the proposed scheme caused by different mobility models. We also analysis probability of the signal error Nakagami-m distribution parameters caused by the existence of the Additive White Gaussian Noise (AWGN).

***Index Terms*—IEEE 1069.4, Nakagami Propogation, Additive White Gaussian Noise (AWGN), Coordination Scheme, ns 3.18 simulator**

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) has recently become one of the most research topics in the area of Intelligent Transportation System (ITS) and wireless networking [1]. A VANET is mainly characterized by high mobility and the restricted movement patterns governed by roads and traffic rules [2]. These characteristics lead to many challenges in designing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication protocols [3].

Due to its decentralized nature, a VANET is highly preferred by a variety of safety applications which cannot easily obtain help from central nodes, such as cooperative collision avoidance, blind sport warning, and approaching emergency warning [4]. It introduces a modification to IEEE 802.11a at the PHY layer in order to cope with the fast-fading propagation environment [3]. At the MAC layer, IEEE 802.11p relies on the prioritized channel access of IEEE 802.11e MAC [3].

The standard of the IEEE 1609 protocols family, which supports multichannel operation and enhances IEEE 802.11p MAC layer, is IEEE 1609.4 [1]. This standard describes seven different channels with different features and usage [1].

Specifically, IEEE 1609.4 defines with seven 10 Mhz-wide channels are available in the frequency band of 5.85–5.925 GHz. i.e. one control channel (CCH) and six service channels (SCHs) [3]. The channel access time is divided into synchronization intervals with a fixed length of 100 ms [3]. A synchronization interval is further divided into CCH and SCH intervals. Each interval lasts 50 ms long [3]. According to the channel switching scheme, all devices must stay tuned to CCH during the CCH interval for exchanging safety and control messages [3]. A device can actively be switched from the CCH to a specific SCH for its desired non-safety application services. IEEE 1609.4 defines a guard interval (GI) at the beginning of both the CCH and SCH [3].

Channel coordination is designed to support data exchanges involving one or more switching devices with concurrent alternating operation on the CCH and an SCH [5]. This allows, for example, a single-PHY device access to high-priority data and the management traffic

doi:10.4304/jnw.9.12.3454-3461

during the CCH interval, as well as general higher layer traffic during the SCH interval [5]. Figure 1 illustrates two examples of channel access: continuous access, which requires no channel coordination, and alternating access, which does require channel coordination [5].

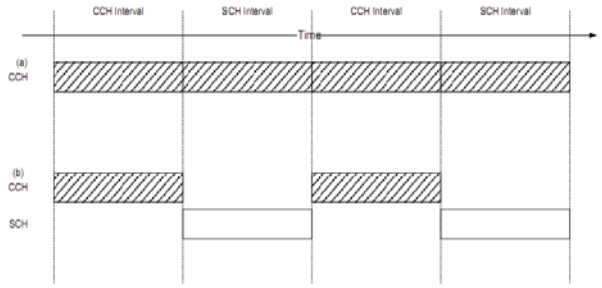


Figure 1. Channel access examples: (a) continuous and (b) alternating [5]

IEEE 1609.4 makes the CCH and SCH intervals to be synchronized to an external time reference, the Coordinated Universal Time (UTC) which is provided by the Global Positioning System (GPS) [3]. However, if a device fails to get the UTC from its local GPS, it should get time information from other nodes over the air [3]. This becomes possible by using wave time advertisement (WTA) frames, which is available in the IEEE 802.11p specification [3]. Given the UTC, a node aligns the start of the CCH interval with the UTC or a multiple of 100 ms after the UTC [3].

A sync interval and its CCH interval and SCH interval components are shown in Figure 2 [5]. The duration of the CCH and SCH intervals are stored in the MIB attributes *CchInterval* and *SchInterval*, respectively, and the values of these attributes sum to the length of the sync interval [5]. There shall be an integer number of sync intervals in 1 s [5]. Coordinated Universal Time (UTC) defines the common time base for WAVE channel coordination [5]. At each UTC second, the beginning of a sync interval shall align with the beginning of the UTC second, as shown in Figure 2 [5]. The first part of each channel interval (CCH interval or SCH interval) is a guard interval as shown in Figure 2, used to calculate for radio switching and timing inaccuracies among different devices [5].

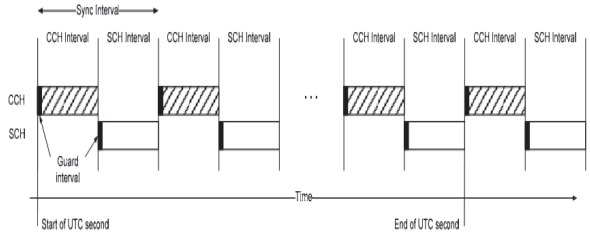


Figure 2. Syn interval, guard interval, CCH interval, and SCH interval [5]

The problem addressed in this paper is to evaluate the multiple issues that reduce the Quality of Service (QoS) based on the multichannel operations IEEE 1609.4 standard. It also analyzed the Nakagami distribution parameter caused by Additive White Gaussian Noise (AWGN).

The contribution of this paper is to propose a coordination scheme to enhance the saturated throughput of the SCHs and to reduce transmission delay IEEE 1609.4 standard. It also evaluate the propose scheme due to its highly dynamic topology, the high mobility, change trajectory. This paper also analyzed the probability of signal error the Nakagami-m distribution parameters caused by Additive White Gaussian Noise (AWGN).

This paper is organized as follows. In section II, we provide a number of related work and motivation. In Section III, we provide a scenario and simulation for the coordination schemes based on the IEEE 1609.4 standard. In section IV, we evaluate the performance of proposed coordination caused by mobility models. We also evaluate the performance probability of the signal error Nakagami-m distribution parameters caused by Additive White Gaussian Noise (AWGN) based on IEEE 1609.4 standard. Finally, we conclude the paper and suggest the future work in Section V.

II. RELATED WORK AND MOTIVATION

Wang, Q. *et al.* [6-8] proposed a Variable CCH Interval (VCI) multichannel MAC protocol to enhance the saturation throughput of SCHs and ensuring the transmissions of safety messages while maintaining the prioritized transmission of critical safety information on CCH. The CCH interval (safety and WSA intervals) is calculated by the roadside unit (RSU). The RSU broadcasts a packet (VCI packet) containing the length of the CCH interval to the nodes under its transmission range. VCI calculates the optimal ratio between WSA and SCH intervals. We use [6-8] to simulate and evaluate the proposed scheme caused by mobility models based on Multi-channel operations of the IEEE 1609.4.

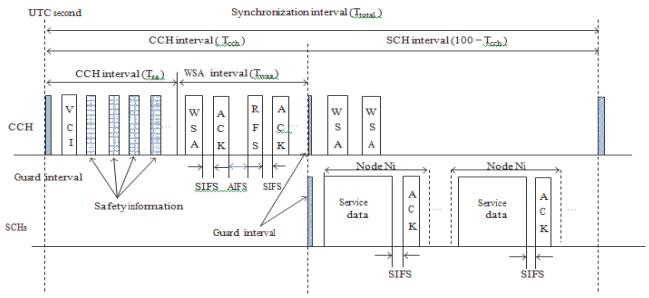


Figure 3. Operations of VCI [3,6]

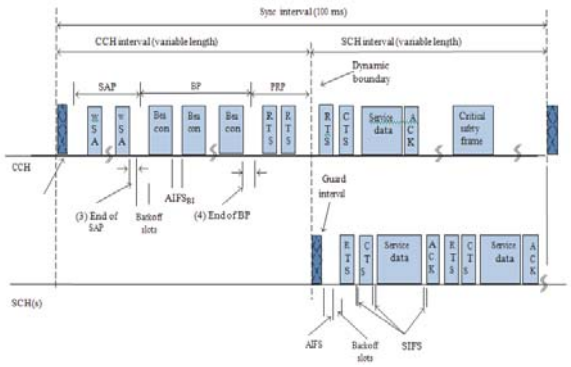


Figure 4. Operations of DID-MMAC [3]

L. Liu *et al.* [9] introduced the Dynamic Interval Division Multichannel MAC (DID-MMAC) to perform the dynamic adjustment SCH / CCH interval. This scheme divides the CCH interval into 3 phases based on the type of different messages : Service Announce Phase (SAP), Beacon Phase (BP), and Peer-to-Peer Reservation Phase (PRP). For dynamically adjusting the intervals of SAP and BP in a distributed manner, DID-MMAC assigns different channel access priorities to different messages by differentiating the contention window (CW) and the interframe space (IFS) [3].

N. Lu *et al.* [10] defined the Dedicated Multichannel MAC (DMMAC) to perform an adaptive broadcasting mechanism to reduce the collision rate and a transmission delay. The research aimed to improve the safety performance of packet delivery ratio. The research did not consider the dynamic adjustment of the CCH interval and analytical studies performed on the model of the proposed scheme.

H. Yoo and D. Kim [11] proposed a Dynamic Safety Interval (DSI) for calculating the optimal safety interval under dynamic traffic conditions in a distributed manner [7]. In particular, DSI calculates the safety interval considering the presence of hidden nodes [3]. We use [11] to simulate and evaluate the propose scheme caused by hideen node based on Multi-channel operations of the IEEE 1609.4.

Nasuf H. *et al.* [12] estimates the Nakagami-m distribution parameters which uses samples corrupted by multipath and shadow fading, phase fluctuations and noise [12]. Expressions for the probability density function and n-th order moment of noisy channel samples are presented. Moment-based estimator for operation in noisy environments is developed based on the presented probability density function. The sample mean and variance of the estimator are determined [12]. We use [12] to evaluate and analysis the probability of signal error the Nakagami-m distribution parameters caused by Additive White Gaussian Noise (AWGN).

M.Kostiü *et al.* [13] proposed analytical approach and performance analysis of the gamma-shadowed Nakagami-m fading channels using the moment matching method. In a study conducted analyzed the outage probability and average bit-error.

George K. K. *et al.* [14] propose a model estimation Moments Generating Function (MGF), the Probability Density Function, Cumulative Distribution Function (CDF), and the moments of the distribution of N * Nakagami. This study also conducted to investigate the suitability of the distribution of N * Nakagami fading using lognormal distribution. We use [14] to analyzed the Nakagami-m distribution parameters using Moments Generating Function (MGF), the Probability Density Function, and Cumulative Distribution Function (CDF).

A. Coordination scheme based on IEEE 1609.4 standard

Channel coordination mechanism is an important scheme for increasing efficiency of transmission at the MAC layer of the IEEE 1609.4 standard. Channel coordination scheme could ensure the saturation throughput of SCHs and reduce the delay transmission of the service packets. The channel coordination scheme is a coordination mechanism between CCHs (safety packets) and SCHs (non-safety packets) standard synchronized by *CchInterval* and *SchInterval* in the IEEE 1069.4 standard.

B. Nakagami-m Distribution Parameter

The Nakagami distribution or the Nakagami-m distribution is a probability distribution related to the gamma distribution. It has two parameters : a shape parameter m and a second parameter controlling spread, Ω. The Nakagami-m distribution having the pdf [12]:

$$p(r) = \frac{2\left({}^{m}/_{\Omega}\right)^{m}}{\Gamma(m)} r^{2m-1} \exp\left(-m{}^{r^2}/_{\Omega}\right), r \geq 0 \quad (1)$$

where $m = \frac{\Omega^2}{E\{(r^2-\Omega)^2\}}$ is the so-called m parameter with $m \geq 0.5, \Omega = E\{r^2\}$is the second moment of distribution and $\Gamma(.)$ is the gamma function [18, p. 255]. Ω also represents shadow fading, slow signal power fluctuations usually described with log-normal pdf, which can be very well modeled with gamma pdf as in [13] :

$$p(\Omega) = \frac{\left({}^{m_s}/_{\Omega_s}\right)^{m_s}}{\Gamma(m_s)} \Omega^{m_s-1} \exp\left(-m_s \frac{\Omega}{\Omega_s}\right), \Omega \geq 0 \quad (2)$$

where $m_s > 0$ is shadow severity parameter and $\Omega > 0$ is real, modified received signal power.

```
Algorithm Procedure in selecting CCH interval
          And SCH Interval
for each N ∈ T (CCH, SCH) do
   Detect the type of service packet ∈ N
      for each of service packet ∈ N
         if N∈S (SendIpPackets and SendWsmpPackets)
            Setting for N∈T (Nakagami Propagation Loss Model)
              if N ∈ T (Distance > 150m, Same Channel Number)
                 Hidden node interference
              else
                 Node not interferer
          // Executed by nodes at the beginning of the CCH interval
           if CIprev not equal zero then
              CIcurr = CIprev
           else
              CIcurr = 50 ms
          repeat
             Randomize SIcurr
             Update (CIvci_f2, CIwsa_f2, CIrfs_f2, CIcurr, CIvci_f,
             CIsi, CIwsa_f, CIack, CIrfs_f)
           until
             CurrentDelay < = PreviousDelay and
             CurrentThroughput > PreviousThroughput
          if receive a VCI frame
              if it is the first time receiving a VCI frame
                 Randomize SIcurr;
                 Update (CIvci_f2, CIwsa_f2, CIrfs_f2, CIcurr,
                 CIvci_f, CIsi, CIwsa_f, CIack, CIrfs_f)
              else if CIcurr < CIvci_f then CIcurr = CIvci_f
                   if receive a WSA/RFS/ACK frame and have not
                      yet received a VCI frame
                      Randomize SIcurr;
                      Update(CIvci_f2, CIwsa_f2, CIrfs_f, CIcurr,
                      CIvci_f, CIsi, CIwsa_f, CIack, CIrfs_f);
                   else if the WSA/RFS/ACK frame is from the node
                           will connect to then
          if CIcurr < CIwsa_f then // Under different RSUs
             CIcurr = CIwsa_f
          end if
          end if
      end for
end for
```

III. SCENARIO AND SIMULATION

By using ns 3.18 simulator, we evaluate the performance propose coordination scheme caused by mobility on IEEE 1609.4 standard. We also analysis Nakagami distribution parameter caused by Additive White Gaussian Noise (AWGN) using Matlab tools. We simulate the scenario with the number of cars range from 10 to 100 nodes and using Manhattan, Traffic sign, and IDM_IM model mobility. The channel configuration using variable values for control and service channel intervals, and the guard intervals value is 4 ms. Table I. presents all parameters used in our simulation.While some parameters stay fixed, others are varied in order for us to observe the changing behavior of the network.

TABLEI.SIMULATION PARAMETERS

Parameters	Values
MAC Protocol	IEEE 1609.4
Number of vehicles	10-100 nodes
Number of CCH	1
Number of SCHs	4
Service packet length	2000 bytes
Data rate of each channel	3 Mbps
PHY header	192 bits
MAC header	256 bits
WSA/RFS	160 bits + PHY header
ACK	112 bits + PHY header
Slot time	20 μs
SIFS	10 μs
DIFS	50 μs

Based on [12], the transmitted signal is assumed known in the estimation of the fading distribution parameters. This is the case for received signal samples taken during the transmission of training sequences (which may be for channel estimation, synchronizer training or equalize training) [12]. This is also the case when the receiver makes correct decisions which occur with high probability in a well designed [12]. The fading signal is corrupted by additive white Gaussian Noise (AWGN), which is independent of the fading. The received signal in the *i*-th symbol period can be expressed as

$$\mathbf{X}i\,(t) = \mathbf{r}i\;\; e^{-j\theta i}\; \mathbf{S}i(t) + \mathbf{W}i\,(t) \qquad (3)$$

where s*i*(t) is the transmitted signal in the *i*-th symbol period, r*i* is the fading amplitude in the *i*-th symbol period having a Nakagami-m distribution. θi is the fading phase (phase fluctuation) in the *i*-th symbol period, where $\theta i \in [-\pi, \pi]$.

In this paper, the propose coordination scheme also considered the hidden node. Based on [11], hidden node refer to the nodes located within r*i* of the intended destination and out of r*c* of the sender.

When a receiver is receiving a packet, if a hidden node tries to start a concurrent transmission, collisions can happen at the receiver [11].

For example as shown in Figure 5, node B is located within interference ranges of both nodes A and D so that node D's transmission interferers with the transmission

from node A to node B [11]. On the other hand, node A's r_t is not overlapped with node E's r_i, since node A and E are separated by a distance denoted by d_{sr} [11]. Therefore, both nodes can concurrently transmit their packets without interfering with each other. d_{sr} is called spatial reuse distance and should be larger than the sum of r_t and r_i [11].

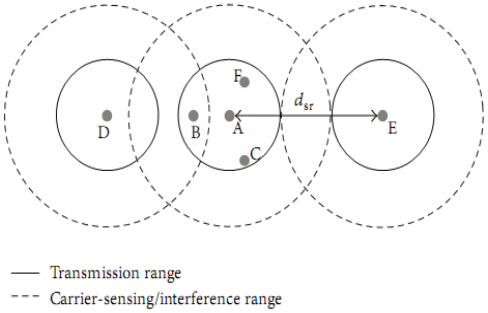


Figure 5. Hidden Node Problem [11]

IV. RESULT AND EVALUATION

Base on the scenario above, in Figure 6, 7, and 8 the simulation was performed to obtain data according to three aspects to be measured, i.e the average delay, number of delivered packet, and throughput.

1) *Performance of Enhanced Variable CCH Interval for Different Mobility on the IEEE 1609.4 standard*

a) *Average Delay*

Fig. 5 shows the average of delay enhanced Variable CCH Interval (VCI) for different mobility models on the IEEE 1609.4 standard, by varying the number of nodes.

We focus on the average access delay which calculate the MAC layer. Delay and access will be used interchangeably on this work by varying the number of nodes. This can be seen in Fig. 6.

The following is the equation for the average delay $E[\delta]$ derived as [16,17] :

$$E[\delta] = E[\chi] + E[\theta] \quad (4)$$

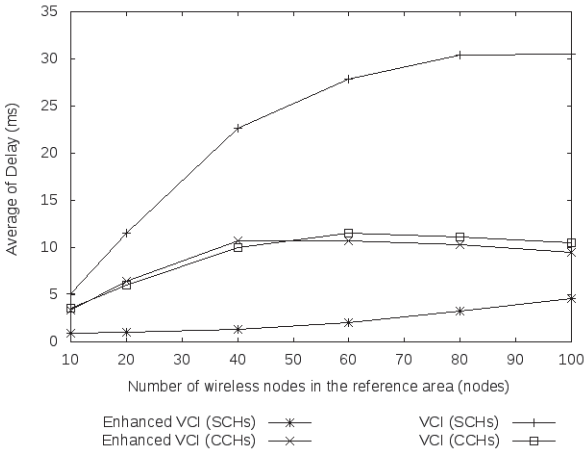


Fig. 6. Average delay of Enhanced Variable CCH Interval

Fig. 6, we found that the average delay of Enhanced Variable CCH Interval lower compared with Variable CCH Interval caused by mobility models based on IEEE 1609.4 standard. We can evaluate from the performance simulation that the new propose coordination schemes, basically the variable CCH interval (safety and and WSA intervals) is calculated by roadside unit (RSU) and neighbor nodes. If there are heavy traffic or congested traffic, the VCI packets may could be heard by other nodes using channel gossip. So the new propose scheme could be handle for heavy traffic, caused by hidden node, and also caused by high mobility on the IEEE 1609.4 standard.

b) *Throughput*

Fig. 7 shows the throughput of Enhanced Variable CCH Interval on the IEEE 1609.4 standard, by varying the number of nodes. Throughput T_i (t) is the rate of successful packet delivery through a network connection per unit time. We focus on the throughput calculated at the MAC layer, then T_i (t) derived as [16,17] :

$$Throughput\ T_i(t) = x^*(1-p)^*d^*data\ rate \quad (5)$$

Where $d = DATA/(DIFS+PACKET+SIFS+ACK)$

x is the number of nodes
T_i (t) is the throughput
a is the distance of nodes
p is the collision probability for a transmission

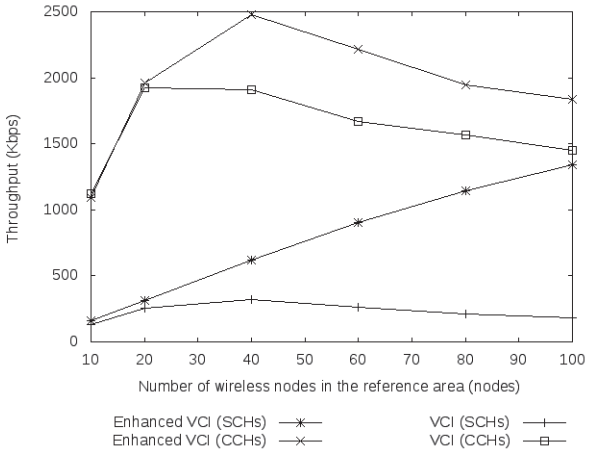


Fig. 7 System throughput of Enhanced Variable CCH Interval

Fig. 7 shows that the throughput of Enhanced Variable CCH Interval higher compared with Variable CCH Interval caused by mobility models based on IEEE 1609.4 standard. We can evaluate from the performance simulation that the new propose coordination schemes, calculates the optimal safety interval and WSA interval based on network traffic conditions for service packet in the CCH interval. If there are heavy traffic or congested traffic, the VCI packets may could be heard by other nodes using channel gossip. So the new propose scheme could be enhance the saturated throughput under heavy traffic or congested traffic.

2) Probability of signal error caused by corrupted Nakagami signal

Based on [12], the m-parameter estimator over Nakagami-m multipath / gamma-shadowed noisy channel is obtained as :

$$\hat{m} = \frac{1}{K} \cdot \sum_{j=1}^{K} \hat{m}_j \quad (6)$$

Where K represents total number of realizations of the shadow fading as a random process.

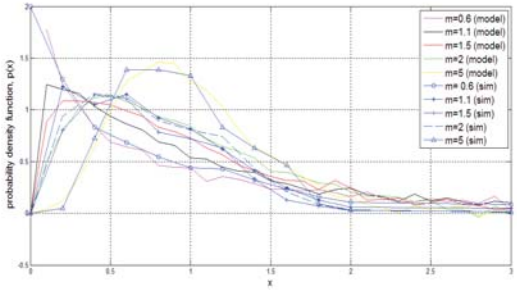


Fig.9 Probability Density Function Corrupted Nakagami Signal for m = 0.6, 1.1, 1.5, 2, 5

Using eqn. (6), we evaluate probability of signal error caused by corrupted Nakagami [15] :

$$P_e = \frac{1}{\frac{\{1+J_0(2\pi f_D T_S)\}\frac{E_b/N_0}{\hat{m}+1}+1}{\{1-J_0(2\pi f_D T_S)\}\frac{E_b/N_0}{\hat{m}+1}+1}} \text{x} \exp\left(-\frac{\hat{m}\frac{E_b/N_0}{\hat{m}+1}}{\frac{E_b/N_0}{\hat{m}+1}+1}\right) \quad (7)$$

$$P_e = \frac{1}{2\left(\frac{E_b/N_0}{\hat{m}+1}+1\right)} \exp\left(-\frac{\hat{m}\frac{E_b/N_0}{\hat{m}+1}}{\frac{E_b/N_0}{\hat{m}+1}+1}\right) \quad (8)$$

Fig.9 shows that the probability density function (pdf) on IEEE 1609.4 standard with different m-parameter estimator over Nakagami-m (m=0.6, 1.1, 1.5, 2, 5). We can evaluate from the performance simulation that m parameter characterise fading and shadowing on the desired signal disturbed by Additive White Gaussian Noise (AWGN). We also can evaluate corrupted signal at m=5 has the highest fluctuative probability function (pdf).

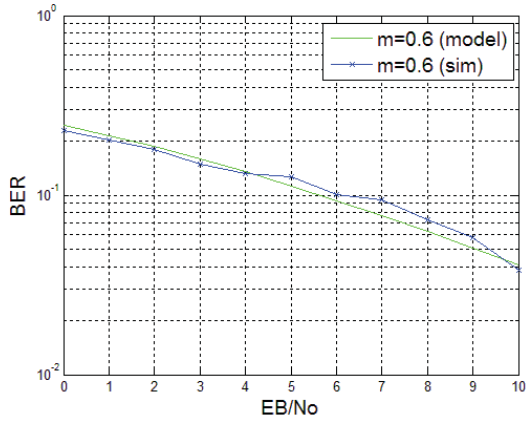


Fig.10 Probability of signal error modeled versus simulation result (m=0.6)

Fig.10 shows that the probability of signal error and Eb/No caused by Additive White Gaussian Noise (AWGN) on IEEE 1609.4 standard slightly decrease. We can evaluate from the performance simulation that the probability of signal error influnced by m-parameter estimator over Nakagami-m (m=0.6).

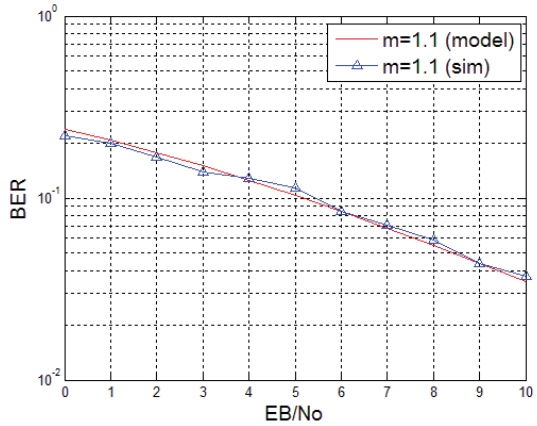


Fig.11 Probability of Signal Error modeled versus simulation result (m=1.1)

Fig.11 shows that the probability of signal error caused by Additive White Gaussian Noise (AWGN) on IEEE 1609.4 standard slightly decrease with Eb/No. We can evaluate from the performance simulation that the probability of signal error influnced by m-parameter estimator over Nakagami-m (m=1.1).

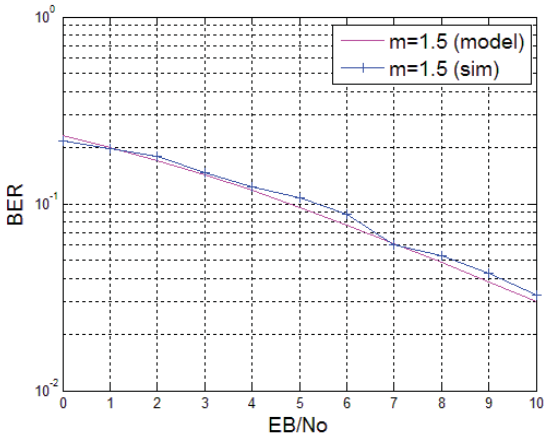


Fig.12 Probability of signal error modeled Vs simulation result (m=1.5)

Fig.12 shows that the probability of signal error caused by Additive White Gaussian Noise (AWGN) on IEEE 1609.4 standard slightly decrease with Eb/No. We can evaluate from the performance simulation that the probability of signal error influnced by m-parameter estimator over Nakagami-m (m=1.1).

V. CONCLUSION

Our performance simulation for the new propose coordination schemes show the enhancement of the saturation throughput and reduction of the delay because it basically the variable CCH interval (safety and and WSA intervals) is calculated by roadside unit (RSU) and neighbor nodes. If there are heavy traffic or congested traffic, the VCI packets may could be heard by other nodes using channel gossip. So the new propose scheme could be handled by heavy traffic, impact of hidden node, and also high mobility on IEEE 1609.4 standard.

Finally, we evaluate the probability of signal error for m = 0.6, 1.1, and 2 using modeled by Nasuf H. et al. compared simulation (ns-3). We also evaluate the Probability Density Function (PDF) corrupted signal Nakagami caused by Additive White Noise Gaussian (AWGN) for m = 0.6, 1.1, 1.5, 2, and 5 using modeled compared simulation (ns-3).

REFERENCE

[1] Jafari, A., Performance Evaluation of IEEE 802.11p for Vehicular Communication Networks. PhD Dissertation, Faculty of Arts, Computing, Engineering, and Sciences, Postgraduate Program, Sheffield Hallam University, South Yorkshire, England, UK, 2011.

[2] J. Harri, F. Filali, and C. Bonnet, "Mobility models for vehicular Ad Hoc networks: a survey and taxonomy," IEEE Communications Surveys and Tutorials, vol. 11, no. 4, pp. 19–41, 2009.

[3] H. Yoo and D. Kim, "A dynamic safety interval protocol for VANETs," in Proceedings of the ACM Research in Applied Computation Symposium (RACS '12), pp. 209–214, October 2012.

[4] R. Chen, W.-L. Jin, and A. Regan, "Broadcasting safety information in vehicular networks: issues and approaches," IEEE Network, vol. 24, no. 1, pp. 20–25, 2010.

[5] IEEE Std 1609.4-2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Multichannel Operation, IEEE, 2011.

[6] Q. Wang, S. Leng, H. Fu, and Y. Zhang, "An IEEE 802. 11p-based multichannel MAC scheme with channel coordination for vehicular Ad Hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 2013, no. 2, pp. 449–458, 2012.

[7] Q. Wang, S. Leng, H. Fu, Y. Zhang, and H. Weerasinghe, "An enhanced multi-channel MAC for the IEEE 1609.4 based vehicular Ad Hoc networks," in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM '10), San Diego, Calif, USA, March 2010.

[8] Q. Wang, S. Leng, Y. Zhang, and H. Fu, "A QoS supported multichannel MAC for vehicular Ad Hoc networks," in Proceedings of the IEEE 73rd Vehicular Technology Conference (VTC '11), Budapest, Hungary, May 2011.

[9] L. Liu, W. Xia, and L. Shen, "An adaptive multi-channel MAC protocol with dynamic interval division in vehicular environment," in *Proceedings of the lst International Conference on Information Science and Engineering (ICISE '09)*, pp. 2534–2537, Nanjing, China, December 2009.

[10] N. Lu, Y. S. Ji, F. Q. Liu, and X. H. Wang, "A dedicated multi-channel MAC protocol design for VANET with adaptive broadcasting," in *Proc. WCNC*, 2010, pp. 1–6.

[11] H. Yoo and D. Kim, "A dynamic safety interval protocol for VANETs," in *Proceedings of the ACM Research in Applied Computation Symposium (RACS '12)*, pp. 209–214, October 2012.

[12] Nasuf H., Mirza M., Melita A.C., and Mesud H., "Estimation of Nakagami Distribution Parameters Based on Signal Samples Corrupted with Multiplicative and Additive Disturbances," 49th International Symposium ELMAR-2007, 12-14 September 2007, Zadar, Croatia.

[13] M.Kostiü, "An analytical approach to performance analysis for channel subject to shadowing and fading", IEEE Proc. On Communications, vol. 152, No. 6, 2005, pp. 821-827

[14] George K. Karagiannidis, Niko C.S and P. Takis Mathiopoulos "The N * Nakagami Fading Channel Model," IEEE Communication Letters 2005.

[15] Sasamori, F., Yamano, A. ; Handa, S. ; Maehara, F. ; Takahata, F. ; Oshita, S., "Approximate Equation of Bit Error Rate in OFDM Systems over Specular Multipath Fading Channels", Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE (Volume:3), 20 March 2003, pp. 2096 - 2101 vol.3, ISSN : 1525-3511.

[16] Doan Perdana and Riri Fitri Sari, "Mobility Models Performance Analysis using Random Dijkstra Algorithm and Doppler Effect for IEEE 1609.4 Standard", *International Journal of Simulation, Systems, Science, and Technology, United Kingdom Simulation Society*.

[17] Ali J. Ghandour, Marco Di Felice, Hassan Artail and Luciano Bononi, "Modeling and Simulation of WAVE 1609.4-based Multi-channel Vehicular Ad Hoc Networks", 5th ACM International Conference on Simulations Tools and Techniques (SIMUTools 2012), March 19-23, 2012, Sirmione-Desenzano, Italy.

[18] M. Abramowitz and I.A. Stegun, Eds. Handbook of Mathematical Functions.New York: Dover, 1972.

Doan Perdana received his BSc and MSc degrees in Telecommunication Engineering, from the Institute of Technology Telkom in 2004 and 2012, respectively. He is currently undergoing doctoral study in Electrical Engineering Department, University of Indonesia. His interests include Telecommunication Systems and Computer Engineering.

Riri Fitri Sari, PhD is a Professor of computer engineering at Electrical Engineering Department of Universitas Indonesia. She received her BSc degree in Electrical Engineering from Universitas Indonesia. She completed her MSc in Computer Science and Parallel Processing from the University of Sheffeld, UK. She has awarded a PhD in Computer Science received from the University of Leeds, UK. Riri Fitri Sari is a senior member of the Institute of Electrical and Electronic Engineers (IEEE).

