Journal of Software

ISSN 1796-217X

Volume 9, Number 1, January 2014

Contents

An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform *

Tan, Wen Xue[1,2,3] Zhao, Chun Jiang* [1,3] Wu, Hua Rui [1] Wang, Xi Ping [4]

1. National Engineering Research Center for Information Technology in Agriculture, Beijing, 100097, China
2. College of Computer Science and Technology, Hunan University of Arts and Science, Changde, 415000, China
3. College of Computer Science, Beijing University of Technology, Beijing, 100022, China
4. College of Economy and Management, Hunan University of Arts and Science, Changde, Hunan, 415000, China
Email: {twxpaper,zhaocjnercita}@163.com; wuhr@nercita.org.cn; wxp7973@163.com

Abstract— **Along with a rapid growth of cloud computing technology and its deep application in Agriculture Intelligent Information System, Agriculture Industry information security and privacy has become a highlight of the issue about Agriculture Cloud Information System. Encrypting is a conventional information security means, however, hitherto almost all encryption scheme cannot support the operation based on cipher-text. As a result, it is a difficult to build up the corporate and individual information security and privacy-securing in the information system based on cloud computing platform. In order to construct the information security and privacy of cloud computing infrastructure, down to the practicality of Agriculture Information System the project crew brings forward An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform, OCEVMO for short, which takes root in the theory of matrix, and supports a series of cipher-text-operation essential to build a secure communication protocol between user, owner and cloud server. Beside the conventional encryption-decryption operation, OCEVMO implements 4 operations of cipher-text-numerical-value data such as adding, subtracting, multiplying and dividing. Theoretical analysis and experimental performance estimation demonstrates that OCEVMO is of IND-CCA security, capable of performing crypo-function with a moderate speed. Its favorable versatile performance gives promise of the interactive operation Securing corporate-individual privacy in the area of Agriculture Intelligent Information System.**

Index Terms— **Cloud computing; Agriculture Intelligent System; Data Encryption; Matrix-Operation; Privacy-Securing; IND-CCA.**

Submitted date: 2012-09-01;Revised date: 2013-06-25.

(*) This work is funded by Chinese National Natural Science Foundation (61271257, 61102126); Chinese National Science and Technology Support Program (2013BAJ04B04, 2011BAD21B02, 2012BAD52G01); Beijing Natural Science Foundation (4122034); Hunan Provincial Natural Science Foundation of China (12JJ9020); Hunan Provincial Science and Technology Plan(2013GK3135, 2012GK3125); Project of the Education Department of Hunan Province No. 11C0900 and Project of Hunan University of Arts and Science, No. JGYB1223.

(⋆) Corresponding Author: Zhao, Chun Jiang. China National Engineering Research Center for Information Technology in Agriculture(NERCITA) , Beijing Agriculture Science and Technology Building A, Room A320, Beijing Shuguang Garden Middle Road No. 11, Haidian District West Suburb, Beijing,China.

I. INTRODUCTION

Cloud computing has become a welcome computing mode based on Internet by providing user with more economical and flexible IT service such as the ability of storage, computing and network access in demand than the traditional IT technology. Since the idea of cloud computing caters to the current social trend of " Green-Computing " and " Low-Carbon Economy " [1], governments and corporations all over the world are trying their best to advocate and develop the cloud computing oriented traditional and basic industries, which activates some outstanding innovation in the area of computation and commerce in turn.

A. Status of Corporate and Individual Cloud Security

However, in the cloud computing system which has been constructed and in operation, the crux of privacy-security has been annoying people,which has become one of main factors that hold back its development and generalization.

Corporative privacy may be some data whereby to identify an individual corporation or an aggregate corporation itself such as phone number, corporation address, credit card number. In addition,some sensitive information and some expensive digital information asset of Agriculture Intelligent System and of the like system all belongs to the focus of security concern [2], [3]. For examples, the individual health reports from Diagnosing System, the Knowledge Rules of Agriculture Expert System [4], [5] and financial records from Stock System and so on.

Cloud privacy-security originates from data-trusting and service-leasehold which are 2 outstanding characteristics of cloud platform. Once people trust the third part with their data which then is stored in the cloud-server and lose the manipulative ability to their data. As a result, the event of revealing or abusing user's sensitive information occurs frequently. In recent years, some cases of cloud service provider losing or revealing user's data happened to Google and MediaMax, which

doi:10.4304/jsw.9.1.1-10

suggests people's concern about cloud privacy securing be far from unwanted [6].

Encryption is a conventional method to secure privacy. But, nowadays most of the encryption algorithm cannot support cipher-text operation such as fuzzy indexing-comparing,similarity distance calculating in encrypted document, and arithmetic operating or encrypted financial data items for Statistical Analysis Report. These operations are essential to Agriculture Cloud Intelligent System sustaining open access [7], [8].

B. Related Work and Our Contribution

According to present research , the encryption scheme addressed to sustaining cipher-text-operation, it may be classified into two classes: the search-sustaining and the compute-sustaining.

[6] brought forward a cipher-text searching method based symmetric encryption, and [9] proposed an algorithm with alike function based public encryption.However, these schemes is effective only to exact-search and is out of action when spelling errors and format mistakes occur.

[1] designed the encryption scheme based product of scalar quantity, which is compatible with K-Nearest-Neighbor (KNN) computing toward the encrypted database. In addition, some well-known homomorphic schemes such as Elgamal, Pailler and Unpadded-RSA only compatible with one homomorphic operation either homomorphic addition or homomorphic multiplication [10], [11]. As to fully homomorphic algorithm, these existed algorithms are too high computational complex to be applied in cloud computing system [12], [13].

To the issues listed above, in this paper, a novel Homomorphic Encryption Scheme oriented to Cloud Computing System is brought forward, which is rooted in the theory of vector and matrix, and supports cipher-text computation and is a promising scheme to secure privacy in the course of cloud-storing and cloud-computing.

II. Formulation of Problem

A. Privacy-Securing Model of Cloud Platform

Let abstract the cloud computing model supporting privacy-securing to Figure 1, which depicts the interaction between the Owner of data, the User of data,and Service Provider (SP for short) which is a trustee of contracted data. The following steps are introduction details.

Step 1. Owner encrypts the private-sensitive data items denoted by m_i, and returns $\mathcal{E}(m_i)$, then trust service provider with $\mathcal{E}(m_i)$ and which is stored on the server.

step 2. After being permitted or empowered by Owner, User encrypts the $para$ which denotes the operation type and the data in User's care and involved into computation, then submits all the encryption result to SP.

Step 3. Responding to the User's request, SP authenticates the User's privilege then computes $\mathcal{E}(m_i)$ in the scope denoted by $para$ according to the operation type and $para$. At last, the output denoted by $\mathcal{E}(Output)$ is returned to User.

Step 4. Use decrypts $\mathcal{E}(Output)$ and gets $Output$ in state of plain-text.

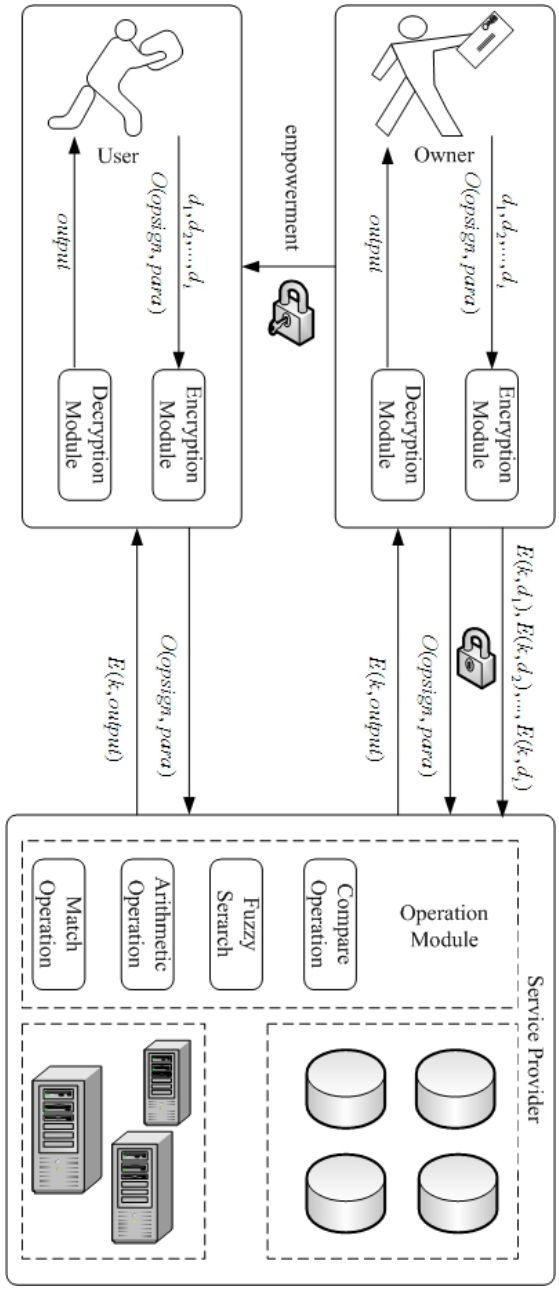


Figure 1. Privacy-Securing Model of Cloud Platform.

In this flow, both User and Owner encrypt the trusted sensitive data, the operation parameter respectively and hide their privacy in good condition. However, it is a fresh question to arise subsequently how SP operates the encrypted data and maintains operation output equivalent [14]. If it were not solved effectively, Owner and User could not exert the computer resource of cloud computing system to process sensitive data, and its advantage would be out of action [14], [15]. In such background, this literature proposes an innovative encryption scheme which may be a potential to reverse such a predicament.

B. Related Definitions

Definition 1. **Operable-Cipher-text Encryption Scheme** (OCES for short) $\bigsqcup = (\mathcal{E}, \mathcal{D}, \mathcal{G}, \mathcal{O})$, which is composed of 4 algorithms as follows.

Key-Generating algorithm $\mathcal{G}$, which is called to generate secret key k from User's random secure parameter $para$ and is denoted by (1).

$$\mathcal{G}(para) \rightarrow k \tag{1}$$

Encryption algorithm $\mathcal{E}$. Let $\widehat{X}$ and $\widehat{Y}$ denote the domain and range of $\mathcal{E}$. Address to a message $m \in \widehat{X}$, $c \in \widehat{Y}$, it is defined as (2) which is maybe either a determinate algorithm or a probable algorithm.

$$\mathcal{E}(m, k) \rightarrow \ c \tag{2}$$

Decryption algorithm $\mathcal{D}$ is defined as (3), and ϕ indicates the rootlessness of $\mathcal{D}$ operated on cipher-text. $\mathcal{D}$ must be a determinate algorithm.

$$\mathcal{D}(c, k) \rightarrow \{m\} \bigcup \{\phi\} \tag{3}$$

Cipher-text operation algorithm $\mathcal{O}$. Given a set $\{c_1, c_2, ...c_i\}, c_i \in \widehat{Y}$, (4) expresses the mathematic implication of $\mathcal{O}$, and $opsign$ represents the operation type, maybe anyone of Fuzzy-Matching and arithmetic operation $+$, $-$,$\times$,$\div$.

$$\begin{aligned} &\mathcal{D}(\mathcal{O}(c_1, c_2, ...c_i, opsign)) \rightarrow \mathcal{O}(\mathcal{D}(c_1, k) \\ &\mathcal{D}(c_2, k), ...\mathcal{D}(c_i, k), opsign) \end{aligned} \tag{4}$$

Definition 2. **Correctness** of $\bigsqcup$. OCES is defined to be correct where (5) is satisfied.

$$\begin{aligned} &I. \forall m \in \widehat{X}, \mathcal{D}(\mathcal{E}(m, k)) = m \\ &II. \exists \mathcal{O}(m_1, m_2, ...m_i, opsign) = \mathcal{D}(\mathcal{O}(\mathcal{E}(m_1, k), \\ &\mathcal{E}(m_2, k), ...\mathcal{E}(m_i, k), opsign), k) \end{aligned} \tag{5}$$

Definition 3. **Security** of $\bigsqcup$ OCES is defined to be secure subject to 2 items as follows. (1) $\bigsqcup$ is able to maintain security of Indistinguishability Against Chosen Cipher-text Attack (IND-CCA for short) in the event that the oracle of cipher-text and the oracle of plain-text about the trusted data are provided. (2). $\bigsqcup$ assures that it is impossible for SP to deduce any knowledge about original plain-text or intermediate result or the last result during the course of running $\mathcal{O}$ for operating cipher-text [14].

Definition 4. Given $c_1, c_2, c_3 \in \widehat{Y}$, a binary operant as $opsign$ defined in the above text denoted by $\circ$ so that for all $m_1, m_2, m_3 \in \widehat{X}$ it holds that $m_3 = m_1 \circ m_2$ and $c_1 = \mathcal{E}(m_1, k)$,$c_2 = \mathcal{E}(m_2, k)$ then (6) is negligible. Then it is defined that scheme $\mathcal{E}$ is homomorphic to operant $\circ$, so-called the **Homomorphic Property**.

$$Prob[\mathcal{D}(c_1 \circ c_2, k) \neq m_3] \tag{6}$$

III. Operable Cipher-text Encryption based on Vector-Matrix Operation

In this Section, an Operable Cipher-text Encryption Scheme based on Vector-Matrix Operation is constructed, which is abbreviated to OCEVMO. OCEVMO realizes the cipher-text computing such as addition, substraction, multiplication and dividing of numeric digital data under the condition that information security of both User and Owner of data is warranted.

A. Formal Definition of OCEVMO

Definition 5. $\mathbf{OCEVMO} = \{\mathcal{G}, \mathcal{E}, \mathcal{D}, \mathcal{C}\}$,which covers 4 algorithm as follows.

$\mathcal{G}$ is a key generation algorithm which is defined as (7). $para$ denotes Users' secure parameter. A key $\mathbf{K}$ is a $d \times d$ reversible matrix.

$$\mathcal{G}(para) \rightarrow \{\mathbf{K}\} \tag{7}$$

$\mathcal{E}$ is an encryption algorithm. Let $\widehat{X}$ and $\widehat{Y}$ denote the domain and range of $\mathcal{E}$. $\mathbf{m} \in \widehat{X}$ which is a d-dimension vector transformed from plain-text message, define $\mathcal{E}$ as (8), $\mathbf{c} \in \widehat{Y}$, which is a d-dimension vector and is the cipher-text of m .

$$\mathcal{E}(\mathbf{m}, \mathbf{K}) \rightarrow \mathbf{c} \tag{8}$$

$\mathcal{D}$ is a decryption algorithm which is defined as (9), $opsign$ indicates the the type of operation operated on cipher-text. $opsign = null$ denotes the operation is to decrypt the cipher-text $\mathbf{c}$ which is a direct encryption result of $\mathbf{m}$; $opsign = +$ denotes the cipher-text to be decrypted is a addition-operation result of some 2 cipher-text; $opsign = -$ denotes the cipher-text to be decrypted is a subtraction-operation result of some 2 cipher-text; $opsign = \times$ denotes the cipher-text to be decrypted is a multiplication-operation result of some 2 cipher-text; $opsign = \div$ denotes the cipher-text to be decrypted is the quotient result of some 2 cipher-text.

$$\mathcal{D}(\mathbf{c}, \mathbf{K}, opsign) \rightarrow \{\mathbf{m}\} \tag{9}$$

$\mathcal{O}$ is a cipher-text operation algorithm. Its form is as (10), which operates $\mathbf{c_1}, \mathbf{c_2}, ...\mathbf{c_i}, \mathbf{c_i} \in \widehat{Y}$, and outputs corresponding result according to $opsign$ defined in the above text. $\mathbf{c}'$ is subjected to $\mathbf{c}' \in \widehat{Y}$.

$$\mathcal{O}(\mathbf{c_1}, \mathbf{c_2}, ...\mathbf{c_i}, opsign) \rightarrow \mathbf{c}' \tag{10}$$

B. Transformation of Numeric Data

Data of cloud computing system is divided into 2 parts: numeric data and character data or string data, which is an primary idea of OCEVMO. Numeric data is often operated some mathematic operation such as addition and multiplication, while query and fuzzy-indexing is fit to character data [16]. In this literature, the former is the focus of the discussion.