Error Performance Analysis of Multiuser CDMA Systems with Space-time Coding in Rician Fading Channel

Dingli Yang [1], Qiuchan Bai [1], Yulin Zhang [1], Rendong Ji [1, 2], Yazhou Li [1], and Yudong Yang [1]
1. Faculty of Electronic and Electrical Engineering, Huaiyin Institute of Technology, Huai'an 223003, China
2. College of Science, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
Email: yangdingli@163.com, bqcbzn@163.com, zhangyulin@hyit.edu.cn , jrd7933@163.com, 115035409@qq.com, yyudong@163.com

***Abstract*—In this paper, the error performance of multiuser CDMA system with space-time coding is studied in Rician fading channel, and the corresponding bit error rate (BER) and symbol error rate (SER) analysis are presented. Based on the performance analysis, a simple and effective multiuser receiver scheme is developed. The scheme has linear decoding complexity when it compares to the existing scheme. Based on the performance analysis, and using mathematical manipulation, the BER and SER of multiuser space-time coded CDMA system are derived, respectively. As a result, accurate closed-form expressions of BER and SER are respectively obtained. With these expressions, the performance of multiuser CDMA system with space-time coding can be evaluated effectively. Computer simulation shows that the developed receiver scheme has almost the same performance as the existing scheme, and the theoretical BER and SER can match the corresponding simulation results well.**

***Index Terms*—Space-Time Coding; Code Division Multiple Access (CDMA); Rician Fading; Low Complexity; Bit Error Rate; Symbol Error Rate**

I. INTRODUCTION

Recently, multiple-input and multiple-output (MIMO) technique is well known to offer improvements in bandwidth efficiency along with diversity and coding benefits over wireless fading channels [1-4]. Especially space-time block coding (STBC) in MIMO systems can provide effective diversity for combating fading effect [5-10], and has received much interests. However, the conventional STBC scheme is only used for single-user environment, and thus it will be not suitable for multiuser scenario in practice. Hence, it is necessary to extend the STBC scheme into multiuser CDMA scenario for practical purposes. Based on different multiuser space-time coded system models, the receiver schemes are designed in references [11-18] and references therein. In reference [11], the bit error rate (BER) analysis is provided for space-time coded CDMA system with the conventional matched filter receiver, but the analysis method and system model are applicable only to the BPSK modulation and downlink, and does not provide the closed-form BER expression for Rician fading channel. The given symbol error rate (SER) expression for space-time codes needs summing from 0 to infinity, whereas the infinity is difficult to decide. In reference [12], a minimum variance linear receiver scheme for multiuser MIMO system is proposed, but the system needs to design and optimize the weighted matrix to suppress the multiuser interference (MUI). As a result, the computational complexity is very complicated. In reference [13], the performance of multiuser CDMA system with transmit diversity is studied, but the analysis is limited in BPSK modulation and two transmit antennas. For multicarrier-CDMA (MC-CDMA) system, a least mean-square based adaptive receiver scheme is proposed for MC-CDMA with Alamouti's STBC [14], but the scheme is limited in two transmit antennas and one receive antenna. The performance of space-time coded MC-CDMA system is analyzed in Nakagami fading channel [15], but the analysis is limited in Alamouti's STBC and BPSK modulation. Blind space-time multiuser detection schemes are presented in reference [16] for MC-CDMA system. The performance of space-time coded MIMO system with cross-layer design is analyzed in spatially-correlated and Keyhole Nakagami fading channel [17], but the analytical method is applicable only to single user system. Reference [18] gives the effective combination of CDMA system and different space-time codes, and the developed decorrelative receiver scheme can decouple the detection of different users, but the decoding complexity is exponential for each user, which will not benefit practical application. Moreover, the above schemes basically do not provide the error performance analysis, and are limited in Rayleigh fading channel, whereas in practice, the system may experience the Rician fading due to the direct-path propagation.

Due to the reason above, the error performance of space-time coded CDMA system in Rician fading channel is studied. Firstly, a multiuser space-time coded CDMA system model is presented, and then a low-complexity multiuser receiver scheme is proposed by utilizing maximum ratio combining (MRC) method and orthogonality of space-time coding. The presented space-time coded CDMA system can achieve effective MUI suppression by using multiuser detection method. After

doi:10.4304/jnw.9.12.3462-3469

decorrelating, each user has linear rather than exponential decoding complexity. According to the performance analysis, and using mathematical calculation, the average BER and SER of the system are derived in detail. As a result, accurate and approximate closed-form expressions of BER and SER are attained for space-time coded CDMA with orthogonal and quasi-orthogonal spreading code, respectively. Simulation results show that the proposed low-complexity scheme can obtain almost the same performance as the existing scheme. Theoretical BER and SER will be in good agreement with the corresponding simulations. Thus, the effectiveness of the theoretical formulae is verified.

Note: the superscripts $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$ are used to stand for the transpose, complex conjugate, and Hermitian transpose, respectively. $E\{\cdot\}$ and $\mathrm{I_N}$ denote the statistical expectation and identity matrix, respectively. $\mathrm{vec}(?)$ stand for matrix vectorization operator.

II. System Model

In this paper, a synchronous CDMA communication system with N transmit antennas and L receive antennas and U active users that operates over a flat and quasi-static Rician channel is considered. The multiuser CDMA system employs the space-time block coding schemes (such as conventional full-diversity $\mathrm{G_2}$, $\mathrm{G_3}$, $\mathrm{H_3}$, $\mathrm{G_4}$, $\mathrm{H_4}$ code [5,8], full-rate X code [7]) to transmit the data. For each user u, the channel gain $\mathrm{h}_{u,ln}$ denotes the channel gain from the nth transmit antenna to the lth receive antenna, which is assumed to be constant over a frame of T symbols and varied from frame to frame. For Rician fading channels, the $\{\mathrm{h}_{u,ln}\}$ are modeled as independent complex Gaussian random variables with respective means m_I and m_Q for the real and imaginary parts and variance of 0.5 per dimension [11, 19], and $\beta = \sum_{n=1}^{N}\sum_{l=1}^{L} |\, h_{u,\mathrm{ln}}\,|^2$ obeys a noncentral chi-square distribution with $2NL$ degrees of freedom. According to reference [19] and changing variable, the probability density function (pdf) of β can be obtained by

$$f(\beta) = (\beta / x^2)^{(NL-1)/2} (2\sigma^2)^{-1} e^{-(x^2+\beta)/(2\sigma^2)} \cdot I_{NL-1}(\sqrt{x^2\beta}/\sigma^2),\ \beta > 0 \quad (1)$$

where $x^2 = NL(m_I^2 + m_Q^2)$ is the noncentrality parameter, $\sigma^2 = 0.5$, and $\mathrm{I_v(x)}$ is the vth-order modified Bessel function of the first kind [20-21].

III. Low-Complexity Multiuser Receiver

In this section, A low-complexity multiuser receiver design for multiuser space-time coded CDMA system is given. For multiuser CDMA system with space-time coding, the block length of space-time code is set equal to Q chip periods. Then according to reference [18], the transmitted signal matrix of user u at qth ($\mathrm{q} = 1,2,\ldots,\mathrm{Q}$) chip period is

$$V_u(q) = D_u C_u(q) \quad (2)$$

where $\mathrm{D_u}$ is a $N \times T$ space-time coding matrix of user u, $\mathrm{C_u(q)}$ is $T \times 1$ spreading code, and $\mathrm{C_u} = [\,\mathrm{C_u}\,(1),\ldots,\mathrm{C_u}\,(\mathrm{Q})]$ corresponds to T normalized spreading codes of length Q used to spread $\mathrm{D_u}$ for user $u\,(u = 1,2,\ldots U)$, here conventional orthogonal Walsh-Hadamard code and quasi-orthogonal Gold code in CDMA system are considered. These different spreading codes for different users are employed as well. Based on the analytical method in [18], obtain the baseband received signal at qth ($q = 1,2,\ldots,\mathrm{Q}$) chip period is obtained as follows

$$y(q) = \sum_{u=1}^{U} \sqrt{\lambda_u} H_u V_u(q) + w(q),\ q = 1,2,\ldots,\mathrm{Q} \quad (3)$$

where $\mathrm{H_u} = [\mathrm{h_u}]_{\mathrm{l,n}}$ is $L \times N$ channel matrix of user u. $\mathrm{w(q)}, \mathrm{q} = 1,\ldots,\mathrm{Q}$ is $L \times 1$ noise vector, whose element $\{\mathrm{w_l(q)}, \mathrm{l} = 1,\ldots, \mathrm{L}, \mathrm{q} = 1,\ldots,\mathrm{Q}\}$ are independent, identically distributed ($i.i.d$) complex Gaussian random variables with zero-mean and unit-variance. $\mathrm{N}\lambda_{\mathrm{u}}$ denotes the average signal-to-noise ratio per receive antenna for user u at the receiver during the transmission of space-time coding matrix $\mathbf{D}_u$ (which corresponds to Q chip periods), this SNR adopts the definition similar to Ref.[18] for comparison consistency.

Substituting (2) into (3), the received signal at qth chip period can be expressed as

$$y(q) = \sum_{u=1}^{U} \sqrt{\lambda_u} H_u D_u C_u(q) + w(q),\ q = 1,2,\ldots,\mathrm{Q} \quad (4)$$

In order to express (4) more compactly, the matrices is defined as: $S_u = \sqrt{\lambda_u} H_u D_u$, $\mathrm{S} = [\mathrm{S_1}, \mathrm{S_2},\ldots,\mathrm{S_U}]$, $\mathrm{C_u} = [\,\mathrm{C_u}\,(1),\ldots,\mathrm{C_u}\,(\mathrm{Q})]$, $\mathrm{C} = [\mathrm{C_1^T},\ldots,\mathrm{C_U^T}]^{\mathrm{T}}$, $\mathrm{Y} = [\mathrm{y(1)},\ldots,\mathrm{y\,(Q)}]$, and $\mathrm{W} = [\mathrm{w(1)},\ldots,\mathrm{w(Q)}]$. Thus, (4) is changed to

$$Y = \sum_{u=1}^{U} S_u C_u + W = SC + W \quad (5)$$

Then according to reference [22], obtain the ML estimate of S conditioned on $\{\mathrm{H_u}\}$ and $\{\mathrm{D_u}\}$ is obtained as

$$\hat{S} = YC^H (CC^H)^{-1} = S + WC^H (CC^H)^{-1} \quad (6)$$

Here, the Moore-Penrose inverse matrix $\mathrm{C^H}\ (\mathrm{CC^H})^{-1}$ can be expressed as a multiuser decorrelator [18, 22], and thus the ML estimate $\hat{S}$ is an effective output of the decorrelator with the input being the received data Y. By this decorrelator, the multiuser interference is cancelled, and the detection of different users is decoupled. Based

on the block structure of S , the ML estimate $\hat{S}_u$ of S_u can be easily achieved. While for user u , all data information on the transmitted code matrix $\mathbf{D}_u$ is contained in S_u . Hence, the code matrix and corresponding information symbols via the achieved $\hat{S}_u$ is evaluated. According to the definition of S_u , Assuming that $\hat{S}_u = [\hat{s}_{u,1}^T, \hat{s}_{u,2}^T, ..., \hat{s}_{u,L}^T]^T$, where $\hat{s}_{u,l}$ is a $1 \times T$ row vector. Thus when G_3 code scheme is employed, T=8. Considering that S_u has the receiver signal form similar to the conventional STBC in single user scenario [7-8], the simple decoding scheme for the space-time coded CDMA system with G_3 code after performing multiuser decorrelation is obtained by utilizing the MRC method and complex orthogonality of STBC, i.e.,

$$\hat{d}_{u1} = \arg\min_{d_{u1}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l1} h_{u,l1}^* + \hat{s}_{u,l2} h_{u,l2}^* + \hat{s}_{u,l3} h_{u,l3}^* + \hat{s}_{u,l5} h_{u,l1}^* + \hat{s}_{u,l6}^* h_{u,l2} + \hat{s}_{u,l7}^* h_{u,l3} - 2\sqrt{\lambda_u} \sum_{n=1}^{3} |h_{u,\ln}|^2 d_{u1}) \|^2$$

$$\hat{d}_{u2} = \arg\min_{d_{u2}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l1} h_{u,l2}^* - \hat{s}_{u,l2} h_{u,l1}^* + \hat{s}_{u,l4} h_{u,l3}^* + \hat{s}_{u,l3} h_{u,l3}^* + \hat{s}_{u,l5}^* h_{u,l1} + \hat{s}_{u,l6}^* h_{u,l2} + \hat{s}_{u,l7}^* h_{u,l3} - 2\sqrt{\lambda_u} \sum_{n=1}^{3} |h_{u,\ln}|^2 d_{u2}) \|^2$$

$$\hat{d}_{u3} = \arg\min_{d_{u3}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l1} h_{u,l3}^* - \hat{s}_{u,l3} h_{u,l1}^* - \hat{s}_{u,l4} h_{u,l2}^* + \hat{s}_{u,l5} h_{u,l3}^* - \hat{s}_{u,l7}^* h_{u,l1} - \hat{s}_{u,l8}^* h_{u,l2} - 2\sqrt{\lambda_u} \sum_{n=1}^{3} |h_{u,\ln}|^2 d_{u3}) \|^2$$

$$\hat{d}_{u4} = \arg\min_{d_{u4}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l3} h_{u,l2}^* - \hat{s}_{u,l2} h_{u,l3}^* - \hat{s}_{u,l4} h_{u,l1}^* - \hat{s}_{u,l6} h_{u,l3}^* + \hat{s}_{u,l7}^* h_{u,l2} - \hat{s}_{u,l8}^* h_{u,l1} - 2\sqrt{\lambda_u} \sum_{n=1}^{3} |h_{u,\ln}|^2 d_{u4}) \|^2 \quad (7)$$

When G_2 code [5] is used, T=2, $\hat{S}_u = [\hat{s}_{u,1}^T, \hat{s}_{u,2}^T]^T$, the corresponding simple decoding scheme can be given by

$$\hat{d}_{u1} = \arg\min_{d_{u1}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l1} h_{u,l1}^* + \hat{s}_{u,l2}^* h_{u,l2}) \|^2$$

$$\hat{d}_{u2} = \arg\min_{d_{u2}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l1} h_{u,l2}^* - \hat{s}_{u,l2}^* h_{u,l1}) \|^2 \quad (8)$$

Besides, when X code [7] is employed, T=4, $\hat{S}_u = [\hat{s}_{u,1}^T, \hat{s}_{u,2}^T, \hat{s}_{u,3}^T, \hat{s}_{u,4}^T]^T$, the simple decoding scheme can be given by can be attained as

$$\hat{d}_{u1} = \arg\min_{d_{u1}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l1} h_{u,l1}^* - \hat{s}_{u,l2}^* h_{u,l2}) \|^2$$

$$\hat{d}_{u2} = \arg\min_{d_{u2}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l1} h_{u,l2}^* + \hat{s}_{u,l2}^* h_{u,l1}) \|^2$$

$$\hat{d}_{u3} = \arg\min_{d_{u3}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l3} h_{u,l2}^* + \hat{s}_{u,l4}^* h_{u,l3}) \|^2$$

$$\hat{d}_{u4} = \arg\min_{d_{u4}\in\Psi} \| \sum_{l=1}^{L} (\hat{s}_{u,l3} h_{u,l3}^* - \hat{s}_{u,l4}^* h_{u,l2}) \|^2 \quad (9)$$

From (7) and (8) as well as (9), it is observed that the developed decoding scheme has linear complexity. For Ref.[18], its receiver decoding schemes with coherent detection (i.e. (44) and (45) in [18]) are shown as follows:

1) For general spreading codes:

$$\hat{D}_u = \arg\min_{\{d_{u,1},...,d_{u,p}\}\in\psi} \{vec^H(\hat{S}_u - \sqrt{\lambda_u} H_u D_u) \Phi_k^{-1} \cdot vec(\hat{S}_u - \sqrt{\lambda_u} H_u D_u)\} \quad (10)$$

2) For orthogonal spreading codes:

$$\hat{D}_u = \arg\min_{\{d_{u,1},...,d_{u,p}\}\in\psi} \| \hat{S}_u - \sqrt{\lambda_u} H_u D_u \|_F^2 \quad (11)$$

From the above two equations, it can be seen that the decoding scheme in [18] has exponential complexity. Namely, if Ψ is a constellation consists of M symbols, the search times that need to obtain the transmitted P symbols is M^P . Thus, when M and P become larger, the complexity will be much higher. As a result, the implementation complexity of the system will be increased significantly. While for our scheme, the needed search times are MP only. Based on this, the complexity comparison between the developed scheme and the existing scheme [18] in Table.1 is given. From Table 1, it can be seen that the proposed scheme has lower complexity than the existing scheme.

TABLE I. COMPARISON OF COMPLEXITY

Scheme	QPSK (M=4, P=2)	8PSK (M=8, P=2)	16QAM (M=16, P=3)	16QAM (M=16, P=4)
Existing scheme	16	64	4096	65536
Developed scheme	8	16	48	64

IV. SYSTEM PERFORMANCE ANALYSIS IN RICIAN FADING CHANNEL

In this section, the error performance analysis of space-time coded CDMA system in Rician fading channel is given, and the closed-form expressions of average BER and SER is derived.

Let $\tilde{W} = WC^H (CC^H)^{-1}$ and W_u be the $L \times T$ submatrix of $\tilde{W}$ consisting of the columns starting from $(u\text{-}1)T+1$ to uT , then $\tilde{W} = [W_1, ..., W_U]$. According to reference [18], the covariance matrix of vec($\tilde{W}$) is expressed as

$$E\{vec(\tilde{W}) vec^H(\tilde{W})\} = [(CC^H)^{-1}]^T \otimes I_L \quad (12)$$

With Eq.(12), the matrix $V_W = E\{\tilde{W}^H \tilde{W}^H\}$ is calculated as follows:

$$V_W = (CC^H)^{-1} \quad (13)$$

Let $\tilde{C}$ be $(\mathrm{CC}^{\mathrm{H}})^{-1}$, then with (12) and (13), the following equations can be obtained.

$$V_{W_u} = E\{W_u^H W_u\} = \tilde{C}_{(u-1)T+1:uT,(u-1)T+1:uT},\ \mathrm{u}=1,\ldots,\mathrm{U} \qquad (14)$$

When the orthogonal Walsh-Hadamard codes are used for spreading codes, the matrix $\tilde{C}$ will be identity matrix $\mathbf{I}_{\mathrm{TU}}$, and accordingly, V_{W_u} is also identity matrix (i.e. $\mathbf{I}_{\mathrm{T}}$). While the quasi-orthogonal Gold codes are employed for spreading codes, $\tilde{C}$ will be a symmetric Toeplitz matrix with first row being $[a,u,u,...u]$, where (UT-1)μ is included. Thus, V_{W_u} is also a symmetric Toeplitz matrix with first row being $[a,u,u,...u]$, where (T-1)μ is included.

According to the above analysis, the elements of $\tilde{W}$ are complex Gaussians variables with mean zero. So the elements $\{w_{u,lt}\}$ of $\mathrm{W_u}$ $(\mathrm{u}=1,\ldots,\mathrm{U})$ are also complex Gaussians variables with mean zero and variance unit for orthogonal spreading code case, while in the case of quasi-orthogonal spreading code, their covariance is a or μ. Namely, $E\{|w_{u,lt}|^2\}=a$ and $E\{w_{u,lt}w^*_{u,l't'}\}=\mu$, $l\neq l'$ or $t\neq t'$. Using Eq.(6) and the definition of S_u, the effective output of the decorrelator of user u can be written as:

$$\hat{S}_u = S_u + W_u = \sqrt{\lambda_u}H_u D_u + W_u,\ u=1,2,\ldots,U. \qquad (15)$$

A. Orthogonal Walsh-Hadamard Code Case

When the orthogonal Walsh-Hadamard code is used for spreading code, the covariance of $\mathrm{W_u}$ will be identity matrix, and its elements are *i.i.d* . complex Gaussian variables with mean zero and variance unit. Based on this, utilizing the orthogonality of space-time block coding, the effective SNR for user u at the receiver is given by

$$\gamma = \lambda_u \sum_{l=1}^{L}\sum_{n=1}^{N}|h_{u,ln}|^2/R = \lambda_u \|\mathbf{H}_u\|_F^2/R = \lambda_u \beta/R$$

$$\gamma = \lambda_u \sum_{l=1}^{L}\sum_{n=1}^{N}|h_{u,\mathrm{ln}}|^2/R = \lambda_u \| \qquad (16)$$

Using (1) and changing variable, the pdf of γ in (16) with Rician factor $K=(m_I^2+m_Q^2)/(2\sigma^2)$ can be obtained as

$$f(\gamma) = \left(\frac{R}{\lambda_u}\right)^{(NL+1)/2}\left(\frac{\gamma}{NLK}\right)^{(NL-1)/2}\cdot$$

$$e^{-NLK-R\gamma/\lambda_u} I_{NL-1}\left(2\sqrt{\frac{RNLK}{\lambda_u}\gamma}\right),\ \gamma\geq 0 \qquad (17)$$

The cumulative distribution function (cdf) of γ can be expressed as

$$F(\gamma) = 1 - Q_{NL}(\sqrt{2NLK}, \sqrt{2R\gamma/\lambda_u}), \qquad (18)$$

where $Q_m(\,,\,)$ is the generalized Marcum Q-function [19, 21]. With Eq.(17), the pdf of γ for Rayleigh fading channel can be obtained by setting $K=0$.

According to Refs.[19-20, 23], the BER of coherent M-ary QAM (MQAM) with Gray coding over an Additive White Gaussian Noise (AWGN) channel is given as

$$\mathrm{P}_{b,q}(\gamma) = \sum_j \zeta_j \,\mathrm{erfc}(\sqrt{k_j\gamma}) \qquad (19)$$

where M is the constellation size, $\mathrm{erfc}(\cdot)$ is the complementary error function, ζ_j and k_j are constants which depend on M, and the values of the constant sets $\{\zeta_j, k_j\}$ for MQAM can be found in [19]. Besides, the high-accuracy approximate BER for MPSK with Gray coding over AWGN channel is given as [23]

$$\mathrm{P}_{b,p}(\gamma) \cong \sum_{j=1}^{2}\mathrm{erfc}(\sqrt{k_j\gamma}) \qquad (20)$$

where the $\{\zeta_j, k_j\}$ are given by $\{(1/\log_2^M, \sin^2(\pi/M))$, $(1/\log_2^M, \sin^2(3\pi/M))\}$ for MPSK.

By using Eqs.(17)-(20), the average BER for multiuser space-time coded CDMA system with MQAM or MPSK modulation is evaluated as follows

$$\bar{P}_b = \sum_j \zeta_j \int_0^{+\infty}\mathrm{erfc}(\sqrt{k_j\gamma})f(\gamma)d\gamma = \sum_j \zeta_j G(k_j) \qquad (21)$$

where $G(\alpha)$ denotes the integration in (21) defined as

$$G(\alpha) = \int_0^{+\infty} f(\gamma)\,\mathrm{erfc}(\sqrt{a\gamma})d\gamma,\ \alpha>0. \qquad (22)$$

Substituting (17) and (18) into (22) gives

$$G(a) = 1-\sqrt{a/\pi}\int_0^{\infty} Q_{NL}(\sqrt{2NLK}, \sqrt{2R\gamma/\lambda_u})\gamma^{-1/2}e^{-a\gamma}d\gamma$$

$$= [1-\sqrt{v/\pi}\int_0^{\infty} Q_1(\sqrt{2NLK}, \sqrt{2R\gamma/\lambda_u})\gamma^{-1/2}e^{-a\gamma}d\gamma] -$$

$$\sqrt{\frac{a}{\pi}}e^{-NLK}\sum_{n=1}^{NL-1}\left(\frac{R}{\lambda_u NLK}\right)^{n/2}\cdot$$

$$\int_0^{\infty}\gamma^{(n-1)/2}e^{-(R/\lambda_u+a)\gamma} I_n\left(2\sqrt{\frac{RNLK}{\lambda_u}\gamma}\right)d\gamma = g_1 - g_2 \qquad (23)$$

where the equality

$$Q_m(a,b) = Q_1(a,b) + e^{-(a^2+b^2)/2}\sum_{i=1}^{m-1}(b/a)^i I_i(ab)$$ is

utilized. Using change of variables and the results of Appendix I in [24], $\mathrm{g_1}$ in Eq.(23) can be expressed as

$$g_1 = 1-\sqrt{2/\pi}\int_0^{\infty} Q_1(\sqrt{2NLK}, \sqrt{R/(a\lambda_u)}t)e^{-t^2/2}dt$$

$$= 2Q_1(v,\bar{w}) - [1+\sqrt{\lambda_u a/(\lambda_u a+R)}]\cdot$$

$$\exp[-(v^2+\bar{w}^2)/2]I_0(v\bar{w}) \qquad (24)$$

where

$$v=\sqrt{\frac{NLK[R/2+\lambda_u a-\sqrt{\lambda_u a(R+\lambda_u a)}]}{R+\lambda_u a}},$$

$$\bar{w}=\sqrt{\frac{NLK[R/2+\lambda_u a+\sqrt{\lambda_u a(R+\lambda_u a)}]}{R+\lambda_u a}}.$$

According to Eq.(23), g_2 is written as:

$$g2=\sqrt{\frac{a}{\pi}}e^{-NLK}\sum_{n=1}^{NL-1}(\frac{R}{\lambda_u NLK})^{n/2}.$$

$$\int_0^{\infty}\gamma^{(n-1)/2}e^{-(R/\lambda_u+a)\gamma}\ I_n(2\sqrt{\frac{RNLK}{\lambda_u}\gamma})d\gamma=\frac{\exp(-NLK)}{\sqrt{\pi}}\cdot$$

$$\sum_{n=1}^{NL-1}\frac{\Gamma(n+1/2)}{\Gamma(n+1)}\frac{R^n(a\lambda_u)^{1/2}}{(a\lambda_u+R)^{n+1/2}}F_1(n+\frac{1}{2};n+1;\frac{RLKN}{a\lambda_u+R}) \quad (25)$$

The above derivation utilizes Eq.(6.643), Eq.(9.220) and Eq.(9.215) in reference [21] .

With Eqs.(24) and (25), $G(a)$ in (21) can be expressed as

$$G(a)=2Q_1(v,\bar{w})-[1+\sqrt{a\lambda_u/(a\lambda_u+R)}]\cdot$$
$$\exp[-(v^2+\bar{w}^2)/2]I_0(v\bar{w})-\frac{\exp(-NLK)}{\sqrt{\pi}}\cdot$$

$$\sum_{n=1}^{NL-1}\frac{\Gamma(n+1/2)}{\Gamma(n+1)}\frac{R^n(a\lambda_u)^{1/2}}{(a\lambda_u+R)^{n+1/2}}F_1(n+\frac{1}{2};n+1;\frac{RLKN}{a\lambda_u+R}) \quad (26)$$

where v and $\bar{w}$ are defined in (24) and F $_1$ (x,y;z) is the confluent hypergeometric function [21]. Substituting (26) into (21) yields

$$\bar{P}_b=\sum_j\zeta_j\{2Q_1(v,\bar{w})-[1+\sqrt{k_j\lambda_u/(k_j\lambda_u+R)}]\cdot$$
$$\exp[-(v^2+\bar{w}^2)/2]I_0(v\bar{w})-\frac{\exp(-NLK)}{\sqrt{\pi}}\cdot$$
$$\sum_{n=1}^{NL-1}\frac{\Gamma(n+1/2)}{\Gamma(n+1)}\frac{R^n(k_j\lambda_u)^{1/2}}{(k_j\lambda_u+R)^{n+1/2}}F_1(n+\frac{1}{2};n+1;\frac{RLKN}{k_j\lambda_u+R})\} \quad (27)$$

Eq.(27) is an accurate BER expression for multiuser space-time coded CDMA system with MQAM, and it is also a high-accuracy approximate BER expression for multiuser space-time coded CDMA system with MPSK modulation, which is shown to match the simulation well.

According to Refs. [19-20], utilizing (17) and (26), a closed-form approximate expression of average SER of multiuser space-time coded CDMA system with MPSK modulation is obtained as:

$$\bar{P}_{s,p}\cong\int_0^{+\infty}f(\gamma)\mathrm{erfc}(\sqrt{\gamma})\sin(\pi/M))d\rho=G(\sin^2(\pi/M)) \quad (28)$$

Similarly, the average SER of the system with MQAM is evaluated as

$$\bar{P}_{s,q}=1-[1-(1-1/\sqrt{M})G(1.5/(M-1))]^2 \quad (29)$$

Equation (29) is accurate closed-form expressions of the average SER of multiuser space-time coded CDMA with MQAM in Rician fading channels.

B. Quasi-orthogonal Gold Code Case

In this subsection, the BER and SER performance of the system is studied when quasi-orthogonal Gold code is used for spreading code. Under this scenario, the covariance of W_u will be not identity matrix. For the simplicity of analysis, the G_3 code is taken as an example to analyze the corresponding system performance. When G_3 code is employed, the decision metrics for the detection of the transmitted symbols $\{\mathrm{d}_{\mathrm{u,p}}, p=1,\ldots,4\}$ according to (7) is evaluated. Due to symmetry considerations, the symbols $\mathrm{d}_{\mathrm{u},1}$, $\mathrm{d}_{\mathrm{u},2}$, $\mathrm{d}_{\mathrm{u},3}$, $\mathrm{d}_{\mathrm{u},4}$ have the same error probability. So just one of decision metrics and the corresponding effective SNR is analyzed. Without loss of generality, symbol $\mathrm{d}_{\mathrm{u},1}$ is considered, then with (7) and (15), the corresponding decision metrics is

$$z=2\sqrt{\lambda_u}\sum_{l=1}^{L}(|h_{u,l1}|^2+|h_{u,l2}|^2+|h_{u,l3}|^2)d_{u1}+w' \quad (30)$$

where

$$w'=\sum_{l=1}^{L}w_{u,l1}h_{u,l1}^*+w_{u,l2}h_{u,l2}^*+w_{u,l3}h_{u,l3}^*+w_{u,l5}^*h_{u,l1}+$$

$w_{u,l6}^*h_{u,l2}+w_{u,l7}^*h_{u,l3}$ is an equivalent noise. According to the previous analysis, it will be a complex Gaussian random variable with mean zero, and the variance is

$$\mathrm{var}\{w'\}=2a\sum_{l=1}^{L}[\sum_{n=1}^{3}|h_{u,ln}|^2+(h_{u,l1}^*h_{u,l2}+h_{u,l2}^*h_{u,l1}+$$
$$h_{u,l1}^*h_{u,l3}+h_{u,l3}^*h_{u,l1}+h_{u,l3}^*h_{u,l2}+h_{u,l2}^*h_{u,l3})\mu]$$
$$\le 2(a+\mu)\sum_{l=1}^{L}\sum_{n=1}^{3}|h_{u,ln}|^2 \quad (31)$$

where the inequality $h_{u,ln}h_{u,lm}^*+h_{u,lm}h_{u,ln}^*\le|h_{u,ln}|^2+|h_{u,lm}|^2$ is utilized. Thus the lower bound of effective SNR γ by $\gamma_l=R^{-1}[\rho_u/(a+\mu)]\|H_u\|_F^2=R^{-1}\lambda_{ul}\|H_u\|_F^2$ can be obtained by using (30) and (31).

$$\lambda_{ul}=\lambda_u/(a+\mu) \quad (32)$$

It is well known that the CDMA system performance with quasi-orthogonal spreading code is worse than that with orthogonal spreading code. Namely, the BER of the former is higher than that of the latter, and the corresponding effective SNR (denoted by γ_{no}) is lower than the latter γ_o (i.e. γ in (16), is effective SNR for the orthogonal spreading code case). Hence, γ_o can be regarded as the upper bound of γ_{no}. Thus: $\gamma_l\le\gamma_{no}<\gamma_o$. Moreover, μ is small and a is slightly larger than 1 in general, and thus γ_l in (32) is indeed lower than γ_o in

(16). Hence, the upper bound and lower bound of γ_{no} exist. To obtain the approximate BER or SER expression, the mean value between the upper bound and lower bound of γ_{no} is taken as its approximate value, that is,

$$\bar{\gamma}_{no} = (\gamma_l + \gamma_o)/2 = R^{-1} \| \mathbf{H}_u \|_F^2 \ (\lambda_{ul} + \lambda_u)/2$$
$$R^{-1} \| \mathbf{H}_u \|_F^2 \ \bar{\lambda}_{no} \quad (33)$$

is regarded as an approximate value of γ_{no}, and $\bar{\lambda}_{no} = (\lambda_{ul} + \lambda_u)/2 = [1 + (a+\mu)^{-1}]\lambda_u / 2$ is an approximate value of effective SNR accordingly. By substituting γ_u with $\bar{\lambda}_{no}$, and utilizing (27), the closed-form expression of average BER of the multiuser space-time coded CDMA system with quasi-orthogonal spreading code can be given by

$$\bar{P}_b \cong \sum_j \zeta_j \{2Q_1(v,\bar{w}) - [1 + \sqrt{k_j \bar{\lambda}_{no} / (k_j \bar{\lambda}_{no} + R)}] \cdot$$
$$\exp[-(v^2 + \bar{w}^2)/2] I_0(\mu\nu) - \frac{\exp(-NLK)}{\sqrt{\pi}} \cdot$$
$$\sum_{n=1}^{NL-1} \frac{\Gamma(n+1/2)}{\Gamma(n+1)} \frac{R^n (k_j \bar{\lambda}_{no})^{1/2}}{(k_j \bar{\lambda}_{no} + R)^{n+1/2}} F_1(n+\frac{1}{2}; n+1; \frac{RLKN}{k_j \bar{\lambda}_{no} + R})\} \quad (34)$$

By substituting λ_u with $\bar{\lambda}_{no}$ into (26), and then using (28) and (29), the closed-form approximate expressions of average SER of the multiuser space-time coded CDMA system with MPSK and MQAM for quasi-orthogonal spreading code case is obtained as follows.

$$\bar{P}_{s,p} \cong \tilde{G}(\sin^2(\pi / M)) \quad (35)$$

and

$$\bar{P}_{s,q} \cong 1 - [1 - (1 - 1/\sqrt{M}) \tilde{G}(1.5/(M-1))]^2 \quad (36)$$

where :

$$\tilde{G}(a) = 2Q_1(v,\bar{w}) - [1 + \sqrt{a\bar{\lambda}_{no} / (a\bar{\lambda}_{no} + R)}] \cdot$$
$$\exp[-(v^2 + \bar{w}^2)/2] I_0(v\bar{w}) - \frac{\exp(-NLK)}{\sqrt{\pi}} \cdot$$
$$\sum_{n=1}^{NL-1} \frac{\Gamma(n+1/2)}{\Gamma(n+1)} \frac{R^n (a\bar{\lambda}_{no})^{1/2}}{(a\bar{\lambda}_{no} + R)^{n+1/2}} F_1(n+\frac{1}{2}; n+1; \frac{RLKN}{a\bar{\lambda}_{no} + R})\}$$

Based on the above analysis, the closed-form expression of average BER/SER of multiuser CDMA system with other space-time codes (such as H_3, H_4, G_4, G_2, X code) can be easily obtained.

V. Simulation Results and Theoretical Evaluation

In this section, the effectiveness of the developed scheme and the derived theoretical expressions by computer simulation for different space-time coded CDMA systems are evaluated. The G_2, G_3, H_3, G_4, H_4 codes are used for evaluation. In simulation, the channel is assumed to be quasi-static flat Rician fading. Every data frame includes 480 information bits, and Gray mapping of the bits to symbol is employed. The Monte-Carlo method is employed for simulation. For different STBCs, the different modulation modes to maintain the same the transmission rate is employed. 6 active users are considered in the system, and conventional Gold codes (P=63) and Walsh-Hadamard (W-H) code (P=64) are used for spreading code, respectively. The simulation results are shown in Fig.1-Fig.4. In these figures, 'G_2-CDMA', 'G_3-CDMA', 'H_3-CDMA', 'G_4-CDMA' and 'H_4-CDMA' denote the CDMA system with G_2, G_3, H_3, G_4 and H_4 code, respectively. 'scheme 1' and 'scheme 2' represent the existing decoding scheme in [18] and our improved scheme, respectively. The average BER and SER are obtained by averaging over 10^7 Monte-Carlo realizations, and thus the results can be accurate enough to reflect the actual values.