Operations fit to numeric data are arithmetic operation, as is referred in the above text. In order to implement these operations, message m is preprocessed into the

vector $\mathbf{m}$. The elements of vector are partitioned into 2 parts, the adding factor which is a computation array, denoted by $FAdd$ used to implement addition of cipher-text and the multiplication factor which is also a computation array, denoted by $FMul$, used to construct multiplication of cipher-text. The dimension of $FAdd$ and $FMul$ are denoted by d_a, d_m, subject to $d_a \in N, d_a > 2, d_m \in N, d_m > 3$. No doubt, process is to be a reversible course.

Let m be a plain-text numeric data, the process whereby it is transformed into a d dimension vector is composed of following steps. At first, select d_a-1 random real number $(r_{+1}, r_{+2}, ..., r_{+d_a-1}), r_{+i} \in \mathcal{R}, i \in [1, d_a - 1]$, and extract another element by (11). So a d_a dimension vector denoted by $\mathbf{m}$ is returned as (12). Choose d_a random real number $\{r_1, r_2, ..., r_{d_a}\}, r_i \in \mathcal{R}, i \in [1, d_a]$ a second time, by which $\mathbf{m}$ is transformed into $\mathbf{m}'$ as (13).

$$r_{+d_a} = m - \sum_{i=1}^{d_a-1} r_{+i} \tag{11}$$

$$\mathbf{m} = (r_{+1}, r_{+2}, ..., r_{+d_a-1,}, r_{+d_a})^T \tag{12}$$

$$\mathbf{m}' = (r_{+1} + r_1, r_{+2} + r_2, ..., r_{+d_a} + r_{d_a})^T \tag{13}$$

Secondly, select d_m-1 random real number $(r_{\times 1}, r_{\times 2}, ..., r_{\times d_m-1}), r_{\times i} \in \mathcal{R}, i \in [1, d_m - 1]$, the multiplication inverse of $r_{\times i}$ is a limited fraction and extract another element $r_{\times d_m}$ by (14). Thus the owner of data can transform $\mathbf{m}'$ into $\mathbf{m}''$ as (16), what should be noticed is the dimension of $\mathbf{m}''$ is $d_m + d_a$.

$$r_{\times d_m} = m \div \prod_{i=1}^{d_m-1} r_{\times i} \tag{14}$$

$$\begin{aligned}\mathbf{m}'' = (&r_{+1} + r_1, r_{+2} + r_2, ..., r_{+d_a} + r_{d_a},\\ &r_{\times 1}, r_{\times 2}, ..., r_{\times d_m})^T\end{aligned} \tag{15}$$

Thirdly, by tailing a random computation array, the owner extends $\mathbf{m}''$ into a $d_m + d_a + k$ dimension vector denoted by $\mathbf{m}'''$ which is a final vector of preprocess of encryption as (16), random number $r_{\phi i} \in \mathcal{R}, k \in N, k > 2$ and $r_{\phi k}$ subjected to (17).

$$\begin{aligned}\mathbf{m}''' = (&r_{+1} + r_1, r_{+2} + r_2, ..., r_{+d_a} + r_{d_a},\\ &r_{\times 1}, r_{\times 2}, ..., r_{\times d_m}, r_{\phi 1}, r_{\phi 2}, ..., r_{\phi k-1}, r_{\phi k})^T\end{aligned} \tag{16}$$

$$r_{\phi k} = -\sum_{i=1}^{d_a} r_i \tag{17}$$

At last, Owner encrypts $\mathbf{m}'''$ and get $\hat{\mathbf{c}}$ by (18) with which is trusted SP and saved on the storage system of server by its Owner. Decryption of $\hat{\mathbf{c}}$ is an inverse process of encryption obviously, as is omitted here [17], [18].

$$\hat{\mathbf{c}} = \mathbf{K} \times \mathbf{m}''' \tag{18}$$

The steps whereby users transform query parameter into vector is similar with the course above. So, whether the trust data or query parameter is to be preprocessed through the same procedure and the result will be a vector.

From the course aforementioned, preprocessing of vector transforming scatters and hides the original information into all components of the vector. In the meantime, through an ingenious designment of each component, it becomes practical to maintain arithmetic operation equivalence between plain-text and cipher-text.

However, the computation complexity similar to " dimension curse " will arise, which means that computation workload increases in proportion to the growth of vector dimension.

Let m_p, m_q be 2 plain-text numeric data, and their corresponding final vectors be $\mathbf{p}''', \mathbf{q}'''$, and their corresponding cipher-text vectors be $\hat{\mathbf{p}}, \hat{\mathbf{q}}$. In the next text, how to implement various operation of cipher-text will be discussed in detail.

C. Addition Operation

SP operates addition on $\hat{\mathbf{p}}, \hat{\mathbf{q}}$ directly as (19).

$$\begin{aligned}&\hat{\mathbf{p}} + \hat{\mathbf{q}} = \mathbf{K} \times \mathbf{p}''' + \mathbf{K} \times \mathbf{q}'''\\ &= \mathbf{K} \times [(p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a},\\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T +\\ &(q_{+1} + q_1, q_{+2} + q_2, ..., q_{+d_a} + q_{d_a}, q_{\times 1}, q_{\times 2}, ...,\\ &q_{\times d_m}, q_{\phi 1}, q_{\phi 2}, ..., q_{\phi k-1}, q_{\phi k})^T]\\ &= \mathbf{K} \times [(p_{+1} + p_1 + q_{+1} + q_1, p_{+2} + p_2 + q_{+2} +\\ &q_2, ..., p_{+d_a} + p_{d_a} + q_{+d_a} + q_{d_a}, p_{\times 1} + q_{\times 1}, p_{\times 2} +\\ &q_{\times 2}, ..., p_{\times d_m} + q_{\times d_m}, p_{\phi 1} + q_{\phi 1}, p_{\phi 2} + q_{\phi 2}, ...,\\ &p_{\phi k-1} + q_{\phi k-1}, p_{\phi k} + q_{\phi k})^T = \mathbf{K} \times (\mathbf{p}''' + \mathbf{q}''')\end{aligned} \tag{19}$$

Then, SP returns it to User. User decrypts it as (20).

$$\begin{aligned}&\mathbf{K^{-1}} \times (\hat{\mathbf{p}} + \hat{\mathbf{q}}) = \mathbf{K^{-1}} \times \mathbf{K} \times [(p_{+1} + p_1 + q_{+1}\\ &+q_1, p_{+2} + p_2 + q_{+2} + q_2, ..., p_{+d_a} + p_{d_a} + q_{+d_a} +\\ &q_{d_a}, p_{\times 1} + q_{\times 1}, p_{\times 2} + q_{\times 2}, ..., p_{\times d_m} + q_{\times d_m}, p_{\phi 1} +\\ &q_{\phi 1}, p_{\phi 2} + q_{\phi 2}, ..., p_{\phi k-1} + q_{\phi k-1}, p_{\phi k} + q_{\phi k})^T\\ &= (p_{+1} + p_1 + q_{+1} + q_1, p_{+2} + p_2 + q_{+2} + q_2, ...,\\ &p_{+d_a} + p_{d_a} + q_{+d_a} + q_{d_a}, p_{\times 1} + q_{\times 1}, p_{\times 2} + q_{\times 2},\\ &..., p_{\times d_m} + q_{\times d_m}, p_{\phi 1} + q_{\phi 1}, p_{\phi 2} + q_{\phi 2}, ...,\\ &p_{\phi k-1} + q_{\phi k-1}, p_{\phi k} + q_{\phi k})^T = \mathbf{p}''' + \mathbf{q}'''\end{aligned} \tag{20}$$

After getting a d-dimension vector $\mathbf{p}''' + \mathbf{q}'''$, according to preprocess procedure expressed by (11),(16) and (17) from message to vector, User sums its the former d_a elements and the last element, then the result is returned which just is the addition of m_p, m_q as (21).

Multi-Adding operation of cipher-text is supported in this scheme under the condition of not being decrypted.

$$\begin{aligned}&p_{\phi k} + q_{\phi k} + \sum_{i=1}^{d_a} (p_{+i} + p_i + q_{+i} + q_i) = -\sum_{i=1}^{d_a} (p_i)\\ &-\sum_{i=1}^{d_a} (q_i) + [\sum_{i=1}^{d_a} (p_{+i}) + \sum_{i=1}^{d_a} (p_i) + \sum_{i=1}^{d_a} (q_{+i})\\ &+\sum_{i=1}^{d_a} (q_i)] = \sum_{i=1}^{d_a} (p_{+i}) + \sum_{i=1}^{d_a} (q_{+i}) = m_p + m_q\end{aligned} \tag{21}$$

D. Subtraction Operation

SP subtracts $\hat{\mathbf{q}}$ from $\hat{\mathbf{q}}$ by (22).

$$\begin{aligned}&\hat{\mathbf{p}}-\hat{\mathbf{q}}=\mathbf{K}\times\mathbf{p}'''-\mathbf{K}\times\mathbf{q}'''\\&=\mathbf{K}\times[(p_{+1}+p_1,p_{+2}+p_2,...,p_{+d_a}+p_{d_a},\\&p_{\times1},p_{\times2},...,p_{\times d_m},p_{\phi1},p_{\phi2},...,p_{\phi k-1},p_{\phi k})^T-\\&(q_{+1}+q_1,q_{+2}+q_2,...,q_{+d_a}+q_{d_a},q_{\times1},q_{\times2},...,\\&q_{\times d_m},q_{\phi1},q_{\phi2},...,q_{\phi k-1},q_{\phi k})^T]\\&=\mathbf{K}\times[(p_{+1}+p_1-q_{+1}-q_1,p_{+2}+p_2-q_{+2}-\\&q_2,...,p_{+d_a}+p_{d_a}-q_{+d_a}-q_{d_a},p_{\times1}-q_{\times1},p_{\times2}-\\&q_{\times2},...,p_{\times d_m}-q_{\times d_m},p_{\phi1}-q_{\phi1},p_{\phi2}-q_{\phi2},...,\\&p_{\phi k-1}-q_{\phi k-1},p_{\phi k}-q_{\phi k})^T=\mathbf{K}\times(\mathbf{p}'''-\mathbf{q}''')\end{aligned}\tag{22}$$

Its result is returned and User can decrypt it as (23).

$$\begin{aligned}&\mathbf{K^{-1}}\times(\hat{\mathbf{p}}-\hat{\mathbf{q}})=\mathbf{K^{-1}}\times\mathbf{K}\times[(p_{+1}+p_1-q_{+1}\\&-q_1,p_{+2}+p_2-q_{+2}-q_2,...,p_{+d_a}+p_{d_a}-q_{+d_a}-\\&q_{d_a},p_{\times1}-q_{\times1},p_{\times2}-q_{\times2},...,p_{\times d_m}-q_{\times d_m},p_{\phi1}-\\&q_{\phi1},p_{\phi2}-q_{\phi2},...,p_{\phi k-1}-q_{\phi k-1},p_{\phi k}-q_{\phi k})^T\\&=(p_{+1}+p_1-q_{+1}-q_1,p_{+2}+p_2-q_{+2}-q_2,...,\\&p_{+d_a}+p_{d_a}-q_{+d_a}-q_{d_a},p_{\times1}-q_{\times1},p_{\times2}-q_{\times2},\\&...,p_{\times d_m}-q_{\times d_m},p_{\phi1}-q_{\phi1},p_{\phi2}-q_{\phi2},...,\\&p_{\phi k-1}-q_{\phi k-1},p_{\phi k}-q_{\phi k})^T=\mathbf{p}'''-\mathbf{q}'''\end{aligned}\tag{23}$$

User totals its the former d_a elements and the last element and the output is returned, which just is the difference between m_p and m_q as (24). Multi-Subtracting operation of cipher-text is acceptable in this scheme before being decrypted.

$$\begin{aligned}&p_{\phi k}-q_{\phi k}+\sum_{i=1}^{d_a}(p_{+i}+p_i-q_{+i}-q_i)=-\sum_{i=1}^{d_a}(p_i)\\&+\sum_{i=1}^{d_a}(q_i)+[\sum_{i=1}^{d_a}(p_{+i})+\sum_{i=1}^{d_a}(p_i)-\sum_{i=1}^{d_a}(q_{+i})\\&-\sum_{i=1}^{d_a}(q_i)]=\sum_{i=1}^{d_a}(p_{+i})-\sum_{i=1}^{d_a}(q_{+i})=m_p-m_q\end{aligned}\tag{24}$$

E. Multiplication Operation

At first, introduce the principle of implementing multiplication in this scheme by a specific case. Let m_p, m_q be 2 plain-text numeric data, and their corresponding final vectors be 2 6-dimension vector $\mathbf{p}''', \mathbf{q}'''$ as (25) and (26).

Obviously $m_p = p_{+1} + p_{+2} = p_{\times1} \times p_{\times2}$ and $m_q = q_{+1} + q_{+2} = q_{\times1} \times q_{\times2}$ according to (11) and (14). $p_1, p_2, q_1, q_2, p_{\phi1}, q_{\phi1}$ be random real number. Then, watch the multiplication result of ${\mathbf{p}'''}^T$ and $\mathbf{q}'''$ denoted by 6×6 Matrix $\mathbf{R}$ as (31) and (32) and its column components as expressed by (27) $\sim$ (30).

$$\mathbf{p}'''=(p_{+1}+p_1,p_{+2}+p_2,p_{\times1},p_{\times2},p_{\phi1},p_{\phi2})^T\tag{25}$$

$$\mathbf{q}'''=(q_{+1}+p_1,q_{+2}+q_2,q_{\times1},q_{\times2},q_{\phi1},q_{\phi2})^T\tag{26}$$

$$\mathbf{R_{*1}}=\begin{bmatrix}p_{+1}q_{+1}+p_{+1}q_1+p_1q_{+1}+p_1q_1\\p_{+2}q_{+1}+p_{+2}q_1+p_2q_{+1}+p_2q_1\\p_{\times1}q_{+1}+p_{\times1}q_1\\p_{\times2}q_{+1}+p_{\times2}q_1\\p_{\phi1}q_{+1}+p_{\phi1}q_1\\p_{\phi2}q_{+1}+p_{\phi2}q_1\end{bmatrix}\tag{27}$$

$$\mathbf{R_{*2}}=\begin{bmatrix}p_{+1}q_{+2}+p_{+1}q_2+p_1q_{+2}+p_1q_2\\p_{+2}q_{+2}+p_{+2}q_2+p_2q_{+2}+p_2q_2\\p_{\times1}q_{+2}+p_{\times1}q_2\\p_{\times2}q_{+2}+p_{\times2}q_2\\p_{\phi1}q_{+2}+p_{\phi1}q_2\\p_{\phi2}q_{+2}+p_{\phi2}q_2\end{bmatrix}\tag{28}$$

$$\mathbf{R_{*3,*4}}=\begin{bmatrix}p_{+1}q_{\times1}+p_1q_{\times1}&p_{+1}q_{\times2}+p_1q_{\times2}\\p_{+2}q_{\times1}+p_2q_{\times1}&p_{+2}q_{\times2}+p_2q_{\times2}\\p_{\times1}q_{\times1}&p_{\times1}q_{\times2}\\p_{\times2}q_{\times1}&p_{\times2}q_{\times2}\\p_{\phi1}q_{\times1}&p_{\phi1}q_{\times2}\\p_{\phi2}q_{\times1}&p_{\phi2}q_{\times2}\end{bmatrix}\tag{29}$$

$$\mathbf{R_{*5,*6}}=\begin{bmatrix}p_{+1}p_{\phi1}+p_1p_{\phi1}&p_{+1}p_{\phi2}+p_1p_{\phi2}\\p_{+2}p_{\phi1}+p_2p_{\phi1}&p_{+2}p_{\phi2}+p_2p_{\phi2}\\p_{\times1}p_{\phi1}&p_{\times1}p_{\phi2}\\p_{\times2}p_{\phi1}&p_{\times2}p_{\phi2}\\p_{\phi1}p_{\phi1}&p_{\phi1}p_{\phi2}\\p_{\phi2}p_{\phi1}&p_{\phi2}p_{\phi2}\end{bmatrix}\tag{30}$$

$$\mathbf{R}=(R_{*1},R_{*2},R_{*3,*4},R_{*5,*6})\tag{31}$$

$$\mathbf{p}'''\times{\mathbf{q}'''}^T=\mathbf{R}\tag{32}$$

It is found that if we multiply $\mathbf{R}[3][3]$ and $\mathbf{R}[4][4]$ the product of m_p, m_q will be extracted as (30).

$$\begin{aligned}&\prod_{i=3}^{4}\mathbf{R}[i][i]=p_{\times1}q_{\times1}\times p_{\times2}q_{\times2}\\&=p_{\times1}p_{\times2}\times q_{\times2}q_{\times1}=m_p\times m_q\end{aligned}\tag{33}$$

So, the product of any cipher-text-pair may be computed similarly. According to the analysis above, SP operates the cipher-text-pair $\hat{\mathbf{p}}, \hat{\mathbf{q}}$ as (34).

$$\begin{aligned}&\hat{\mathbf{p}}\times\hat{\mathbf{q}}^{\mathbf{T}}=\mathbf{K}\times\mathbf{p}'''\times(\mathbf{K}\times\mathbf{q}''')^T\\&=\mathbf{K}\times\mathbf{p}'''\times{\mathbf{q}'''}^T\times\mathbf{K}^T\\&=\mathbf{K}\times(p_{+1}+p_1,p_{+2}+p_2,...,p_{+d_a}+p_{d_a},\\&p_{\times1},p_{\times2},...,p_{\times d_m},p_{\phi1},p_{\phi2},...,p_{\phi k-1},p_{\phi k})^T\times\\&(q_{+1}+q_1,q_{+2}+q_2,...,q_{+d_a}+q_{d_a},q_{\times1},q_{\times2},...,\\&q_{\times d_m},q_{\phi1},q_{\phi2},...,q_{\phi k-1},q_{\phi k})\times\mathbf{K}^T\end{aligned}\tag{34}$$

The result of (34) is a $d \times d$ matrix which is to be returned to User by SP. User can decrypt it as (35).

$$\begin{aligned}&\mathbf{K}^{-1} \times \mathbf{K} \times (p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a},\\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T \times\\ &(q_{+1} + q_1, q_{+2} + q_2, ..., q_{+d_a} + q_{d_a}, q_{\times 1}, q_{\times 2}, ...,\\ &q_{\times d_m}, q_{\phi 1}, q_{\phi 2}, ..., q_{\phi k-1}, q_{\phi k}) \times \mathbf{K}^T \times \mathbf{K^{-1}}^T\\ &= (p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a},\\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T \times\\ &(q_{+1} + q_1, q_{+2} + q_2, ..., q_{+d_a} + q_{d_a}, q_{\times 1}, q_{\times 2}, ...,\\ &q_{\times d_m}, q_{\phi 1}, q_{\phi 2}, ..., q_{\phi k-1}, q_{\phi k}) = \mathbf{p'''} \times \mathbf{q'''}^T\end{aligned} \tag{35}$$

The result of (35) also is a $d \times d$ matrix denoted by $\mathbf{R}$. Then, User computes the multiplication of m_p, m_q as (36). Only is one-time multiplication permissable in this scheme in the state of cipher-text.

$$\prod_{i=d_a+1}^{d_a+d_m} \mathbf{R}[i][i] = m_p \times m_q \tag{36}$$

F. Division Operation

Let us recall the referred case about 6-dimension vector firstly. Examine the third column of $\mathbf{R}, \mathbf{R_{*3}}$,and sum its elements No. 1, No. 2 and No. 6 as (37).

$$\begin{aligned}&p_{+1}q_{\times 1} + p_1 q_{\times 1} + p_{+2}q_{\times 1} + p_2 q_{\times 1} + p_{\phi 2} q_1 =\\ &p_{+1}q_{\times 1} + p_1 q_{\times 1} + p_{+2}q_{\times 1} + p_2 q_{\times 1} - (p_1 + p_2)\\ &\times q_{\times 1} = (p_{+1} + p_{+2}) \times q_{\times 1} = m_p \times q_{\times 1}\end{aligned} \tag{37}$$

Similarly, as to the fourth column of $\mathbf{R}, \mathbf{R_{*4}}$, and sum its elements No. 1, No. 2 and No. 6 as (38).

$$\begin{aligned}&p_{+1}q_{\times 1} + p_1 q_{\times 2} + p_{+2}q_{\times 1} + p_2 q_{\times 2} + p_{\phi 2} q_2 =\\ &p_{+1}q_{\times 2} + p_1 q_{\times 2} + p_{+2}q_{\times 2} + p_2 q_{\times 2} - (p_1 + p_2)\\ &\times q_{\times 2} = (p_{+1} + p_{+2}) \times q_{\times 2} = m_p \times q_{\times 2}\end{aligned} \tag{38}$$

Extract the product of (37) and (38), rewrite and reduce its mathematic process and (39) may be returned.

$$\begin{aligned}&\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[j][i]) = m_p \times q_{\times 1} \times m_p \times q_{\times 2}\\ &= m_p^2 \times m_q\end{aligned} \tag{39}$$

Pay attention to the third row of $\mathbf{R}$, and sum its elements No. 1, No. 2 and No. 6 as (40), another approximate relation is to be found.

$$\begin{aligned}&p_{\times 1}q_{+1} + p_{\times 1}q_1 + p_{\times 1}q_{+2} + p_{\times 1}q_2 + p_{\times 1}q_{\phi 2} =\\ &p_{\times 1}q_{+1} + p_{\times 1}q_1 + p_{\times 1}q_{+2} + p_{\times 1}q_2\\ &-p_{\times 1}(q_1 + q_2) = p_{\times 1} \times (q_{+1} + q_{+2}) = p_{\times 1} \times m_q\end{aligned} \tag{40}$$

As to the fourth row of $\mathbf{R}$,and sum its elements No. 1, No. 2 and No. 6 as (41).

$$\begin{aligned}&p_{\times 2}q_{+1} + p_{\times 2}q_1 + p_{\times 2}q_{+2} + p_{\times 2}q_2 + p_{\times 2}q_{\phi 2} =\\ &p_{\times 2}q_{+1} + p_{\times 2}q_1 + p_{\times 2}q_{+2} + p_{\times 2}q_2\\ &-p_{\times 2}(q_1 + q_2) = p_{\times 2} \times (q_{+1} + q_{+2}) = p_{\times 2} \times m_q\end{aligned} \tag{41}$$

Extract the product of (40) and (41), rewrite and reduce its mathematic process and (42) may be returned.

$$\begin{aligned}&\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[i][j]) = m_q \times p_{\times 1} \times m_q \times p_{\times 2}\\ &= m_q^2 \times m_p\end{aligned} \tag{42}$$

Divide the right of (39) by that of (42) and the quotient of $m_p \div m_q$ is to be output as (43).

$$\frac{\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[j][i])}{\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[i][j])} = m_p \div m_q \tag{43}$$

By the analysis of the case, it is easy to give an algorithm of dividing-operation of encipher-text. At first, SP operates the cipher-text-pair $\hat{\mathbf{p}}, \hat{\mathbf{q}}$ as (34) and the result of (34) is a $d \times d$ matrix which is to be returned to User by SP, User can decrypt it as (35) and the preprocessing course is the same with multiplication operation. In order to get dividing result, User must execute the further operation as (44),(45) and (46).

$$\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[j][i]) = m_p^{d_m} \times m_q \tag{44}$$

$$\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[i][j]) = m_q^{d_m} \times m_p \tag{45}$$

$$\sqrt[d_m-1]{\frac{\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[j][i])}{\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[i][j])}} = m_p \div m_q \tag{46}$$

it is self-evident that the right of " = " in (46) is just the answer, i.e. the quotient of dividing m_p by m_q. What is notable is that only one-time division operation is permitted in this scheme in the event of encryption.

IV. Proof of Correctness

As a cipher-text operable encryption scheme, correctness of OCEVMO should be demonstrated in two respects: exactness of encrypting-decrypting and its homomorphic compatibility [19]. So, its proof question is to be broken into two sub-questions as follows.

1.$\forall m \in \mathbf{X}$,proof $\mathcal{D}[\mathcal{E}(m, \mathbf{K}), \mathbf{K}] = m$.

2.For $\forall\{\hat{\mathbf{p_1}}, \hat{\mathbf{p_2}}, ..., \hat{\mathbf{p_t}}\}$,and subjected to $\hat{\mathbf{p_i}} \in \mathbf{Y}$, proof that (47) should come into existence.

$$\begin{aligned}&\mathcal{O}(\hat{\mathbf{p_1}}, \hat{\mathbf{p_2}}, ..., \hat{\mathbf{p_t}}, opsign) = \mathcal{E}\{\mathcal{O}[\mathcal{D}(\hat{\mathbf{p_1}}, \mathbf{K}),\\ &\mathcal{D}(\hat{\mathbf{p_2}}, \mathbf{K}), ..., \mathcal{D}(\hat{\mathbf{p_t}}, \mathbf{K}), opsign], \mathbf{K}\}\end{aligned} \tag{47}$$

Proof 1. OCEVMO is based on Matrix operation. $\mathbf{K}$ is a $d \times d$ reversible matrix, so the matrix multiplication is reversible. In addition,the course of transforming plain-text m into vector $\hat{\mathbf{m}}_\mathbf{p}$ is recoverable, which is denoted by $\mathcal{T}(m) = \mathbf{m_p}$. In sum, the process of transformation is to be expressed by (48) and its reversibility and correctness is self-evident.

It is the end of proof 1.

$$\begin{aligned}&\mathcal{D}\{\mathcal{E}(m, \mathbf{K}), \mathbf{K}\} = \mathcal{T}^{-1}\{\mathcal{D}[\mathcal{E}(\mathcal{T}(m), \mathbf{K}), \mathbf{K}]\\ &= \mathcal{T}^{-1}\{\mathcal{D}[\mathcal{E}(\mathbf{m_p}, \mathbf{K}), \mathbf{K}]\} = \mathcal{T}^{-1}\{\mathbf{m_p}\} = m\end{aligned} \tag{48}$$

Proof 2. Where $opsign = \text{“}+\text{”}$ and $t = 2$, the proof object may be adapted into (49).

$$\begin{aligned}&\mathcal{O}(\hat{\mathbf{p_1}}, \hat{\mathbf{p_2}}, +) = \\ &\mathcal{E}\{\mathcal{O}[\mathcal{D}(\hat{\mathbf{p_1}}, \mathbf{K}), \mathcal{D}(\hat{\mathbf{p_2}}, \mathbf{K}), +], \mathbf{K}\}\end{aligned} \tag{49}$$

(49) can be rewritten into (50) further.

$$\begin{aligned}&\hat{\mathbf{p_1}} + \hat{\mathbf{p_2}} = \mathcal{E}\{\mathcal{O}[\mathbf{p_1}''', \mathbf{p_2}''', +], \mathbf{K}\} \\ &= \mathcal{E}\{\mathbf{p_1}''' + \mathbf{p_2}''', \mathbf{K}\} = \mathbf{K} \times (\mathbf{p_1}''' + \mathbf{p_2}''')\end{aligned} \tag{50}$$

It is obvious that the left and the right of (50) just may be formed into by substituting variables of (19). In the same way, alter $opsign = \text{“}+\text{”}, \times, \div$ in turn and make reference to (22), (34) and (46), satisfiability of other case can be build up easily. In one word, predication 2 is true.

It is the end of proof 2.

V. Analysis of Security

Theorem 1. OCEVMO **is distance-unrecoverable.**

Proof. Suppose OCEVMO is distance-unrecoverable, there must exist a function denoted by f subject to (51).

$$\begin{aligned}&f[\mathcal{E}(m_p, \mathbf{K}), \mathcal{E}(m_q, \mathbf{K})] = d(m_p, m_q) \\ &\forall\{m_p, m_q\} \in \mathbf{X}\end{aligned} \tag{51}$$

Choose 2 different keys $\mathbf{K_1}, \mathbf{K_2}$ and 2 different message $\{m_x, m_y\} \in \mathbf{X}$,and OCEVMO satisfies (52).

$$\begin{aligned}&(i).\ \alpha_1 = \mathcal{E}(m_p, \mathbf{K_1}) = \mathcal{E}(m_x, \mathbf{K_2}) \\ &(ii).\ \alpha_1 = \mathcal{E}(m_q, \mathbf{K_1}) = \mathcal{E}(m_y, \mathbf{K_2}) \\ &(iii).\ d(m_p, m_q) \neq d(m_x, m_y)\end{aligned} \tag{52}$$

Because of (51),then:

$$\begin{aligned}&f(\alpha_1, \alpha_2) = f(\mathcal{E}(m_p, \mathbf{K_1}), \mathcal{E}(m_q, \mathbf{K_1})) \\ &= d(m_p, m_q); f(\alpha_1, \alpha_2) = f(\mathcal{E}(m_x, \mathbf{K_2}), \\ &\mathcal{E}(m_y, \mathbf{K_2}) = d(m_x, m_y) = d(m_p, m_q)\end{aligned} \tag{53}$$

Obviously, the last item of (53) is a contradiction to the last item of (52). So,there must not exist the function f, and OCEVMO cannot but distance-unrecoverable.