Fig. 1 shows the BER versus SNR for different space-time coded CDMA systems with the Rician factor K=0, 5dB, where single receive antenna (1Rx) is considered, and Gold code is used for spreading code. For G_2-CDMA, 8PSK modulation is employed, while for H_3-CDMA, 16QAM is used instead. Thus, the overall transmission rate is 3 bit/s/Hz. From Fig. 1, it can be seen that H_3-CDMA performs better than G_2-CDMA due to its larger diversity gain. Moreover, it is observed that multiuser space-time coded CDMA system with the developed scheme 2 has almost the same performance as multiuser space-time coded CDMA system with the existing scheme 1 due to better approximation and full utilization of complex orthogonality of space-time block coding, but the implement complexity of scheme 2 is much lower than scheme 1 because of the linear decoding. It means that our scheme 2 is valid and makes a good tradeoff between performance and complexity. Besides, the average BER in Rician fading channel is obviously lower than that in Rayleigh fading channel ($K = 0$) due to the presence of direct path. In the following simulation, the scheme 2 will be employed for the system evaluation due to its simplicity.

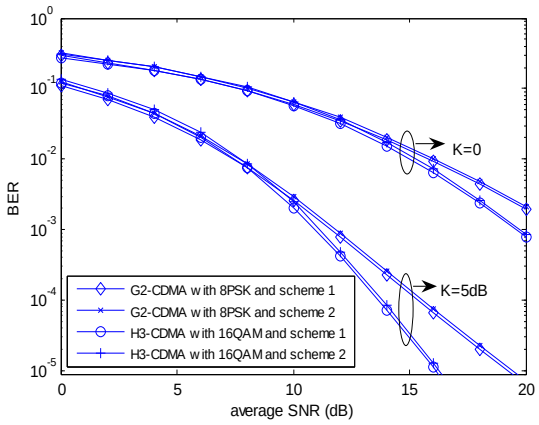


Figure 1. BER versus SNR for space-time coded CDMA systems with one receive antenna.

In Fig. 2, the theoretical average BER/SER and simulation results of different space-time coded CDMA systems with 1Rx and orthogonal W-H code are given.

The space-time codes G_2 and G_3 are considered, and the Rician factor K=6dB. Regarding modulation, 4QAM is employed for G_2-CDMA, whereas 16QAM is used for G_3-CDMA, resulting in the overall transmission rate of 2bit/s/Hz. The (27) and (29) are employed for computing the theoretical BER and SER of the system, respectively. It is found that the theoretical BER and SER are in good agreement with the simulated values. Moreover, G_3-CDMA system outperforms G_2-CDMA system due to greater diversity. The above results show that the derived theoretical formulae for space-time coded CDMA system with orthogonal W-H code are valid for performance evaluation.

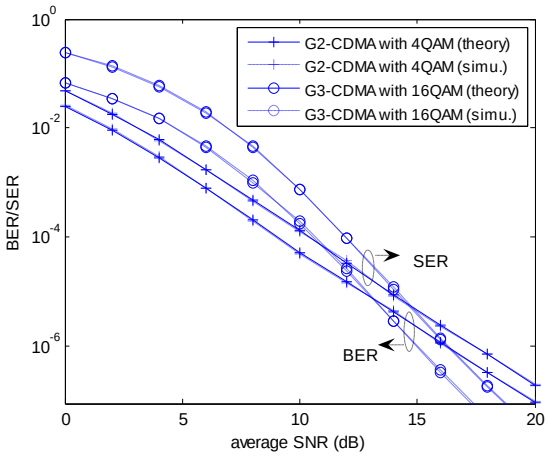


Figure 2. BER/SER versus SNR for space-time coded CDMA systems with one receive antenna (K=6dB)

In Fig. 3, it plots the theoretical average BER and simulation results of space-time coded CDMA systems with Gold code and two receive antenna, where G_2 and H_4 code are considered, and Rician factor K=6 dB. For G_2-CDMA, 8PSK modulation is used, while for H_4-CDMA, 16QAM modulation is employed. Thus, the overall transmission rate is 3 bit/s/Hz. The (34) is employed for the theoretical BER calculation of the system. The SER performance expressions (35) and (36) are used for MPSK and MQAM, respectively. From Fig.3, it can be seen that the theoretical BER and SER are very close to the corresponding simulation results. Besides, it is found that H_4-CDMA system outperforms G_2-CDMA system due to high diversity gain. The above results show the derived BER and SER expressions for space-time coded CDMA system with Gold code are also effective for performance evaluation.

VI. Conclusions

The error performance of multiuser space-time coded CDMA systems over Rician fading channel is investigated. A simple and effective multiuser receiver scheme is developed for space-time coded CDMA systems. The scheme can effectively suppress MUI via multiuser detection method, and greatly reduce the high decoding complexity of the existing scheme. According to the performance analysis of the system, and using the mathematical derivation, accurate and approximate closed-form expressions of BER and SER are obtained, respectively. With these expressions, the error performance of space-time coded CDMA can be effectively assessed. Simulation results show that the derived theoretical BER and SER expressions are in good agreement with the corresponding simulation results. The developed receiver scheme can obtain almost the same performance as the existing scheme, and it has lower complexity than the latter.

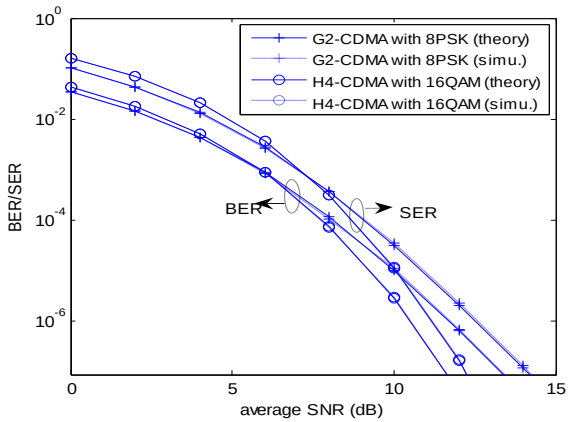


Figure 3. BER/SER versus SNR for space-time coded CDMA systems with two receive antennas (K=6dB)

Acknowledgment

The authors would like to thank the anonymous reviewer for his valuable comments. This research was supported in part a grant from the national natural science foundation of China(GrantNo. 61203056), Foundation of Huaian industrial projects (GrantNo. HAG2013064), and foundation of Huaiyin Institute of Technology (GrantNo. HGB1202).

References

[1] Chae, C.-B., Forenza, A., W.Heath, R., McKay, M. and Collings, I., Adaptive MIMO transmission techniques for broadband wireless communication systems. *IEEE Commun. Magazine*, 48 (2010), 112-118.

[2] X. Hu, Z. Chen, and F. Yin, "Impulsive Noise Cancellation for MIMO Power Line Communications," *Journal of Communications*, vol. 9, no. 3, pp. 241-247, 2014.

[3] Siam, M.Z., Krunz, M., An overview of MIMO-oriented channel access in wireless networks. *IEEE Wireless Communications*, 15(2008), 63-69.

[4] X. Shao and C. H. Slump, "Opportunistic Error Correction for MIMO-OFDM: From Theory to Practice," Journal of Communications, vol. 8, no. 9, pp. 540-549, 2013.

[5] Tarokh, V., Jafarkhani, H. and Calderbank, A.R., Space-time block codes from orthogonal designs. *IEEE Trans. Inform. Theory*, 45 (1999), 1456-1467.

[6] M.M. KAMRUZ ZAMAN and Li Hao, "Performance of Turbo-SISO, Turbo-SIMO, Turbo-MISO and Turbo-MIMO system using STBC," *Journal of Communications*, vol. 6, no.8, pp.633-639, 2011.

[7] Yu Xiangbin, Xu Dazhuan and Bi Guangguo, Full-rate complex orthogonal space-time block code for multiple antennas. *Wireless Pers. Commun.*, 40 (2007), 81-89.

[8] Tarokh, V., Jafarkhani, H. and Calderbank, A.R., Space-time block coding for wireless communications: performance results. *IEEE J. Select. Areas Commun*. 17(1999), 451-460.
[9] Larsson, E.G. and Stoica, P., *Space-time block coding for wireless communications*. Cambridge University Press, 2003.
[10] J. Gao and Y. Bai, "Quasi-Orthogonal Space-Time Block Code with Givens Rotation for SC-FDE Transmission in Frequency Selective Fading Channels," *Journal of Communications*, vol. 8, no. 12, pp. 832-838, 2013.
[11] Zhang, H. Gulliver, T.A., Capacity and error probability analysis for orthogonal space-time block codes over fading channels. *IEEE Trans. Wireless Commun*., 4 (2005) 808-819.
[12] Shabazpanahi, S., Beheshti, M., Gershmann, A.B., et al., Miniumum variance linear receivers for multiaccess MIMO wireless systems with space-time block coding. IEEE Trans. Signal Process. 52 (2004), 3306-3312.
[13] Sacramento, A. and Hamouda, W., Performance of multiuser-coded CDMA systems with transmit diversity over Nakagami-m fading channels. IEEE Trans.Veh.Technol., 58 (2009), 2279-2287.
[14] Seo, B., Ahn, W.-G., Jeong, C. and Kim, H.-M., Fast convergent LMS adaptive receiver for MC-CDMA systems with space-time block coding. IEEE Communication Lett., 14 (2010), 737-739.
[15] Z. Li and M. Latva-aho, "Performance of space-time block coded MC-CDMA in Nakagami fading channels," *IEE Electronics Letters*, vol. 39, no. 2, pp. 222-224, 2003.
[16] Zhang Xiaofei, Feng Gaopeng, Gao Xin, Xu Dazhuan, Blind multiuser detection for MC-CDMA with antenna array. Computers and Electrical Engineer*ing*, 36 (2010), 160-168.
[17] Qi, S. Aissa, A. Maaref, "Cross-Layer Design for MIMO Orthogonal STBC Systems Over Spatially-Correlated and Keyhole Nakagami-m Fading Channels," Wiley Journal Wireless Communications and Mobile Computing, in press; published online Aug. 2009.
[18] Li, H. and Li, J., Differential and coherent decorrelating multiuser receivers for space-time coded CDMA systems. *IEEE Trans. Signal Process.*, 50 (2002), 2529-2536.
[19] Proakis, J.G., *Digital communications*, 5th ed. New York: McGraw-Hill, 2007.
[20] Simon, M.K. and Alouini, M.S., *Digital communication over fading channels: a unified approach to performance analysis.* New York: Wiley, 2000.
[21] Gradshteyn, I.S. and Ryzhik, I.M., *Table of integrals, series, and products*. 7th ed. San Diego, CA: Academic, 2007.
[22] Verdu, S., *Multiuser detection*. Cambridge, U.K: Cambridge university press, 1998.
[23] Lu, J., Letaief, K.B., Chuang, J.C.-I., *et al*, M-PSK and M-QAM BER computation using signal-space concepts, *IEEE Trans. on Commun*., 47 (1999), 181-184.
[24] Lindsey, W.C., Error probabilities for Rician fading multichannel reception of binary and n-ary signals. *IEEE Trans. Inf. Theory*, 10 (1964), 339-350.

Dingli Yang received his M.S. degree in electronic and information engineering from Southeast University, China, in June 2006. His current research interest includes communication, digital signal processing, image processing.

Qiuchan Bai received his M.S. degree in electronic and information engineering from Northwestern polytechnical University, China, in June 2006.His current research interest includes image processing, and pattern recognition.

Yulin Zhang received his Ph.D. degree in communication and control engineering, from Jiangnan University, China, in 2010. His current research interest includes communication, pattern recognition.

Rendong Ji received his M.S. degree in electronic and information engineering from Qufu Normal University, China, in June 2006. His current research interest includes digital signal processing. Now he is pursuing a Ph.D in Nanjing University of Aeronautics and Astronautics.

Yazhou Li received his M.S. degree in electronic and information engineering from Chongqing University, China, in June 2008. His current research interest includes communication, image processing.

Yudong Yang received his M.S. degree in school of information science and engineering from Southeast University, China, in 2004, and received his Ph.D. degree in School of Electronic and Optical Engineer from Nanjing University of Science & Technology, China, in 2012. His current research interest includes communication, pattern recognition.

Detecting Access Point Spoofing Attacks Using Partitioning-based Clustering

Nazrul M. Ahmad*, Anang Hudaya Muhamad Amin, and Subarmaniam Kannan
Thundercloud Research Lab, Faculty of Information Science & Technology (FIST), Multimedia University (MMU),
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
*Corresponding author, Email: {nazrul.muhaimin, anang.amin, subar.kannan}@mmu.edu.my

Mohd Faizal Abdollah and Robiah Yusof
Faculty of Information and Communication Technology (FTMK), University Teknikal Malaysia Melaka (UTeM),
76100 Durian Tunggal, Melaka, Malaysia
Emil: {faizalabdollah, robiah}@utem.edu.my

***Abstract*—The impersonation of wireless Access Point (AP) poses an unprecedented number of threats that can compromise a wireless client's identity, personal data, and network integrity. The AP impersonation attack is conducted by establishing rogue AP with spoofed Service Set Identifier (SSID) and MAC address same as the target legitimate AP. Since these identities can be easily forged, there is no identifier can be used to identify the legitimate AP. Due to strong correlation between the AP signal strength and the distance, in this paper, we propose a client-centric AP spoofing detection framework by exploiting the statistical relationship of signal strength from the legitimate and rogue APs. We show the relationship between the signals can be determined by using two classical partitioning-based clustering methods, K-means and K-medoids analysis. The experimental results show that both analysis methods can achieve over 90% detection rate.**

***Index Terms*—Spoofing Attack; Wireless Network; K-Means; K-Medoids; Radio Signal Strength; AP Impersonation**

I. INTRODUCTION

The proliferation of wireless network in public places such as universities, cafes, airports, commercial buildings and hotels provides seamless internet access connectivity anywhere at any time to the wireless clients. Even though many wireless networks are often unprotected, unmanaged and unencrypted, this does not prevent the client from actively connecting to the network. The real problem is that the network Access Point (AP) is always trusted. The adversary can impersonate a legitimate AP (LAP) or setup a rogue AP (RAP) to commit espionage, and to launch evil-twin attack, session hijacking, session side-jacking and eavesdropping [1, 2]. Moreover, the impersonation of LAP allows the adversary to conduct Denial of Service (DoS) attack, bypass control mechanism, or falsely advertise services to client [3].

The underlying premise of setting up RAP is to imitate the LAP so that adversary can attract the client who trying to get the connectivity through what they believe to be LAP. To masquerade the LAP, the adversary launches the spoofing attack by forging the Service Set Identifier (SSID) and MAC address same as LAP but with stronger signal strength. The primary step to restrain the threat of RAP is to detect the presence of spoofing attack.

In this paper, we explore the AP spoofing attack detection by using wireless physical-layer information namely Received Signal Strength (RSS). We propose a client-centric detection framework where the client passively monitors and sniffs the RSS of the wireless frames before the client begins to associate with target AP. The detection approach will alert the client once the target AP is classified as RAP. The framework is capable to detect the threats without the assistance from a network administrator and without the support of extra network infrastructure such as monitoring sensors. Moreover, the framework only activates the detection when the clients are trying to connect to network or to re-connect once they are disconnected. Therefore, it is resource saving detection method. For detecting the spoofing attack threat, in this work, we adapt the work undertaken in [3, 4] and [5]. Then, we extend their work by comparing the performance of detection mechanism by using partitioning-based clustering methods, K-means and K-medoids. In those works, by clustering of RSS sequences from multiple APs, the spoofing attack can be detected since the RSS sequences are not highly correlated to each other.

The remainder of the paper is organized as follows: Section 2 describes the recent work of spoofing detection. Section 3 provides an overview on spoofing attack and then formulates the attack detection problem. Section 4 proposes a client-centric AP spoofing framework by using partitioning-based clustering methods. Section 5 presents the experimental results and evaluates the performance of the clustering methods. Finally, we conclude the work in Section 6.

II. RELATED WORK

Several works have been reported in the literature on wireless spoofing attack detection. Most of the detection mechanisms focus on the intrinsic properties of MAC-

doi:10.4304/jnw.9.12.3470-3477

layer headers and wireless physical-layer information. Both layers are generally independent of higher-layer protocols and not encrypted [6]. Existing mechanisms for detecting spoofing attack include the irregularities of MAC sequence number, beacon frame Inter-Arrival Time (IAT) and the correlation of RSS sequences.

MAC sequence number has been used in [7] to perform spoofing attack detection. In this mechanism, it assumes that LAP produces a linearly increasing sequence number. Hence, any dramatic changes or abnormal gap in sequence number from the same MAC address indicates a spoofing attack. However, the availability of open-source drivers and reverse-engineered firmware allow per frame sequence number manipulation. Thus, MAC header field can be spoofed [8]. On the other hand, Martinez et al. proposed the detection mechanism by monitoring the IAT of two consecutive beacon frames [9]. The spoofing attack is detected whenever the IAT is not satisfied the regular beacon interval.

Recent works focus on the monitoring of the per-frame RSS in order to develop the dynamic profile of the wireless device or to partition RSS sequences from the LAP and RAP. Many of the commercial 802.11 wireless cards provide per-frame RSS measurement. Sheng et al. proposed to build RSS profile between the transmitter or AP and sniffer by using Gaussian Mixture Model (GMM) [6]. Once the profile is established, any abrupt or unusual RSS pattern deviation from the constructed profile is considered as a potential spoofing attack. This mechanism requires infrastructural commitment to place the sniffers in the network.

This work investigates the use of RSS spatial correlation to detect the spoofing attack. RSS sequence from the AP is highly correlated with the distance in the physical space. RSS is hard to falsify and it is unspoofable. Under non-spoofing attack scenario, if the RSS sequence from one AP is partitioned into two sequences, those two sequences are highly correlated to each other. In contrast, the presence of spoofing attack causes the mixture of the RSS sequences from the LAP and RAP. These two RSS sequences are correlated to the distinct locations and thus not highly correlated to each other. Several works have been proposed to separate the RSS sequences in order to detect the spoofing attack. The mechanisms include median filtering [10], normalization technique [11], Pearson correlation coefficient [12], K-means clustering [3, 4] and K-medoids clustering [5]. In this work, we propose a client-centric AP spoofing detection framework by adapting the work undertaken in [3, 4, 5]. We use partitioning-based clustering methods, K-means and K-medoids, to separate the RSS sequences from APs.

III. Detecting Access Point Spoofing Attacks

In this section, we describe a brief overview of spoofing attack. Then, we formulate the spoofing attack detection problem in IEEE 802.11 wireless network. This section also discusses the experimental methodology that we use to evaluate the detection framework.

A. Spoofing Attacks

Spoofing attack occurs when malicious adversary impersonates another device or user in order to gain access to restricted resources or to steal information. Spoofing attacks provide a rich set of ways for identity thieves and corporate espionage agents to launch a variety of traffic injection, Denial of Service (DoS) attacks, and RAP. Phishing AP or Evil Twin AP is a term of RAP that intentionally deployed by the adversary to impersonate LAP and to trick the victim to connect to it through the illegitimate connection [13]. RAP is established by imitating all the configurations of the LAP namely SSID, MAC address, operating channel, and etc. Since the SSID and MAC address of the AP are easily forged by the adversary, there is no other form of identification to identity the LAP.

Adversary that launches the spoofing attack allows his RAP to advertise the same SSID as that of the LAP. This may cause the wireless client to unwittingly connect to the RAP. Moreover, the adversary can force a DoS or deauthentication attack to the LAP to interrupt existing connections, and then waits for the client to re-connect and to trap into RAP. In addition, for IEEE 802.11 networks, the clients select AP by the strength of the receiving signal. The adversary only needs to ensure that his RAP has greater signal strength as seen by the client. To accomplish that, the adversary tries to place his RAP nearer to the client than LAP.

B. Formulation of Attack Detection

In IEEE 802.11 wireless network, RSS is a measure of relative power level being received by the physical layer at the antenna. The Radio Frequency (RF) signal strength can be measured in either an absolute decibel milliwatts (dBm) or relative manner such as Radio Signal Strength Indicator (RSSI). The strength of RF signal is inversely proportional to the square of the distance between AP and wireless client. Moreover, the signal is further deteriorated by signal absorption, reflection, refraction, and interferences [14]. In general, RSS is closely correlated with the location in physical space. RSS sample values that are collected at the same physical location are similar or fluctuate around the mean value. Conversely, RSS sample values at different locations in physical space are distinctively varied [5].

The variation of RSSs as perceived by the wireless client is clearly shown in Fig. 1. This figure exhibits two important scenarios: non-spoofing attack and under spoofing attack. In the first phase of the variation, the values of RSS which emanating from single LAP are normally exhibit low fluctuation. However, when the RAP exists in the physical space and launches spoofing attack, there is a rapid fluctuation of RSS sample values due to the mixture of two separate RSS sequences, one from LAP and one from RAP.

Due to this observation, it is impossible for an adversary to accurately imitate RSS of the LAP as perceived by the wireless client. Unless, the adversary will need to be at exact location with LAP and use the same set of radio equipment. Therefore, this intrinsic

property of IEEE 802.11 wireless network is useful as it is unspoofable and computationally inexpensive to measure. The real problem is how to feasibly distinguish the aforementioned scenarios. This observation suggests that we can perform cluster analysis on the received RSS sample values to find the distance in signal space. By using clustering method, we can partition the RSS sample values into *k* disjoint clusters since the RSS of beacon frames that are coming from different locations are distinctive.

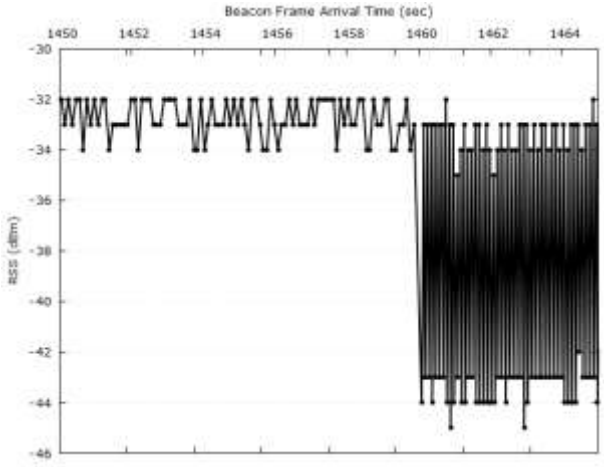


Figure 1. The fluctuation of RSSs from APs in the physical space

C. Experimental Methodology

To empirically evaluate the effectiveness of our detection framework, a set of experiment was conducted at second floor of FIST building. The floor consists of three computer laboratories as depicted in Fig. 2. The deployed 802.11 network is equipped with home wireless router TP-LINK TL-WR740N as LAP. Acer Netbook with 150 Mbps TP-LINK TL-WN721N USB Wireless Adapter is used as wireless client and RSS collection terminal. To imitate the LAP, we run hostapd [15] as soft AP on Ubuntu-based Lenovo Y500 Series Notebook with 150 Mbps TP-LINK TL-WN727N USB Wireless Adapter. The small red stars on the floor map are the locations used for RAP to launch the spoofing attack.

In these experiments, we launch the spoofing attack at 24 different locations across the floor. At each location, we collect 20 sets of RSS sequences. Each RSS sequence consists of 100 frame-level RSS sample values. To extract the RSS sample value from beacon frame, we write sniffing script using scapy, a python-based packet crafting tool [16]. In this work, we assume the situation where the client is stationary and its location is fixed at one location which is the centre of the testing floor, and the RAP locations are scattered in physical space. We emulate the real public wireless network by assuming that RAP attempts to launch spoofing attack against the wireless client in different location from the LAP's real location. Under normal scenario or non-spoofing attack, the RSS sample values are from LAP only whereas under spoofing attack, RAP at one of pre-determined locations will be activated and hence the RSS samples values from same identifiers APs, i.e. same SSID and MAC address, are the mixture between two RSS sequences from LAP and RAP.

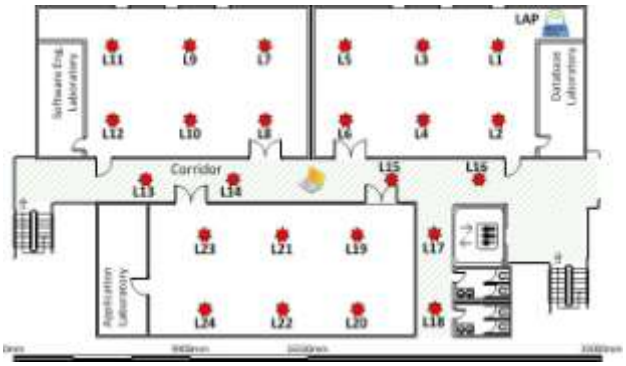


Figure 2. Layout of LAP location and RAP testing locations

IV. Cluster-based AP Spoofing Detection Framework

Clustering is an unsupervised learning technique which is used for exploratory data mining and analysis. The technique groups a set of objects into groups of similar objects. Such groups are called clusters. A cluster is defined as a division of objects which are similar between them and are dissimilar to the objects grouping to other clusters. Clustering methods are extensively deployed in various fields such as machine learning, pattern recognition, image analysis, information retrieval, bioinformatics, economics and etc. In general, clustering methods can be classified into several categories: partitioning, hierarchical, grid-based, density-based, and model-based. In this paper, we aim to explore two classical partitioning-based clustering methods to detect AP spoofing, namely K-means and K-medoids.

Partitioning-based clustering method is a one-level partitioning where *n* data objects are grouped into *k* disjoint clusters. The goal of this clustering method is to optimize a chosen dissimilarity function by iteratively relocating the data objects between clusters until a locally optimal partition is achieved. The most intuitive and popular dissimilarity function is squared Euclidean distance. Equation (1) is the definition of squared Euclidean distance between two data objects.

$$d(x_i, x_j) = \left\| x_i - x_j \right\|^2 \tag{1}$$

A. K-means

K-means is perhaps the most widely used clustering method [17]. The basic principle is to represent each cluster by its mean value, i.e. centroid. All data objects are grouped into clusters by examining dissimilarity between each data object and centroids. In other words, the data object is assigned to the nearest centroid. Once all data objects are bound to the clusters, the new centroid is recalculated over the data objects assigned to the respective cluster and the entire procedure is repeated until the centroid is converged. Algorithm 1 shows the pseudocode for K-means clustering.

Algorithm 1 K-means
Input:
$X = \{x_1, x_2, ..., x_n\}$ - set of points
k – number of clusters
Output:
$C = \{c_1, c_2, ..., c_k\}$ - set of centroids
$Z = \{z_1, z_2, ..., z_n\}$ - set of cluster labels of X
1: Select a dissimilarity metric, d
2: Arbitrarily choose k points from X as the initial cluster means, C
3: repeat
$C' \leftarrow C$
for each $x_i \in X$ do
$z_i = \arg\min_{j \in \{1,...,k\}} d(x_i, c_j)$
for each $c_j \in C$ do
$c_j = \frac{1}{N_j} \sum_{\{i: z_i = j\}} x_i$
until $C' = C$

B. K-medoids

K-means clustering is popular due to its easy implementation and fast convergence, however, it is sensitive to outliers. A data objects with an extremely large value may substantially distort the distribution of data [18]. Instead of taking mean value as the centroid of the cluster where it is not necessarily to be a real data object in the cluster, medoid can be used to represent the cluster. A medoid is data object itself and it is the most centrally data object in the cluster. K-medoid or partitioning around medoids (PAM) is more robust in the presence of noise and outliers in comparison with K-means clustering [19]. Pseudocode of K-medoids clustering is shown in Algorithm 2.

Each cluster is initialized by arbitrarily selecting k of the n data objects to be medoids. The remaining data objects are grouped into the same cluster as the medoid that it is closest to under the chosen dissimilarity function. Once the partitioning process is completed, a new medoid is selected from non-medoid data objects and the two objects are swapped. Then, the total dissimilarity cost of the configuration is computed. Configuration with the lowest total dissimilarity cost is selected and the entire procedure is repeated until the medoid is converged.

C. AP Spoofing Detection Framework

In this section, we present client-centric AP spoofing detection framework by using partitioning-based clustering method as shown in Fig. 3. This framework extends the functionalities of the wireless client's device by increasing its awareness towards APs in the vicinity. The client passively monitors and sniffs the wireless frame traffics when the client begins to associate with the AP. The detection framework will alert the client once the target AP is classified as RAP. Our detection framework consists of three phases: collection of RSS, classifications of RSS and AP spoofing detection.

Algorithm 2 K-medoids
Input:
$X = \{x_1, x_2, ..., x_n\}$ - set of points
k – number of clusters
Output:
$M = \{m_1, m_2, ..., m_k\}$ - set of medoids
$Z = \{z_1, z_2, ..., z_n\}$ - set of cluster labels of X
1: Select a dissimilarity metric, d
2: Arbitrarily choose k points from X as the initial cluster medoids, M
3: repeat
$M' \leftarrow M$
for each $x_i \in X$ do
$z_i = \arg\min_{j \in \{1,...,k\}} d(x_i, m_j)$
for each $m_j \in M$ do
$p_j = \arg\min_{\{i: z_i = j\}} \sum_{\{h: z_h = j\}} d(x_i, x_h)$
$m_j = x_{p_j}$
until $M' = M$

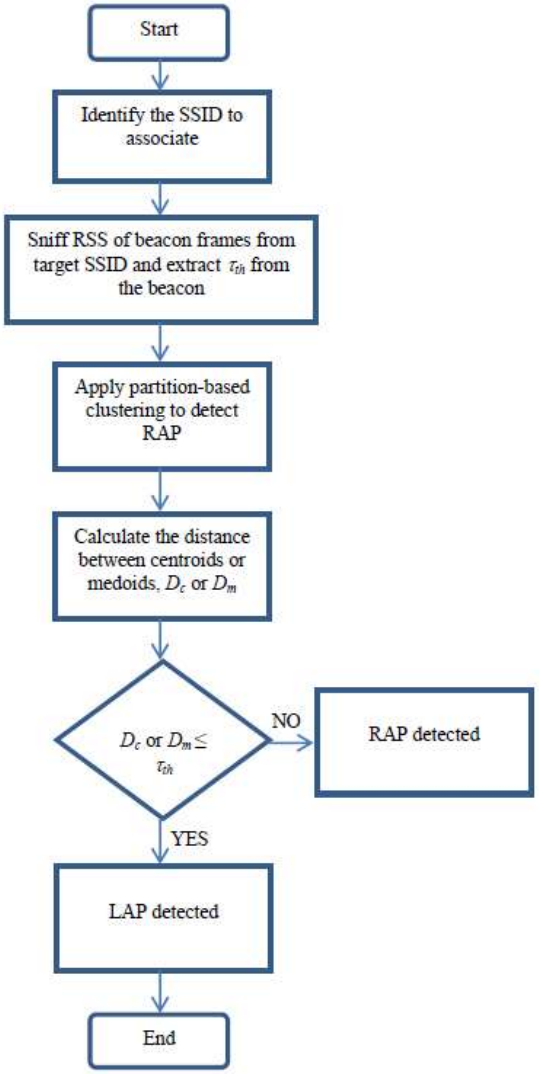


Figure 3. Client –centric spoofing attack detection framework

Collection of RSS: In this phase, the wireless client passively sniffs the RSSs from the target SSID. The client listens to the beacon frames that, by default, are sent every 100 milliseconds. Then, the RSS sample values are extracted from radiotap header from the received beacon

frames. A sequence of RSSs is represented as data object, X . Apart from that, the client also will extract the detection threshold, τ_{th} , which is advertised in beacon frame. The AP embeds the threshold in the extra Information Element (IE) in the beacon frame. This enables clients to use the information to detect the attack without association to the target AP.

Classification of RSS: In this phase, we use cluster analysis particularly K-means and K-medoids to partition the received RSS sequence into two clusters. In this work, regardless how many RAPs that launch the spoofing attacks, we only aim to detect the presence of attacks. The strong spatial correlation between RSS and location in physical space make one or multiple spoofing attacks disrupt the distribution of RSS sequences. Therefore, by setting $k = 2$, the classification phase is capable to determine the disturbance to the RSS sequences [5]. The distance between centroids or medoid, D_c or D_m respectively, is used as testing parameter for the AP spoofing detection as shown in Equation (2).

$$D_c = \left\| c_i - c_j \right\| \text{ or } D_m = \left\| m_i - m_j \right\| \quad (2)$$

The RSS sample values which emanating from single AP are normally exhibits low fluctuation. Therefore, D_c or D_m should be close to each other as the RSS sample values are from a single physical location. In contrast, when under spoofing attack, beacon frames are transmitted from two distinct physical locations. Hence, RSS samples from LAP and RAP are mixed together and D_c or D_m will result in larger distance. This is due to the fact that, centroids or medoids are derived from multiple RSS sequences associated with different physical locations.

AP Spoofing Detection: We formulate AP spoofing detection framework as a sequential hypothesis testing problem. We define two hypotheses H_0 and H_1 as follows: H_0 is the null hypothesis that no spoofing attack is detected, i.e. only one LAP exists whereas H_1 is alternative hypothesis that spoofing attack is detected and alarm needs to be raised, i.e. LAP and RAP co-exist in the physical space. To test against H_0, we choose D_c or D_m as test statistic for AP spoofing detection. Equation (3) defines the condition that AP is under spoofing attack.

$$D_c \text{ or } D_m > \tau_{th} \quad (3)$$

where τ_{th} is detection threshold. The detection threshold is empirically determined during training stage.

V. Results and Discussion

Here, we present the experimental result of AP spoofing detection framework. First, we investigate the distance between centroids or medoids in signal space under non-spoofing attack and under spoofing attack. Next, we evaluate the performance of detection framework. We quantify the performance using the following metrics: True Positive Rate (TPR) – the fraction of LAP correctly detected and False Positive Rate (FPR) – the fraction of RAP identified as LAP (e.g., false alarm). Lastly, we discuss the accuracy of the detection framework at each testing location.