Definition 6 Unsolvable Equation. Let $\widehat{\mathbf{P}}$ be the set of d dimension vector, $\widehat{\mathbf{K}}$ be the set of $d \times d$, as to $\forall \hat{p}_i \in \widehat{\mathbf{P}}, \forall \mathbf{K}_j \in \widehat{\mathbf{K}}$ there exists the equation denoted by $f(\hat{p}_i, \mathbf{K}_j) = \hat{p}_k, \hat{p}_k \in \widehat{\mathbf{P}}, i, j, k \in N$, subject to $s_L > s_R$ and s_L, s_R denote the number of the unknowns in both sides of “ = ” respectively, so that the equation $f(\hat{p}_i, \mathbf{K}_j) = \hat{p}_k$ is defined an **Unsolvable Equation** [20].

Theorem 2. As to encryption-decryption and the mathematic operation of numeric plain-text, OCEVMO is of security under IND-CCA if the number of adding factor $d_a > 3$.

Proof. Case 1. An adaptive chosen cipher-text attacker $\widetilde{H}$ oracles to have gotten t pair of plain-cipher text by means of encrypting-decrypting trust data generated by **OCEVMO**. In **OCEVMO**, let the dimension of vector be $d = n+k$ and the size of matrix be $d \times d$ where n is the number of computational elements and k is the number of random elements. To $\widetilde{H}$, the number of the unknown in $\mathbf{K}$ is $d \times d$, and the number of the unknown in the known part of each cipher-plain text is $d_a + (n-2) + (k-1)$, that of another part is d [21]. In addition, according to the section III, the unknown number in the both sides of the equation of **OCEVMO** and their relationship can be expressed by (54). So, due to d^2, t be positive, if $d_a > 3$ is satisfied, (54) is sure to be true, and the equation group derived from the matrix **OCEVMO** is unsolvable.

$$\begin{aligned}&d \times d + t \times (d_a + (n-2) + (k-1)) > \\ &t \times d \Longrightarrow d^2 + (d_a - 3) \times t > 0\end{aligned} \tag{54}$$

Case 2. Hacker $\widetilde{H}$ kicks off attack against **OCEVMO** following steps as follows. 1. $\widetilde{H}$ picks up two items of data m_1, m_2 and sends them to Owner, who encrypts either of them at random denoted by $m_r, r \in 0, 1$ and returns the cipher-text $\hat{\mathbf{m}}_r$ to $\widetilde{H}$. 2. $\widetilde{H}$ selects some plain-text (or cipher-text) and query Owner for **OCEVMO** encryption (or decryption), some corresponding result is returned back. 3. $\widetilde{H}$ repeats the step 2 until there are t pairs plain-cipher text couples denoted by $(m_1, \hat{\mathbf{m}}_1)$,$(m_2, \hat{\mathbf{m}}_2)$,...$(m_t, \hat{\mathbf{m}}_t)$ in $\widetilde{H}$'s hand. 4. $\widetilde{H}$ tries his best to compute and output m' as his oracle of m_b [22].

According to the transformation procedure of numeric data, the cipher-text of m_p is $\hat{\mathbf{p}}$ extracted by (55).

$$\begin{aligned}&\hat{\mathbf{p}} = \mathbf{K} \times \mathbf{p}''' \\ &= \mathbf{K} \times (p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a}, \\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T\end{aligned} \tag{55}$$

In (55), beyond $p_{+d_a}, p_{\times d_m}, p_{\phi k}$, the left elements are random real numeric, which are sampled at random with respect to m_p. On principle of Vector-Matrix operation, each element of the vector is determined by including all the elements of matrix and vector that plays the role of the operand, in the meantime, is affected by random numeric too [23]. Thus, it is assured that if the same numeric plain-text m_p is encrypted by the same key $\mathbf{K}$ time after time, the output cipher-text of each time are different. Because the range of **OCEVMO** is $\mathcal{R}$, and let $\parallel \mathcal{R} \parallel$ denote the element number of $\mathcal{R}$, the advantage probability of $m' = m_b$ in $\widetilde{H}$'s hand may be measured by (56).

$$\begin{aligned}&Adv(\widetilde{H}) = |Prob[m' = m_b] - \tfrac{1}{2}| \\ &= |(\tfrac{1}{2} - \tfrac{1}{\parallel \mathcal{R} \parallel}) - \tfrac{1}{2}| = |\tfrac{1}{\parallel \mathcal{R} \parallel}|\end{aligned} \tag{56}$$

Hence, where $d_a > 3$, the advantage probability of $m' = m_b$ in $\widetilde{H}$'s hand is a negligible quantity.

Case 3. While math operation is performed on cipher-text, it is stated in the section III that the indeterminacy of cipher-text is not influenced upon by a bit during the course of operation, and the advantage probability of giving a success oracle in $\widetilde{H}$'s hand is the same with Case 2 in that $\widetilde{H}$ is not in the know about key.

Sum up Case 1, 2, and 3, it is drawn that when the number of adding factor $d_a > 3$, OCEVMO is of security under IND-CCA [24].

It is the end of Proof.

VI. Performance Testing Analysis

In this Section, the performance of OCEVMO is estimated by drawing a parallel between the algorithm unpadded_RSA which supports multiple homomorphic, and the algorithm Piller which is compatible with additional homomorphic in terms of running performance. The indexes of performance include encrypting-decrypting speed, arithmetic operation performance and loads of storing and communication. All of the experiment is deployed on the platform named by **ArgSoSo** [25],which is the Agriculture Information Intelligent Searching Platform developed by the project crew of Chinese National Engineering Research Center for Information Technology in Agriculture based on Web technology and Cloud Computing, the hardware of which is a cluster consisted of 10 servers named DeepCom made by Lenovo [26].

TABLE I.
Performance of OCEVMO & concerned schemes

Algos	U_RSA	Piller	OCEVMO			
Para	50-bits- key		d			
			10	30	80	100
E	0.024	0.067	0.022	0.051	2.945	5.487
D	0.033	0.049	0.026	0.077	2.738	5.794
SP+	\	0.028	0.033	0.002	0.002	0.001
SP-	\	0.029	0.002	0.002	0.002	0.001
U+	\	0.050	0.002	0.019	0.045	0.096
U-	\	0.050	0.018	0.021	0.043	0.098
SP×	0.002	\	0.004	0.015	0.128	0.209
SP÷	0.002	\	0.004	0.015	0.107	0.274
U×	0.021	\	0.055	0.497	8.679	9.345
U÷	0.021	\	0.047	0.495	8.677	9.428
cLen	11	21	44	130	347	427

A. Experimental Statistics

In the experiment, 50-bits-key is used as secret key in unpadded_RSA and Piller. Statistics is listed in Table I in detail. What is a supplementary explanation is that SP_+ represents the addition operation is carried by SP; U denotes User and U_+ marks the addition operation is operated by User. Other symbols not referred here is to be explained analogically.“ E ”,“ D ” and “ cLen ” indicate original Encryption and Decryption operation, cipher-text Length respectively.

B. Analysis of the Statistics

From Table I, the results are discovered as follows. (1). In the case of $d < 10$, the encryption-operation time of OCEVMO is longer than unpadded_RSA [27], [28] and shorter than Piller [29], [30]; as to storing-communication loads, OCEVMO is the biggest among 3 schemes; the theoretic complexity of running and storing-communication are $O(d^2)$ and $O(d)$ respectively. (2). Addition time of OCEVMO and subtraction OCEVMO are equal nearly, while on condition of $d < 100$, the addition-substraction time of OCEVMO is shorter than that of Piller; because the theoretic complexity of running is $O(d)$, the things is to be reversed on condition that d increases to some critical point. (3). Add-subtract output decryption time of OCEVMO is pretty much the same thing, which with the theoretic complexity $O(d^2)$ is shorter than Piller in case of $d < 80$. (4). multiplication-time of OCEVMO and dividing-time OCEVMO are equal nearly, which is far more than that of unpadded_RSA and can be expressed by $O(d^2)$. (5). Multiple-divide output decryption time of OCEVMO is pretty much the same thing too, which is with the theoretic complexity $O(d^3)$ longer than unpadded_RSA .

Taking one with another, OCEVMO is characterized as follows: a favorable encryption performance, a moderate cost time of addition-subtraction while a relatively long cost time of multiplication-division, a burdensome load of storing-communicating, and that the magnitude of each index swells up with the increasing dimension of vector.

VII. Conclusion

Addressed to the question of privacy-securing in cloud computing system, this literature pioneers a cloud computing model supporting privacy-securing and designs An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform OCEVMO, which realizes 4 operations of numeric data, i.e. addition, subtraction, multiplication and division. Theoretic analysis demonstrates that 4 operations of numeric data OCEVMO is of IND-CCA security in case of the adding factor bigger than 3. Experimental statistics and its estimation proves that OCEVMO is characterized by a better encryption performance, an effective implementation of cipher addition-subtraction, a favorable versatile performance and it is a promising scheme to secure privacy in the course of storing and computing and other Agriculture Intelligent Applications based cloud platform.

On the next research practice, We will focus on how to better the multiplication-division performance of this scheme, and strive to implement multi-time multiple-divide operation, in the meantime to reduce the storing-communication load and further to optimize its versatile performance.

Acknowledgement

This work is funded by Chinese National Natural Science Foundation (61271257, 61102126); Chinese National Science and Technology Support Program (2013BAJ04B04, 2011BAD21B02, 2012BAD52G01); Beijing Natural Science Foundation (4122034); Hunan Provincial Natural Science Foundation of China (12JJ9020); Hunan Provincial Science and Technology Plan(2013GK3135, 2012GK3125); Project of the Education Department of Hunan Province No. 11C0900 and Project of Hunan University of Arts and Science, No. JGYB1223.

The authors also gratefully acknowledge the helpful comments and suggestions from the reviewers, which contribute to a refined paper presentation.

REFERENCES

[1] Wand W C,Li Z W,Owens R; Secure and Efficient Access to outsourced Data,*Proceedings of 2009 ACM Workshop on Cloud Computing Security*, Chichgo, Inninois, USA, pp. 55-55, 2009.

[2] Li, Daoliang; Yang, Simon X; INTELLIGENT AUTOMATION AND CONTROL SYSTEMS FOR AGRICULTURE, *INTELLIGENT AUTOMATION AND SOFT COMPUTING*, Vol. 18, No. 5, pp. 439-441, 2012.

[3] Lukose, Dickson; World Wide Semantic Web of Agriculture Knowledge, *JOURNAL OF INTEGRATIVE AGRICULTURE*,Vol. 11, No. 5, pp. 769-774, 2012.

[4] Peres, Emanuel; Fernandes, Miguel A. ; Morais, Raul; An autonomous intelligent gateway infrastructure for in-field processing in precision viticulture, *COMPUTERS AND ELECTRONICS IN AGRICULTURE*, Vol. 78, No. 2, pp. 176-187, 2011.

[5] Aquino-Santos, Raul; Gonzalez-Potes, Apolinar; Edwards-Block, Arthur;Developing a New Wireless Sensor Network Platform and Its Application in Precision Agriculture, *SENSORS*, Vol. 11, No. 1, pp. 1192-1211, 2011.

[6] Liu Q,Wang G J,Wu J; An effiecent privacy preserving keyword search scheme in cloud computing,*Proceeding of the 12th IEEE International Conference on Computational Scinece and Engineering* , Vancouver, Canada, pp. 715-720, 2009.

[7] Satake, Yuichi; Yamazaki, Tomihiro; Using Food and Agriculture Cloud to Improve Value of Food Chain , *FUJITSU SCIENTIFIC & TECHNICAL JOURNAL*,Vol. 47, No. 4, pp. 378-386, 2011.

[8] LOU Xiao-ping,DAI Jun. Research and implement of a voice encryption method in the trunking communication, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 20, No. 4, pp. 75-78, 2008.

[9] Bonech D,Crescenzo G D,Ostrovsky R,Public Key Encryption with keyword search ,*Proceedings of the Eurocrypt 2004*, Interlaken, Swizerland, pp. 506-522, 2004.

[10] Muhammad Asif, Nitin Tripathi. Evaluation of OpenID-Based Double-Factor Authentication for Preventing Session Hijacking in Web Applications ,*Journal of Computers*,vol. 7, No. 11. pp. 2623-2628, 2012.

[11] Pang Liao-Jun, Li Hui-Xian, Jiao Li-Cheng, et.al. Design and Analysis of a Provable Secure Multi-Recipient Public Key Encryption Scheme, *Journal of Software*, vol. 20, No.10, pp. 2907-2914, 2009.

[12] ZHANG Xiao-dan;XIAO Xiao-qiang. A Fast Algorithm on Pairs for Elliptic Curve Cryptosystems, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 21, No. 4, pp. 83-85, 2007.

[13] Yue, Jun; Li, Zhenbo; Liu, Lu; An Improved Ant Colony Algorithm for Agricultural Knowledge Storage Scheduling Under Grid Environment , *SENSOR LETTERS*,Vol. 10, No. 1-2, pp. 562-569, 2012.

[14] Douglas Stebila and Nicolas Theriault. Unified Point Addition Formula and Side-Channel Attacks,*M. CHES, Springer-Verlag*, Berlin,pp.354-368, 2006.

[15] Tan WenXue,Wang XiPing; A novel practical Certificate-Less digital signing system based on super-elliptic bilinear map parings,*Journal of Software*,Vol. 6,No. 8, pp. 1403-1408, August 2011.

[16] PAN Bao-guo; XIAO Xiao-qiang. Parameters estimation of a bilinear model, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 21, No. 4, pp. 9-12, 2009.

[17] Wang xue-liPei ding-yi; Theory and Implementation On Elliptic and super-Elliptic Curve Cryptography,*Bei Jing-Science Press*,pp. 448-475, 2006.

[18] WenXue Tan , YiYan Fan , XiPing Wang; An Innovative Scalar Multiplication Method Based on Improved m-ary,*Journal of Software*,Vol. 7,No. 11, pp. 2470-2477, 2012.

[19] MENG Yang, FU Guang-sheng. Grover Quantum Algorithm and Security Analysis of DES, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 18, No. 3, pp. 78-79, 2006.

[20] Marc Joye. Highly Regular Right-to-Left Algorithms for Scalar Multiplication ,*CHES, LNCS 4727,Springer-Verlag,Berlin*, pp. 135-147, 2007.

[21] WenXue Tan,YiYan Fan and XiaoPing Lou; Research on a Novel Point Multiplication Method Based on Addition-Chain of Flexible-Window-Width,*ICIC Express Letters, Part B: Applications*, Vol. 3, No. 2, pp. 297-304, 2012.