A. Spatial Correlation of RSS

Fig. 4 shows the Cumulative Distribution Function (CDF) of D_c or D_m in signal space using K-means and K-medoids clustering methods. For non-spoofing attack, since the RSS sample values are emanating from a single source, i.e. LAP, D_c and D_m are relatively small. To achieve 95% probability, K-medoids shows the RSS fluctuation from the LAP is in the range of 3 dBm whereas K-means exhibits slightly higher range of 4 dBm. On the other hand, when the RAP and LAP co-exist in the physical space, we observe that the curves of D_c and D_m are skewed to the right under spoofing attacks. A great percentage of high D_c or D_m compares to the distances recorded under non-spoofing attack scenario. Therefore, this observation deduces that D_c or D_m can be used as testing parameter the test the validity of the detection framework.

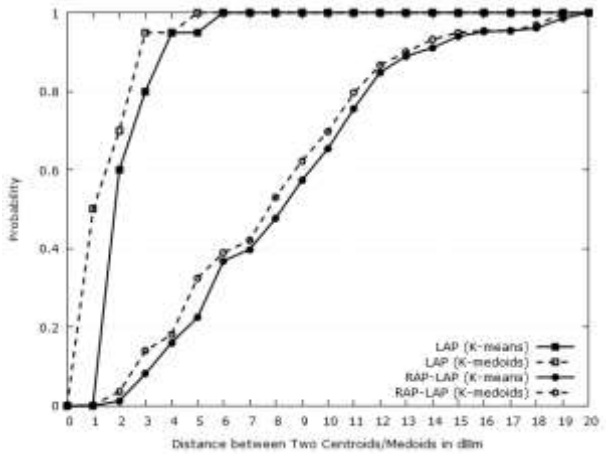


Figure 4. CDF of distance between centroids or medoids

B. Detection Threshold

Detection threshold τ_{th} defines the critical region for the spoofing attack detection to be robust against false alarms. Fig. 5 illustrates the detection rate, i.e. TPR, and FPR under different threshold settings. To achieve FPR less than 5%, the detection rates for K-means and K-medoids are 70% and 65% respectively, under τ_{th} = 2.239 dBm. By setting a slightly higher threshold, the detection framework can obtain better detection rate. For instance, K-means with τ_{th} = 4 dBm records more than 95% detection rate whereas K-medoids can obtain the same detection rate with lower τ_{th} . However, both methods show an increment in FPR up to 15%. As discussed in the previous section, D_c or D_m are estimated to be in the range of 4 dBm and 3 dBm respectively, when under non-spoofing attack scenario. If

the τ_{th} is set to be in this range, the result shows we can obtain higher detection rate. But, the detection framework generates a lot of false alarms at the same time. High percentage of false alarms is caused by the location of LAP and RAP in the physical space. We will discuss the finding in the next section.

C. Detection Accuracy

In this section, we investigate the detection accuracy at each RAP testing locations. We define the detection accuracy as the fraction of the combination between LAP correctly detected and RAP correctly identified. Fig. 6 shows the detection accuracy when τ_{th} = 2.239 dBm and the FPR is kept less than 5%. The result exhibits there are two locations in physical space cause the deterioration of the detection accuracy. Referring to Fig 2, RAP at L12 and L24 is about the same distance with the location of LAP as perceived by the wireless client. Thus, RSS sequences from both LAP and RAP are fluctuated around the same mean. Therefore, the detection framework performs poorly at those two locations.

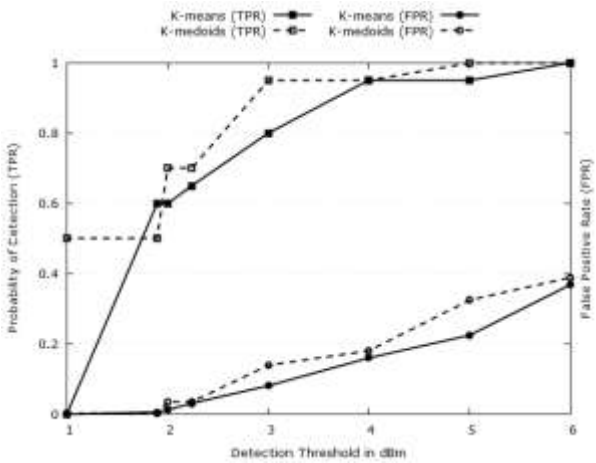


Figure 5. Spoofing attack detection performance against the detection thresholds

Fig. 7, on the other hand, shows the detection accuracy when τ_{th} = 3 dBm and τ_{th} = 4 dBm for K-medoids and K-means respectively, and the FPR is kept less than 15%. As we can observe, the higher percentage of FPR is mainly caused by false alarms generated at locations L12 and L24. Moreover, the higher detection threshold also contributes to the accuracy deterioration at some other locations in the physical space. For instance, L19 is mainly located behind the thick concrete wall. Even though the adversary located the RAP near to the client, but the severe obstruction affects the signal strength coming from RAP.

As overall, since the RSS sequence is highly correlated with the distance, we found that the performance of AP spoofing detection framework by using partitioning-based clustering method is effective when the locations of the LAP and RAP are distinct in the physical space. However, it is interesting to notice that the detection framework suffers from many false positives whenever the attenuation of RSS sequences from APs exhibits the similarity due to multipath propagation effect and when the wireless client is stationed at equal-distance away between the APs. Moreover, as comparison between K-means and K-medoids clustering methods, K-medoids shows better detection rate for any τ_{th} value. However, at the same time, K-medoids also exhibits high FPR as compared to K-means. Since K-medoids is robust against the RSS outliers, we can observe that the D_m between two RSS sequences is relatively small against D_c.

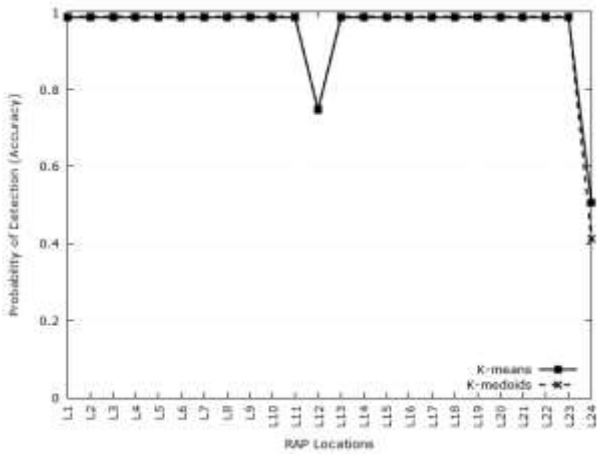


Figure 6. Detection accuracy when the FPR is kept less than 5%

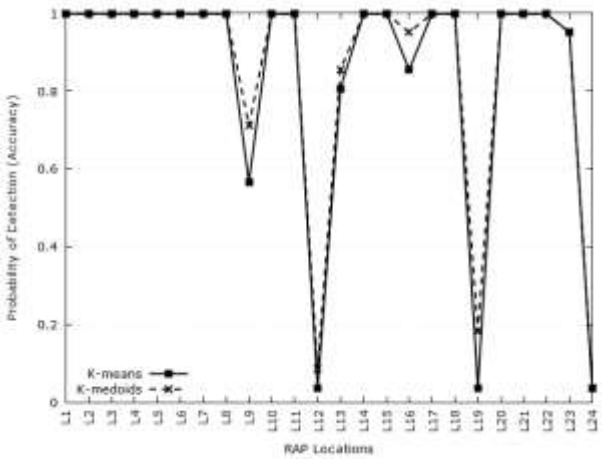


Figure 7. Detection accuracy when the FPR is kept less than 15%

VI. CONCLUSIONS

In this paper, we present a spoofing detection framework to protect the wireless client against the AP impersonation attack. The framework measures the correlation of RSS values from the target AP in order to determine whether the sequence is from the LAP only or the mixture of RSS values from LAP and RAP. Using partitioning-based clustering methods, namely K-means and K-medoids, we group the RSS sequence into two clusters. We found that if the RSS values are coming from LAP only, the distance between centroids or medoids is relatively small compared to the RSS values that are emanating from RAP and LAP. Therefore, we exploit this property to detect the presence of spoofing

attack. Even though the framework can achieve more than 90% detection rate, it is worth noting that many false alarms are raised at some locations in the testing environment due to numerous obstacles and the client to have equal-distance away between legitimate and rogue APs. This finding may warrant further research in the future.

ACKNOWLEDGMENT

The work was supported by Ministry of Education (MOE) Malaysia under Fundamental Research Grant FRGS/1/2013/ICT04/MMU/03/2.

REFERENCES

[1] D. Takahashi, Y. Xiao, Y. Zhang, P. Chatzimisios, and H. Chen, "IEEE 802.11 User Fingerprinting and its Applications for Intrusion Detection," *Computers & Mathematics with Applications*, Vol. 60, No. 2, 2010, pp. 307-318

[2] Y. Song, C. Yang, and G. Gu, "Who is Peeping at your Passwords at Starbucks? — To Catch an Evil Twin Access Point," *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2010, pp. 323-332,

[3] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks," *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 5, 2010, pp. 2418-2434

[4] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," *Conference of the 4th Annual IEEE Communications Society*, 2007, pp. 193-202

[5] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 24, No. 1, 2013, pp. 44-58

[6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," *IEEE The 27th Conference on Computer Communications*, 2008

[7] F. Guo, and T. Chiueh, "Sequence Number-based MAC Address Spoof Detection," *In Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection*, 2005, pp. 309-329

[8] M. Neufeld, J. Fifield, C. Doerr, A. Sheth, and D. Grunwld, "SoftMAC: Flexible Wireless Research Platform," *Proc. of the 4th Workshop on Hot Topics in Networks*, 2005

[9] A. Martinez, U. Zurutuza, R. Uribeetxeberria, and M. Fernandez, "Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks," *The 3rd International Conf. on Availability, Reliability and Security*, 2008, pp. 520-525

[10] D. Papini, "Lightweight MAC-Spoof Detection Exploiting Received Signal Power and Median Filtering," *Int. J. of Critical Computer-Based Systems*, Vol. 3, No. 4, 2012, pp. 247-261

[11] T. Kim, H. Park, H. Jung, and H. Lee, "Online Detection of Fake Access Points Using Received Signal Strengths," *Conference of the 75th IEEE Vehicular Technology*, 2012, pp. 1-5

[12] J. Yang, Y. Chen, and W. Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments," *Conference of the 6th Annual IEEE Communications Society*, 2009, pp. 1-9

[13] L. Ma, A. Y. Teymorian, X. Cheng, and M. Song, "RAP: Protecting Commodity Wi-Fi Networks from Rogue Access Points," *In QShine '07: Proceedings of the 4th International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks*, 2007

[14] R. Gill, J. Smith, M. Looi, and A. Clark, "Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks," *AusCERT Asia Pacific Information Technology Security Conference*, 2005

[15] Linux Wireless: Hostapd Linux Documentation Page, Available: http://wireless.kernel.org/en/users/Documentation/hostapd

[16] Scapy, Avalable: http://www.secdev.org/projects/scapy/

[17] J. B. MacQueen, "Some Methods for Classification and Analysis of Multivariate Observations," *Proc. of 5th Berkeley Symposium on Mathematical Statistics and Probability*, 1967, pp. 281-297

[18] S. Bandyopadhyay, and S. Saha, *Unsupervised Classification: Similarity Measures, Classical and Metaheuristic Approaches, and Applications*, Springer, 2012

[19] L. Kaufman, and P. J. Rousseeuw, *Finding Groups in Data: An Introduction to Cluster Analysis*, Wiley Series in Probability and Statistics, 1990

Nazrul M. Ahmad is a lecturer in the Faculty of Information Science and Technology (FIST), Multimedia University (MMU), Malaysia. He is currently pursuing his PhD degree with the Faculty of Information and Communication Technology, University Technical Malaysia Melaka (UTeM). He received a BEng. (Hons.) in Electronics with Communication Engineering from University of York, UK and the MSc. in Information Technology from MMU. His research interests include wireless communication and security, and cloud computing.

Mohd Faizal Abdollah is currently working as a senior lecturer under Department of Computer and Communication System, Faculty of Information and Communication Technology, University Technical Malaysia Melaka (UTeM). He received his first degree and Master degree from University Utara Malaysia and University Kebangsaan Malaysia. Dr Mohd Faizal obtained his PhD from University Technical Malaysia Melaka in Computer and Network Security. Previously, he worked as a MIS Executive at EON Berhad, Selangor and as a System Engineer at Multimedia University, Melaka for six years. His interest is mainly in network and wireless technology, network management and network and wireless security.

Robiah Yusof received the BSc (Hons) of Computer Studies and Master of Information Technology from Liverpool John Moore's University, UK and Universiti Kebangsaan Malaysia respectively. She obtained the Doctor of Philosophy, Network Security from Universiti Teknikal Malaysia Melaka (UTeM) and currently a senior lecturer at

the UTeM. Her research interests include network security, computer system security, network administration, network management and network design.

Anang Hudaya Muhamad Amin is a senior lecturer in the Faculty of Information Science and Technology, Multimedia University, Malaysia. He received a BTech (Hons.) in Information Technology from Universiti Teknologi PETRONAS, Malaysia, and Master of Network Computing and PhD in Artificial Intelligence from Monash University, Australia. His research interests include artificial intelligence with specialization in distributed pattern recognition and bio-inspired computational intelligence, wireless sensor networks, and cloud computing.

Subarmaniam Kannan is a lecturer in the Faculty of Information Science and Technology, Multimedia University,

Malaysia. He received a BA (Hons.) in Social Science from University Malaya, Malaysia, and Master of Computer Science from University Putra Malaysia and PhD in Semantic Learning from Multimedia University, Malaysia. His research interests include artificial intelligence with specialization in Semantic Web Technology, Cloud Computing, Data Warehousing, Big Data Analytics and Networking.

Customized Interface Generation Model Based on Knowledge and Template for Web Service

Rui Zhou, Jinghan Wang, Guowei Wang, and Jing Li
School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China
Email: {rayzhou, heiswjh, weiking}@mail.ustc.edu.cn, lj@ustc.edu.cn

***Abstract*—With the development of Service-Oriented Architecture, more and more researches have provided automatic and semi-automatic approaches to end-user. Users can construct their own applications with web services. However, it is hard for most end-users to customize the interfaces of applications with current service composition methods. To address this issue, an interface generation model was proposed to provide customized user interface and interaction workflow. In this model, knowledge was involved to instruct the workflow of interaction. Templates were adopted to describe the user interface. Some significant points, such as user definition, data profile, user interaction workflow, interface description, were discussed in detail. A prototype system was implemented. Some demos have been shown to verify the customized interface generation model. With this model, end-users can define the interfaces and interaction workflows of web services with rules and templates. It supplies the gap of user interface in service composition. Compared with the current interface generation in service composition, the proposed model is more flexible and more effective for end-users.**

***Index Terms*—Interface Generation; Service Composition; Knowledge-Based; End-User Development**

I. INTRODUCTION

In recent years, with the development of Service-Oriented Architecture (SOA)[1], more and more researches have proposed automatic or semi-automatic approaches to end users to construct their own applications [2] [3] [4]. In these researches, the end-users are able to take the advantage of the SOA to design a variety of applications. However, unlike the enterprise SOA, the most of end-user defined applications with automatic service composition methods lack suited user interfaces and interaction workflows. In applications for end-user, user interactions are important [5]. Without interaction, the information from different services cannot be displayed for users in appropriate way. It will cause that the service composition systems become unacceptable for users. Hitherto, there are approaches and systems can be chosen to make service composition by end-user, but few of them can provide customizable user interaction model. In resolve this gap, the user interface and interaction workflow in web services composition is explored.

The models of user interaction for services composition have been extensively studied. Some researchers tried to generate interfaces from web service descriptions. For example, an annotation tool based on WSDL was involved to enhance the user interface generation process for services [6]. The developers or users should add annotations to define UI features. A match algorithm based on descriptions has been proposed to support the discovery of UI components and the provision of suggestions that can help to develop user interfaces for service-based applications [7]. And the match relies on descriptions about functions and components of UI. Those suggestions can be used to generate an interface. However, this approach still needs manual adjustments in most time. An adaptive user interface generation framework for web services was proposed [8]. The framework involved the WSDL and user's profile to generate a suitable interface. The developers of web services were required to add an extra description.

Some researches were focused on UI composition in application composition. An implemented approach was proposed to reuse user interfaces while composing services [9]. This approach relied on abstracting these applications to be composed and these methods of web services. Then, it achieved a composition at the abstract level to regenerate a concrete user interface in a target language. An application composition driven by UI composition was proposed [10]. It was based on existing application's UIs and their semantic descriptions. Generally, these methods were only suitable to those services with their own user interfaces.

In other service composition systems, there are researches on user interaction model. For example, in [11], the service-oriented user interface modeling and composition has discussed. This model suits a system of interface composition. Another interface composition approach in presentation layer has been shown in [12]. In [13], a method which includes interface define is provided for end user by mash up in web page. A tool for composing user interface in mobile for end user has been introduced in [14]. An automatic web-based user interface model is discussed for SOA-based system in [15]. However, in the systems of knowledge based service composition, user defined interaction and interface method is not sufficient.

In our previous research, a knowledge-based development approach for end-user in cloud computing, called Cloud Brain, have been proposed in [16]. Its main idea is that the user's knowledge can be stored in cloud in

doi:10.4304/jnw.9.12.3478-3485

the form of rules. With the innumerable computing and storage resources in cloud, these rules can accumulate and reason, which can help the users to think and provide functions for them. As a user-oriented system, it is significant to find a perfect way to provide information and actions from system for user in a suitable manner. In the Cloud Brain system, the information and actions are produced by web services. These services are called with rules. Therefore, they cannot send the information and actions to users directly. Then, the client program in user's device hardly faces to various data from different web services. Furthermore, users have some obstacles to use these actions and information for further operations.

In this paper, an end-user customized user interface generation model is proposed in the Cloud Brain system. The UI template is involved to describe the interface. With this model, some key points have been considered, and a prototype system has been developed. End-users can make use of this interface generation model to define customized interface and interaction workflow in the procedure of service composition. Compared with the current interface generation in service composition, the proposed model is more flexible and more effective for end-users.

The paper is organized as follow: The user interface generation model and some key points are discussed in Section 2 in detail. Then the development of prototype system and demo are demonstrated in Section 3 and Section 4. In final, we conclude the approach and expect the future work.

II. User Interface Generation Model

A. Knowledge-Based Interface Generation

The user interaction model in this paper is combined with the knowledge-based service composition method in Cloud Brain [16]. In the service composition model, Users select services and define their execution process by defining the rules. These rules are the representation of users' knowledge. Every rule includes two parts. One is Left Hand Side (LHS), which describes the conditions of the rule. The other part is Right Hand Side (RHS), which describe the actions. These two sections make up the "IF-THEN" statement. If the condition in LHS is matched by some facts which indicate the user's context, the rule will be fired, and the actions in RHS will be executed. For services composition, the output of services can be matched with the conditions as a fact. The matched fact will be send to these services as parameter. In this way, rules connect different web services to compose applications for users. These applications are not integrated software running on client device or server. So, there is a problem that how the users can interact with the applications. Therefore, a user interface generation model was proposed to solve the problem. The model of interaction can blend in the Cloud Brain user development system well.

As shown in Fig. 1, the user interface generation model has two stages. The first stage is user interaction definition, in which users define the interaction process. The other stage is user interaction action, in which users interact with the system and web services.

The following components will be concerned in the user interface generation model of Cloud Brain: end-device, knowledge editor, UI template editor, UI service, template repository, fact base, rule engine and some web services. In Cloud Brain, these components exist as different roles. The end-devices are the user access devices, such as mobile phone, notebook and tablet PC. It collects user's input and operation. The knowledge editor is a tool for end-user to edit their own rules. In the UI template editor, end-user can define the user interface with an easy way. The UI service is a main component to response user interaction specially. The template repository stores the UI templates. Fact base manages the facts from different devices and sources. The rule engine is the core component of Cloud Brain. It maintains the rules, matches the facts, and executes the actions. Web services existing in internet provide all kinds of functions for user. These components will be described in detail in later sections.

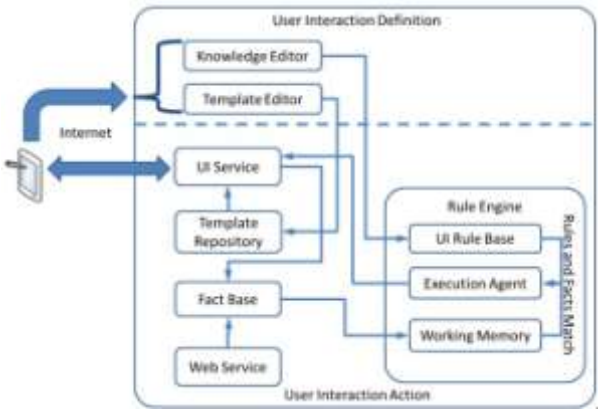


Figure 1. User interface generation model

In the proposed user interface generation model, the users need to define their interactions before the interaction executing. So, there are two stages in the model as follow.

The first stage is user interface definition stage. In this stage, user can define the interaction workflow by rules. In these rules, the facts, which will be displayed to user, are referred. At this time, users can choose a UI template to display these facts. The template comes from template repository or template editor. User can design the display form of the facts and events that can be triggered in the interaction.

The other stage is user interaction execution stage. The process of this stage is follow:

1. A fact is produced by web service. The fact will match the conditions of rules in the rule engine, if the facts need to output to user.

2. When some rules' conditions match the fact successfully, the right hand side of the interaction rule will be executed. The UI service will be invoked. The template referred in the rule and the matched fact will be used as parameters of the service.

3. The UI service will merge the fact and template together into an interaction interface. The interface will be pushed and displayed in user's device.

4. User can operate in the interface. It will produce some operation events. These events will be inserted into fact set in the form of facts. So, they can take part in later procedures of reasoning and interaction.

B. Interaction Rule

In this interface generation model, the interaction rule is a form of regular rule in the Cloud brain system. The structure of interaction rule is same as other rules. Therefore, they can take the reasoning with each other. The interaction rule also has the left hand side (LHS) and the right hand side (RHS). Conditions in the LHS will be mainly used to check the facts which need to be displayed or interacted. These facts come from the output of web services usually. For example, the weather fact is from the weather web service. In the RHS of interaction rule, the UI service is called with the parameters. The parameters are the UI template ID and the matched facts normally.

C. User Interface Description

In order that users can define their interfaces, an UI template is involved into this model to describe the user interface.

In the UI template, the framework of interface, the form of information display, and the operation event are defined. The UI template is described in XML. It includes two parts: display and operation. The high level tags <show> and <operation> respectively present these two parts. In the display part, the information from web service is presented in the form of HTML. In the HTML, there are some special tags to indicate the location of the facts contents. These tags are in exceptional type of HTML, in order to distinguish it from the tags in HTML. In the <operation> section, the candidate operations are described by the components <event>. These events can be triggered by users' operation in the interface. In every <event> tag, type attribute and the content of event are included. The type attribute indicates the type of the event, such as button click, form submitting, and text input.

```
<?xml version="1.1" encoding="gb2312"?>
<interface>
        <type>
        </type>
        <show>
        <!-- the "show" frame describe the style and content which the web service
output. In the tag, HTML code will be refered. -->
                HTML code here...
        </show>
        <operation>
        <!-- the eventoption tag describe the candidate events which can be choosed by
user and listed by user. The events choosed will create facts in the facts set. -->
                <event type="button" >
                        <fact>
                        </fact>
                </event>
                <event type="form" >
                        <fact>
                        </fact>
                </event>
        </operation>
</interface>
```

Figure 2. An empty user interface template

As mentioned above, the UI template describes the interface framework of system-user interaction. The system can combine the template with facts data, and produce a web page to display in user's device. In the system, a template can be combined with some kinds of facts, and there are many kinds of templates stored in template repository. An editor tool was designed to users to define new template. When users define their interfaces, they can choose a template from the repository or edit a new template by the editor. The templates can be involved in the interaction rules with their ID.

The Fig. 2 is an empty user interface template XML file. It shows the structure of template description.

D. User Interface Service

In order to display these interfaces to users, a user interface service is provided in our system. This service is designed to generate interfaces and send them to users. It is implemented in our system, but it can be involved as a web service. Users can define interaction rules to invoke the UI service. There are two input parameters in the invocation. They are fact and template. The fact can be transmitted by the rule from the fact database, when the fact matches the rule. The template will be selected from UI template repository.

In the UI service, a web servlet was designed to generate HTML web page to users. When the UI service is called, it will insert fact data into the HTML segment in the template. The special tags in this segment can indicate this operation. In addition, the events in the template will be connected this fact, in order to make the events correlation with fact. These segments in the template will be converted to HTML document. The web servlet can send the web page to user's browser.

E. Data Profile

For the user interaction, some input data and output data are maintained in the system. In order to integrate them into the cloud brain system, the interaction data can be consider as some kinds of facts, which is the basic data represent form in the cloud brain model. As mentioned in the cloud brain, the facts are managed by ontology. In the facts ontology, some types named "input" and "output" exists to indicate these user interaction facts. These facts mainly consist of user request event and users UI display data which can match with rules. The ontology semantic structure can describe these relations with services and system.

F. The Lifetime of the Ui Data

The lifetime is the remaining time of data in the system. In this user interaction model, the lifetime of the data is the period when the input and output data stay in the working memory of rule engine. If some data still exist in the system after the correlative rules are triggered, in some situations, they will make some incorrect operations by fire new rules. On the contrary, if some data are retracted from memory before being invoked completely, the functions and the data of the interaction will be damaged. For the input and output facts, the impacts of their lifetime to interaction procedure are different. If the input event facts persist in the system after their function complete, they will match some rules again incorrectly when some new relevant facts or rules are inserted into

the system. It may cause reduplicate response to user's one operation. On the contrary, if the input facts are removed earlier, it can cause some required services have no response. Because one operation event can match and trigger several rules and services in this model, the fact removed in the former rules can causes the mismatch in the posterior rules. For the output data and facts, if these facts remain in system after send to users the output notices to users can be repeated. For these output facts which will be invoked by another service, if they disappear after output, the subsequent services will hardly get these data. Consequently, the lifetime of every interaction fact is significant to the correct interaction.

In order to resolve the problem of interaction facts lifetime, two methods have been purposed to control the lifetime in these model. They are automatic extinction by system and deletion in rules by user definition. The first method, fact extinction by system, is automatic, according to the definition of fact. As mentioned above, the facts are defined and managed with ontology semantic descriptions. In the descriptions, user or service provider can define the lifetime of these facts. The system will control the extinction of facts according to the definitions. In the other method, users can add the fact retraction operation in rules. These rules will dispose facts when they are triggered. The retract operation can either be added in the RHS of interaction rules or be involved in a separate rule with special conditions. When severalrules are triggered by a set of facts simultaneously, the different action sequences will influence the result of interaction. It will make mistake or function deficiency, when the retract fact operations exist in rules especially. In this situation, users can define priority for rules, in order to control the lifetime of facts and avoid that the retract operation affects other operations. When some rules have same priority or have no priority, the retraction operation in them also do not affect other actions in meantime.

G. User Interaction Workflow Specification

UI workflow specification matching is as important as interface for users and services. Even if the rule-based matching results for the visual template profile and the data profile are identical, it is not sufficient to establish that the user interaction is the one that is actually needed. The order and timing of data must also match, because they can also influence the result of interaction. For example an authentication UI may just simply send the user's ID and password by interaction event facts.

Various workflow specification languages have been proposed to model the application behavior including BPEL-WS [17], and PSML-S [18]. However, matching based on the workflow is difficult, and thus a simplified workflow model is required. The workflow profile needs to catch the essential inter-operation relation of the user interaction and the other services from the application.

Each type of user interaction classifications in the cloud brain system has a corresponding workflow. Hybrid interactions have more complicated workflows that are composed from the following basic interaction workflow. In this system, there are several user interaction workflow models mainly.

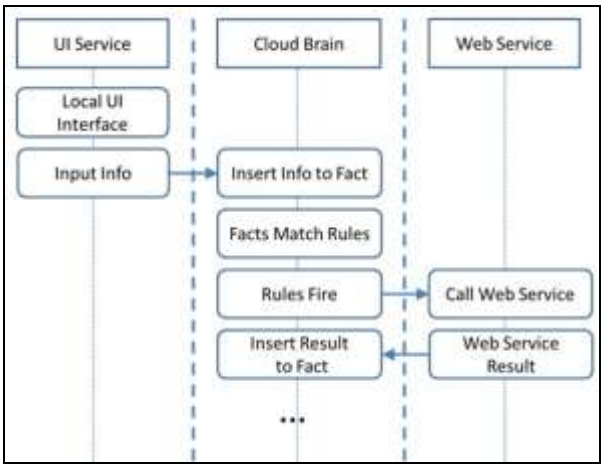


Figure 3. Data collection user interaction workflow

Data collection user interaction workflow: This type of user interaction workflow often has some sequential step to collect input events and data from users and send them to web services. The steps are shown in Fig. 3.

The first step of collection workflow is that user inputs data or operation by local user interface in user's device. The local user interface is a part of application in mobile device. User can edit information in a special form with the interface. The information may express user's situation, emotion, requirement, and other input. Then the input information will be sent to cloud brain system and be inserted to fact. As mentioned before, the collected data are expressed in form of fact. They can be treated as a part of context or situation. The fact can match rules in rule engine. Then some web services may be called and return the result or response.

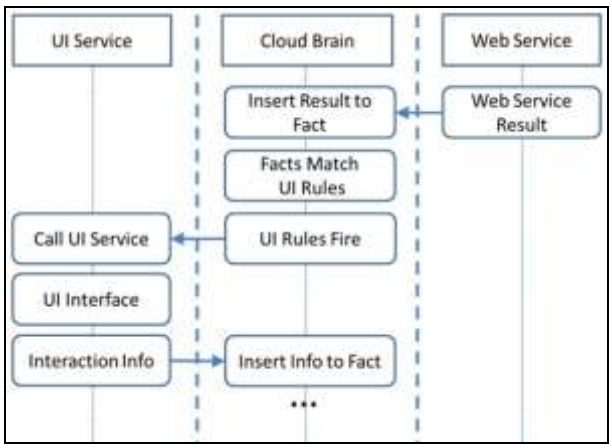


Figure 4. Data presentation user interaction workflow

Data presentation user interaction workflow: This type of UI often has an interactive workflow. An interaction initiates by a web service result, displays it to user and waits the response of user. The workflow diagram is shown in Fig. 4. It often has a sequential workflow. When some web services return results, which are required to present to user, the workflow starts. The data in the

results will match the interaction rules and the matched data will be sent to user's device with UI service and template. Then user can see the information and operate with it as required. After user operation, the workflow becomes as data collection.

Monitor user interaction workflow: This kind of UI workflow is a periodical interaction workflow. In this workflow, the period is considered in the definition of rules. The periodic rules will fired with some condition in cycle. Then some web service will be called and return result to system. User can acquire prompt on time. User can define periodic rules to request some services like weather, social network, and schedule at regular intervals. For example, a weather query rule can be defined to call the weather service every morning. The Fig. 5 shows the process of monitor user interaction workflow.

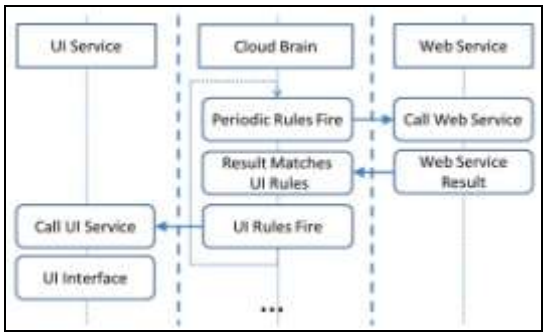


Figure 5. Monitor user interaction workflow

III. System Implementation

A. Prototype System Architecture

In order to verify this user interaction model, a prototype has been implemented in our cloud brain architecture. Fig. 6 shows the whole implementation of cloud brain. In this figure, elements in the red rectangle are specialized for user interaction. In the implementation of cloud brain, the rule engine is based on Drools [19]. The fact base is a fact management system with Jena [20] and MySQL.

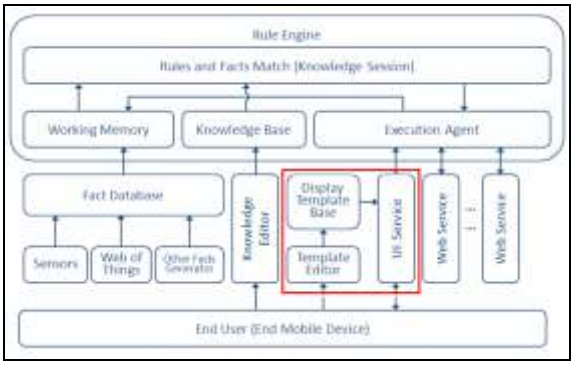


Figure 6. Cloud brain architecture

The interaction prototype consists of server side and client side. In the server, rule engine and fact base of cloud brain are involved in the interaction procedure. Besides these, a UI service is implemented to deal with the interface.

B. UI Service

As mentioned before, the UI service consists of a web service access and a web servlet server. For implementation, a message queue and a push server are involved to transmit data. Fig. 7 shows the UI service and mobile device side of the interaction prototype. The web service provides an interface based on SOAP protocol. These rules can invoke the service with the protocol directly. The fact and UI template are sent to the UI service as parameters. In the service, template parser is involved to analyze the interface XML description. The result will be used to construct a HTML page in HTML generator. A message queue based on RabbitMQ [21] maintains and transmits these HTML documents. For notice in user's device, a push server can push a notice to user's device when a new HTML document is generated into the message queue. In this prototype, the push server is designed to respond to Android application polling. In this notice, a URL for the UI interface is attached. When a user accesses the URL by a browser in his device, a request will be sent to servlet server. The servlet server in UI service can extract the HTML document from the message queue, and return the web page to user's device as response. When the user operates in the web page, servlet server will respond to this operation and insert an event fact into the system.