[22] Xiangguo Cheng, Shaojie Zhou, Jia Yu, Xin Li, Huiran Ma. A Practical ID-Based Group Signature Scheme,*Journal of Computers*,Vol. 7, No. 11, pp. 2650-2654, 2012.

[23] Liu Duo, Dai Yi-Qi. A New Algorithm of Elliptic Curve Multi-Scalar Multiplication, *Chinese Journal of Computers*, Vol. 31, No. 7, pp. 1113-1137, 2008.

[24] Tan WenXue,Pan MeiSen,Wang XiPing,Shu XiaoHe; A method of security gradation against RSA IEA,*2010 1st ACIS International Symposium on Cryptography, and Network Security, Data Mining and Knowledge Discovery, E-Commerce and Its Applications, and Embedded Systems, CDEE 2010*, Vol. 1, pp. 170-174, 2010.

[25] Zhao Chunjiang, Wu H R, Gao R H. Realistic and Detail Rendering of Village Virtual Scene Based on Pixel Offset,*Applied Mathematics & Information Sciences*, Vol. 6, No. 3, pp.769-775, 2012.

[26] Yvo Desmed, Rosario Gennaroy Kaoru. A new and improved paradigm for hybrid encryption secure against chosen cipher text attack,*Journal of cryptology*, Vol. 23, No. 1,pp. 91-120, 2010.

[27] Gerald R Morris, Khalid H Abed; Mapping Floating-Point Kernels onto High Performance Reconfigurable Computers,*Journal of Computers*,Vol. 8, No. 4, pp. 1340-1344, 2013.

[28] Tan WenXue,Xi JinJu,Wang XiPing; A RSA key security gradating algorithm based on threshold attack time,*Journal of Software*, Vol. 6,No. 9, pp. 1873-1880, 2011.

[29] Huang Ru-Wei,Gui Xiao-Lin,Yu Si,Zhuang Wei;Privacy Preserving Computable Encryption Scheme of Cloud Computing,*Chinese Journal of Computers*,Vol. 34, No. 12, pp. 2391-2402, 2011.

[30] Tang-cenglin, Li-shirong. CI-Section or Maximal Completion of Maximal Subgrops and Solvable Fintte Groups, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 19, No. 3, pp. 1-4, 2007.

Tan, Wen Xue (1973-). He is a PhD candidate of College of Computer Science, Beijing University of Technology. He graduated with Master's of Science in Information technology and Earth Exploring from East China Institute of technology, Jiang-xi, Mainland of P. R. China,2003. In 2004, he joined Hunan university of Art and Science as a lecturer,being approved and authorized as computer software System Analyst by Chinese Ministry China in 2005, and being promoted to Associate professor and Senior Engineer in 2008. His

current research interests include Agriculture Information Technology and Artificial Intelligence,Cloud Information Security.

Zhao, Chun Jiang (1968-). He is a PhD candidate supervisor of College of Computer Science, Beijing University of Technology, and is a professor of China National Engineering Research Center for Information Technology in Agriculture. He received the Ph.D. degree in agronomy from China Agricultural University, Beijing, China, in 1991. He is currently a Senior Scientist and the Director of the National Engineering Research Center for Information Technology in Agriculture. He is also a Member of the Science and Technology Commission, Ministry of Agriculture, China. He received the Excellent Scientist Award by Ministry of Science and Technology of China in 2001. His research interests include precision farming, intelligent information technology in agriculture, and crop decision support system.

Wu, Hua Rui (1975-). He is a professor of China National Engineering Research Center for Information Technology in Agriculture. He received the Ph.D. degree in Computer Science and Technology from Beijing University of Technology,Beijing, China, in 2010. He is interested in studying Artificial Intelligence. In recent years, he has participated in 18 national and provincial key scientific research projects, and published over 20 academic papers. He got the first prize of Beijing Science and Technology in 2005, and third prize of agricultural technology promotion in 2003. His research interests include Intelligent Information Technology for agriculture.

Wang, Xi Ping (1980-). She is a Graduate of Changsha University of Science and Technology and an Instructor of Hunan University of Arts and Science. She graduated with Bachelors of Marketing from East China Institute of Technology, Jiangxi, China, 2004. Her current research interests include Electronic Commerce and Information Security, Logistic Engineering.

CWAAP: An Authorship Attribution Forensic Platform for Chinese Web Information

Jianbin Ma[1], Ying Li[2], Guifa Teng[1]
[1]College of Information Science and Technology, Agricultural University of Hebei, Baoding, China
[2]College of Economic and Trade, Agricultural University of Hebei, Baoding, China
Email: majianbin@hebau.edu.cn, sxliying@hebau.edu.cn, tguifa@hebau.edu.cn

***Abstract*— Illegal web information is common on the Internet. To prevent phenomena of illegal web information from happening, providing effective evidence for court to punish the criminals by means of law is one effective method. In this paper, an authorship attribution platform for Chinese web information, CWAAP, is described. Based on the language characteristics of Chinese web information, lexical features and structural features which can express the author's writing habit are extracted. Support vector machines (SVM) are used for learning author's writing features. To test the effectiveness of CWAAP, literature, Blog and BBS datasets are used in the experiments on the platform. Five experiments are performed. Experimental results show that lexical features and structural features are effective. The number of words in training samples should exceed 200 at least. By Information Gain feature selection methods, 800 lexical features can express the authors' writing style. There is a small difference between the authors' topics. All the parts of speech reserved are perfect. These results confirm that the platform is effective and feasible for cybercrime forensic.**

***Index Terms*—CWAAP, Authorship attribution, Forensic, Support Vector Machine, Chinese, Web information**

I. INTRODUCTION

Various Internet service such as E-mail, BBS, Blog, Microblog has been widely applied to people's daily life. While Internet provides convenient to people, a lot of problems appear at the same time. Some illegal web information, such as antisocial information, fraud information, pornographic information, terroristic threatening information, gambling information, appears by means of E-mail, BBS or Blogs. The Internet provides criminals new criminous space and means. Illegal web information affects social stabilization and national security seriously. Some measures should be taken urgently. Now, installing filtering software to filter the information containing sensitive words is the main method to prevent these phenomena. However, this passive defensive method cannot stop these phenomena, because criminals can make use of some substitute words to break through the defense of the filtering software. Punishing the criminals by means of law can strike these crimes effectively. Many states have made interrelated laws. However, due to lacking effective evidence, many cases cannot be brought to the court. If web information's authorship is attributed by technical means, criminal's evidence for computer forensic can be collected. This will provide an important application value and practical significance to law enforcement, social safety and stabilization, Internet environments' purification.

Footprint, handwriting, signalment have been used to obtain evidence for courts. But the evidence of criminals via Internet is difficult to collect, because Internet is a free and open place and the messages on the Internet are spread anonymously. Criminals being hidden in any online corner can commit a crime. Though Internet services such as e-mail or BBS require users to fill out their personal information when registering, criminals always forge their real information or log on anonymously. So registering information, IP address, and e-mail's header information cannot provide convincing evidence for the court. However the text's content and structure can be obtained from web information, the same as their handwriting. Authors of web information have their inherent writing habits. The writing habits cannot be changed easily (although the criminals will always try), which embody a writing style such as usage of certain words, the length of sentences and paragraphs, and the format of the text.

Stylometry is the application of the study of linguistic style, usually to written languages. Stylometry is the theoretical basis of authorship attribution which attributes authorship of unidentified writing on the basis of stylistic similarities between the authors' known works and the unidentified piece. Researchers have focused on academic and literary applications ranging from the questions of the authorship of Shakespeare's works to forensic linguistics. The research language of authorship attribution has been mainly English, Arabic, and Japanese etc. However, there were little related authorship attribution researches on the Chinese language. The language characteristics of the Chinese language are very different from other languages such as English and Indo-European languages, where the feature extraction methods for authorship attribution are different. In this

Manuscript received September 1, 2012; revised June 5, 2013; accepted June 20, 2013.
Corresponding author: Guifa Teng

doi:10.4304/jsw.9.1.11-19

paper, an authorship attribution platform for Chinese web information, CWAAP, was introduced and described. Based on the language characteristics of Chinese web information, various authors' writing features including lexical features and structural features which could express the authors' writing habits were extracted. Support vector machines (SVM) were used for learning the writing features.

The remainder of the paper is organized as follows. Section 2 presents a general review of stylometry and previous related work. Section 3 describes the framework of CWAAP. Section 4 is our feature selection and extraction methods. Section 5 provides our experimental methodology and analyses the experimental results. Section 6 draws the conclusions of the paper.

II. Related Work

A. Stylometry and Authorship Attribution

Stylometry is the study of the unique linguistic styles and writing behaviors of individuals in order to determine the authorship. It is an interdisciplinary study of statistics and computer science etc. The research of stylometry is based on the premise of two assumptions. The first assumption is that all authors have distinctive writing habits, which can be captured from a number of quantitative features such as certain vocabulary usage, sentence complexity, and phraseology. The second assumption is that these habits are unconscious. Even if some authors make a conscious effort to disguise one's writing habits, the effect is not obvious. Stylometry focuses on defining authors' subconscious writing features and determining statistical methods to measure these features so that the similarity between two or more pieces of text can be analyzed.

Stylometry is the basis of authorship analysis. Authorship analysis can be divided into three distinct problems, namely, authorship attribution, authorship characterization, and plagiarism detection. The aim of authorship attribution is to determine the author of a piece of text by comparing the similarity of writing style between the author's known works and unknown ones. Authorship characterization attempts to formulate author's sociolinguistic profile by making inferences about gender, educational, and cultural background on the basis of writing style. The purpose of plagiarism detection is to calculate the similarity of two or more pieces of text and to determine if a piece of text has been plagiarized.

The following are several typical authorship attribution studies. "The Federalist Papers" are a series of 85 articles or essays serially in The Independent Journal and The New York Packet between October 1787 and August 1788 with the aim of advocating the ratification of the United States Constitution. 12 articles have disputed authorship between Hamilton and Madison. Pioneered authorship attribution methods were famously used by Mosteller and Wallace in the early 1960s to attempt to answer this question. Frequencies of a set of function words selected from articles were compared. Mosteller and Wallace(1964)[1] came to the conclusion that the 12 disputed articles were written by Madison. Another well-known study is the attribution of disputed Shakespeare works. Elliot (1991)[2] compared the writing style of Shakespeare's work "Earl of Oxford". The writing style included unusual diction, frequency of certain words, choice of rhymes, and habits of hyphenation. "And Quite flows the Don" was written by Sholokhov between 1928 and 1940. Sholokhov was accused of plagiarizing from Kryukov. Kjetsaa(1979)[3] draw the conclusion that Sholokhov was the true author of "And Quiet Flows the Don" by comparing the statistical features of Sholokhov and Kryukov. The features included the length of sentences, part of the speech, sentence structure etc. "Dream of the red chamber" is a masterpiece of Chinese literature and is generally acknowledged to be the pinnacle of classical Chinese novels. For a long time, the first 80 chapters written by Cao Xueqin and the 40 additional chapters written by Gao E were recognized universally. Professor Chen Bingzao at university of Wisconsin researched on the authorship of "Dream of the red chamber" for the first time. Computers were used to calculate and analyze the frequency of words occurring in the masterpiece. He came to the conclusion that all the 120 chapters were written by Cao Xueqin.

B. Authorship Attribution Features

The frequency of certain word-usage, the length of sentences etc can be used to attribute authorship. The former researchers have focused on what the features could represent the writing style of authors. However, no fixed features set were agreed on. The following is several types of features.

(1) Word-length and Sentence-length

The origins of stylometry might be traced back to the work of Mendenhall (1887)[4] on word-lengths. Morton (1968)[5] used sentence-lengths for tests of authorship of Greek prose.

(2) Function Words

Word-usage was usually used for discrimination in authorship of texts. In the same author's work, some words vary considerably in their rate of use, while other words show remarkable stability. Function words were used to attribute the author of "The Federalist Papers" by Mosteller and Wallace (1964)[1]. Morton (1978)[6] developed techniques of studying the position and immediate context of individual word-occurrences. However the method had come under much criticism and Smith (1985)[7] had demonstrated that it could not reliably distinguish between the works of Elizabethan and Jacobean playwrights. Burrows (1987)[8] proposed the common high-frequency words (at least 50 strong). Holmes and Forsyth (1995)[9] had successfully applied the technique to the classic "The Federalist Papers" problem.

(3) Vocabulary Distributions

One of the fundamental notions in authorship attribution is the measurement of richness of an author's vocabulary. The frequency of word-usage can be estimated by analyzing a text produced by a writer. Mathematical models for the frequency distributions of

the number of vocabulary items appearing exactly r times (r=1,2,3....) have aroused the interest of statisticians ever since the work of Zipf (1932)[10]. The best fitting model attributed to Sichel (1975)[11], and the Sichel model in addition to the once-occurring words (hapax legomena) and twice-occurring words (hapax dislegomena) were useful stylometric tools.

C. Authorship Attribution Methods

Some technical means have been used to analyze the writing features to arrive at the purpose of attributing a text's authorship. Mathematical methods and intelligent algorithms were adopted. The techniques vary with different periods. The following is summary of three common authorship analysis approaches.

(1) Probabilistic and Statistical Approaches

Efron and Thisted (1976)[12] considered how many words Shakespeare knew. Probabilistic techniques were used to study the number of words used once, twice in the Shakespeare canon. A parametric empirical Bayes model and a nonparametric model were examined. The models supposed that Shakespeare knew at least 3,5000 more words, which could be regarded as evidences of Shakespeare's authorship. Smith (1983)[13] selected the average word-length, the average sentence-length, collocations, and measures of words in certain positions in sentences as features. Chi squared statistic methods were used to detect differences between Shakespeare and Marlowe. Farringdon (1996)[14] used the Cusum technique to test authorship of a small number of text samples.

(2) Computational Approaches

With the development of computer technology, sensitive classification techniques rather than simple count statistics have been applied to authorship attribution. Burrows (1992)[15] analyzed the frequency of words. The Pearson product-moment method correlated each word with all others. Principal component analysis methods were used to transform the original variables to a set of new uncorrelated variables. Holmes (2001)[16] described how traditional and non-traditional methods were used to identify seventeen previously unknown articles that were believed to be written by Stephen Crane. 3000 word samples of text were analyzed for frequencies of 50 common words. Principal component analysis was used as the method of discrimination.

(3) Machine Learning Approaches

Machine learning is a scientific discipline concerned with the design and development of algorithms that allow computers to evolve behaviors based on empirical data. In recent years, machine learning approaches have been applied to stylometry. Neural network classifiers were employed for stylometry by Merriam and Matthews (1994)[17]. Kjell (1994)[18] used neural networks and Bayesian as classifiers. Hoorn et al. (1999)[19] used neural network with letter sequences as the feature set for authorship analysis of three Dutch poets. Holmes (1998)[20] compared the effects of vocabulary richness, and word frequency analysis with a genetic rule based learner on the problem of attributing "The Federalist papers".

D. Web Information Authorship Attribution for Forensic Investigation

Authorship analysis has been widely used in resolving authorship attribution of literary and conventional writing. With increasing cybercrime arising in Internet, web information authorship attribution began to draw researchers' attention.