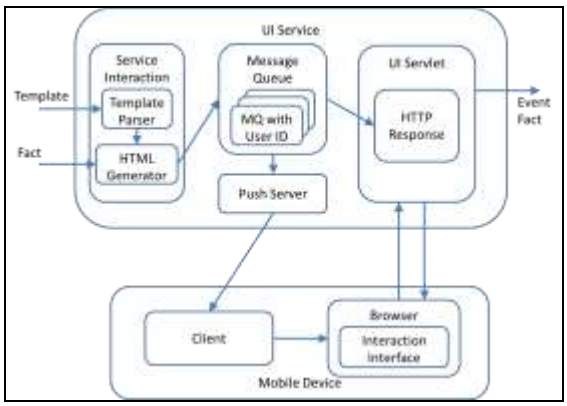


Figure 7. UI service and client implement

In the client side, the Android mobile device is considered in the prototype. A client application and browser will take part in user interaction. The client is a service in Android system. The browser can be original or from the third-party.

In this prototype, the interaction client application is designed for Android mobile system. It includes a background service. For hardly using the push service in Android systems, roll polling is adopted to get notices from the push server. After receiving the notice, the service will extract the UI servlet URL and call a browser to access it. Thereby, user can operate in the interface in browser.

C. Knowledge Editor

A knowledge editor has been developed for end-user to compose their rules. The tool is also based on android mobile system. users can view, edit and create rules in a graphic user interface. For the purpose of creating a rule,

the interface can be separated into two parts: condition and action. To create a condition, a user can choose the condition class and the property from the drop-down box. Then the condition value can be given by the text editor. A user can add more conditions by the "add condition" button. Likewise, a user can define actions by the action part of the interface. Finally, the rule will be inserted into the knowledge base after the "insert rule" button is pressed. Fig. 8 shows the interface of the knowledge editor.

Figure 8. The interface of rule editor

Likewise, users are not required to create all the rules by themselves. Some rule libraries are available to users. In these libraries, the common senses of interaction and fact reasoning are defined. Users can import them to their own knowledge base.

D. Template Editor

Besides the knowledge editor, a template editor was also implemented for users to define the interface template. The Fig. 9 shows the structure of the template editor. The template editor contains the following elements:

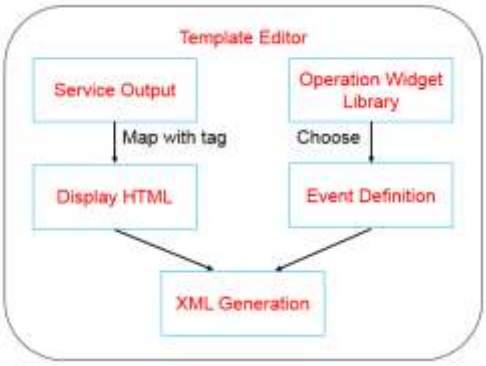


Figure 9. The template editor structure

Type list of web service output: users can choose the type of outputs which the new interface template suits for. These outputs will map to these tags in HTML.

Display HTML generation: it is a simple HTML editor with graphic user interface like Frontpage. Users can editor a HTML page to display the web service output.

Operation widget library: it contains a set of UI widgets, such as button, check box, drop list, and so on. Users can choose the suited widget into the template. In the generated interface, these widgets will produce UI events when a user operates in them.

Event definition: it defines the operation events by the chosen widgets

XML generation: finally, both the display HTML and event definition will be packed into a template xml file.

IV. DEMO

In order to demonstrate the process of the user interaction model and prototype, a demo has been designed with the prototype system. In this demo, some interaction rules have been edited in the rule engine. For example, an interaction rule named "Weather Fact Display" is shown in Fig. 10. This rule can be run by the rule engine in the prototype.

If the rule is triggered, a data presentation workflow will start. When the fact, whose type is "Weather Fact", is produced in the fact base by a weather web service, it will make the rule start to execute. Then the UI service will be called with the interaction template "template.xml". Finally, the weather fact will be retracted from fact base, in order to avoid wrong repetitive execution.

Some other rules were also considered in the demo. For example, the "MapDisplay" rule defines the interface of the map in user's device, and the "ScheduleDisplay" rule defines the calendar notice interface for user. Other rules also can be added in to the system with the knowledge editor.

```
rule "WeatherFactDisplay"
    //include attributes such as "salience" here...
    when
        //conditions
        $fact:ContextFact(type == "WeatherFact", $info:info )
    then
        //actions
        DisplayServiceAgent.showDisplay($fact,"template.xml");
        System.out.println("WeatherFactDisplay\n");
        retract($fact);
end
```

Figure 10. Interaction demo rule

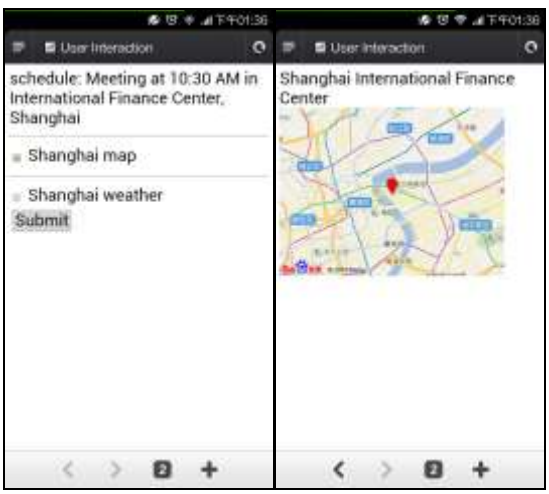


Figure 11. Device display of schedule service and map service

Figure 12. Device display of weather service

In the UI service, a user interface page based on HTML is generated, when interaction rules are triggered. After that, this page will be pushed to user's smart phone. The user can hit the notice in Android device to view the interface in a browser.

Fig. 11 is outputs of the schedule service and the map service. In the schedule service interface, the check box "map" and "weather" are invoked to produce UI operation events. Users can choose these items or not. For example, if a user chooses the "map" and submit, a map requiring event will be inserted into fact database. Then, the system will execute rules to request map service. The output of map service will trigger the "MapDisplay" rule, and show the map to user like the right one of Fig. 11.

Fig. 12 is the smart phone screenshot of the weather display interface. For the weather service in this demo, a Chinese web service is invoked. So, the weather information is displayed in Chinese.

The demo can verify the correction of the presentation workflow in the proposed model and prototype. Some other rules like "Interface event for weather" and "Interface event for map" are constructed to complete other workflow. These results will be no longer described because of space cause. All of these basic workflows can be supported in the prototype system.

Through the prototype system and these demos, users can custom the interfaces of services. Compared with other methods, the knowledge-based approach is more flexible. End-users who have no programming ability can define the interface and interaction workflow by creating rules and UI templates.

V. Conclusion and Future Work

In this paper, we propose an end-user customized user interface generation model, which is suitable for the service composition system based knowledge. Users can define the interaction workflow and interface depending on their knowledge and templates. To realize the model, the architecture and approach have been described. Furthermore, special details of related rules, interface description, user interface service and the data profile have been discussed to make the proposed model more concrete and comprehensive. Finally, a prototype and a demo have been illustrated to verify this model.

For the future work, we will consider more types of facts into our interface model. For example, we will invoke user's context and the sensors from device and web of things. Then, the context of the device will also be considered to using to generate more suited interface for different device hardware.

Acknowledgement

The work is supported by the National Key Technology R&D Program under Grant No.2012BAH17B03, USTC-Lenovo Joint Laboratory for Cloud Computing, Supercomputing Center of USTC, and the USTC Innovation Foundation of Graduate Student.

Reference

[1] Erl, Thomas. *Soa: principles of service design. Vol. 1*, Upper Saddle River: Prentice Hall, 2008.

[2] Casati F, Ilnicki S, Jin L J, et al. Adaptive and dynamic service composition in eflow. *Seminal Contr. to Inf. Systems Eng*, 2013: 215-233.

[3] Hatzi O, Vrakas D, Bassiliades N, et al. The PORSCE II framework: Using AI planning for automated semantic web service composition. *The Knowledge Engineering Review*, 2013, 28(02): 137-156.

[4] He J, Chen L., Wang X., et al. Web Service Composition Optimization Based on Improved Artificial Bee Colony Algorithm. *Journal of Networks*, 2013, 8(9).

[5] M.P. Papazoglou, P. Traverso, S. Dustdar, et al. Service-oriented computing: State of the art and research challenges. *Computer*, 2007, 40(11): 38-45.

[6] Izquierdo P, Janeiro J, Hubsch G, et al. An annotation tool for enhancing the user interface generation process for services, *Microwave & Telecommunication Technology, 2009. CriMiCo 2009. 19th International Crimean Conference*. IEEE, 2009: 372-374.

[7] Liebing C, Mennerich R, Schill A. A Pragmatic Approach for Matching UI Components on Web Service Operations, *Services (SERVICES-1), 2010 6th World Congress on*. IEEE, 2010: 621-628.

[8] He J, Yen I. L. Adaptive user interface generation for web services, *e-Business Engineering, 2007. ICEBE 2007. IEEE International Conference on*. IEEE, 2007: 536-539.

[9] Joffroy C, Caramel B, Dery-Pinna A. M, et al. When the functional composition drives the user interfaces composition: process and formalization, *Proceedings of the 3rd ACM SIGCHI symposium on Engineering interactive computing systems*. ACM, 2011: 207-216.

[10] Brel C, Renevier-Gonin P, Occello A, et al. Application composition driven by UI composition, *Human-Centred Software Engineering*. Springer Berlin Heidelberg, 2010: 198-205.

[11] W.T. Tsai, Q.Huang, J. Elston, et al. Service-oriented user interface modeling and composition, ICEBE'08, *IEEE International Conference on e-Business Engineering.*, 2008: 21-28.

[12] T. Nestler, M. Feldmann, A. Preussner, et al. Service composition at the presentation layer using web service annotations *Proc. of the 1st Intl. Workshop on Lightweight Integration on the Web (ComposableWeb'09)*. 2009.

[13] C. Cappiello, F. Daniel, M. Matera, et al. Enabling end user development through mashups: requirements,

abstractions and innovation toolkits, *End-User Development*. Springer Berlin Heidelberg, 2011: 9-24.
[14] R. Zhou, H. Meng, X. Liu, et al. Design and implementation of mobile widget composition framework and tool for end-user, *Computing Technology and Information Management (ICCM), 2012 8th International Conference on.* IEEE, 2012, 2: 767-770.
[15] M. Kopel, J. Sobecki, A.Wasilewski, Automatic Web-Based User Interface Delivery for SOA-Based Systems, *Computational Collective Intelligence, Technologies and Applications*. Springer Berlin Heidelberg, 2013: 110-119.
[16] R. Zhou, J. Li, J. Wang, G. Wang, A Knowledge-Based Development Approach with Fact and Service for End-User in Cloud Computing, *IEEE 37th Annual Computer Software and Applications Conference Workshops* 2013: 277-282
[17] J. Pasley. How BPEL and SOA are changing Web services development, *Internet Computing*, IEEE, 2005, 9(3): 60-67.
[18] W.T. Tsai, R.A. Paul, B. Xiao, et al. PSML-S: A process specification and modeling language for service oriented computing, *The 9th IASTED international conference on software engineering and applications (SEA)*, Phoenix. 2005: 160-167.
[19] Drools http:// www.jboss.org/drools/
[20] Jena http://jena.apache.org/
[21] RabbitMQ http://www.rabbitmq.com/

Rui Zhou is a PhD student in Computer Science and Technology at the University of Science and Technology of China. He received his bachelor degree in Xidian University in 2009. His research interests include Cloud computing, service-oriented computing, mobile computing and context-aware. He is author of some research papers published at conference proceedings.

Jinghan Wang is a master student in Computer Science and Technology at the University of Science and Technology of China. He received his bachelor degree in Hefei University of Technology in 2011. His research interests include Cloud computing, rule-based computing, mobile computing and distribute computing.

Guowei Wang is a PhD student in Computer Science and Technology at the University of Science and Technology of China. He received his bachelor degree in the University of Science and Technology of China in 2012. His research interests include Cloud computing, rule-based computing, mobile computing and distribute computing.

Jing Li received his B.E. in Computer Science from University of Science and Technology of China (USTC) in 1987, and Ph.D. in Computer Science from USTC in 1993. Now he is a Professor in the School of Computer Science and Technology at USTC. His research interests include Distributed Systems, Cloud Computing and Mobile Computing. He is author of a great deal of research studies published at national and international journals, conference proceedings as well as book chapters.

Algorithm and Its Implementation of Vehicle Safety Distance Control Based on the Numerical Simulation

Jingguo Qu, Yuhuan Cui, and Weiliang Zhu
Qinggong College, Heibei United University, Tangshan, China
Email: qujingguo@163.com

***Abstract*—Nowadays, the traffic safety problem has become the focus of attention and making a sound and reasonable traffic rules and regulations is the trend. In this paper, based on the traffic rules of driving on the right lane unless overtaking happen, the study first establish the car-following and overtaking model .In car-following model, analyzing the traffic features to obtain the function relationship between the safety distance and speed change; in the overtaking model, TWOPAS stimulation model is adopted to analyze the traffic capacity of highway, and obtain the speed-flow relation graph, overtaking ratio—flow relation scatter graph. It is known through the graph analysis that: (1)when the traffic is sparse, most drivers tend to do free driving with less overtaking, and the traffic rules have no obvious facilitation function on traffic smooth; (2)with the increase of the car flow, the lane becomes narrower, and the overtaking rate decreases continually until it becomes zero. In the process of changing, when the overtaking rate is $[4\%,14\%]$, overtaking stimulates the traffic flow; when the overtaking rate is $[0,4\%]$, overtaking has a decreasing facilitation effect on traffic flow until it becomes zero. Then, construct the analytical model about speed, flow and traffic capacity only in the state of car following. It is found that overtaking has less influence on traffic capacity. And the role this traffic rule plays on traffic smooth is not obvious.**

***Index Terms*—Car-Following Model; Overtaking Model; Numerical Stimulation**

I. INTRODUCTION

Nowadays, traffic safety problem has become the focus of attention, and stipulating sound and reasonable traffic rules is an important part of traffic safety. In most countries, driving on the right side is a common traffic rule to be abode by, and drivers are required to be on the right lane in highway with many lanes unless they want to overtake other cars [1]. When overtaking happens, the driver should move to the left lane to surpass other cars and return to the original lane after it is over. At present, there have been many scholars studied the traffic security problems, puts forward the feasible suggestions for this problem, and relevant conclusions.

De Shengxin and others in the context of "Driver's dynamic visual impact on traffic safety and detection system. Doctoral dissertation of Jilin University". From the Angle of view of the road traffic safety engineering, through the logic analysis, system analysis, literature and other mathematical methods, questionnaire survey, field visits, get the data, and the data processing, a research model based on road traffic safety is established [2]. Paper points out that: The traffic problem has become the focus of the public life, hurt in a traffic accident every year, even more and more the number of people lost their lives, investigate its reason, the government's management of transport mechanism, public awareness of traffic safety, driver's driving behavior normative, and many other factors are the main cause of the traffic safety accident [3].

MaJun in the text of "on the driver's awareness and safety management measures ",the driver's awareness as the main research direction, by studying its awareness [4], then the paper analyses the problems appeared in the process of safety management, and put forward the corresponding countermeasures. Papers consulted a large amount of data, using the logic analysis, system analysis, questionnaire investigation and other methods for the analysis, and combining previous research results of final conclusions. Paper points out that: Eyes, ears and so on human sense organs is the driver to complete the main way of perception. The driver through sight, hearing, smell and touch driving environment and vehicle information [5]. In order to ensure the driver has keen perception, should improve the traffic safety management mechanism, strengthen the training of drivers' awareness.

Dian-Ye Zhang in the text of "driver's dynamic visual field and the safety reliability", research from the Angle of the driver, the driver in the process of the driving field and safety reliability. The paper draws on the predecessors' research results, specific analysis and study their content, through the methods of questionnaire and on-the-spot visiting, obtain reliable data, and by using mathematical method, combining with related software for data analysis, further finally draw the conclusion: During the process of driving, the driver's dynamic visual field affect their attitude, mood, and can affect the driver's awareness [6]. This has led to the driver in the driving process, there are some safety hidden danger. To this end, the driver should adapt to the changing dynamic environment, adjust the mood, avoid fatigue driving, driving safety.

doi:10.4304/jnw.9.12.3486-3493

This paper draws on a lot of predecessors' research results, in vehicles unless overtaking drive on the right of the traffic rules [7], based on the numerical simulation of vehicle safety distance control algorithm and the implementation model, further study of traffic security problems. Considering car-following drive and overtaking drive on the highway with the traffic rule of driving on the right side as the legal one [8]. First of all, the vehicles are doing car-following drive and overtake other cars when the overtaking condition is met, and then return to car-following drive. The same driving trend is repeated again and again. Finally get a safe distance and a function of the speed change. Second, speed and flow rate is established and the analysis model of road traffic capacity, it is concluded that overtaking or not effect on the flow is not big. Due to the fact that motorways have speed limit and it is not the same in different regions, the model in this paper is based on highway regulations in most parts of China with the speed limit of 60-120 km.

II. CAR-FOLLOWING MODEL

In the car-following model, the driver's driving behavior and visual characteristics are analyzed first. Then the following characteristics of the vehicle and safety distance are taken into account.

A. Visual Characteristics

In the process of the vehicle running, 80% of the driver information comes from visual sense [9]. Its visual ability is closely related to driving behavior, determining the running safety of vehicles.

People's view can be divided into static vision and dynamic vision, and dynamic vision is less than static vision. When the car is in high speed, the driver's fixation point moves forward, the vision becomes narrow, and the sense of perimeter becomes less, which greatly influence the traffic safety [2-4]. As is shown in Figure 1, with the improvement of the car speed, the driver's vision sensitiveness decreases, resulting in the decrease on perception ability of visual field information, and having a more likelihood of traffic accidents [5-9].

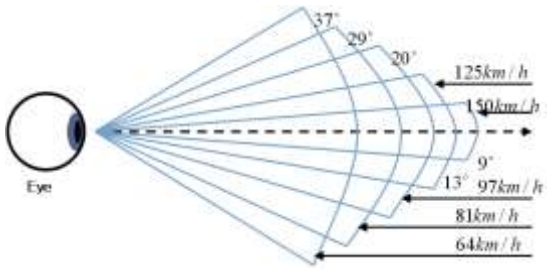


Figure 1. Visual change in terms of different vehicle Speed

Vision capacity refers to the ability to distinguish the minimum distance between two points of, for short, it is called eyesight. The Transfer speed of fixation point for average person is usually 1000/s~2000/s, and the fastest speed can reach 5000/s [10].

Drivers' dynamic vision changes with the change on the speed of the vehicle. The higher the vehicle speed is, the faster the dynamic vision decreases. Dynamic vision is also affected by age. The older the driver is, the bigger the dynamic vision scope decreases.

Vision is also affected by brightness .Night vision is the basic visual function required by the drivers at night, which is the driver's ability to identify the object in darkness. The general night vision decreases about 1/3 than that of eyesight during the day.

In addition, the driver's psychological, physiological and other characteristics will have different degrees of influence on the driving behavior.

B. Car Following Features

In the car following process, the driver accepts the stimulus by the leading car and completes the vehicle speed control by responding to the status change of the leading car through speeding up or slowing down, so as to maintain the safety distance between the leading car and one's own car. This reaction can be reflected in the acceleration speed change of the following car [11].

1) Conditionality

In the motorcade, the driver's following speed is restricted dually by the travel efficiency and safety.

▲In order to achieve desired travel efficiency, the following-car driver is unwilling to be far behind the leading car in the process of driving. Instead, the following-car driver follows the leading car's route closely.

▲From the safety perspective, to avoid collision with leading vehicle, the following-car has to meet two conditions. On one hand, it is to guarantee the "speed condition" (the following-car's speed can only range near the leading-car's speed, and cannot have a faster speed for quite a long time). On the other hand, it is to meet the "distance condition" (there must be sufficient vehicle spacing, so when the leading guide sudden brakes, the following vehicle has enough time to response and brake).

2) Retardance

According to the above conditionality in the process of following vehicle, with the change of leading vehicle's driving state, the state of the following car changes accordingly. But due to the fact that the following car driver needs time to make response to the changes on the driving state of the leading car, and the changes on the flowing car lags behind that of the leading car, the changes of the two vehicles cannot be synchronized. Therefore, the retardance, that is, the time lag phenomenon does exist.

The reaction process includes the four stages of driver's feeling, cognition change, decision-making and implementation about the leading vehicle's running state changes. Viewing from the braking time process, the time spent on driver's feeling, cognition and judgment is called consciousness reaction time, implementation time is time required to move the foot. Set the reaction time as τ_1, including reaction time τ_1' and feet moving time τ_1''. The following vehicle will give response to the leading vehicle at the point of $\tau_1 + t$ about the leading car's behavior at the point of t because of retardance.

The whole reaction time is 0.3~1.0 seconds in common. When human factor and external condition are prominent,

the reaction time will vary greatly [12]. The vehicle braking process is illustrated in figure 2.

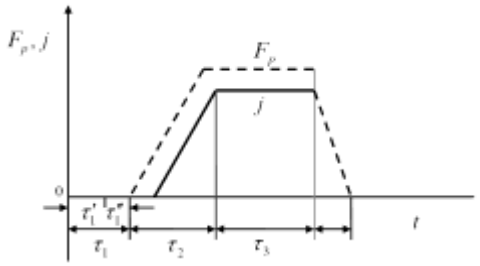


Figure 2. Vehicle Braking Process

3) Transitivity

In the process of car following, the first car's running status restricts the second car, and the second car restricts the third car. Analogy can be made accordingly. Therefore, the number n car restricts the $n+1$ car. If the leading vehicle changes its running status, its effect will be passed down from the following cars one by one until the last car, so it is the transitivity [13]. The information with retardance, passed down backward is not smooth and consistent, but like the pulse being intermittent and continuous.

C. Required Safety Distance

Safe braking distance is the vehicle moving distance during the time the driver finds the leading vehicle's state change, perceives and analyzes relevant information, finally takes emergency braking, until the vehicle stops [13].The corresponding braking safety distance model can be represented as follows:

$$S = v_0 t_d + \frac{v_0^2}{2a} + d \tag{1}$$

But the safety distance model in the braking process mainly considers traffic safety requirements, assuming the leading vehicle stops on the spot suddenly. As a result, the safe distance determined by the model is too big, greatly decreasing the traffic efficiency [14]. To solve the disadvantages of traditional safety distance model, we put forward the concept of required safety distance.

As is shown in Figure 3, in terms of direction, the required safety distance is categorized into forward, lateral and backward safe distance.

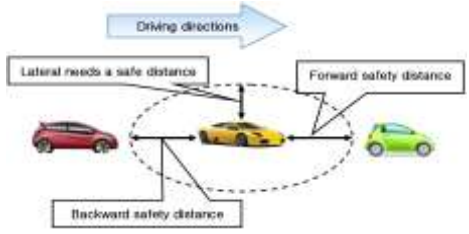


Figure 3. Following car required safety distance

Taking following-car 1 for example, its far end of required safety distance from the leading car is called demand front, and its far end of required safety distance from the following-car 2 is called demand back. The demand frond is equal to the demand back in terms of the distance. In order to distinguish between the lengthways and lateral following safety, the forward and lateral safety distance are called the required safety distance. In the process of car following, the required demand front is controlled by the car-following driver actively while the demand back is passively obtained by the following-car, and it is the required distance set by the leading car.

The required safety distance refers to the minimum distance required by following-car driver, given a certain speed, from the time the driver perceives the leading vehicle movement state change, gives response until the driver operates the car to make the brake.

In the process of driving, traffic speed change will affect traffic flow density. The higher the speed, the greater the need to keep the distance between vehicles, which is reflected in the corresponding sections of traffic flow, that is, the small density. And the micro manifestation of density is car spacing.

Before and after the following conditions is the team two cars there are nonlinear relations and spacing of the average car speed [15, 16], its formula is:

The average space head way and speed of the cars in car-following state enjoy nonlinear relationship, its formula is:

$$S = l + \beta V + \alpha V^2 \tag{2}$$

In the formula: l refers to the car length (m); β refers to the reaction time (s), α is the maximum deceleration function between the leading car and the following car.

Parameter α is nonlinear, the driving speed of the motorcade is constant (or near constant), space headway is equal, α can be approximate:

$$\alpha = 0.5(\alpha_F^{-1} - \alpha_L^{-1}) \tag{3}$$

In the formula: α_F , α_L refers to maximum deceleration of the leading and following car.

Therefore, the distance between the following-car head and the leading car trail [17] can be expressed as:

$$X_n = s - l = \beta V + \alpha V^2 \tag{4}$$

The appropriate distance sought by the following car is to choose a safe distance, namely, the following-car driver's self-perception. That is, if the leading vehicle makes emergency braking, the driver can also avoid the collision with and maintain the minimum distance. The chosen safe distance should have the following characteristics:

(1) The chosen safe distance is distance from the following car front to the leading car back;

(2) The chosen safe distance is in the car following state. It is term for the leading car, is the practical braking distance under constraint condition;

(3) The chosen safe distance is the passive attribute of the following car and is constrained by the leading car.

The required safe distance is different the chosen safe distance:

(1) The required safe distance is just for one car, and is the individual behavior characteristic of one car; the chosen safety distance is for a series of cars, and reflects the state condition of the following car compared to the leading car.

(2) The required safe distance is the active attribute of the following car, determined by itself; the chosen safe distance is the passive attribute of the following car, relied on the leading car and restricted by the leading car.

(3) The required safety distance is the immediate sate parameter, and is determined by the immediate speed; the chosen safe distance is the post state parameter, and is the result after comparing with the leading car.

The speed of car waiting in front of the stop line is zero, namely when $V_F = V_L = 0$, station space is not zero, doesn't deviate a lot from the average station space $\overline{X}_S$. Assume the safe distance when the car stops is $\overline{X}_S$, then formula (4) can be expressed as:

$$X_c = \begin{cases} \overline{X}_S & V_F = V_L = 0 \\ \beta V_L + \alpha V_L^2 & V_L \neq 0 \end{cases} \quad (5)$$

As is shown in Figure 4, distance demand saturation index coefficient: $C = X_n / L$, analyze the chosen safe distance of the car following in three ways.

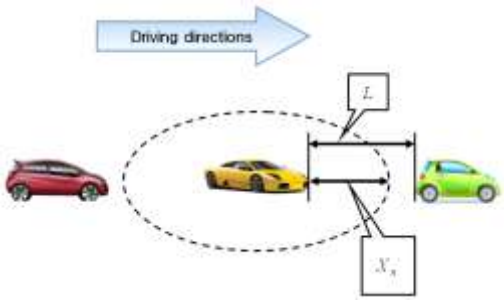


Figure 4. The car following state

In formula (5), find derivation in $(0,+\infty)$, the result is:

$$\dot{X}_c = \beta + 2\alpha V \quad (6)$$

Because $\dot{X}_c > 0$, $\dot{X}_c = \beta V + \alpha V^2$ is monotone increasing in the range of $(0,+\infty)$.

When the speed of the following car is smaller than that of the leading car, the required safe distance of the following car is less than the required safe distance of the leading car $X_{nF} < X_{nL}$, See figure 5.

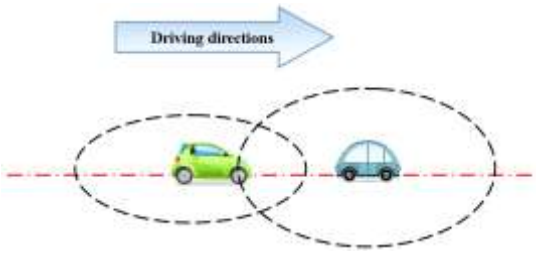


Figure 5. The required safe distance per following unit ($X_{nF} < X_{nL}$)

It is seen in figure 5 that the required front lags behind the leading car, namely $C < 1$. The distance between the following car and the leading car is bigger than the required safe distance of the following car, and the actual car distance is enough for the following car to make brake to stop. At that time, the required safe distance of the leading car is far bigger than the distance between the front and back cars, but it will not influence the driving safety of the following car. Due to the fact that the chosen safe distance is bigger than the required safety distance of the following car, the following car can guarantee safety by maintaining the current speed. But considering the following car's efficiency, the driver can speed up until the required front touches the leading car, and keep to follow the leading car.

Figure 6. The required safe distance per following unit ($X_{nF} > X_{nL}$)

As is shown in figure 6**,** when the following car's speed is bigger than the leading car, the required safe distance of the leading car is less than that of the following distance. The required front of the following car surpasses the leading car. If the leading car doesn't make emergency brake, the car space between the front and the back cars cannot satisfy the following car's requirement to make brake, so there is a likelihood that the cars may collide with each other. When the leading car cannot provide the required safe distance of the following car, the following car driver will decrease the car speed automatically to guarantee the driving safety, seek the leading car's required back edge, maintain the same speed of the leading car, and follows it. Under the new balance state, the following car's demand front space just touches the leading car, namely $C = 1$.

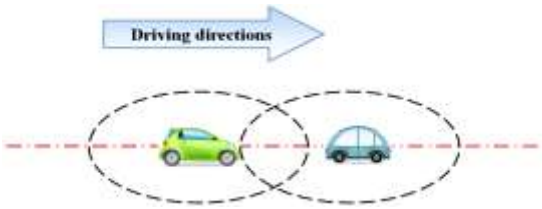


Figure 7. The required safe distance per following unit ($X_{nF} = X_{nL}$)

As is shown in Figure 7, when the following car speed is equal to that of the leading car, the required safe distance of the two cars are identical. The following car required front just falls on the back part of the leading ca, and the leading car's required back front just falls on the car head edge of the following car. Under this circumstance, the following car can lag behind and avoid traffic accident, so as to guarantee a safe and effective state to drive following the leading car [18]. In this way

keeping $C=1$ is a safe and effect state, considered to be following balance state. In short, it is called a balance state.

It is concluded that under imbalance state, the following car takes the chosen safe distance as the goal to adjust the driving state. The driver seeks to follow the route of the leading car's required back edge, and maintain the same speed with the leading car. When the driver chooses the safe distance, in fact, it is the motivating force for the motorcade to keep balance. In the process of following-drive, the driver seeks the required back edge of the leading car, and chooses the leading car's required safe distance.

The fact is that even if the leading car has less speed than the following car, the driver will still choose to speed up so as to shorten the distance between the leading car and the following car.

According to the following motion characteristics, the following model expression is:

$$\ddot{X}_F = \frac{\lambda_3}{mT^2}(L - X_{nF}) + \frac{\lambda_4}{nT}(\dot{X}_L - \dot{X}_F) + \frac{\lambda_5}{hT^2}(L_3 - L) \quad (7)$$

In the expression: L is the immediate car space; $\dot{X}_L$ is the immediate speed of the leading car; $\dot{X}_F$ is the immediate speed of the following car; $\dot{X}_{nF}$ is the required safety distance of the following-car at the speed of X_F; L_3 is the car distance between the two balances; $\frac{1}{m}, \frac{1}{n}, \frac{1}{h}$ refers to weight coefficient respectively; the reaction time for the driver from perceiving the signal, identifying, judging to giving the final behavior, is marked as T; λ_3 , λ_4 , λ_5 need to be obtained by experiment.

III. Overtaking Model

A. Analysis of the Overtaking Process

When the vehicle drives in the two-lane express way, without the interference of the surroundings or the interfering factors are relieved, with the overtaking will of drivers, as well as the overtaking condition is met, the driver can begin overtaking other vehicles.

The overtaking process in the two-lane express way can be mainly divided into the following procedures: the judgment of overtaking willingness; the choice of overtaking mode; the inspection of overtaking condition; the implementation of overtaking behavior; the return to the previous lane when overtaking is over.

(1) Judgment of overtaking willingness. When the free driving car comes near the front car or the car is under the car-following state, if the current speed is less than its expected speed, the car will try to overtake other cars to change its driving state. Under this circumstance, the driver will have an overtaking will.

(2) The choice of overtaking mode. The car with overtaking will decides which mode to take. If the car is just moving freely and comes near toward the front car, then it is an overtaking mode with equal speed. If the car is driving by following the previous car intentionally, and comes near the front car, then the mode is overtaking by accelerating the speed.

(3) The inspection of overtaking condition. Three conditions must be inspected before the overtaking behavior for cars with overtaking will is implemented:

★Consider whether overtaking is restricted by some factors, such as the lane line, no overtaking area, etc.

★Whether the car can accomplish the overtaking, namely, passing sight distance is less than the distance from the coming car in the opposite direction.

★Whether the surrounding environment is suitable for overtaking, namely whether there is enough space for the vehicle flow driving in the same direction to return to the original lane after overtaking.

The computation formula of passing sight distance is shown in (8):

$$S_0 = S_1 + S_2 + S_3 = \left\{ \left(\frac{V_0}{3.6} \times t_1 + \frac{a \times t_1^2}{2} \right) + \frac{V}{3.6} \times t_2 + S_3 \right\} \quad (8)$$

In the formula S_0 —passing sight distance (meter);

S_1 —the accelerating distance for overtaking vehicle (meter);

S_2 —the constant speed distance for overtaking vehicle on the left lane. (meter);

S_3 —when overtaking finishes, the safe distance between vehicle $n+1$ and vehicle $n-1$ (meter);

$S_3 =$ 30~100 (meter), usually $S_3 =$ 40 (meter);

V_0 —the speed of the vehicle before overtaking (kilometer/hour);

V —the constant speed of the overtaking vehicle,

$V = V_0 + a \times t_1$ (kilometer/hour)

t_1 —acceleration time (second);

t_2 —constant speed time of overtaking vehicles (second);

a —average acceleration of the overtaking vehicle (meter/second^2).

(4) The implementation of overtaking behavior. When the fast vehicle surpasses the slow vehicle, when sight distance and left lane vehicle flow meet the requirement of overtaking, the left lane is adopted to accomplish the overtaking [19]. To guarantee the safety, when the overtaking vehicle drives on the left lane, it should keep enough safety distance with its right ahead vehicle. When the original lane has enough space, the overtaking vehicle returns to the original lane and finishes the overtaking process.

(5) The return to the previous lane when the overtaking is over. During the process of overtaking, when it fails to make the overtaking requirements, then the overtaking process should be stopped and the vehicle comes back to its original lane. It happens when the space between the overtaking vehicle and the right front car on the left lane is not sufficient, or the returning space is too small.

Due to the diversity of overtaking behavior and the driver's features, the overtaking process is complicated,

and influenced by many factors of road environment, the road shape, sight distance, vehicle type, speed and drivers, etc. The current study mainly deals with the parameter of the cars.

In the overtaking model, the speed limit is taken into account. In China, the highway speed range is 60-120 km/h.

B. Utilize Overtaking Rate to Determine the Traffic Capacity

The overtaking rate reflect the driving freedom degree of the vehicles in the highway, which can be taken as an indicator of analyzing the highway traffic capacity.

Adopt the simulation model to analyze the traffic capacity of highway. Figure 8 is the speed-flow relational graph by using the highway stimulation system TOWPAS to make simulation experiment. In graph 10, with the increase of traffic flow, the speed is on the declining curve, but the critical point of the traffic flow state cannot be found. Figure 9 the overtaking rate-flow scatter graph by using TWOPAS. In figure 9, at the beginning stag, with the increase of the traffic flow on the highway, the overtaking rate is increased till its maximum; later, with the flow increase, the overtaking rate decreases. When the flow reaches 2900pcu/h, the overtaking rate is nearly zero, taking the stimulation flow at this critical point as the traffic capacity of highway. Therefore, it is recommended that the traffic capacity of China's standard highway is 2900pcu/h.

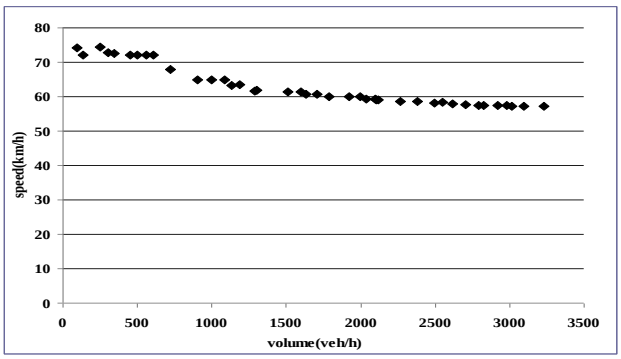


Figure 8. TWOPAS simulation relation of speed))volume

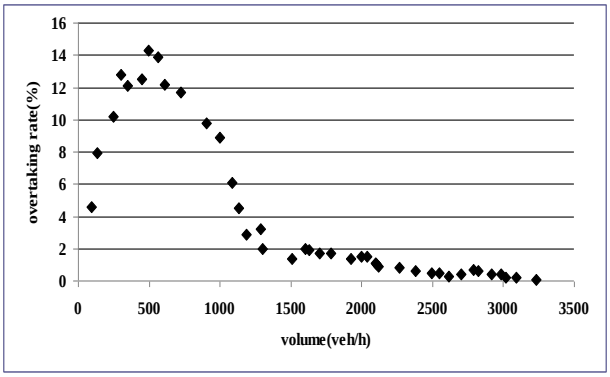


Figure 9. TWOPAS simulation relation of overtaking ratio)) volume

Adopt TWOPAS model to make stimulation experiment, obtain overtaking rate, and analyze the traffic capacity and other traffic flow traits.

Figure 9 is the relation curve with the change law reflecting the traffic rule performance of sparse traffic and heavy traffic and it is in line with the real situation.

(1) When the traffic is sparse, that is when the highway flow is small, vehicles can drive freely with few overtaking. With the traffic flow increase, the overtaking requirement is increased gradually, and the space between cars is sufficient, so as to provide more overtaking opportunity for vehicles with good performance and high expectation for speed. Therefore, the overtaking rate increases until its highest point, then the traffic vehicle volume is increased with the overtaking rate.

(2) When the traffic is heavy, that is with the flow growing increasingly, the road becomes narrower, the interference among cars becomes bigger, and the supplied overtaking space becomes smaller [20]. Therefore, the overtaking rate decreases continually until overtaking is stopped. Viewing the declining process of the overtaking rate, it is found that the overtaking rate decreases obviously at the beginning, showing that the interference among cars becomes bigger, the overtaking rate becomes sensitive to the flow increase. But the vehicle can still maintain a relatively high driving freedom. After then, the overtaking change rate becomes smaller because the interference becomes bigger and driver's driving freedom is influenced greatly. It is not very obvious for the number of vehicles with overtaking capacity to become less with the traffic flow increases continually. When the flow is close to the traffic capacity, the overtaking rate is zero.

C. Adopt the Available Space oeturning to the Original Lane to Determine Traffic Capacity

After referring to relevant material, take 3.1 seconds as a car following indicator. Based on the study result of HCM2000, given the overtaking rate is 94% when the traffic flow in China highway reaches its traffic capacity. Utilize TWOPAS simulation to obtain the overtaking rate—volume relation, as is shown in Figure 10. The overtaking rate increases with the increase of the flow, it is gradually near 100%.

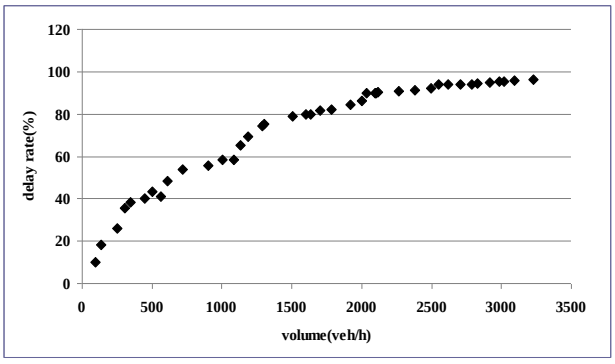


Figure 10. TWOPAS simulation relation of follow ratio volume

Table 1 reflects the overtaking rate of TWOPAS when the simulation flow is 2800pcu/h—3200pcu/h. It is seen from Table 1 that when the flow is 2800pcu/h—3200pcu/h, the overtaking rate is 94%—95%. And when

the flow is 2900pcu/h, the overtaking rate is 94%. When the flow reaches 3200pcu/h and above, the overtaking rate is 96%, and stay static. Therefore, the traffic capacity of the overtaking rate—flow relation simulation graph is 2900pcu/h.

TABLE I. TWOPAS SIMULATION VOLUME AND OVERTAKING RADIO

Simulation volume (pcu/h)	2800	2900	3000	3100	3200
overtaking radio (%)	94	94	95	95	96

D. Analysis of the Speed, Flow and Traffic Capacity

When studying whether the traffic rule of "driving on the right side unless overtaking is required" is effective or not, consider the influence of the speed change on the traffic flow when overtaking and following-drive are considered, so as to obtain the result.

◆ Relation model of Single lane flow q and the vehicle speed v

Factors influencing the traffic capacity are: vehicle speed, length of single car, safety distance, drivers' feeling, and reaction time, etc. Assume:

(1) Vehicle speed is v (unit: m/h), that is the driving distance of the motorcade per hour;

(2) Flow is q (unit: veh/h), that is the number of vehicles passing the observation point per hour in the single lane;

(3) Feeling-reaction time is T (unit: s), that is the time interval that the drivers on the back car press on the brakes when there is a condition or take other suitable treatment measures;

(4) The length of the single car is a (unit: m).

Under the above assumption of (1)-(4), the car's driving speed per second is $\frac{v}{3600}(m)$. Due to the fact that the car distance is the safe distance between the front car and the back car. It refers to the driving distance during the time interval that the drivers on the back car press on the brakes when there is a condition or take other suitable treatment measures. The car distance is: $\frac{v}{3600}\times T$. Therefore, the required safe road-occupying length for the driving car (called the space headway) is $\frac{v}{3600}\times T + a$.

Because the traveling distance for the motorcade per hour is $l = v$. The cars during this length can all pass the observation point, and the cars passing the observation point are just the cars driving on this length. Therefore, the flow q is the vehicle number during the road whose length is $l = v$ per hour.

$$q = \frac{l}{\frac{v}{3600}\times T + a} = \frac{v}{\frac{v}{3600}\times T + a} \tag{9}$$

(9) is relation function model, revealing the relationship between the single lane car flow q and the car speed v, that is $q = q(v)$.

◆ Property and limit flow of the relation function between flow and car speed

In (4-10), the derivation of the function $q(v)$ toward v, it is obtained that

$$q'(v) = \frac{a}{\left(\frac{v}{3600}\times T + a\right)^2} > 0$$

The flow $q(v)$ is monotone increasing function of the car speed v, that is when the speed v becomes bigger, the flow $q(v)$ becomes bigger, namely there is no so-called maximum flow and maximum speed, and because

$$\lim_{v\to\infty} q(v) = \lim_{v\to\infty} \frac{v}{\frac{v}{3600}\times T + a} = \lim_{v\to\infty} \frac{1}{\frac{1}{3600}\times T + \frac{a}{v}} = \frac{3600}{T} \tag{10}$$

The limit exists, and combine the condition that the flow $q(v)$ is monotone increasing function of the car speed v. It is know in (10) that the limit value $\frac{3600}{T}$ is the traffic capacity of the one way traffic in single lane. We call this limit as the limit flow of the single lane(or limit traffic capacity). If the feeling-reaction time $T = 1.0s$, then the limit flow per hour on the single lane is 3600.

◆the flow when the parameter is known

Single car length $a = 5m$, feeling—reaction time $T = 1.0s$, speed $v = 60km/h$. Based on (4-10), it is known the flow per hour on the one lane (that is the road traffic capacity) is

$$q(60000) = \frac{60000}{\frac{60000}{3600}\times 1 + 5} = 2769(veh/h)$$

In the same way, when feeling—reaction time $T = 2.0s$,

$$q(60000) = \frac{60000}{\frac{60000}{3600}\times 2 + 5} = 1565(veh/h)$$

When feeling—reaction time $T = 3.0s$, the traffic capacity $q(60000) = 1090(veh/h)$.

TABLE II. DATA FLOW TABLE PER HOUR ON THE SINGLE LANE

v (km/h)	T (s)		
	1	2	3
6	900	720	600
20	1894	1241	923
40	2482	1469	1043
60	2769	1565	1090
80	2938	1617	1116
100	3050	1651	1132
120	3130	1674	1142
∞	3600	1800	1200

The parameter single length $a = 5m$, feeling—reaction time, the several concrete value of car speed, the flow data per single lane per hour is shown in(9) (traffic flow capacity), see Table 2.

It is known from Graph 2: when the car legnth $a = 5m$, feeling—reaction time $T = 3.0s$, when motorcade drives in high speed ($60km/h < v < 120\ km/h$), speed has little influence on the flow. This conclusion can be obtained through relation function of the flow $q(v)$ and speed v in (9).

It is concluded that the speed change has little influence on the flow, that is the traffic rule has less obvious function on the traffic smooth.

IV. CONCLUSIONS

The establishment of the car-following model and the overtaking model vividly describe the movement status of the vehicle driving on the highway by following the traffic rule of driving on the right lane. Make objective and effective analysis of the relationship among different variables under this rule. Consider the problem with a comprehensive perspective and obtain reasonable and effective results.

ACKNOWLEDGMENT

This research was supported by the National Nature Foundation of China (Grant No. 61170317) and the National Science Foundation for Hebei Province (Grant No.A2012209043), all support is gratefully acknowledged.

REFERENCES

[1] Hongfei Jia. City Road car following behavior neural network simulation model. *Changchun: Jilin University*, 2002.

[2] Wenqing Wang, Wuhong Wang, Yonggang Zhong Etc. And the fuzzy inference is realized following safe distance control algorithm based on. *Journal of traffic and Transportation Engineering*, 2003, 3(1): 72-75.

[3] De Shengxin, Xiao Longlin, Yun Hualu. Driver's dynamic visual impact on traffic safety and detection system. *Doctoral dissertation of Jilin University 84. Automotive Engineering*, 1998, 20(3): 82-86

[4] Zhanhong Zhang. Study on the driver's state of emergency brake reaction time simulator based on. *Journal of North China Institute of Science and Technology*, 2009, 6(3): 27-30.

[5] Jun Ma. Perceptual characteristics and Countermeasures for safety management on drivers'. *Traffic science and technology*, 2000, 17(10): 89-92.

[6] Dianye Zhang. Dynamic visual field of driver and driving safety reliability. *Journal of Southwest Jiao Tong University*, 2000, 35(6): 319-322.

[7] Jie Xu, Wen Du, Hong Sun. Following the analysis of vehicle safety distance. *Journal of traffic and Transportation Engineering*, 2002, 2(1): 101-104.

[8] Haoran Zhang, Wei Wang, Gang Ren. With the safety car following model based on the distance. *Beijing: The second Chinese international road traffic safety products exposition and intelligent traffic Forum*, 2006.

[9] Lisbeth Harms. Variation in drivers congunative load effects of driving through village areas and rural junctions. *Ergonomics*, 1991, 34: 19-23.

[10] Thomas A, Ranney. Models of driving behavior: a review of their evaluation. *Accident Analysis and Prevention*, 1994, 26(6): 733~750.

[11] Brackstone M, Sultan B, McDonald M. Motorway driver behaviour: Studies on car following. *Transportation Research Part F*, 2002, 5(1): 31-46.

[12] Davis L C. Modifications of the optimal velocity traffic model to include delay due to driver reaction time. www. elsevier. com/locate/physa. 2007, 6

[13] Helly. Simulation of bottlenecks in single lane traffic flow. In symposium on theory of traffic flow. *Research Laboratories, General Motors, proceedings*, 1959: 207-238.

[14] Regulinski T L, Askren W B. Stochastic modeling of human Performance effectiveness functions. *In Proceedings of 1972 Annual Reliability and Maintainability Symposium*, 1972, 02: 45-48

[15] Rumar K. The basic driver error: Late detection. *Ergonomics*, 1990, 33: 1281-1290.

[16] Deng Pan, Yingping Zheng. Calculation of hyperbolic function of vehicle deceleration strategies and safe following distance based. *Computer and communications*, 2007, 25(5): 54-58

[17] Narendra K S, Balakrishnan J. Transportation Research Board of the National Academies. *Automatic Control, IEEE Transactions on.* 8(6), 2002.

[18] Zhang Quan, Metro Vehicle Safety Monitoring System. *Scientific and technological information*, 2012.

[19] Yan Bin, China University of Science and Technology Research Tunnel vehicle safety technology entropy state model based on, 2013.

[20] Zhang Yongbo. Problems and countermeasures vehicle safety operation management. *Chongqing Jiaotong University*, 2014.

Jingguo Qu Male, born in 1981, Master degree candidate. Now he acts as the Math teacher in Qinggong College, Hebei United University. He graduated from Harbin University of Scince and Technology, majoring fundamental mathematics. His research directions include mathematical modeling and computer simulation, the design and analysis of parallel computation, elastic problems numerical simulation, and etc.

Yuhuan Cui Female, born in 1981, Master degree candidate. Now he acts as the Math teacher in Qinggong College, Hebei United University. She graduated from Yanshan University, majoring computational mathematics. Her research directions include mathematical modeling and computer simulation, the design and analysis of parallel computation, elastic problems numerical simulation, and etc.

The Study and Improvement of Unidimensional Search about Nonlinear Optimization

Yuhuan Cui, Jingguo Qu, and Weiliang Zhu
Qinggong College, Heibei United University, Tangshan, China
Email: qujingguo@163.com

***Abstract*—This paper, which introduces the destination of one dimensional search, search interval and solving method, improves on the basic method and builds faster method of one dimensional search which includes inexact research and exact research. And then this paper concludes the method of global optimization and makes a further contrast and discuss about its convergence .At the last, this paper checking the effectiveness of this method by putting it into use to special case.**

***Index Terms*—One Dimensional Search; Global Optimization; Convergence; Inexact Research; Exact Research**

I. INTRODUCTION

The method of one dimensional search is a basic method resolving the problem of nonlinear optimization. Looking for a fast and efficient one dimensional search is a basic issue. At present, there are many methods about one dimensional search, which can be grouped into two categories. [1] (1) Trial Method such as golden section and bisection method and so on. (2) Function Approximation Method such as Newton tangent method, quadratic interpolation method and rational interpolation method and so on. This paper introduces a hybrid method protected by a factitious interval, and this method combines Trial Method and Function Approximation Method.

In 2012, Chen Lin in the text of "Several types of the nonlinear optimization problem solution set" [2], under the unchanged generalized convexity studies several main kinds of nonlinear optimization problem solution set. This paper introduces the solution set depict the research status of nonlinear optimization problem. On Dini directional derivative definition, study of nonlinear optimization problem solution set. The author gives the definition on Dini directional derivative, some properties of several kinds of unchanged generalized convexity, and the solution set of nonlinear optimization problem, the objective function is the same convex, constraint function is a pseudo linear. When the objective function and constraint functions are pseudo linear, further results are obtained. Article also in Clarke sub differential is defined, the no smooth pseudo invariant with though laser by words are given some properties of convex optimization problem, the solutions for these problems, and example is given. The article pointed out that in general target space vector optimization problems were studied in two true efficient point - Henig efficient point and cone characterizations Hurwicz really effectively. The main use of the collection at some point of the cone and normal cone of dependence and the feasible direction cone for the vector optimization problems effectively depict the characteristics.

In 2006, Yonghong Ren in the text of "Nonlinear Langrange method of solving nonlinear optimization problems" [3], established on multiplier is a linear function of a class of nonlinear theory frame of Langrange method. First, several assumptions are given to ensure the convergence of the nonlinear Lagrnage algorithm, at the same time these conditions to build based on the analysis of the nonlinear Langrange function duality theory and Heses Lagrnage function matrix condition number are necessary. Paper discussed two factorial convergence of iterative method, the function if the problem is proved Heses array LipshcZti conditions, the sequence produced by 2 factorial sub iteration method with second order linear convergence rate.In the end, given by the paper is verified by numerical experiments based on the nonlinear nage La bad function of dual effectiveness of the algorithm. The paper established on multiplier is a nonlinear function theory frame of another class of nonlinear though laser method, and gives some assumptions in place to ensure that the class of nonlinear Lagrnage convergence of the algorithm. These conditions in the analysis of condition number of Heses Lagarnge function matrix, and to establish corresponding duality theory are necessary, To verify the existing in the literature many nonlinear Lagrnage function meet these conditions. At the same time, also set up for a class of nonlinear Lagrnage method based on the NCP function structure of the theoretical framework.

In 2007, Jinli in the text of "A differential equation solving constrained nonlinear optimization method" [4], constructs the differential equation method for solving nonlinear optimization problems, including the system of two differential equation, the first system based on the function of the first order information, the second system based on second order information. The two systems have properties: Local optimal solution of the nonlinear optimization problem is their asymptotic stability of equilibrium point, and the initial point is feasible, the solution trajectory are falls in the feasible region. Paper proves that the system of two differential equation

doi:10.4304/jnw.9.12.3494-3501

discrete iterative format of the convergence theorem and the second system based locally quadratic convergence properties of the discrete iterative format. At the same time, the discrete iterative method based on the two systems are given numerical example, the numerical results show that the differential equation method based on second order information faster.

Base on one dimensional search of the golden section method building a method of solving the global optimal solution [1] is a fairly simple and effective method. It has three main features [4], (1) Approximating global optimal solution by any precision; (2) Overcoming the shortcomings of the direct solution requires a large amount of computer memory; (3) Having low requires about the objective function and being suitable for those optimal issue that only know the time sequence but the function expressions do not know, let alone the gradient information of the function. The innovation of this article lies in one-dimensional search for specific, detailed introduced the global optimization method, convergence. With accurate one dimension search comparison, carries on the corresponding improvement, greatly reduce the workload to relevant studies.

II. One Dimensional Search

A. Destination of One Dimensional Search

One dimensional search, also known as linear search, refers to a single-variable function optimization and multi-variable function is optimized foundation. In multi-variable optimization function, the iteration scheme [5]

$$x_{k+1} = x_k + \alpha_k d_k \tag{1}$$

Construct the search direction d_k and step length factor α_k, suppose

$$\phi(\alpha) = f(x_k + \alpha d_k) \tag{2}$$

Thus, from x_k, and along the search direction of d_k, determining the step length factor α_k $\phi(\alpha_k) < \phi(0)$. This is one dimensional search.

When seek α_k, which makes objective function reaching reaches its minimum at the direction of d_k,

$$f(x_k + \alpha_k d_k) = \min_{\alpha>0} f(x_k + \alpha d_k)$$

or

$$\phi(\alpha_k) = \min_{\sigma>0} \phi(\alpha)$$

Thus claimed that such one dimensional search for the optimal one dimensional search, or exactly one dimensional search, and α_k is the most optimal step length factor. While if α_k makes the objective function to obtain an acceptable amount of decline, even though the amount of decline $f(x_k) - f(x_k + \alpha_k d_k) > 0$ is acceptable to the user, such a one-dimensional search claimed approximate one-dimensional search, or inexact one-dimensional search, or an acceptable one-dimensional search.

B. Search Interval and the Method of Determining the Interval

Destination 1 Suppose $\phi: R \to R$, $\alpha^* \in [0, +\infty)$ and $\phi(\alpha^*) = \min_{\sigma\geq 0} \phi(\alpha)$

If there is a closed interval $[a,b] \subset [0,+\infty)$, which makes $\alpha^* \in [a,b]$, this paper claim $[a,b]$ is search interval of one-dimensional minimization $\min_{\sigma\geq 0} \phi(\alpha)$.

One simple method determining search interval named advance and retreat. Its basic idea is starting from one direction, at a certain step, trying to determine the function value presents three "high - high - low". If the direction is wrong, return to, and then looking in the opposite direction. Specifically, determining the initial point α_0, the initial step $h_0 > 0$, if

$$\phi(\alpha_0 + h_0) > \phi(\alpha_0)$$

Then lengthening step length and starting from the new point $\alpha_0 + h_0$ search forward continue. However, if $\phi(\alpha_0 + h_0) > \phi(\alpha_0)$ that the next step starts from α_0. And search in the opposite direction. Stop when the objective function rises. Thus, getting a search interval and this method named advance and retreat.

★Steps of advance and retreat:

Step 1: Select the initial data. $\alpha_0 \in [0, +\infty)$, $h_0 > 0$, double-coefficient $t > 1$, calculate $\phi(\alpha_0)$, $k := 0$.

Step 2: compare the value of objective function. Let $\alpha_{k+1} = \alpha_k + h_k$, calculate $\phi_{k+1} = \phi(\alpha_{k+1})$, if $\phi_{k+1} < \phi_k$, to step 3, if not, to step 4.

Step 3: lengthen step length. Let $h_{k+1} := th_k$, $\alpha := \alpha_k$, $\alpha_k := \alpha_{k+1}$, $\phi_k := \phi_{k+1}$, $k := k+1$, to step 2.

Step 4: searching at opposite direction. If $k = 0$, change direction, let $h_k := -h_k$, $\alpha_k := \alpha_{k+1}$, to step 2; Or stop, let

$a = min\{\alpha, \alpha_{k+1}\}$, $b = max\{\alpha, \alpha_{k+1}\}$

Exporting the $[a,b]$.

III. Exact One Dimensional Search

Exact one dimensional search includes 0.618, Dichotomy and Interpolation (quadratic interpolation and Cubic Interpolation). The method proposed by this paper basing on golden section to resolve global optimal solution is simple and effective.

A. Fundamental Principle

Golden section method [6], being famous for simple and effect and basis of most optimization, is a classic method. Taking points $x_1 = a + 0.382(b-a)$ and $x_2 = a + 0.618(b-a)$ from $[a,b]$, if $f(x_1) > f(x_2)$, let $a = x_1$; if $f(x_1) \leq f(x_2)$, let $b = x_2$, and restart. The search interval narrows range of 0.382 or 0.618 times until reduce to a point by this way. Golden section method is a fast convergence of the one-dimensional search method [7].

B. Calculate Method

Suppose objective function is $f(x) \in C^1$, $x \in D \subset R^2$, $f(x)$ has lower bound in region D. the way proposing optimization problems:

$$x^* = \arg\min_{x \in D} f(x)$$

Resolving the optimal solution of convex function $z = f(x, y)$, depends on the region $D = \{(x, y) | a \le x \le b, c \le y \le d\}$.

Method steps:

Step1: $\varepsilon > 0$, Points a, b, c, d, whose diameter is ϕ_0 and the center is (x_0^*, y_0^*), the function value is f_0^* at the point.

Step2: Calculate and determine the position of a_1, b_1, c_1, d_1, $p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8$.

Step3: Judge whether diameter of each small rectangle less than ε. If it is, judge whether the function value at the centre point of rectangle less than f_0^*, if it less than f_0^*, then, endow the coordinate of centre to (x_0^*, y_0^*), replace the f_0^* with the function value at the centre point. Or turn to step4.

Step4: Endow the four vertices of the new rectangle to a, b, c, d, then to step2.

Step5: Print (x_0^*, y_0^*) and f_0^*.

This is a direct solution for one-dimensional unconstrained global search optimal solution. The classic method is extended 0.618 to two-dimensional by the one-dimensional, the original scope of the algorithm consists of a single peak function is extended to a multi-modal function, so it can resolve the global optimal solution, the algorithm has a simple structure, high precision, computer hardware requirements low.

C. The Analysis of Convergence

The common style of unconstrained optimal solution is follow:

First step: determine $x_0 \in R^n$, $0 \le \varepsilon << 1$.

k Step: calculate the direction of decline d_k;

Calculate step length factor α_k, makes

$$f(x_k + \alpha_k d_k) = \min_{\alpha \ge 0} f(x_k + \alpha d_k) \quad (3)$$

Let

$$x_{k+1} = x_k + \alpha_k d_k \quad (4)$$

if $\|\nabla f(x_{k+1})\| \le \varepsilon$, stop; or, repeat the steps above.

Let

$\phi(\alpha) = f(x_k + \alpha_k d_k)$

Apparently

$\phi(0) = f(x_k)$, $\phi(\alpha) \le f(x_k)$

It is difficult to resolve the minimum point about $\phi(\alpha) = f(x_k + \alpha_k d_k)$ by equation (3). Generally, it always gets the first stationary point of $\varphi(\alpha)$, then select α_k, makes

$$\alpha_k = \min\{\alpha | \nabla f(x_k + \alpha d_k)^T d_k = 0, \alpha > 0\} \quad (5)$$

Because it should resolve the minimum point and stationary point depending on equation (3) and (5), so the equation (3) and (5) were claimed one dimensional exact research principle or linear exact research principle. Let $\langle d_k, -\nabla f(x_k) \rangle$ represents the angle between the vectors d_k and $-\nabla f(x_k)$. then

$$\cos\langle d_k, -\nabla f(x_k) \rangle = -\frac{d_k{}^T \nabla f(x_k)}{\|d_k\| \|\nabla f(x_k)\|}$$

Theorem 1 Suppose α_k >0 is the solution of (3), $\|\nabla^2 f(x_k + \alpha d_k)\| \le M$, it is effective for $\alpha > 0$, M present a certain normal number, then

$$f(x_k) - f(x_k + \alpha d_k) \ge \frac{1}{2M} \|\nabla f(x_k)\|^2 \cos^2 \langle d_k, -\nabla f(x_k) \rangle \quad (6)$$

Theorem 2 Suppose $f(x)$ is a continue differentiable functions, and any minimization algorithms compliance with standards $f(x_{k+1}) \le f(x_k)$, $\forall k : \nabla f(x_k)^2 d_k \le 0$. Suppose $\bar{x} \in D$ is accumulation point of sequence $\{x_k\}$, K_1 is index set meeting $\lim_{k \in K_1} x_k = \bar{x}$. Assuming there is $M > 0$, makes $\|d_k\| < M$, $\forall k \in K_1$. Suppose $\bar{d}$ is one of the accumulation points on the sequence $\{d_k\}$, then

$$\nabla f(x)^T \bar{d} = 0 \quad (7)$$

Further, assuming quadratic function $f(x)$ is continue and differentiable on the region D. Then

$$\nabla^2 f(\bar{x}) \bar{d} \ge 0 \quad (8)$$

Theorem 3 suppose $\nabla f(x)$ exist on the level set $L = \{x \in R^n | f(x) \le f(x_0)\}$ and uniform continuity .The angle θ_k between the vectors d_k produced by the method and $-\nabla f(x_k)$ meeting

$$\theta_k \le \frac{\pi}{2} - \mu, \text{ for } \mu > 0 \quad (9)$$

For a certain k, $g_k = 0$, or $f_k \to -\infty$, or $\nabla f(x) \to 0$.

Lemma 1 Suppose function $\varphi(\alpha)$ is quadratic continue and differentiable in the closed interval $[0, b]$, and $\varphi'(0) < 0$. If the minimal point of $\varphi(\alpha)$ is $\tilde{\tilde{\tilde{\alpha}}}^* \in (0, b)$, then

$$\tilde{\tilde{\tilde{\alpha}}}^* \ge \bar{\alpha} = \frac{\varphi'(0)}{M} \quad (10)$$

$\varphi''(\alpha) \le M, \forall \alpha \in [0, b]$.

Lemma 2 Suppose function $f(x)$ is quadratic continue and differentiable in R^n, then for any vectors x, $d \in R^n$ and any real number α meeting

$$f(x+\alpha d) = f(x)+\alpha g^T d+\alpha^2 \int_0^1 (1-t)[d^T G(x+t\alpha d)d]dt \quad (11)$$

Lemma 3 Suppose function $f(x)$ is quadratic continue and differentiable in the neighborhood of minimal point x^*, and exist $\varepsilon > 0$ and $M > m > 0$, makes when $\|x-x^*\| < \varepsilon$,

$$m\|y\|^2 \le y^T G(x) y \le M\|y\|^2, \forall y \in R^n \quad (12)$$

$$\frac{1}{2}\|x-x^*\|^2 \le f(x)-f(x^*) \le \frac{1}{2}M\|x-x^*\|^2 \quad (13)$$

$$\|g(x)\| \ge m\|x-x^*\| \quad (14)$$

There is a theorem about convergence rate.

Theorem 4 Suppose the sequence $\{x_k\}$ produced by the method convergence to x^*,which is the minimal point of the function $f(x)$. If $f(x)$ is quadratic continue and differentiable in a tertian neighborhood of minimal point x^*, and exist $\varepsilon > 0$ and $M > m > 0$, makes when $\|x-x^*\| < \varepsilon$

$$m\|y\|^2 \le y^T G(x) y \le M\|y\|^2, \forall y \in R^n \quad (15)$$

Then, the sequence $\{x_k\}$ is linear convergence [2].

At the last, the paper gives the declining contents estimates equation of the function produced by the way accurate a number.

Theorem 5 Suppose α_k is step length factor produced by the way accurate a number, $f(x)$ meeting

$$(x-z)^T[\nabla f(x)-\nabla f(z)] \ge \eta\|x-z\|^2 \quad (16)$$

Then

$$f(x_k)-f(x_k-\alpha_k d_k) \ge \frac{1}{2}\eta\|\alpha_k d_k\|^2 \quad (17)$$

D. Algorithm for Example

To solve the optimization problem, we use mathematical methods and principles to realize, but for the objective function we take appropriate limits, that objective function is differentiable. As for the objective function that is not differentiable or derivative are difficult to obtain, this paper adopt the iterative method to obtain derivative. In the one-dimensional search, iterative method is compressed so that the length of the search interval infinitely narrow and tends to zero, in order to meet the termination criteria to achieve, obtain the approximate optimum. Here we have a specific one-dimensional search method given program.

Golden section method: search interval $\langle t_1, t_2 \rangle$, $f(t)$ is a single valley function for the interval $\langle t_1, t_2 \rangle$, for given termination criterion ε and points scale factor $R = 0.618$.

① Calculate $t_{22}=t_1+\beta(t_2-t_1)$, $f(t_{22})$;

② Calculate $t_{11}=t_1+(1-\beta)(t_2-t_1)$, $f(t_{11})$;

③ Calculate $f(t_{11}) \le f(t_{22})$, then $t_{22}=>t_2$, $t_{11}=>t_{22}$, $f(t_{11})=>f(t_{22})$, turn ⑤;

④ Calculate $f(t_{11}) > f(t_{22})$, then $t_{11}=>t_1$, $t_{22}=>t_{11}$, $f(t_{22})=>f(t_{11})$, turn ⑥;

⑤ Calculate $|t_1-t_2| < \varepsilon$, then $(t_1+t_2)/2=>t^*$, turn ⑦, otherwise, turn ②;

⑥ Calculate $|t_1-t_2| \ge \varepsilon$, then $(t_1+t_2)/2=>t^*$, turn⑦, Otherwise calculate $t_{22}=t_1+\beta(t_2-t_1)$; $f(t_{22})$, turn ③;

⑦ export t^*, termination.

So, Achieve one-dimensional search method can be drawn by means of procedures similar to the advantages of accuracy depends on the merits of the termination criterion ε limit values,the range of floating-point variables as $1.0\times10^{-38} \sim 1.0\times10^{+38}$, Therefore, very accurate results can approximate the advantage to minimize the error.

IV. Inexact One-Dimensional Search Method

A. Two Major Criteria

1) Armijo-Goldstein Standards

Armijo and Goldstein propose inexact one-dimensional search process. Suppose

$$J = \{\alpha > 0 \mid f(x_k+\alpha d_k) < f(x_k)\} \quad (18)$$

The interval is $J = (0, a)$. In order to ensure that the objective function decreases monotonically, while requiring f drop not too small, α must be selected to avoid too close interval J endpoint. A reasonable requirement is

$$f(x_k+s_k) \le f(x_k)+\rho g_k^T s_k \quad (19)$$

$0 < \rho < \frac{1}{2}$, $s_k = a_k d_k$. α_k meeting (19) constitute the interval $J_1 = (0, c]$, J rejection of the right end point of the interval. In order to avoid the situation that α is too small, we add another requirement:

$$f(x_k+s_k) \ge f(x_k)+(1-\rho)g_k^T s_k \quad (20)$$

This requires the exclusion of the left end of the interval J near the point. α Meeting (19) and (20) constitute the required interval $J_2 = [b, c]$. (19) And (20) named Armijo-Goldstein inexact line search standards, or Armijo-Goldstein standards [3]. Once the resulting step size α to meet (19) and (20), it is an acceptable step

factor. It, $J_2 = [b,c]$ called acceptable interval that meets (19) and (20).