E-mail is a special type of web information. With rapid growth of e-mail misuse phenomena, E-mail authorship analysis has been researched for forensic investigation. De Vel (2000, 2001)[21-23] applied the support vector machine classification model over a set of linguistic and structural features for e-mail authorship attribution for the forensic purpose. Tsuboi (2002)[24] studied authorship attribution of e-mail messages and World Wide Web documents written in Japanese. The sequential word patterns or word n-grams with n=2 and 3 from each sentence in the documents was used as features set. Zheng (2003, 2006)[25-26] analyzed the authorship of web-forum, using a comprehensive set of lexical, syntactical, structural features, and content-specific features. Abbasi (2005, 2006, 2008)[27-29] analyzed the authorship identification and similarity detection of web information. Iqbal (2008)[30] mined write-prints called frequent patterns for authorship attribution in e-mail forensic.

The above researches are for English, Japanese, and Arabic documents' authorship analysis. However, techniques of authorship analysis used for feature extraction are dependent on languages, and in fact differ dramatically from one language to another. For example, Chinese does not have word boundaries explicitly in texts. In fact, word segmentation itself is a difficult problem in the Chinese-like languages. So feature extraction methods for Chinese documents are different from other languages such as English and other Indo-European languages.

III. THE FRAMEWORK OF CWAAP

Figure 1 presents the framework of CWAAP (Chinese web information authorship attribution platform). According to the process of Chinese web information authorship attribution, there are six steps, namely information collection, information pre-processing, Chinese word segmentation, feature selection and extraction, authorship training, and authorship attribution.

The precondition of authorship attribution is that the web information of suspected authors can be obtained. We assume that there is enough web information of suspected authors. By analyzing the known author's web information, the author's writing style is gained. Then the author of unidentified information can be attributed. So the first step of authorship attribution is to collect web information of suspected authors as much as possible.

There are many categories of web information, such as e-mail, BBS, and Blog. The object of authorship attribution is the text of web information. Disorderly information such as photos, sound, and advertising

information should be removed. So it is necessary to pre-process the web information and leave the useful texts of web information to be analyzed.

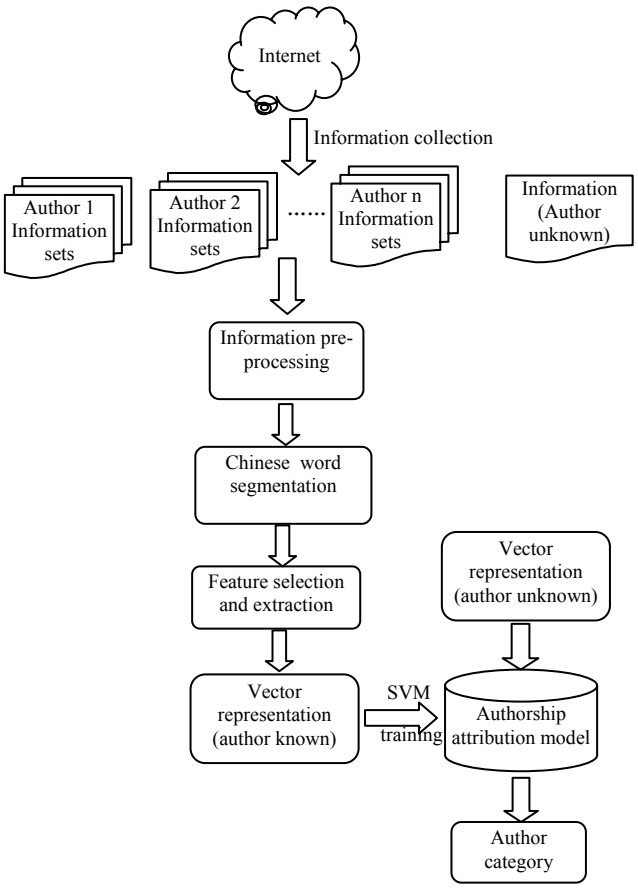


Figure 1. The framework of CWAAP

Different from the English language, Chinese does not have clear natural word segmentation markers. The lexical features are main writing features to extract. The precision of word segmentation relates to the effect of feature extraction. Now a lot of Chinese word segmentation software packages are available for use. However, the latest appearing words such as newbie are difficult to segment correctly. In CWAAP, word segmentation software named segtag developed by Professor Xiaodong Shi at Xiamen University was used for word segmentation and part of speech tagging. An additional dictionary was used to supply the new appearing words. In the case of incorrect word segmentation, the platform provides adjustment functions manually.

What features set can represent web information authors' writing style is the next step. In the feature extraction step, the extensive stylometric features including lexical features, structural features were extracted. The writing features were represented by the vector space model (VSM). Thus one web information document was denoted as a dot in the high dimensional space.

Machine learning techniques including decision trees, neural networks, and support vector machines(SVM) are the most common analytical approaches used for authorship attribution in recent years. The distinctive advantage of the SVM is its ability to process many high-dimensional applications such as text classification and authorship attribution. Zheng (2006)[25] and Abbasi (2005)[27] have drawn the conclusion that SVM significantly outperform neural networks and decision trees in authorship analysis. In our study, support vector machines were used for learning the authors' writing features, and authorship attribution model was gained.

The unknown authorship of web information could be attributed automatically by the authorship attribution model that was trained in authorship training step.

IV. Feature Selection and Extraction

A. The Characteristics of Chinese Web Information

As the particular pictograph in the world, Chinese language is highly uniform and canonical. Compared with English and other European languages, Chinese has the following characteristics.

(1) Form: blank spaces are regarded as the delimiters of words in English texts. Chinese texts don't have natural delimiter between words.

(2) Syntax: the components of the sentence depend on word order and empty word. Maybe the same of word order has different meanings.

(3) Glossary: In English language, words are composed of 26 letters. Sentences consist of several words. In Chinese language, there are above 90,000 Chinese characters totally. Just the commonly used Chinese characters amount to above 7,000. There are many more words than the characters, because words are composed of several characters.

With the popularization of Internet, cyber-language begins to spread, which has struck the criterion of the traditional languages. Cyber-language is free in use and not restricted with grammar. The style of cyber-language has the following characteristics.

(1) The words are typed into the computer's screen by keyboard. So to save typing time, users do not obey the rules of the usual writing. Elliptical sentences and incomplete sentences are common in web information. Furthermore, the writing is free in the Internet. A lot of blank line and blank spaces are inputted at will. The sentences are brief. Sentences usually consisting of two or three words are common.

(2) Writing in the Internet doesn't obey the rules of punctuation. Interrogation marks, exclamatory marks, and suspension points are used frequently. Authors input a succession of exclamatory mark when they approve others viewpoint and input several suspension points when they do not understand others viewpoint.

(3) New words appear in the Internet frequently. They are spread by egregious speed. For example, the word geili has been popular in Internet and everyday communication since 2010.

Authors writing in the Internet have formed fixed writing styles. Grasping web information authors' writing style is easier than literary writing. Based on analyzing the characteristics of Chinese web information, the

author's writing features were divided into two types, namely, lexical features and structural features.

B. Lexical Features Extraction and Selection Methods

The frequency of certain words reflects author's preference or habit for usage of some specific words. In our study, the frequency of certain words was expressed as lexical features.

Lexical features could be extracted by tf-idf techniques which had been used in the research of text classification. The weight of lexical features was calculated as formula 1.

$$W(t,\vec{d}) = tf(t,\vec{d}) \times \log(N / n_t + 0.01) \quad (1)$$

where $W(t,\vec{d})$ is the weight of term t in document d, $tf(t,\vec{d})$ is the frequency of term t in document d, N is the total number of documents, n_t is the number of documents that contain term t.

If all the words were treated as lexical features, the number of features can reach thousands of the dimensions. But some features are useless, which can waste storage space and result in system degradation. In our study, information gain (IG) feature selection method was adopted to select effective features. The information gain of lexical features was calculated as formula 2.

$$Gain(w) = -\sum_{i=1}^{m} p(c_i) \log P(C_i) + p(w) \sum_{i=1}^{m} p(c_i / w) \log P(c_i / w) + P(\overline{w}) \sum_{i=1}^{m} p(c_i / \overline{w}) \log p(c_i / \overline{w}) \quad (2)$$

where w denotes a certain feature. m is the number of classes. c_i denotes one certain class. $\overline{w}$ denotes that the feature w doesn't appear. $P(w)$ denotes the probability that the feature w appears. $P(\overline{w})$ denotes the probability that the feature w doesn't appear. $P(c_i \mid w)$ denotes the probability that the document belongs to class c_i on condition that the document contains feature w. $P(c_i \mid \overline{w})$ denotes the probability that the document belongs to class c_i on condition that the document does not contain feature w.

C. Structural Features Extraction Methods

In web texts, authors always ignore some punctuations or use incorrect punctuations. The authors can write freely on the premise of expressing the author's meaning. So the structure of web texts is loose. Furthermore, the authors have a preference for part of speech usage which can reflect the authors' degree of education. So we extracted three aspects of structural features, namely, punctuations features, structural characteristics, and part of speech features. Table Ⅰ shows the structural features.

The web text should be inputted by keyboard. At the same time, authors always ignore the difference of Chinese and English punctuation, which can treated as writing habits to extract. Table Ⅱ is the punctuation features. The weight of punctuation features is the ratio of the number of a particular punctuation in the document to the total number of punctuations in document.

The rate of parts of speech can reflect the preference for word class usage. For example, some authors always use exclamation, however some authors hardly ever. The usage of parts of speech can reflect the authors' degree of education. Chinese has 12 categories parts of speech in common use which are listed in table Ⅲ. The weight of parts of speech is the ratio of number of the parts of speech in the document to total number of parts of speech in the document.

TABLE I.
STRUCTURAL FEATURES

Features
Number of distinct punctuations/total number of punctuations
Number of distinct words/total number of words
Mean sentence length
Mean paragraph length
Number of digital characters/total number of words
Number of lowercase letters/total number of words
Number of uppercase letters/total number of words
Number of space/total number of words
Number of blank lines/total number of lines
Number of indents/total number of words

TABLE Ⅱ.
THE PUNCTUATION FEATURES

Chinese Punctuations			English Punctuations		
——	…	。	,	.	,
、	；	：	?	:	?
!	“	”	〔	(	)
〕	《	》	•	“	!
.	‘	’	–	;	‘

TABLE Ⅲ.
THE PUNCTUATION FEATURES

Number	Features	Number	Features
1	noun	7	adverb
2	verb	8	preposition
3	adjective	9	conjunction
4	numeral	10	auxiliary
5	quantity	11	exclamation
6	pronoun	12	onomatopoeia

V. EXPERIMENTS ON CWAAP

Figure 2. The main interface of CWAAP

CWAAP was developed in Visual c++ development environment. The operating system was Windows XP. Other software tools including segtag(Chinese word segmentation software package), libsvm-2.9(support vector machine software package) were used. The system was composed of four modules, which were web information's content extraction, web information's features extraction, web information's authorship training, and web information's authorship attribution. Figure 2 shows the main interface of CWAAP.

A. Datasets and Experimental Methods

To test the effectiveness of CWAAP, three datasets including literature, BBS, and Blog were collected, and several experiments were made. The detail information of the three datasets was showed in table Ⅳ.

TABLE IV.
THE INFORMATION OF THREE DATASETS

Dataset	Number of authors	Average number of documents	Document size(words)	
			Min	Max
literature	9	51	12	21334
blog	7	198	11	4046
BBS	6	72	3	489

The literature dataset was collected from one online books library. The blog dataset came from the website http://blog.sina.com.cn/. We gained the BBS dataset from one web forum. Every dataset's author was different from others.

A linear kernel function was used as the kernel function of support vector machine. Since there were only a small amount of data to produce a model of authorship attribution, the experiments results were measured by k-fold cross-validation to provide a more meaningful results. Accuracy was used to evaluate the experimental results. Five experiments were performed. The first experiment is to test the validity of two types of features. The second experiment is to test the effect of document size on experimental results. The third experiment is to test the effect of number of lexical features on experimental results. The effect of author's topics was tested in the fourth experiment. Different parts of speech were tested in the fifth experiment.

B. Experimental Results and Discussions

(1) The first experiment

To test whether the two types of features extracted in our study are effective, the first experiment was made. Different features and features combination on different dataset were tested. 1000 lexical features were selected by the IG features selection method in formula 2. 5-fold cross-validation was used to validate the experimental results. The experimental results are showed in table V.

From table V., we can see that accuracy of lexical features on literature, BBS and Blog dataset were 77.02%, 56.26% and 80.51% respectively. Accuracy of structural features was 94.97%, 62.86% and 84.35% respectively. Accuracy of combination of lexical and structural features was 95.62%, 70.99% and 89.06% respectively. Accuracy of structural features on all dataset was higher than lexical features, which proves that structural features were one effective feature. Accuracy of combination of lexical and structural features was higher than structural features, which shows that the combination of lexical and structural features was more effective than lexical features or structural features singly. The accuracy exceeded 80% by experimenting on Blog datasets. The accuracy of BBS dataset was low, which might be caused by too few words in BBS document.

TABLE V..
EXPERIMENTAL RESULTS OF DIFFERENT FEATURE COMBINATION ON DIFFERENT DATASET

Dataset	Feature type	Accuracy(%)
literature	T_L	77.02
	T_S	94.97
	T_{L+S}	95.62
BBS	T_L	56.26
	T_S	62.86
	T_{L+S}	70.99
Blog	T_L	80.51
	T_S	84.35
	T_{L+S}	89.06

T_L：lexical feature T_S：structural feature
T_{L+S}：lexical+ structural feature

(2) The second experiment

The former study on authorship attribution needs 1000 words in one sample at least, which can express author's writing style better. However, the number of words in web information is small. Two or three words in BBS or E-mail texts are common. How many words in one document can be used to attribute authorship reliably? We made experiments on the literature dataset. Three authors' samples were experimented. Every author had 30 samples. The number of words in samples was 50, 100, 200, 500, and 1000. 5-fold cross-validation was used to validate the experimental results. The experimental results that were measured as table VI.

TABLE VI
THE EXPERIMENT RESULTS OF DIFFERENT NUMBER OF WORDS

Number of words	Accuracy(%)
50	85.78
100	88.89
200	95.58
500	97.53
1000	98.82

From table VI, we could see that the accuracy increased with the increase of words in samples. That was because the more words in samples, the writing style could be expressed better. The experimental results showed that the accuracy did not have distinct change when the number of words exceeded 200. Conclusion could be draw that words in samples reached 200 could be used to attribute web information's authorship.

(3) The third experiment

To test IG feature selection method, the number of lexical features from 100 to 2000 was tested on Blog dataset. 5-fold cross-validation was used to validate the experimental results. Table VII and figure 3 were the experimental results.