2) Wolfe-Powell Standards

Armijo-Goldstein standards likely to exclude the minimal value of step factor α outside acceptable range. So, Wolfe-Powell criterion gives a simpler condition (20)

$$g_{k+1}^T d_k \geq \sigma g_k^T d_k, \sigma \in (\rho,1) \tag{21}$$

Or

$$\begin{aligned} \varphi'(\alpha_k) &= \left[\nabla f(x_k + \alpha_k d_k)\right]^T d_k \\ &\geq \sigma \nabla f(x_k)^T d_k = \sigma\varphi'(0) > \varphi'(0) \end{aligned} \tag{22}$$

Geometric interpretation: the tangent at an acceptable point $\varphi'(\alpha_k)$ is greater than or equal to σ times the initial slope, (19) and (21) named Wolfe-Powell inexact line search criteria, or Wolfe-Powell standards. Its acceptable range is $[e,c]$.

B. Global Optimization Methods

A class of deterministic global optimization is Covering Method, which gradually will detect the global minimum free area removed until the remaining area is small enough and contains a global minimum. There are also established a number of methods for Lipschitz functions, a widely used class method called branch and bound method, whose main idea is to divide the feasible region was gradually refined, the objective function to build the community and non-increasing sequence of non-decreasing lower bound until the upper and lower bounds of the objective function close enough so far. Recently, the concept LBFS has been introduced to the global optimization for it limited convergence [5].

1) Basic Symbols and Definitions

Consider the global optimization as follow

$$\min_{x \in s \subset R} f(x) \tag{23}$$

S, a compact set belongs to R, $f: S \to R$ is continuously differentiable functions.

Point $x^* \in s$ meet

$$f(x^*) \leq f(x),\ \forall x \in s \tag{24}$$

Called x^* is (23) global optimal solution. The following points x meet

$$f(x) < f(x^*) + \in \tag{25}$$

$\in -$ Global referred to (23) of the optimal solution, Q is (23) the precision parameter.

Definition2 The function $f(x)$ is called a linear lower bound function in the A restricted in G, if $P \in R, \beta \in R, \gamma \in R$, make

$$f(x) \geq \gamma x + \beta, \forall x \in A \tag{26}$$

$$f(p) = \gamma p + \beta \tag{27}$$

And G is bounded, that

$$\gamma \leq G \tag{28}$$

The numerical G is a finite real number.

2) Inexact Research Boundary Function Method

Suppose $A \subset S$ be an interval, and $x_0 \in A$. In order to find the point $x_1 \in A$, it has a function value smaller than x_0, use the following inexact searches. Let

$$x_1 = x_0 - rf'(x_0) \tag{29}$$

The r appropriately selected to ensure compliance with:

$f(x_1) \leq f(x_0)$

Let

$r = min\{1, r_1, r_2\}$

Among $r_1 = max\{r \geq 0 | x_0 - rf'(x_0) \in A\}$ and $r_2 = (2-\in)/M$, $0 < \in < 1$, M is constant and meet $M \geq \max_A |f''(x)|$, for non-precision search has the following lemma.

Lemma 4 Obtained x_1 from (29) meet $f(x_1) \leq f(x_0)$.

Proof Taylor formula

$$f(x_1) = f(x_0) + f'(x_0) f(x_1 - x_0) + f''(\xi)(x_1 - x_0)^2 / 2$$

(The ξ between x_0 and x_1) (30)

The (29) into (30) we have:

$$f(x_1) = f(x_0) + r[\frac{1}{2} rf''(\xi) - 1][f'(x_0)]^2 \tag{31}$$

So

$$\frac{1}{2} rf''(\xi) - 1 \leq -\frac{\in}{2} < 0$$

So

$f(x_1) \leq f(x_0)$

End.

The main idea of the inexact search linear boundary search function is progressively deleted without the global minimum point S sub-region; the remaining area is reduced successively until $\in -$ the global optimal solution [9].

Firstly start from P selected from S, p_1 is obtained with an inexact search, meeting $f(p_1) \leq f(p)$.

Let

$\alpha = f(p_1) - \in$

The function $f(x)$ configured in a linear boundary function $I^0 = A$ to the matching point $p \in A \subseteq S$.

$$l(x) = \gamma x + \beta \tag{32}$$

(Typically a range of A, P is the endpoint). Let the intersection of $l(x)$ and $y = \alpha$ is represented by $x_1 \in A$. If $f(x_1) > f(p_1)$, obviously $\in -$ global optimal solution will not be reached in the following collection

$$A_c = \{x | x \in A,\ l(x) > \alpha\} \tag{33}$$

Deleted A_c from the A. Provable A_c is the interval of the form $[p, x_1]$ or $[x_1, p]$. Repeat the process above to get the point x_1, make it meet $f(x_1) < f(p)$. Then x_1 is starting to get new p_1 with inexact search, According to (33) and then on the remaining amendments α subset construction linear boundary functions. So go iterations can be obtained $\in-$ global optimal solution of (23) at the time of termination.

When the remaining iteration termination criterion is a subset of the empty set when to stop iterations, the latest available p_1 and $f(p_1)$ is $\in-$ Global optimal solution and the corresponding function value [9]. Specific algorithm is as follows:

① Initialization: Divided S into finite subintervals and P indicates that this division; P elements in order to produce according to their arrangement;

② Step 1: From p get p_1 with inexact search making $f(p_1) \le f(p)$; let $\alpha = f(p_1) - \in$; save p_1 and $f(p_1)$;

③ Step 2: selected p point from the $A \in P$; p is constructed to match point on A, $f(x)$ linear boundary function $l(x) = \gamma x + \beta$;

④ Step 3: let

$$A^0 = A \cap \{x | \gamma x + \beta \le \alpha\} \tag{34}$$

If $A^0 = \phi$, remove the interval A from P; or A^0 instead A.

⑤ Step 4: $A^0 = \phi$, Let P previously generated for the new sub-interval A. If P is empty in this case, the termination of the iteration;

⑥ Step 5: Selected $p \in A \subseteq S$, A confirmed non-empty; if $f(p) < f(p_1)$, then go to step 1, otherwise, go to step 2. Then there is the following lemma:

Lemma 5 Step 3 corresponds to the algorithm set A_c:

$$A_c = \{x | x \in A, rx + \beta > \alpha\} \tag{35}$$

Non-empty set and the lower are bound of its length.

Proof if $A_c = \phi$, Then, for each point $x \in A$

$$\gamma x + \beta \le \alpha = f(p) - \in < f(p) \tag{36}$$

The point $p \in A$ is the matching point, Therefore, it satisfies $\gamma p + \beta = f(p)$; this contradict with (36), so A_c non-empty. The intersection of $l(x)$ and $y = \alpha$ is represented by x_1; $|x_1 - p|$ is the length of the A_c. The formula $\gamma(p - x_1) = f(p) - \alpha \ge f(p_1) - \alpha = \in$ obtained from $\gamma p + \beta = f(p)$ and $\gamma x_1 + \beta = \alpha$. Then by γ are bounded to know $(|x_1 - p| \ge \frac{\in}{|\gamma|} \ge \frac{\in}{G}$. End.

Theorem 6 Assuming global optimization the objective function $f(x)$ twice continuously differentiable of (23) , and $f(x)$ is assumed to create a linear function (26) of the limits of any subinterval S, And wherein the boundary parameter C has the same; Then the algorithm will get points x in finite iteration steps, make

$$f(x) \le f(x^*) + \in \tag{37}$$

Proof [10] First, when the global optimal solution in step 4 criteria are met, the iteration for only a limited step. Easy to see that P is limited in any sub-interval length (S is a finite lengths, P is limited by the division S). According to Lemma 5, non-empty set $A_c = \{x | x \in A, \gamma x + \beta > \alpha\}$ and the lower bound are its length.

Secondly, We prove that the global optimal solution $\in-$ when the method stop can be obtained. From just the front does argumentation can know, iteration terminates in finite steps. Therefore, (32) in α_m contains the minimum value of α. When the iteration termination, each point of S has been in an iteration of step 3 was deleted. There are parameters of γ, β, α for S each point, make

$$f(x) \ge \gamma x + \beta > \alpha > \alpha_m \tag{38}$$

Use the p_m representation the matching point corresponding to α_m,

$$\alpha_m = f(p_m) - \in \tag{39}$$

The formula $f(x) \ge f(p_m) - \in$ can be obtained by (38), (39), that is $f(p_m) \le f(x) + \in$, $\forall x \in S$, therefore p_m is (37) $\in-$ global optimal solution.

The last, if the termination standards of 4 in the iterative process are always not satisfied, leads to a contradiction. If the algorithm is never ending, we have included S sequence in $\{p^i\}$ (the i iteration step by step 2 or 5 to determine the matching point) and $\{\alpha_i\}$ (when the i iteration by step 1 to determine) and meet

$$f(p^i) = l(p^i) = \gamma p^i + \beta \tag{40}$$

And $\alpha_i = f(p^i) - \in$, here the i iteration by inexact search that is p^i. From know the process of p^i and p^i selection

$$f(p^i) \ge f(p^i) = \alpha_i + \in \tag{41}$$

Because S is a compact set, the sequence $\{p^i\}$ has a convergent subsequence, taking $p^* \in S$ as the limit, $\{p^i\}$ indicates the convergent subsequence. The intersection step 3 that denoted as x^i, x^i meet

$$l(x^i) = \gamma x^i + \beta \tag{42}$$

Because $x^i = p^{i+1}$, so $\{x^i\}$ has the same limit p^*. By (40), (41), (42) can know, i meet

$$x^i = \frac{\alpha_i - \beta}{\gamma} = \frac{\alpha_i - f(p^i)}{\gamma} + p^i \qquad (43)$$

So the establishment of

$$\left|x^i - p^i\right| = \frac{f(p^i) - \alpha_i}{|\gamma|} \geq \frac{f(p^i) - \alpha_i}{\gamma} \geq \frac{\in}{G} \qquad (44)$$

Note that x^i and p^i have the same limit, when $i \to \infty$ get: $\frac{\in}{G} \leq 0$ In (44). This contradicts with the selected parameter G, end.

V. NUMERICAL EXAMPLES

Numerical example 1

Global Optimization

$$minf(x) = \sin x + \sin(10x/3) \qquad (45)$$

Here are $x \in [27, 7.5]$. The objective function of the problem has three local minima, one of which is the global minimum. An iterative calculation process is shown in Fig.1.

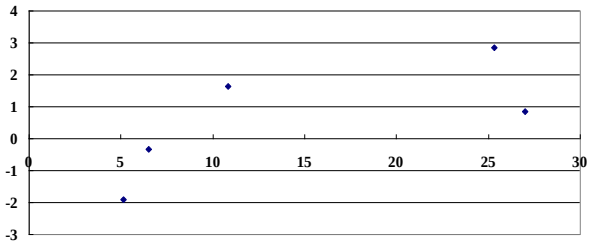


Figure 1. Iterative process to calculate the one-dimensional search method

Let $\in = 10^{-6}$ and $M = 16, I^0 = [27, 7.5]$.

The initial iteration can be selected $p = 27$, $f(p) = 0.8394984$, with $\gamma = 1/8$ for inexact search. By the end of 5 times iterations, get the $\in -$ global optimal solution $x = 5.1457931$, the corresponding value is -1.8995993.

The accuracy of $\in = 10^{-6}$ given the same circumstances, number of iterations required by our algorithm is 5, number of iterations required for 5 times interval algorithm, 10 is the times of iterations required for Hansen algorithms. An iterative calculation process is shown in Fig. 2.

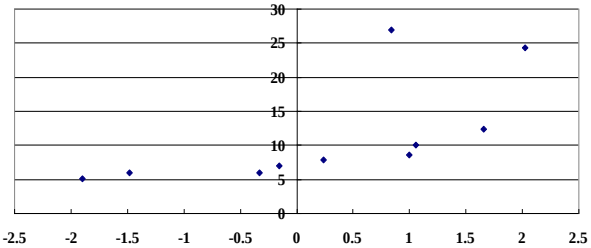


Figure 2. Hansen algorithm iterative process

A deterministic global optimization method is presented in this paper, a single variable function; the convergence theory and its effectiveness are discussed. Solving the method can be used for a class of global optimization problems. In addition, a more effective method to explore the structure of the linear boundary function will further enhance the effectiveness of inexact search method.

Numerical example 2

Calculate $f(x) = e^{x_1}(4x_1^2 + 2x_1^2 + 4x_1x_2 + 2x_2 + 1)$

$$x_1 + x_2 = 0$$

s.t. $1.5 + x_1x_2 - x_1 - x_2 \leq 0$

$$-x_1x_2 - 10 \leq 0$$

Search interval is $[1,1.5]$, $\beta = 0.62$, $\varepsilon = 1.0 \times 10^{-3}$

Calculated as follows:

① Calculate $t_{22} = t_1 + \beta(t_2 - t_1)$, $f(t_{22})$

$t_{22} = 1 + 0.5 \times 0.62 = 1.31$, $f(1.31) = 2.34$

② Calculate $t_{11} = t_1 + (1-\beta)(t_2 - t_1)$, $f(t_{11})$

$t_{11} = 1 + (1 - 0.62)(1.5 - 1.0) = 1.19$, $f(1.19) = 2.16$

③ If $f(t_{11}) \leq f(t_{22})$, then $t_{22} => t_2$, $t_{11} => t_{22}$, $f(t_{11}) => f(t_{22})$, transfer ⑤;

④ If $f(t_{11}) > f(t_{22})$, then $t_{11} => t_1$, $t_{22} => t_{11}$, $f(t_{22}) => f(t_{11})$, transfer ⑥;

⑤ If $|t_1 - t_2| < \varepsilon$, then $(t_1 + t_2)/2 => t^*$, transfer ⑦, If not to ②;

⑥ If $|t_1 - t_2| \geq \varepsilon$, then $(t_1 + t_2)/2 => t^*$, transfer ⑦, If not to calculate $t_{22} = t_1 + \beta(t_2 - t_1)$; $f(t_{22})$, transfer ③;

⑦ Export t^*, end.

According to the results ① ② calculated, we can see that the next step should be ⑤.

$|t_1 - t_2| = 0.5 > \varepsilon$, $\frac{1+1.5}{2} = 1.25$

Export $f(1.25) = 1.89$

Using Matlab programming directly on the objective function calculation procedure is complex. It is calculated from the results of $f(1.225) = 1.8951$. Comparison of the t

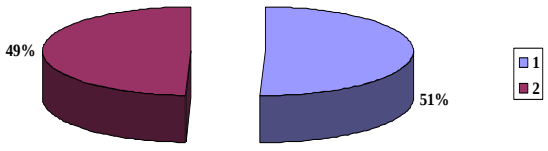


Figure 3. Error comparison chart in x

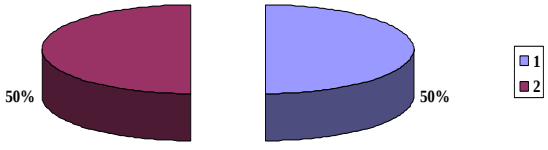


Figure 4. Error comparison chart in y

The two different methods of calculation are compared. From the figure3 and figure4, we found that the computed results are basically the same, and thus explain the rationality of one-dimensional search method.

VI. CONCLUSION

This paper mainly describes the one-dimensional search, detailed introduction on the method of global optimization and convergence. And simple introduces the inexact one-dimensional search, and made some research and exploration, let it compared with the exact one-dimensional search, corresponding improvement, is a complex work. For the inexact one-dimensional search algorithm, it's through produced a series of iterative point; it's the process of successive approximation the minimum point., the convergence rate does not depend on the exact one-dimensional search, spend less time at work.

ACKNOWLEDGMENT

This research was supported by the National Nature Foundation of China (Grant No. 61170317) and the National Science Foundation for Hebei Province (Grant No.A2012209043), all support is gratefully acknowledged.

REFERENCES

[1] Yuan Yaxiang, Sun Wenyu. Optimization theory and methods, *Beijing: Science Press*, 1997
[2] Sui Yunkang. Solutions for nonlinear equation and one dimensional search by using inverse functions, *Journal of Dalian University of Technology*, 33(2), 1993
[3] Zhang Yongfu. The Constringent Comparison of the One-Dimension Search, *Journal of Inner Mongolia University for Nationalities*, 23(2), 2008
[4] Zhang Zhibin, Jin Fujiang, Tang Yiping. An Improved Exponential Optimization Algorithm of One-Dimensional Search, *Journal of Huaqiao University (Natural Science)*, 33(5), 2012
[5] Wang X and Chang TS. A Multivariate Global Optimization Using Linear Bounding Functions. *Journal of Global Optimization*, 1998, 12
[6] Deng Naiyang. Numerical methods for unconstrained optimization, *Beijing: Science Press*, 1982
[7] Chen lin. Several types of the nonlinear optimization problem solution set, Master degree theses of master of chongqing normal university, 2012.
[8] Yonghong Ren. Nonlinear Langrange method of solving nonlinear optimization problems, *Ph. D. Dissertation of dalian university of technology*, 2006.
[9] Xie Zheng, Li Jianping, Tang Zeying. Nonlinear optimization, *Beijing: National University of Defense Technology press*, 2003
[10] Jinli. A differential equation solving constrained nonlinear optimization method, *Computational mathematics*, 2007, (2) : 164-169.
[11] Yongzheng Zhou. Mathematical modeling. *Shanghai: tongji university press*, 2010.
[12] Xinghuo Wan. Probability and mathematical statistics. *Beijing: science press*, 2007.
[13] XiaoYin Wang. Mathematical modeling and mathematical experiment. *Beijing: science press*, 2010.
[14] Shengke Chen. SPSS statistical analysis from entry to master. *Beijing: tsinghua university press*, 2010.
[15] Yang Shuang, Jia Liping. Quadratic interpolation algorithm for solving one-dimensional symmetry points found hormone problems, *Leshan Teachers College*, 2013, (12): 3-5.
[16] Zhu Zhibin, Wang Shuo. Nonlinear optimization of an ultra-linear convergence of generalized projection feasible direction method, *Journal of Applied Mathematics*, 2014, (1): 179-184.
[17] Su Peng. Studybased on some kind of nonlinear optimization problem of neural networks, *Harbin Institute of Technology master's degree thesis*, 2013
[18] Xia Hongwei, Interfax army of a class of equality constrained nonlinear optimization problem sequential quadratic programming new method, *Chongqing Normal University*, 2014, (2): 1-3.
[19] Zhang Zhibin, etc. An improved one-dimensional search index optimization algorithm, *Huaqiao University*, 2012, (5): 503-505.

Yuhuan Cui Female, born in 1981, Master degree candidate. Now he acts as the Math teacher in Qinggong College, Hebei United University. She graduated from Yanshan University, majoring computational mathematics. Her research directions include mathematical modeling and computer simulation, the design and analysis of parallel computation, elastic problems numerical simulation, and etc.

Jingguo Qu Male, born in 1981, Master degree candidate. Now he acts as the Math teacher in Qinggong College, Hebei United University. He graduated from Harbin University of Scince and Technology, majoring fundamental mathematics. His research directions include mathematical modeling and computer simulation, the design and analysis of parallel computation, elastic problems numerical simulation, and etc.

Multi-Objective Optimal Configuration of Reconfigurable Test Platform: A Modified Discrete Particle Swarm Optimization Approach

Ma Limei [1, 2], Li Guoxiu [1], and Zhao Lixing [2]
1. School of Mechanical, Electronic and control Engineering, Beijing Jiaotong University, Beijing, 100044, China
2. Beijing Automation Technical Research Institute, Beijing, 100009, China
Email: malimei@batri.com.cn, gxli@bjtu.edu.cn, zhaolixing@batri.com.cn

***Abstract*—The reconfigurable test platform (RTP) is designed to test high speed, high reliability and super precision indexes of wafer transmission robot, which can transfer and align wafers in the semiconductor manufacturing. This paper focuses on optimal configuration of the test platform. First, the problem is described considering three important yet conflicting factors: assembly, structural stiffness, and cost. Second, based on the combination sequence of function requirements and the connection relationship of modules, a multi-objective optimal decision-making model was formulated. And then, based on layered network and dependent degree methods, the multi-objective model is improved to be an only one objective optimization problem. Finally, the modified discrete particle swarm optimization (MDPSO) algorithm is proposed to solve the model and generate the best configuration scheme of RTP. Our computational results have shown that the MDPSO algorithm is efficient and robust. And the results demonstrate that the developed methods can be used to improve the test platform design efficiency and reduce the production cost.**

***Index Terms*—Reconfigurable Test Platform; Configuration Design; Multi-Objective; Particle Swarm; Optimization**

I. INTRODUCTION

Wafer transfer robot, which has high speed, high reliability and super precision, can transfer and align wafers during the different working procedures [1]. It has high speed, high reliability and super precision, and the utility of it realizes the automation in wafer productions [2, 3]. Reconfigurable Test Platform (RTP), which consists of certain mechanical modules, is designed for testing the performance, such as positioning accuracy, speed and reliability of wafer transmission robot. Research into the performance test of wafer transfer robot focuses mainly on test methods of each index. Mori and Ishikura used the distance sensor to inspect the movement accuracy of robot, and a simple device was proposed to illustrate its application method [4]. Now, how to test reliably, detect fault and maintain fast becomes one of hot study points in the testing of wafer transfer robot. Here, RTP is designed for the auto and quick test of robot and its configuration is rests on the function and available mechanical modules. The RTP optimization aims to generate superior RTP configuration mainly based on assembly ability, cost, structure performance and other quantitative indexes, and this optimal problem can be described as a discrete combination optimization problem [5]. Genetic algorithm (GA) and particle swarm optimization (PSO) have been broadly used in many fields, such as function optimization, production scheduling, machine learning and data mining, etc. compared with GA, PSO has higher efficiency in the search for the optimal solution. Since the PSO primarily aims at the search operation of continuous function, Wei et al discreted the continuous variable to be the particle probability, which is described as 1 or 0 by current state variable, and proposed a binary PSO algorithm[6]. Due to the inertia of particles during the process of movement and its generated premature convergence, Coello et al proposed the Quantum Discrete PSO (QDPSO) algorithm, and applied the algorithm to the vehicle scheduling problem, and verified the search and optimization effects of DPSO algorithm on the vehicle scheduling issue [7]. In order to solve the traveling salesman problem (TSP), Lei et al. proposed a fuzzy discrete particle swarm optimization algorithm. This algorithm uses fuzzy matrix to indicate the position and velocity of the particles, and adds normalization and fuzzy operations in the iteration process [8]. Coban using PSO method for Off-line learning of Multi feedback-Layer Neural Network (MFLNN), which is a recently proposed recurrent neural network [9]. Cao and Chen utilized a discrete PSO algorithm for optimizing the number of machine cells, and employed a continuous PSO algorithm to perform machine clustering [10]. This paper consolidates the advantages of the above PSO algorithms, and puts forward the Modified Discrete PSO (MDPSO) Algorithm, which suits to solve RTP configuration optimization model. In this approach, the dependent degree and layered networks are used to simulate the configuration process of RTP, and module assembly relationship is used as constrains to accelerate the solution process.

The first part of this paper describes the RTP optimal configuration problem; the second part establishes a optimal decision-making model based on layered network and dependent degree methods; part 3 proposes the MDPSO algorithm and illustrates how the algorithm is

doi:10.4304/jnw.9.12.3502-3509

used to solve the model; part 4 presents theoretical analysis and simulation result on the performance of the algorithm in the case study; part 5 comes to the conclusion.

II. Description of RTP Optimal Configuration Problem

In order to get optimal configuration of RTP, the assembly performance, structure stiffness of RTP after being assembled and cost should be taken into consideration during the optimization process of RTP configuration. Therefore, this paper takes the assembility of parts, structural stiffness, and purchase cost as the three major indicators for the performance evaluation of RTP.

A. Assembility

The assembility of RTP is decided by part-level assembly smoothness (PAS) of each part, which refers to the assembling easiness and smoothness between two parts which has assembly relation with each other. It is also very important to evaluate the overall function of RTP. This index is measured by expected costs and time of assemblies, rather than that of actual value in assembly process. The calculation method is shown in formula 1.

$$PAS = 1 \Big/ (\delta * C_k + (1-\delta) * T_k), \quad \delta \in [0,1], k = 1,2,...,K, K \in N. \tag{1}$$

Among them, C_k is the cost correlation required by assembling from part i to part j ; T_k is the time correlation required by assembling from part i to part j ; K is the sum of assembly relationship times required by one RTP configuration; δ is the impact factor of C_k, whose value is [0,1].

B. Structure Performance

The structural performance of RTP mainly includes static performance, dynamic performance and error of the device, while the structural performance is mainly decided by modules which form the device and the combination sequence of modules. Moon, Angeles et al [12, 13] proposed a static performance, dynamic performance and error evaluation method, which is based on mechanical modules of the equipment. In the equipment configuration, structural stiffness U is an important index for measuring the mechanism's ability of resisting deformation, which exerts an effect on static performance and dynamic performance. Its calculation method is shown in formula 2 and 3.

$$U = \frac{1}{N} \sum_{j=1}^{N} (trace(J^j C J^{jT})^{-1}). \tag{2}$$

$$J^j = \begin{bmatrix} \vec{e}_1 & \cdots & \vec{e}_i & \cdots & \vec{e}_n \\ \vec{e}_1 \times \vec{r}_1 & \cdots & \vec{e}_i \times \vec{r}_i & \cdots & \vec{e}_n \times \vec{r}_n \end{bmatrix}_{6\times n}. \tag{3}$$

wherein, C is the flexibility matrix of the interface j, it is a diagonal matrix of $n*n$, and each diagonal element represents the amount of deformation of the module under per force unit along the axis of motion, namely the Z-axis of the local coordinate system; N is the number of total interfaces, and *trace*() shows the trace of the matrix and the sum of diagonal elements of the matrix. Index value U is the value that can measure the structures rigidity of the device, while j shows the jth interface; It is a unit vector whose direction is defined as the direction of Z-axis of the ith local coordinate system of the jth interface; it is the vector which connects the ith $\vec{e}_i$ local coordinate system with tool coordinate system. n is the number of local coordinate systems, namely, the number of DOF interfaces. This method evaluates the structural stiffness of the whole platform by utilizing the performance of the part module interface $\vec{r}_i$.

C. Cost

Since the cost of assembly has been considered in the assembility index of the test platform, here, the cost involved in the optimization configuration of RTP only considers the cost of the modules comprising the platform, as shown in formula 4.

$$c = \sum_{i=1}^{n} c_i, i = 1,2,...N \tag{4}$$

Among them, is the cost needed for the c_i i_{th} RTP part, N is the total number of RTP parts; and c is the total cost of the parts forming RTP.

In order to make a comprehensive evaluation based on many different kinds of indexes; this paper makes use of dependent function [11] to build a unified quantitative calculate formula for each index, which means to use dependent degree to represent the degree of importance for each index.

III. RTP Optimal Decision-making Model

A. Multi-purpose Optimal Mathematical Model

The aim of RTP optimal configuration is to conduct evaluation and optimization of RTP set, here, $RTP=\{RTP_1, RTP_2, \ldots, RTP_p\}=\{\{MC_{11}, MC_{12}, \ldots, MC_{1n}\}, \{MC_{21}, MC_{22}, \ldots, MC_{2m}\}, \ldots, \{MC_{p1}, MC_{p2}, \ldots, MC_{pq}\}\}$, $p, n, m, p \in N$, and to find an optimal RTP configuration scheme set, $\{MC\}=\{MC_{p1}, MC_{p2}, \ldots, MC_{pn}\}$, and realizefinal objective, such as the best assembling performance, the largest structure stiffness of platform and the minimum cost. Therein, p is the number of RTP configuration scheme options; n, m and p are the number of machine modules in each RTP configuration scheme. Therefore, this optimal problem is an optimization problem with multi-parameter and multi-target.

In order to obtain the optimal solution among RTP configuration schemes, this paper uses the above mentioned quantitative indicators to assess and select the optimized RTP, and the optimization objective is:

① Maximize the assembility of RTP, for the assembility is inversely with the assembly time and cost;

② Maximize the performance of structural of RTP;

③ Minimize the total cost of modules for one RTP configuration.

In order to measure the performance of module with different criteria, the method [14] is used to calculate its dependent degree. The calculation method is as follows:

Determination of optimal point: For different criterion, the optimum point m_i is different. For character C_{ij} for mechanical modules $\{M_i\}$ or joint interfaces $\{R_i\}$, we suppose the value of character C_{ij} is $V_j=(A_j, B_j)$. If the value of character c_{ij} (character c_j of module M_i) $v_{ij}=x_{ij}$, then $A_j=\min(x_{ij})$, $B_j=\max(x_{ij})$; if $v_{ij}=(a_{ij}, b_{ij})$,then $A_j=\min(a_{ij})$, $B_j=\max(b_{ij})$. The optimal point m_j can be determined based on objectives, as shown is formula 5.

$$m_j=\begin{cases} min(A_j,B_j), & objective\ is\ min(V_j) \\ max(A_j,B_j), & objective\ is\ max(V_j) \\ (A_j+B_j)/2, & objective\ is\ mid(V_j) \\ m_e\in(A_j,B_j), & objective\ is\ expected(V_j) \end{cases} \quad (5)$$

Calculation of dependent degree: The dependent degree of a point and an interval can be calculated by the simple dependent function. Suppose a point x with regard to an interval X_0 at the optimum point m. For a finite interval $X_0=[a, b]$, $m\in X_0$, $x\in(-\infty, +\infty)$, For the minimum problem, m is the minimum point $m=a$, for the maximum problem, m is the minimum point $m=b$. The simple dependent function $k(x)$ can be expressed as formula 6.

$$k(x_{ij})=\begin{cases} (x_{ij}-a_j)/(b_j-a_j), x_{ij}<m_j, m_j=a_j \\ (b_j-x_{ij})/(b_j-a_j), x_{ij}>m_j, m_j=a_j \\ (x_{ij}-a_j)/(b_j-a_j), x_{ij}<m_j, m_j=b_j \\ (b_j-x_{ij})/(b_j-a_j), x_{ij}>m_j, m_j=b_j \\ 1, \qquad x_{ij}=m_j, m_j=a_j,b_j \end{cases} \quad (6)$$

The dependent degree u_{ij} of M_i or R_i can be caculate by formula 7. The higher dependent degree means better solution.

$$u_{ij}=\begin{cases} w_j * k_j(v_{ij}), & v_{ij}=x_{ij} \\ w_j * (\int_{a_{ij}}^{b_{ij}} k_j(x) \Big/ (b_{ij}-a_{ij})), & v_{ij}=(a_{ij},b_{ij}) \end{cases} \quad (7)$$

B. The Establish of Optimal Process Model of RTP

Let $G=(V, E)$ be a network [15] with s and t being the source and the sink of G respectively. The weight of an edge between vertices u and v is denoted by c_{uv} or $w(u,v)$, a flow from s to t is denoted by f_{st}. A layered network (LN) [16] is such a network with following characters:

(1) For vertices: There exists a partition $V=\bigcup_{i=0}^{k+1}V_i$, which forms k+2 layers, where$V_0=\{s\}$, and$V_{k+1}=\{t\}$.

(2) For edges: Any edge of G is from layer V_i to the next layer $V_{i+1}(0\leqslant i\leqslant k)$.

Figure 1 shows an example of layered network. v_{ij} means vertex j of i^{th} layers. A path f_{st} is a flow path from node s to node t, is composed of n+1 nodes including each one node from every layers. It is a powerful tool to represent the module selection mode 1 shown in [17].

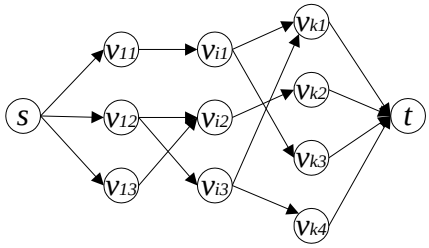


Figure 1. Example of a layered network (LN) with 5 layers

The module selection layered network should represent functions and module components of RTP configuration. Function requirements decide the layers of the layered network, and number of feasible modules of each function requirement decides the number of vertices of each layer. According to graph theory method proposed in that presents the structure of RMTs, we set work table and spindle as layer *1* and layer *k*, the source node *s* as layer *0*, the sink node *t* as layer *k+1*. The combination sequence decides the sequence of layered network.

We set the direction of edge by the combination sequence of FR, in other words, from the node *s* to node *t*. The connection relationship (existing an edge) of modules can be defined according to module assembly matrix [0, 1] and the relationship between module itself and modules of upstream layers. If the value of assembly matrix of module in adjacent layers is 1, then there is an edge. If the value of assembly matrix of module in adjacent layers is 0, but the matrix value between the module and other modules in upstream layers is 1, then there is an edge also.

The optimal process model of RTP has been constructed above; the optimal module-set selection problem can be transferred to selection of a set of nodes in a flow with minimal/maximal weights using special algorithms. For optimal selection problem, the module component has several constrains as follows:

1) Here, suppose each module executes only one function,

2) One and only one module must be selected from each layer,

3) One module can only be selected once for all layers.

The second constrain can be satisfied by the construction of optimal process model of RTP, in which, same module in adjacent layers has no edge connection. The first and third constrains affect feasible flow paths.

Module selection for a RTP configuration means selection of a feasible module set. To find the feasible module-set that satisfy above three constrains of module selection, all flow paths do not satisfy constrains of optimal process model of RTP should be eliminated to get Q feasible flow paths. Based on these constrains, feasible flow paths are generated by modifying the Optimal Process model of RTP. The detailed algorithm for feasible flow path generation is given in table 1.

C. The Improved Model of Optimal Decision

To simplify the process of solving the model, this paper assumes that, m, the number of mechanical components (MC) required for each RTP configuration,

is the same, and *x*, the number of alternative modules of each mechanical module, is the same. The alternative solution for the optimization decision model is shown as the following figure 2.

TABLE I. OPTIMAL PROCESS MODEL OF RTP GENERATION ALGORITHM

Input	*MSLN* model	
Output	*MSSF*	
	Read module constrains: mainly satisfy the first and third constrains.	
steps	*S0*	Find all flows *AF*= { f_{st}^{a} }, *g*=[1, 2, …, *a*], from node *s* to node *t*. Set up the feasible flow set *MSFF*= ∅ .
	S1	Select one flow f_{st}^{g} , check all nodes of this flow. If there exists two or more nodes with same module Subtract this flow from *AF*; Else Subtract this flow from *AF*; Put the flow f_{st}^{g} into set *MSFF*.
	S3	Check set *AF* If *AF* ≠ ∅ Go to *S1*; Else end
	S4	Output *MSFF*={ f_{st}^{q} }, *q* ∈*Q*

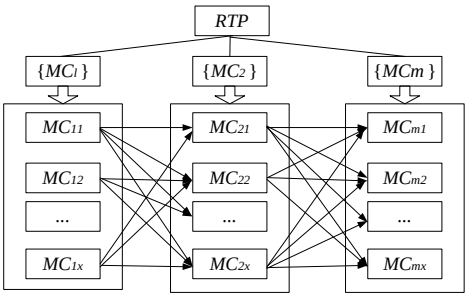


Figure 2. Optimal Process model of RTP

In order to create unified optimization parameters for the model, regarding the connection edge of adjacent MC as an object, set capacity value for this connection edge. Assessment and optimization should be conducted according to the capacity value of RTP connection edge. If the number of alternatives of each mechanical module is *x*, then the number of the connect edges of the adjacent MC is x^2, and the number of the connect edges in the RTP optimization model is $m*x^2$, wherein, *m* is the number of MC types, and RTP optimization model is a layered network diagram with *m-1* layers of connect edges. The capacity calculation method of each connecting line is as shown in formula 8 to 11.

$$c_{mx,m(x+1)} = w_t * (t_{MC_{mx}} + t_{MC_{m(x+1)}}) + w_{pas} * (PAS_{MC_{mx}} + PAS_{MC_{m(x+1)}}) + w_U * (U_{MC_{mx}} + U_{MC_{m(x+1)}}) + w_c * (c_{MC_{mx}} + c_{MC_{m(x+1)}}), m = 2,3,...,M-2, x = 1,2,...,X-1. \quad (8)$$

$$c_{mx,m(x+1)} = w_t * (2*t_{MC_{mx}} + t_{MC_{m(x+1)}}) + w_{pas} * (PAS_{MC_{mx}} + PAS_{MC_{m(x+1)}}) + w_U * (2*U_{MC_{mx}} + U_{MC_{m(x+1)}}) + w_c * (2*c_{MC_{mx}} + c_{MC_{m(x+1)}}), m = 1, x = 1,2,...,X-1. \quad (9)$$

$$c_{mx,m(x+1)} = w_t * (t_{MC_{mx}} + 2*t_{MC_{m(x+1)}}) + w_{pas} * (PAS_{MC_{mx}} + PAS_{MC_{m(x+1)}}) + w_U * (U_{MC_{mx}} + 2*U_{MC_{m(x+1)}}) + w_c * (c_{MC_{mx}} + 2*c_{MC_{m(x+1)}}), m = M-1, x = 1,2,...,X-1. \quad (10)$$

$$w_t + w_{pas} + w_U + w_c = 1, w_t, w_{pas}, w_U, w_c \in (0,1) \quad (11)$$

Among them, w_t, w_{pas}, w_U, w_c are respectively weights of such indicators as the time of processing, assimilability, structural stiffness and cost. Formula 5 is the connecting side capacity of levels from 5 to M-2, and formulas 6 and 7 are the connecting side capacity of level 1 and level M-1.

In order to avoid non-standard error generated by simple linear superposition due to measuring each indicator functions with different units in the above-described formula [18], above formulae are improved based on the correlation degree of all indicators. The uniform measurement method [19-21] is used for each index to eliminate the non-standardized error between each index, as shown in formula 12 to 14.

$$c_{mx,m(x+1)} = w_t * (kt_{MC_{mx}} + kt_{MC_{m(x+1)}}) + w_{pas} * (kPAS_{MC_{mx}} + kPAS_{MC_{m(x+1)}}) + w_U * (kU_{MC_{mx}} + kU_{MC_{m(x+1)}}) + w_c * (kc_{MC_{mx}} + kc_{MC_{m(x+1)}}), m = 2,3,...,M-2, x = 1,2,...,X-1. \quad (12)$$

$$c_{mx,m(x+1)} = w_t * (2*kt_{MC_{mx}} + kt_{MC_{m(x+1)}}) + w_{pas} * (kPAS_{MC_{mx}} + kPAS_{MC_{m(x+1)}}) + w_U * (2*kU_{MC_{mx}} + kU_{MC_{m(x+1)}}) + w_c * (2*kc_{MC_{mx}} + kc_{MC_{m(x+1)}}), m = 1, x = 1,2,...,X-1. \quad (13)$$

$$c_{mx,m(x+1)} = w_t * (kt_{MC_{mx}} + 2*kt_{MC_{m(x+1)}}) + w_{pas} * (kPAS_{MC_{mx}} + kPAS_{MC_{m(x+1)}}) + w_U * (kU_{MC_{mx}} + 2*kU_{MC_{m(x+1)}}) + w_c * (kc_{MC_{mx}} + 2*kc_{MC_{m(x+1)}}), m = M-1, x = 1,2,...,X-1. \quad (14)$$

Among them, *kPAS*, *kU*, *kc* are respectively MC's assembility, structural stiffness and cost correlation.

The consolidated correlation matrix formed by connecting edges set in RTP alternative evaluation model is shown as the formula 15.

$$\begin{bmatrix} c_{11,21} & \cdots & c_{(M-2)1,(M-1)1} & c_{(M-1)1,M1} \\ \vdots & \vdots & \vdots & \vdots \\ c_{1X^2,2X^2} & \cdots & c_{(M-2)X^2,(M-1)X^2} & c_{(M-2)X^2,(M-1)X^2} \end{bmatrix}_{X^2 \times (M-1)} \quad (15)$$

The connecting edges constituting RTP should meet the condition that the end of connection edge in former layer is the beginning of connection edge of the next layer. The greater the correlation of evaluation indexes is, the better the alternative is. Therefore, the optimal goal of the second level of decision-making model is shown as formula 16.

$$\max C_{lk} = \max\left(\sum_{m,n=1}^{M} \sum_{x=1}^{X-2} (c_{mx,n(x+1)} + c_{n(x+1),l(x+2)}), m < n\right). \quad (16)$$

IV. RTP Optimization Based on MDPSO

A. The Modified Discrete Particle Swarm Optimization

The Particle Swarm Optimization (PSO) is inspired and proposed by Eberhart and Kennedy's [22], early be used on research on the modeling and simulation of the group foraging behavior of many birds. They thought that birds exchanged information with each other, and every individual could estimate its position to adapt to the value of its own through certain rules. Each individual can remember its current best position of its own, which is called "*p*best"; In addition, it can remember the best location of all found by the birds in the group, which is called "global best (*g*best)", and these two optimal variables make the birds approach to these directions to some extent. Compared with Genetic Algorithm [23], in PSO, there are no operations of GA such as selection, crossover and mutation etc., and it is a swarm intelligence calculation method which searches through following the optimized particles in the solution space.

In the particle swarm algorithm, each individual is called a "particle", and each particle represents a sub solution to a problem. The model of particle swarm algorithm is shown as Formula 17~23.

$$X = (X_1, X_2, ..., X_n), n \in N. \tag{17}$$

$$X_i = (x_{i1}, x_{i2}, ..., x_{iD})^T, D \in N. \tag{18}$$

$$V_i = (V_{i1}, V_{i2}, ..., V_{iD})^T. \tag{19}$$

$$p_i = (p_{i1}, p_{i2}, ..., p_{iD})^T. \tag{20}$$

$$p_g = (p_{g1}, p_{g2}, ..., p_{gD})^T. \tag{21}$$

$$V_{id}^{k+1} = wV_{id}^k + c_1 r_1 (p_{id}^k - X_{id}^k) + c_2 r_2 (p_{gd}^k - X_{id}^k). \tag{22}$$

$$X_{id}^{k+1} = X_{id}^k + V_{id}^{k+1}. \tag{23}$$

wherein, X represents the group constituted by n particles, indicating the location of particles; X_i represents a D dimensional vector of the particle, which is a solution vector of the problem; V_i represents the speed of the particle; p_i represents the optimum solution of each particle; p and g represent the optimum solutions of the whole group; these two extreme values constantly update themselves to produce the new generation.

Formula 22 and Formula 23 are the refreshing expressions for the speed and position of the particle, wherein, k is the current number of iterations, V_{id}^k is the flying speed of the id_{th} particle at the k_{th} iteration, X_{id}^k is the position of the id_{th} particle at the k_{th} iteration; As constants, c_1 and c_2 become learning factors and regulate the maximum step size of the flight toward the direction of the global optimum particle and the best individual particle respectively; r_1 and r_2 are random numbers within [0, 1], which are used to maintain the diversity of the population; w is the inertial coefficient which has the effect of balancing the local and global bests [24] .

The flowchart of the Modified Discrete PSO (MDPSO) algorithm is shown in figure 3. On the basis of the basic Particle Swarm Optimization algorithm, judgments and adjustments on the refreshed individuals and speeds are added.

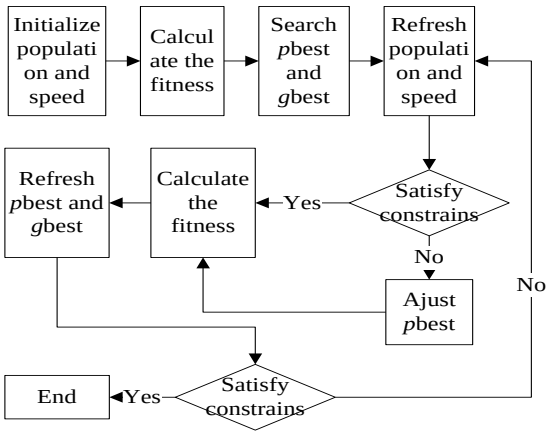


Figure 3. The process MDPSO algorithm

Utilize $m*n$ dimensional matrix to show the location and speed of a certain particle, as is shown in Formula 24~29.

$$X_i = \begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \cdots & & \cdots \\ x_{m,1} & & x_{m,n} \end{bmatrix}, V_i = \begin{bmatrix} v_{1,1} & \cdots & v_{1,n} \\ \cdots & & \cdots \\ v_{m,1} & & v_{m,n} \end{bmatrix}. \tag{24}$$

$$\sum_{i=1}^{m} x_{i,j} = 1. \tag{25}$$

$$x_{i,1} = \begin{cases} 0, \text{if the ith particle is not chosen} \\ 1, \text{if the ith particle is chosen} \end{cases} \tag{26}$$

$$\sum_{i=1}^{m} \mathrm{v}_{i,j} = 0. \tag{27}$$

$$V_{id}^{k+1} = w \otimes V_{id}^k \oplus c_1 r_1 \otimes (p_{id}^k \ominus X_{id}^k) \oplus c_2 r_2 \otimes (p_{gd}^k \ominus X_{id}^k). \tag{28}$$

$$X_{id}^{k+1}{}' = X_{id}^k \oplus V_{id}^{k+1}. \tag{29}$$

wherein, $\oplus$ $\otimes$ $\ominus$ show the addition, multiplication and subtraction of the matrix.

The refreshed speed V_{idk+1} meet formula 27, and the proof is as follows:

① w is a real number, and if V_{idk} meets Condition 27, $w \otimes V_{id}^k$ will satisfy condition 21;

② If location p_{id}^k , X_{id}^k , p_{gd}^k meet Condition 25, $p_{id}^k \ominus X_{id}^k$,and $p_{gd}^k \ominus X_{id}^k$ will meet Condition 24;

③ If $w \otimes V_{id}^k$, $p_{id}^k \ominus X_{id}^k$,and $p_{gd}^k \ominus X_{id}^k$ $w \otimes V_{id}^k$ meet condition 19, then $w \otimes V_{id}^k \oplus c_1 r_1 \otimes (p_{id}^k \ominus X_{id}^k)$ meet condition 27, that is V_{id}^{k+1} meets condition 27.

After refreshing the location and speed of the particle, exam the particles and see whether conditions 15 and 16 are tenable. If not, then the matrix will be rearranged: give only one element the value 1 in each column of the particle matrix, while others are given 0 in each column. If all the elements $X_{id}^{k+1}{}'$ in a specific column equal to 0, then refer to the column vector of $p_{gd}{}^{k}$ column, and set the vector $X_{id}^{k+1}{}'$ equal to it, as shown in formula 30.

$$X_{id}^{k+1} = \begin{bmatrix} x_{i,1}=1 & 0 & 0 \\ \dots & x_{p_{id}}=1 & x_{i,n}=1 \\ 0 & 0 & 0 \end{bmatrix}. \quad (30)$$

B. RTP Optimization Generating

RTP generating algorithm is based on the RTP model, and utilizes MDPSO algorithm to solve the model, then sorts alternative proposals according to the fitness value. The flowchart based on MDPSO algorithm is shown as the Figure 3. Here it mainly carries out detailed introduction to particle initialization, fitness function construction, speed and individual update and selection of algorithm termination conditions, as following:

1) Initialize particle position matrix and speed matrix

According to the features of MC configuration path optimization problem, the selective scheme of a connecting edge of a RTP's hierarchy network graph is regarded as a Particle X_i.

Set initialized particle position matrix and speed matrix as X and V, as shown in the Formula 31~34.

$$X=[X_1,\ X_2,\ \cdots\ X_M], V=[V_1,\ V_2,\ \cdots\ V_M]. \quad (31)$$

$$X_i = \begin{bmatrix} 1 & 0 & x_{1,K-1} \\ \cdots & 1 & \cdots \\ 0 & \cdots & \\ 0 & 0 & x_{x^2,K-1} \end{bmatrix}_{x^2\times(K-1)}, V_i = \begin{bmatrix} v_{1,1} & \dots & v_{1,K-1} \\ \dots & & \dots \\ & & \\ v_{x^2,1} & & v_{x^2,K-1} \end{bmatrix}_{x^2\times(K-1)}. \quad (32)$$

$$\sum_{i=1}^{x^2} x_{i,j}=1, x_{i,j}=0,1. \quad (33)$$

$$\sum_{i=1}^{x^2} v_{i,j}=1. \quad (34)$$

According to the bound combination of connected line, elements inside particle matrix have the constraint relationships as below:

Regarding the elements $x_{i,j}$ inside the particle matrix, make $i=x*n+m$, ($n=0, 1, 2, ..., N; m=1, 2, ..., x; x*n+m \le x2$). The elements of two adjacent columns inside particle matrix have the following relationship, as shown in Formula 35.

$$\begin{aligned} &if\ x_{i,j}=1, then\ x_{i+1,j+1}=1,\ i+1=x*m-(x-1),\\ &x*m-(x-2),...,x*m \end{aligned} \quad (35)$$

2) The Construction of the Fitness Function

The fitness function of MDPSO algorithm is determined on the basis of Formula 16, as shown in Formula 36.

$$f_{C_{lk}} = \sum_{m,n=1}^{M} \sum_{x=1}^{X-2} (c_{mx,n(x+1)} + c_{n(x+1),l(x+2)}), m < n. \quad (36)$$

3) The Update of Speeds and Individuals.

Adopt the Formula 28, 29, 30 and 36 to update the speeds and individuals and to examine and adjust the new individual location matrix.

4) The Termination Conditions of the Selective Algorithm.

That no significant change of the new-generation fitness function value can be adopted as the termination conditions of the algorithm, or the set value G of evolutionary algebra g reaching maximum can be regarded as the termination condition, and multiple relatively excellent individuals in the output group are regarded as alternative RTP for decision-maker to choose.

V. PERFORMANCE ANALYSIS

This paper takes the RTP configuration model shown in figure 4 as an example and utilizes Matlab to implement and verify the optimized generation algorithm for RTP configuration design.

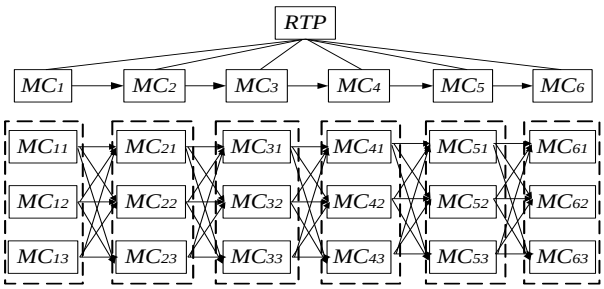


Figure 4. Feasible configuration paths of RTP

According to RTP's cost, structural stiffness and assembility dependent degree, as shown in table 2, the weights of various indexes are {0.55, 0.30, 0.15}, and the capacity matrix of connected lines is obtained, as shown in the Matrix C .

$$C = \begin{bmatrix} 1.548 & 1.296 & 4.403 & 3.323 & 1.044 & 0.625 \\ 1.561 & 1.466 & 4.176 & 3.217 & 1.066 & 1.086 \\ 1.575 & 1.622 & 3.814 & 3.386 & 1.006 & 0.820 \\ 1.466 & 1.309 & 4.213 & 3.456 & 0.938 & 0.647 \\ 1.479 & 1.479 & 4.346 & 3.349 & 0.860 & 1.108 \\ 1.493 & 1.636 & 3.985 & 3.519 & 0.899 & 0.843 \\ 1.622 & 1.323 & 4.370 & 3.095 & 1.107 & 0.578 \\ 1.636 & 1.493 & 4.502 & 2.988 & 0.979 & 1.048 \\ 1.650 & 1.650 & 4.141 & 3.157 & 1.069 & 0.783 \end{bmatrix}.$$

MDPSO algorithm is utilized to conduct combination, optimization and solving on the capacity matrix of the path. The population size is set as 20 and its initialized position and velocity matrices of the particles are shown in the Matrices X and V.

$$X = \begin{bmatrix} \overbrace{\begin{bmatrix} 1&0&0&0&0&0\\ 0&1&0&1&0&0\\ 0&0&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix}}^{X_1} & \overbrace{[\cdots]}^{X_{\cdots}} & \overbrace{\begin{bmatrix} 1&0&0&0&0&0\\ 0&0&0&1&0&0\\ 0&1&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0\\ 0&0&1&0&0&1\\ 0&0&0&0&0&0 \end{bmatrix}}^{X_{20}} \end{bmatrix}.$$

$$V = \begin{bmatrix} \overbrace{\begin{bmatrix} 1&0&-1&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ -1&-1&0&1&0&0\\ 0&0&0&-1&1&0\\ 0&0&0&0&-1&1\\ 0&0&0&0&0&-1\\ 0&0&0&0&0&0 \end{bmatrix}}^{V_1} & \overbrace{[\cdots]}^{V_{\cdots}} & \overbrace{\begin{bmatrix} 1&0&0&0&0&0\\ -1&-1&0&0&0&0\\ 0&1&-1&0&0&0\\ 0&0&1&-1&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&-1&1\\ 0&0&0&0&0&-1 \end{bmatrix}}^{V_{20}} \end{bmatrix}.$$

To verify the effectiveness of the algorithm, the enumeration method is adopted at first. After 2187 enumerations, the fitness values of all paths are obtained. According to the fitness value, 9 best RTPs have been selected hereof, as shown in the Table 3.

TABLE II. COST, STIFFNESS AND ASSEMBILITY DEPENDENCE DEGREE

No.	MC	*kc*	*kss*	*ka*
1	MC11	0.021	0.523	0.456
2	MC12	0.23	0.265	0.505
3	MC13	0.136	0.458	0.406
4	MC21	0.169	0.231	0.6
5	MC22	0.258	0.265	0.477
6	MC23	0.743	0.081	0.176
7	MC31	0.651	0.204	0.145
8	MC32	0.258	0.236	0.506
9	MC33	0.136	0.528	0.336
10	MC41	0.147	0.129	0.724
11	MC42	0.756	0.023	0.221
12	MC43	0.069	0.852	0.079
13	MC51	0.028	0.367	0.605
14	MC52	0.091	0.586	0.323
15	MC53	0.354	0.625	0.021
16	MC61	0.258	0.245	0.497
17	MC62	0.13	0.762	0.108
18	MC63	0.521	0.423	0.056

There is no standard to follow for the selection of MDPSO operator parameters *w*, *c1*, and *c2*, among which, the value of *w* determines the opportunity that the MDPSO finds out the global optimum value, and *c1* and *c2* respectively adjust the maximum step size approaching the direction of the global optimal particle and the individual optimal particle. According to the parameter selection principle of literature [6], the value of *w* is set to be 1 to 2*c1*, *c2* are set to be 2, 2, and the maximum of evolution algebra G=200 is taken as the terminal condition to conduct simulation analysis on the three parameter combinations generated using Matlab, and they are run 50 times respectively. The results are shown in Figure 4, wherein, X is the number of iterations while Y is the fitness value of the iteration. In the process of 200 iterations, the fitness values won't change any more after 20 iterations, that is, respective optimal solutions have been obtained. Therefore, only the first 20 iterative curves need to be analyzed. It can be seen from figure 5 that if *w*=2, *c1*=*c2*=*2*, at the 6th iteration, the maximum fitness value obtained is 13.49. Compared with the result of the enumeration method, it falls into the 2nd local optimal solution. Moreover, in 50 operation processes, the number of the local optimization appearing is 37; if *w*=1 or 1.5, *c1*=*c2*=2, respectively at the 5th and 10th iterations, the optimal solution obtained is 13.51. But in the 50th operation, when *w*=1, the number of appearing optimal solutions is only 2, while *w* =1.5, the number of appearing optimal solution is 35, in which the probability of obtaining optimal solution is apparently increased. Therefore, when the value of *w* is selected in the range [1, 1.5], this algorithm will obtain the optimum solution of this model and the iterations obtaining the optimal solution will be less than 20.

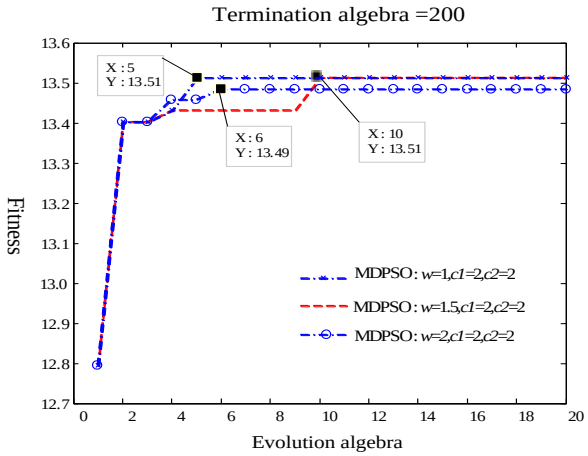


Figure 5. Iterative curves with Different value of w, c1 and c2

TABLE III. 9TH BEST RTP

No.	RTP						fitness
1	MC13	MC23	MC31	MC42	MC53	MC61	13.51
2	MC13	MC22	MC33	MC42	MC53	MC61	13.49
3	MC13	MC21	MC33	MC42	MC53	MC61	13.46
4	MC13	MC23	MC33	MC42	MC53	MC63	13.44
5	MC13	MC23	MC33	MC42	MC51	MC62	13.43
6	MC13	MC23	MC33	MC41	MC53	MC61	13.25
7	MC13	MC22	MC33	MC41	MC53	MC61	13.22
8	MC13	MC23	MC32	MC42	MC51	MC62	13.21
9	MC13	MC23	MC33	MC42	MC53	MC63	13.17

VI. CONCLUTION

This paper has presented an optimal configuration method for RTP design, considering assembly ability, cost, and structure performance indexes. It makes use of layered network and dependent degree method for establishing the configuration model to avoid conflicts in multi-objective optimization problem, and through add constrains to the basic PSO algorithm, the MDPSO algorithm is proposed to solve the RTP configuration model. Theoretical analysis and simulation results show that the MDPSO algorithm can effectively get the solution of the RTP reference model, and improve the test platform design efficiency.

ACKNOWLEDGMENT

This work was supported by Beijing Postdoctoral Research Foundation.

REFERENCES

[1] Ming C, Xu Y, Baohong S, et al. "Research on a novel R-θ wafer-handling robot". *2007. Automation and Logistics, 2007 IEEE International Conference on*, pp. 597-602, 2007.

[2] The importance of position and path repeatability on force at the knee during six-DOF joint motion". *Medical Engineering & Physics*. vol. 31, no. 5, pp. 553-557.

[3] Cong M, Cui D. "Wafer-Handling Robots and Applications". *Recent Patents on Engineering*, vol. 3, no. 3, pp. 170-177, 2009.

[4] Mori K, Ishikura T. "Device for testing wafer transporting robot", *Applied Materials, Inc. Santa Clara CA, USA*, No. US 6401554B1, 2002.

[5] Liu W, Liang M. "A Particle Swarm Optimization Approach to A Multi-objective Reconfigurable Machine Tool Design Problem", *Sheraton Vancouver Wall Centre Hotel, Vancouver, BC, Canada*, pp. 2222-2229, 2006.

[6] Zhang W, Ma D, Wei J, et al. "A parameter selection strategy for particle swarm optimization based on particle positions". *Expert Systems With Applications*. vol. 41, no. 7, pp. 3576-3584, 2014.

[7] Coello C A C, Pulido G T, Lechuga M S. "Handling multiple objectives with particle swarm optimization". Evolutionary Computation, *IEEE Transactions on.* vol. 8, no. 3, pp. 256-279, 2004.

[8] Lei J, Yamada Y, Komura Y. "Layout optimization of manufacturing cells using particle swarm optimization". *Sice 2003 Annual Conference*, Vols 1-3. vol, pp. 392-396, 2003.

[9] Coban R. "Power level control of the TRIGA Mark-II research reactor using the multi feedback layer neural network and the particle swarm optimization". *Annals Of Nuclear Energy*. vol. 69, pp. 260-266, 2014.

[10] Kao Y, Chen C. "Automatic clustering for generalized cell formation using a hybrid particle swarm optimization". *International Journal Of Production Research.* vol. 52, no. 12, pp. 3466-3484, 2014.

[11] Limei M, Jianyong L, Wensheng X, et al. "Network alliance for the total life cycle of reconfigurable machine tool". *2011. 2011 International Conference on Management Science and Industrial Engineering (MSIE)*, pp. 42-47, 2011.

[12] Moon S K. "Error prediction and compensation of reconfigurable machine tool using screw kinematics". *University of Michigan, United States, Michigan*, Ph. D., 2002.

[13] Angeles J. "Fundamentals of Robotic Mechanical Systems Theory, Methods, and Algorithms". *Springer*, 2003.

[14] Ma L M, LI J Y, XU W S. "Extenics Decision Model for Evaluating Mechanical Joint Interface of Reconfigurable Machine Tools". *2011. ICADME*, pp 1972-1976. 2011.

[15] Zhang Y, Hu W, Rong Y, et al. "Graph-based set-up planning and tolerance decomposition for computer-aided fixture design". *International Journal of Production Research.* vol. 39, no. 14, pp. 3109, 2001.

[16] Wakamori F, Masui S, Morita K, et al. "Layered Network Model Approach to Optimal Daily Hydro Scheduling". *Power Apparatus and Systems, IEEE Transactions on.* vol. PAS-101, no. 9, pp. 3310-3314, 1982.

[17] Chen L, Xi F J, Macwan A. "Optimal Module Selection for Preliminary Design of Reconfigurable Machine Tools". *Transactions of the ASME.* vol. 127, 2005.

[18] Coello C, Lamont G, Veldhuizen D. "Evolutionary Algorithms for Solving Multi-Objective Problems". 2007 *Springer Science Business Media*, LLC, 2007.

[19] Ma L, Li J, Wu W, et al. "Extenics Decision Model for Evaluating Mechanical Joint Interface of Reconfigurable Machine Tools". *2011 International Conference on Functional Manufacturing and Mechanical Dynamics*, pp. 1972-1976, 2011.

[20] Lau H C W, Wong C W Y, Lau P K H, et al. "A fuzzy multi-criteria decision support procedure for enhancing information delivery in extended enterprise networks". *Engineering Applications of Artificial Intelligence*. vol. 16, no. 1, pp. 1-9, 2003.

[21] Abdi M R. "Fuzzy multi-criteria decision model for evaluating reconfigurable machines". *Int. J. Production Economics.* vol. 1, no. 15, 2009.

[22] Kennedy J, Eberhart R. "Particle swarm optimization". *1995. Neural Networks, 1995. Proceedings., IEEE International Conference on*, pp. 1942-1948, 1995.

[23] Bryan A, Hu S J, Koren Y. "Assembly system reconfiguration planning using genetic algorithm". *2008 Proceedings of the 9th Biennial Conference on Engineering Systems Design and Analysis.* vol. 1, pp. 163-171, 2009.

[24] Parsopoulos K E, Vrahatis M N. "Particle swarm optimization method in multiobjective problems". 2002. *SAC '02*, pp. 603-607, 2002.

MA Limei, born in 1982, female, Liaocheng City, Shandong Province, Ph.d., School of Mechanical, Electronic and control Engineering,Beijing Jiaotong University, research direction for detection technology and automation devices;

LI Guoxiu, born in 1970, male, Beijing, Professor, School of Mechanical, Electronic and control Engineering, Beijing Jiaotong University, research direction for the control of engine combustion theory and technology, electronic;

Zhao Lixing, born in 1964, male, Beijing, professorate senior engineer, Beijing Automation Technical Research Institute, research direction for automatic control system, industrial automation instrument.

Instructions for Authors

Manuscript Submission

We invite original, previously unpublished, research papers, review, survey and tutorial papers, application papers, plus case studies, short research notes and letters, on both applied and theoretical aspects. Manuscripts should be written in English. All the papers except survey should ideally not exceed 12,000 words (14 pages) in length. Whenever applicable, submissions must include the following elements: title, authors, affiliations, contacts, abstract, index terms, introduction, main text, conclusions, appendixes, acknowledgement, references, and biographies.

Papers should be formatted into A4-size (8.27" x 11.69") pages, with main text of 10-point Times New Roman, in single-spaced two-column format. Figures and tables must be sized as they are to appear in print. Figures should be placed exactly where they are to appear within the text. There is no strict requirement on the format of the manuscripts. However, authors are strongly recommended to follow the format of the final version.

All paper submissions will be handled electronically in EDAS via the JNW Submission Page (URL: http://edas.info/N10935). After login EDAS, you will first register the paper. Afterwards, you will be able to add authors and submit the manuscript (file). If you do not have an EDAS account, you can obtain one. If for some technical reason submission through EDAS is not possible, the author can contact jnw.editorial@gmail.com for support.

Authors may suggest 2-4 reviewers when submitting their works, by providing us with the reviewers' title, full name and contact information. The editor will decide whether the recommendations will be used or not.

Conference Version

Submissions previously published in conference proceedings are eligible for consideration provided that the author informs the Editors at the time of submission and that the submission has undergone substantial revision. In the new submission, authors are required to cite the previous publication and very clearly indicate how the new submission offers substantively novel or different contributions beyond those of the previously published work. The appropriate way to indicate that your paper has been revised substantially is for the new paper to have a new title. Author should supply a copy of the previous version to the Editor, and provide a brief description of the differences between the submitted manuscript and the previous version.

If the authors provide a previously published conference submission, Editors will check the submission to determine whether there has been sufficient new material added to warrant publication in the Journal. The Academy Publisher’s guidelines are that the submission should contain a significant amount of new material, that is, material that has not been published elsewhere. New results are not required; however, the submission should contain expansions of key ideas, examples, elaborations, and so on, of the conference submission. The paper submitting to the journal should differ from the previously published material by at least 30 percent.

Review Process

Submissions are accepted for review with the understanding that the same work has been neither submitted to, nor published in, another publication. Concurrent submission to other publications will result in immediate rejection of the submission.

All manuscripts will be subject to a well established, fair, unbiased peer review and refereeing procedure, and are considered on the basis of their significance, novelty and usefulness to the Journals readership. The reviewing structure will always ensure the anonymity of the referees. The review output will be one of the following decisions: Accept, Accept with minor changes, Accept with major changes, or Reject.

The review process may take approximately three months to be completed. Should authors be requested by the editor to revise the text, the revised version should be submitted within three months for a major revision or one month for a minor revision. Authors who need more time are kindly requested to contact the Editor. The Editor reserves the right to reject a paper if it does not meet the aims and scope of the journal, it is not technically sound, it is not revised satisfactorily, or if it is inadequate in presentation.

Revised and Final Version Submission

Revised version should follow the same requirements as for the final version to format the paper, plus a short summary about the modifications authors have made and author's response to reviewer's comments.

Authors are requested to use the Academy Publisher Journal Style for preparing the final camera-ready version. A template in PDF and an MS word template can be downloaded from the web site. Authors are requested to strictly follow the guidelines specified in the templates. Only PDF format is acceptable. The PDF document should be sent as an open file, i.e. without any data protection. Authors should submit their paper electronically through email to the Journal's submission address. Please always refer to the paper ID in the submissions and any further enquiries.

Please do not use the Adobe Acrobat PDFWriter to generate the PDF file. Use the Adobe Acrobat Distiller instead, which is contained in the same package as the Acrobat PDFWriter. Make sure that you have used Type 1 or True Type Fonts (check with the Acrobat Reader or Acrobat Writer by clicking on File>Document Properties>Fonts to see the list of fonts and their type used in the PDF document).

Copyright

Submission of your paper to this journal implies that the paper is not under submission for publication elsewhere. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in this journal. Submission of a manuscript is interpreted as a statement of certification that no part of the manuscript is copyrighted by any other publisher nor is under review by any other formal publication.

Submitted papers are assumed to contain no proprietary material unprotected by patent or patent application; responsibility for technical content and for protection of proprietary material rests solely with the author(s) and their organizations and is not the responsibility of the Academy Publisher or its editorial staff. The main author is responsible for ensuring that the article has been seen and approved by all the other authors. It is the responsibility of the author to obtain all necessary copyright release permissions for the use of any copyrighted materials in the manuscript prior to the submission. More information about permission request can be found at the web site.

Authors are asked to sign a warranty and copyright agreement upon acceptance of their manuscript, before the manuscript can be published. The Copyright Transfer Agreement can be downloaded from the web site.

Publication Charges and Re-print

The author's company or institution will be requested to pay a flat publication fee of EUR 360 for an accepted manuscript regardless of the length of the paper. The page charges are mandatory. Authors are entitled to a 30% discount on the journal, which is EUR 100 per copy. Reprints of the paper can be ordered with a price of EUR 100 per 20 copies. An allowance of 50% discount may be granted for individuals without a host institution and from less developed countries, upon application. Such application however will be handled case by case.

More information is available on the web site at http://www.academypublisher.com/jnw/authorguide.html.

(Contents Continued from Back Cover)