TABLE VII.
THE EXPERIMENTAL RESULTS OF DIFFERENT NUMBER OF LEXICAL FEATURES

Features	100	200	300	400	500	600	700	800	900	1000
Accuracy	60.14	71.16	76.38	76.09	79.49	78.7	80.36	79.57	80.65	80.51
Features	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000
Accuracy	80.36	80.50	79.71	82.03	82.10	81.09	82.75	80.94	81.88	82.75

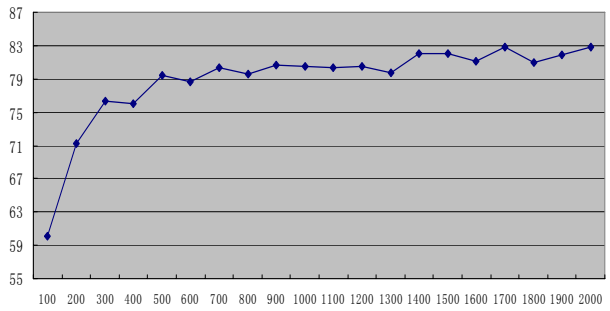


Figure 3. The experimental results of different number of lexical features

The table Ⅶ and figure 3 show that the overall trend of results was ascending in the rough, though waves occurred in the course. The accuracy of 100 lexical features was low, which proved that 100 lexical features could not express authors' lexical writing style adequately. There was not distinct change in experimental results when the number of lexical features reached 800. Too few lexical features could not express the author's writing style adequately. Too many lexical features might result in storage space wasting and system performance degradation, and improve little on the results.

(4) The fourth experiment

If authors' writing topic is same, their lexical usage is similar. Whether their writings are not easy to differentiate is concerned about. The experimental results of lexical features in Blog dataset comparing four authors remarking on the entertainment topic with two authors remarking on the entertainment topic and two authors remarking on the sports topic were given. The results were validated by 5-fold cross-validation. 1000 lexical features selected by IG methods were extracted. The experimental results were showed in table VIII.

TABLE VIII
THE EXPERIMENTAL RESULTS OF DIFFERENT AUTHOR'S TOPIC

Authors' topic	Accuracy(%)
two authors(entertainment topic) two authors(sports topic)	86.38
four authors(entertainment topic)	84.19

Table VIII showed that there were a small difference between the same authors' topic and different authors' topic. That was because that authors' topic was embodied in noun or verb. Some other parts of speech could express authors' writing style well.

(5) The fifth experiment

For text classification, the useless empty words are removed. The substantives such as nouns, verbs, and adjectives are accepted. However, conjunctions, prepositions, and adverbs are useful for attributing authorship. The fifth experiment was concerned about whether all the parts of speech should be reserved to attribute authorship. 1000 features of the Blog dataset selected by the IG method were extracted as features. The results were validated by 5-fold cross- validation. Table Ⅸ showed the experimental results of different parts of speech.

TABLE IX
THE EXPERIMENTAL RESULTS OF DIFFERENT PARTS OF SPEECH

Part of speech	Accuracy(%)	Part of speech	Accuracy(%)
noun	67.25	preposition	40.58
verb	65.72	quantity	40.00
adverb	60.07	auxiliary	35.29
conjunction	53.70	modal particle	27.10
adjective	48.33	n+ v + adv + c + adj + p	76.81
pronoun	55.72	rest	64.64

n+ v + adv + c + adj + p: noun, verb, adverb, conjunction, adjective and pronoun reserved
rest: the rest part of speech reserved except noun, verb, adverb, conjunction, adjective and pronoun

From tableIX, we could see that nouns, verbs, adverbs, conjunctions, adjectives and pronouns tested solely were better. The accuracy of preposition, quantity, auxiliary, modal particle was lower. However, the accuracy that every part of speech tested solely did not exceed the accuracy that all part of speeches reserved. Except for the above six types of part of speech, the accuracy of the rest part of speech was 64.64%, which showed that the rest part of speech had discrimination ability. The fifth experiment showed that the results of all the part of speech reserved were perfect. Some empty words had discrimination ability for attributing authorship, which should be reserved, differing from text classification.

VI. CONCLUSIONS

The crimes utilizing Internet increase rapidly. For the purpose of providing evidences for the court, CWAAP, an authorship attributing platform for Chinese web information was developed. In this paper, the framework of the system was provided. Two types of features including lexical features and structural features were extracted. To test the effect of CWAAP, three datasets were collected. Five experiments were designed and performed. Experimental results proved that the two features extraction methods were effective. The number of words in samples used for authorship attribution exceeded 200 at least. By IG feature selection methods, 800 lexical features could express the authors' writing style. There was a small difference between the authors' topics. All the parts of speech reserved were perfect. The accuracy exceeded 80% by experimenting on the Blog datasets. The experimental results suggest that the platform is effective and feasible to apply for cybercrime forensic.

REFENRENCES

[1] F. Mosteller and D.L.Wallace, *Inference and Disputed Authorship:The Federalist*, In:behavioral science: quantitative methods edition, Massachusetts:Addison-Wesley, 1964.

[2] W. Elliot and R. Valenza, "Was the Earl of Oxford the true Shakespeare?," *Notes and Queries*,vol.38,pp. 501-506, 1991.

[3] G. Kjetsaa, "And Quiet Flows the Don Through the Computer," *Association for Literary and Linguistic Computing Bulletin*,vol.7, pp.248-256, 1979.

[4] T.C.Mendenhall, "The Characteristic Curves of Composition, "*Science*, vol.IX, pp.237-249, 1887.

[5] A. Q. Morton, "The Authorship of Greek Prose," *Journal of the Royal Statistical Society (A)*, vol.128, pp.169-233, 1968.

[6] A. Q. Morton, *Literary Detection*, Scribners New York, 1978.

[7] M. W. A. Smith, "An Investigation of Morton's Method to Distinguish Elizabethan Playwrights," *Computers and the Humanities*,vol.19, pp.3-21, 1985.

[8] J. F. Burrows, "Word Patterns and Story Shapes: The Statistical Analysis of Narrative Style," *Literary and Linguistic Computing*,vol.2, no.4, pp.61-70, 1987.

[9] D. I. Holmes and R. S. Forsyth, "The 'Federalist' Revisited: New Directions in Authorship Attribution," *Literary and Linguistic Computing*,vol.10,pp.111-127,1995.

[10] G. K. Zipf, *Selected Studies of the Principle of Relative Frequency in Language*, Harvard University Press, 1932.

[11] H. S. Sichel, "On a Distribution Law for Word Frequencies," *Journal of the American Statistical Association*,vol.70, pp. 542-547,1975.

[12] R. Efron and B. Thisted, "Estimating the number of unseen species: How many words did Shakespeare know?, "*Biometrika*, vol.63, no.3, pp. 435–447,1976.

[13] M.W.A.Smith, "Recent experience and new developments of methods for the determination of authorship," *ALLC Bulletin*,vol.11, pp.73-82, 1983.

[14] J. M. Farringdon, A. Q. Morton and M. G. Farringdon, *Analysing for Authorship: A Guide to the Cusum Technique*, Cardiff, University of Wales Press,1996.

[15] J. F. Burrows," Computers and the study of literature," *In C. Butler, editor, Computers and Written Text, Applied Language Studies*, Blackwell, Oxford, pp.167–204, 1992.

[16] D. I. Holmes, M. Robertson and R. Paez, "Stephen Crane and the New-York Tribune: A case study in traditional and non-traditional authorship attribution," *Computers and the Humanities*, vol.35, no.3, pp.315-331, 2001.

[17] T. Merriam and R. Matthews, "Neural compuation in stylometry II: An application to the works of Shakespeare and Marlowe," *Literary and Linguistic Computing*,vol.9, pp.1-6, 1994.

[18] B. Kjell, "Authorship attribution of text samples using neural networks and Bayesian classifiers," *In IEEE International Conference on Systems, Man and Cybernetics,* San Antonio, USA; 1994.

[19] J. F. Hoorn, S. L. Frank, W. Kowalczyk, and F. Van Der Ham, "Neural network identification of poets using letter sequences," *Literary and Linguistic Computing*, vol.14, no.3, pp.311-338,1999.

[20] D. I. Holmes, "The evolution of stylometry in humanities scholarship," *Literary and Linguistic Computing*,vol.13,no.3,pp.111-117, 1998.

[21] O. De. Vel, "Mining e-mail authorship," *Proceedings of workshop on text mining. In: ACM international conference on knowledge discovery and data mining (KDD)*, Boston, MA, USA, 2000.

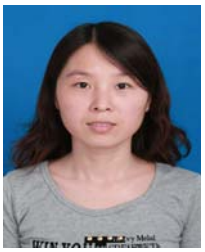
[22] O. De. Vel, A. Anderson, M. Corney and G. Mohay, "Mining e-mail content for author identification forensics," *SIGMOD Record*, vol.30, no.4, pp.55–64, 2001.

[23] O. De. Vel, A. Anderson, M. Corney and G. Mohay, "Multi-topic e-mail authorship attribution forensics," *Proceedings of ACM conference on computer security –*

Workshop on data mining for security applications; Philadelphia, PA, 2001.
[24] Y. Tsuboi, *Authorship Identification for Heterogeneous Documents*, Japanese: Nara Institute of Science and Technology, University of Information Science, 2002.
[25] R. Zheng, J. Li, H. Chen and Z. Huang, "A framework for authorshipidentification of online messages: writing-style features and classification techniques, "*Journal of the American Society for Information Science and Technology.* vol.57, no.3, pp. 378–393, 2006.
[26] R. Zheng, Y. Qin, Z. Huang and H. Chen, "Authorship analysis in cybercrime investigation," *Proceedings of the first international symposium on intelligence and security informatics (ISI),* Seattle Washington, USA , 2003.
[27] A. Abbasi and H. Chen, "Applying Authorship Analysis to Extremist- Group Web Forum Messages," *IEEE Intelligence System,* vol.20, no.5, pp.67-75, 2005.
[28] A. Abbasi and H. Chen, "Visualizing authorship for identification," *Proceeding of IEEE International Conference on Intelligence and Security Informatics*, San Diego, USA, 2006.
[29] A. Abbasi and H. Chen, "Writeprints: a stylometric approach to identitylevel identification and similarity detection in cyberspace," *ACM Transactions on Information Systems,*vol.26,no.2, pp.1-29, 2008.
[30] F. Iqbal, R. Hadjidj, B. C. M. Fung and M. Debbabi, "A novel approach of mining write-prints for authorship attribution in e-mail forensics," *Digital Investigation*, vol.5, supplement, pp.S42-S51, 2008.
[31] M. Asif and N. Tripathi, "Evaluation of OpenID-Based Double-Factor Authentication for Preventing Session Hijacking in Web Applications," *Journal of Computers*, vol.7,no.11, pp.2623-2628, November 2012.
[32] A. Ezzouhairi, A. Quintero, S. Pierre, "Adaptive Decision Making Strategy for Handoff triggering and Network Selection," *Journal of Computers*, vol.6,no.11,pp.2255-2266,November 2011.
[33] Z. Liu, Z. K. Yang and S. Y. Liu, "A Novel Random Subspace Method for Online Writeprint Identification," *Journal of Computers*, vol.7,no.12,pp.2997-3004, December 2012.
[34] X. Q. Yu, "Internal P-set and Security Transmission-identification of Information," *Journal of Computers*, vol.6,no.10, pp.2249-2254, October 2011.

Jianbin Ma received his MSc and PhD degree from agricultural university of Hebei in 2004 and 2010 respectively. Since 2004, he is a lecturer at college of information science and technology, agricultural university of Hebei. His research interests include Software Engineering, Computing, Information Retrieval and Management, Artificial Intelligence.

Ying Li received her MSc degree from agricultural university of Hebei in 2006. Since 2001 to 2008, she is a lecturer at college of science, agricultural university of Hebei. Now, she is teaching and researching in college of economics and trade. Her research interests include Artificial Intelligence, Intelligent Algorithm, Agricultural Economics and Asset Appraisal.



Guifa Teng received his phD degree from peking university in 2005. Since 2001, he is a professor at college of information science and technology, agricultural university of hebei. His research interests include Machine Learning, Software Engineering, Computer Applications.

An Improved Intelligent Ant Colony Algorithm for the Reliability Optimization Problem in Cyber-Physical Systems

Shiliang Luo
School of Automation, Guangdong University of Technology, Guangzhou, China
School of Mathematics & Computer Science, GanNan Normal University, Ganzhou, China
Email: luoshiliang88@163.com

Lianglun Cheng, Bin Ren and Quanmin Zhu
School of Computers, Guangdong University of Technology, Guangzhou, China
School of Electronic Engineering, Dongguan University of Technology, Dongguan, China
Intelligent Autonomous Systems Lab, University of the West of England, Bristol, UK
Email: llcheng@gdut.edu.cn

***Abstract*—In this paper the torsion bar optimization problem of reliability is considered. Since this problem is a difficult optimization problem, an improved intelligent ant colony algorithm is proposed to solve the problem. This algorithm comprises five stages. First stage is the initialization of pheromone and the sensor node configuration. The second stage is to select the next sensor node. The third stage is to update the pheromone of the sensor node path. The fourth stage is to acquire the best path by computing the shortest distance. The last stage is to output the global optimal solution. To evaluate performance of the proposed algorithm, it is compared with the ant colony optimization algorithm and the genetic algorithm. The experimental results show that the proposed algorithm performs better than them.**

***Index Terms*—Intelligence algorithm, CPS, Optimization, Reliability, Manufacturing**

I. INTRODUCTION

Global competition and rapidly changing customer requirements are demanding increasing changes in manufacturing environments.

Enterprises are required to constantly redesign their products and continuously reconfigure their manufacturing systems [1-3]. Traditional approaches to manufacturing systems do not fully satisfy this new situation. Many authors have proposed that artificial intelligence will bring the flexibility and efficiency needed by manufacturing systems.

The growing complexity of industrial manufacturing and the need for higher efficiency, greater flexibility, better product quality and lower cost have changed the face of manufacturing practice [4-7]. In addition to the technical issues, modern manufacturing technology is interdisciplinary in nature and allows the application of different knowledge from other scientific fields such as manufacturing, computer science, management, marketing and control systems [8]. Manufacturing has also shifted from mass production, to a more controlled one. We have to make sure that we can do it effectively if we want to make any profit [9].

Genetic algorithms [10, 11] use ideas from population genetics for solving complex global optimization problems. Bos applies a procedure based on the combination of a genetic and a gradient guided optimization algorithm for the design of a second generation supersonic transport aircraft [12, 13]. Karafyllidis has developed a method for designing a dedicated processor, which executes a cellular automaton algorithm that simulates the photolithography process [14]. The genetic algorithm is used to find a cellular automaton with discrete state space[15], having the smallest possible lattice size and the smallest possible number of discrete states [16], the results of which are as close as possible to the results of the cellular automaton with continuous state space. However a pool of potential candidate solutions evolve through reproduction [17] and mutation of the fittest and elimination of the least promising solutions of each generation are made extinct.

Since the last decade, attempts are being made to solve combinatorial optimization problems using an intelligent ant colony algorithm [18]. Hu and al. proposed an intelligent ant colony algorithm to solve flow shop rescheduling problem. However the intelligent ant colony algorithm is easy to fall into convergence of local optimum [19].

Purpose of this work is to present a new improved intelligent ant colony algorithm to solve the torsion bar optimization problem of reliability in intelligent manufacturing. The aim is to optimize a common objective function which takes into account both reliability and production criteria. The reminder of this

Manuscript received September 15, 2012; revised June 5, 2013; accepted June 15, 2013.
Corresponding author: llcheng@gdut.edu.cn (Lianglun Cheng)

doi:10.4304/jsw.9.1.20-25

paper is structured as follows. Section II illustrates the model and steps of the proposed improved intelligent ant colony algorithm. Section III describes the mechanics model of the torsion bar. Section IV analyzes and compares the results obtained by the proposed algorithm. Finally some conclusions are made in section V.

II. The Improved Intelligent Ant Colony Algorithm

A. Algorithm Model

The system model is expressed as follows.

$$\tau_{ij}^{new} = \rho \cdot \tau_{ij}^{old} + \alpha \cdot \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \tag{1}$$

Where m is the number of ants, ρ is durability, α is the volatile coefficient, τ_{ij} is the residue information between the sensor node i and j.

B. Algorithm Steps

Step 1: The sensor node configuration and the initialization of pheromone.

Step 2: To select the next sensor node according to the expression (2) and (3).

$$p_{ij}^{k}(t+1) = \begin{cases} \dfrac{[\tau_{ij}(t)]^{\alpha}(\eta_{ij})^{\beta}}{\sum_{r\in s}[\tau_{ir}(t)]^{\alpha}(\eta_{ir})^{\beta}}, & j \in \{0,1,\cdots,n-1\} \\ 0, & j \notin \{0,1,\cdots,n-1\} \end{cases} \tag{2}$$

$$j = \begin{cases} \arg\max_{i\in j(k)} \{[\tau_{ij}(t)]^{\alpha}(\eta_{ij})^{\beta}\}, & q \le q_0 \\ S, & q > q_0 \end{cases} \tag{3}$$

Where q_0 is the initial parameters, q is a random number, η_{ij} is the heuristic information transform from the sensor node i to the sensor node j. β is the relative importance of expectation information. S is a random number determined by the expression (2).

Step 3: To update the pheromone of the sensor node path according to the expression (4) and (5).

$$\tau_{ij}(t+1) = \rho\tau_{ij}(t) + (1-\rho)\Delta\tau_{ij}^{k} \tag{4}$$

$$\Delta\tau_{ij}^{k} = \begin{cases} Q, & (i,j) \in T^{k} \\ 0, & (i,j) \notin T^{k} \end{cases} \tag{5}$$

Where Q is an constant, T^k is the past path of the ant k.

Step 4: To acquire the best path by computing the shortest distance when all ants go through all the sensor nodes. To update the pheromone of the best path according the following expression (6) and (7).

$$\tau_{ij}^{new} = \rho \cdot \tau_{ij}^{old} + \alpha \cdot \Delta\tau_{ij}^{k} \tag{6}$$

$$\Delta\tau_{ij}^{k} = \begin{cases} \dfrac{1}{d^{*}}, & (i,j) \in T^{k} \\ 0, & (i,j) \notin T^{k} \end{cases} \tag{7}$$

Where d^* is the distance of the best path.

Step 5: To output the optimal solution.

C. Algorithm Flow Chart

The algorithm flow chart is shown in Fig. 1.

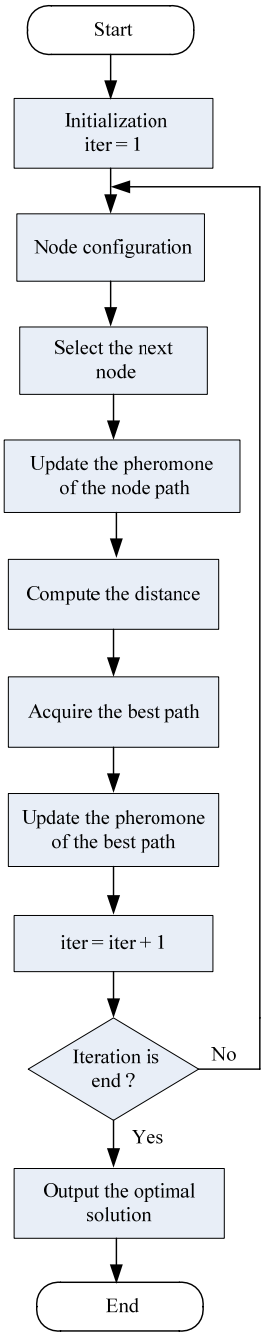


Figure 1. Algorithm flow chart

D. Algorithm Application Case

Coal transportation profit optimization:

We take a coal transportation enterprise as an example, there are three producing areas and five demanding areas. The shipment of the three producing areas is 18, 8, 16 respectively. The demand of five demanding areas is 6, 10, 8, 12, 6 respectively. The transport price of producing area $1^{\#}$ is 9, 19, 4, 8, 9, their upper limit of transportation is 1, 1, 4, 3, 2, and the cost of their transportation losses is 1, 4, 3, 4, 2. The transport price of producing area $2^{\#}$ is 1, 9, 7, 29, 5, their upper limit of transportation is 3, 3, 1, 2, 2, and the cost of their transportation losses is 1, 9, 2, 7, 9. The transport price of producing area $3^{\#}$ is 1, 19, 6, 9, 3, their upper limit of transportation is 1, 3, 0, 2, 4, and the cost of their transportation losses is 6, 9, 11, 1, 9.

According to the conditions given above, the results were got when the algorithm was applied. The results were shown in Table 1. The coal transportation profit is 285 unit according to the simulation results.

TABLE 1

THE OPTIMIZATION RESULTS

Sending area / Transportation area	1	2	3	4	5
1	0	6	8	2	2
2	0	0	0	4	4
3	6	4	0	6	0

E. Algorithm Application Prospect

The application field of the algorithm is wide.

a) Routing problem. Such as the vehicle routing, TSP, etc.
b) Allocation problem. Such as secondary allocation, graph coloring, frequency allocation, etc.
c) Scheduling problem. Such as workflow workshop, project scheduling, group workshop, etc.
d) Subset problem. Such as multiple backpack, maximum independent set, the biggest picture, etc.
e) Machine learning problem. Such as the bayesian network, the fuzzy system, allocation rules, etc.

III. Mechanics Model of the Torsion Bar

The Mechanics model of the torsion bar is shown as the following expression (8).

$$F = \frac{16DT}{\pi(D^4 - d^4)} \tag{8}$$

Where T is the torsion bar and d is the inner diameter. D is the outer diameter.

The torsion bar is shown in Fig. 2.

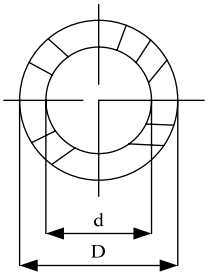


Figure 2. Torsion bar

According to the stress strength interference theory, the state equation is shown as the following expression (9).

$$g(X) = r - F \tag{9}$$

Where r is the material strength. Random variable is shown as the following expression (10).

$$X = [r \;\; d \;\; D \;\; T] \tag{10}$$

For partial derivation, we get the following expression (11).

$$\frac{\partial g(X)}{\partial X^T} = [\frac{\partial g}{\partial r} \;\; \frac{\partial g}{\partial d} \;\; \frac{\partial g}{\partial D} \;\; \frac{\partial g}{\partial T}] \tag{11}$$

IV. Testing Results and Discussions

A. Normal Distribution

The designing parameters of a clothing manufacturing was shown as follows.

$$\begin{cases} (\mu_T, \sigma_T) = (788532, 9973.35)\ N \cdot mm \\ (\mu_r, \sigma_r) = (775.8, 47.7)\ MPa \\ N \geq 6500 \\ \beta > 3 \end{cases} \tag{12}$$

Where β was the reliability index. N was the working cycle.

We defined the objective function as the following expression (13).

$$\begin{cases} f_1(x) = \dfrac{\pi}{4}(x_2^2 - x_1^2) \\ f_2(x) = \dfrac{\partial R}{\partial x_1} \\ f_3(x) = \dfrac{\partial R}{\partial x_2} \end{cases} \tag{13}$$

The geometry size constraint was shown as the following expression (14).

$$\begin{cases} 0 \leq d \leq 50mm \\ 0 \leq D \leq 50mm \end{cases} \tag{14}$$

Position and speed of 150 sensor nodes were randomly generated. We assumed the learning factor was 1.6 and the inertia factor decreased from 1 to 0.2.

After 55 times iteration, we got the optimal solution. The results of the three algorithms were shown in Table 2.

TABLE 2

RESULTS OF THE THREE ALGORITHMS IN NORMAL DISTRIBUTION

GA		ACO		IIACA	
Objective function values	Variable value	Objective function values	Variable value	Objective function values	Variable value
f1=188.57	d=20.8764	f1=175.85	d=20.9985	f1=174.26	d=20.3214
f2=0.5763	D=22.9978	f2=0.5998	D=22.8753	f2=0.5285	D=22.5021
f3=0.7548		f3=0.7989		f3=0.7462	
β=3.1947		β=3.2861		β=3.3975	

It was indicated that the improved intelligent ant colony algorithm could reduce the area of section so as to save materials. It also improved the reliability index. The reason was that the improved intelligent ant colony algorithm could select sensor nodes to grasp the whole face of the solution space. So the improved intelligent ant colony algorithm avoided the possibility of getting into the local optimal solution. It found the global optimal solution. Its searching speed was faster than others.

B. Arbitrary Distribution

The designing parameters of a clothing manufacturing was shown as the expression (15).

We defined the objective function as the expression (13) and the geometry size constraint as the expression (14).

Position and speed of 150 sensor nodes were randomly generated. We assumed the learning factor was 2.5 and the inertia factor decreased from 1 to 0.2.

After 65 times iteration, we got the optimal solution. The results of the three algorithms were shown in Table 3.

TABLE 3

RESULTS OF THE THREE ALGORITHMS IN ARBITRARY DISTRIBUTION

GA		ACO		IIACA	
Objective function values	Variable value	Objective function values	Variable value	Objective function values	Variable value
f1=188.57	d=27.8653	f1=175.85	d=27.5673	f1=289.35	d=27.3857
f2=0.5763	D=34.0991	f2=0.5998	D=33.9842	f2=0.5273	D=32.4165
f3=0.7548		f3=0.7989		f3=0.7659	
β=3.1893		β=3.1952		β=3.2869	

It was indicated that the improved intelligent ant colony algorithm could save materials because it could reduce the area of section. It also improved the reliability. The reason was that the improved intelligent ant colony algorithm could select sensor nodes to grasp the whole face of the solution space. So the improved intelligent ant colony algorithm avoided the possibility of getting into the local optimal solution.

$$\begin{cases} (T) = [7.5169\times10^{5}\,N\cdot mm, 9.738\times10^{3}\,N\cdot mm, 8.5637\times10^{10}\,(N\cdot mm)^{3}, 4.3825\times10^{15}\,(N\cdot mm)^{4}] \\ (r) = (795.6873MPa, 51.1037MPa, -8.1342\times105MPa^{3}, 1.5634\times108MPa^{4}) \\ N \geq 6500 \\ \beta > 3 \end{cases} \tag{15}$$

C. Lost Package Changes

Experiments were finished in the NS-2 simulation environment. The number of sensor nodes was 150 and initial energy of the node was 150 units. Sensor nodes were random distribution. The results of simulations were presented in Fig. 3.

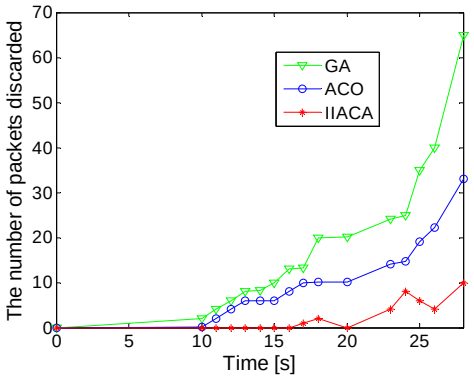


Figure 3. Lost package changes

Abscissa denoted time and y coordinate denoted the number of packets discarded. We assumed sensor nodes would begin to lose package when there were 35 packets in the wait queue. The results showed that the improved intelligent ant colony algorithm was better than others. It was not easy to cause the network congestion because the package was relatively balanced.

D. Surplus Energy Situation of Sensor Nodes

The results of simulations were presented in Fig. 4. Abscissa denoted time and y coordinate denoted the surplus energy. It was indicated that the improved intelligent ant colony algorithm was better than others. Because the energy consumed in each path was balanced in the improved intelligent ant colony algorithm. It would not make the network early lose balance because of too much consume of energy. So the whole network of life was prolonged.

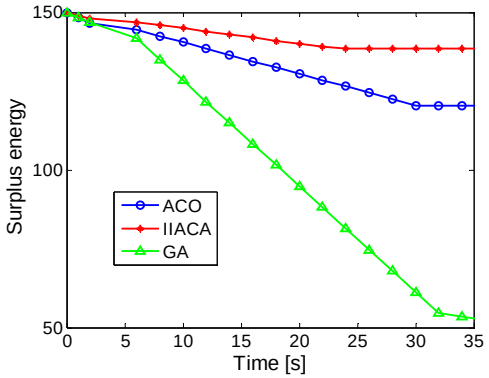


Figure 4. Surplus energy situation

V. CONCLUSIONS

In this paper we developed an improved intelligent ant colony algorithm for solving the optimization problem of reliability which related to material costs and benefits in the intelligent manufacturing industry.

An improved intelligent ant colony algorithm was designed to optimize the reliability of torsion bar in intelligent manufacturing. Then we tested and compared the three existing algorithms. Our analyses showed that the improved intelligent ant colony algorithm performed better than the genetic algorithm and the ant colony optimization algorithm in term of reliability, costs and energy saving. It could improve the performance of the whole network effectively. And it prolonged the lifecycle of the torsion bar in the manufacturing system.

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for their valuable comments and suggestions to improve the presentation of this paper. This work was supported in part by a grant from the National Natural Science Foundation of China (No. 60673132) and the Natural Science Foundation of Guangdong Province of China (No. 8351009001000002).

REFERENCES

[1] Rowland J.G. and Jain L.C., "Knowledge-based systems for instrumentation diagnosis, system configuration and circuit and system design," *Engineering Applications of Artificial Intelligence*, vol. 6, no.5, pp. 437-446, 1993.

[2] Pengshou Xie and Zhiyuan Rui, "Study on the Integration Framework and Reliable Information Transmission of Manufacturing Integrated Services Platform," *Journal of Computers*, vol. 8, no.1, pp. 146-154, 2013.

[3] Mhalla Anis and Dutilleul Simon Collart, "Monitoring of a Milk Manufacturing Workshop Using Chronicle and Fault Tree Approaches," *STUDIES IN INFORMATICS AND CONTROL*, vol. 19, no.4, pp. 379-390, 2010.

[4] Lee Wonhee and Amini Hamed, "Dynamic self-assembly and control of microfluidic particle crystals," *PROCEEDINGS OF THE NATIONAL ACADEMY OF SCIENCES OF THE UNITED STATES OF AMERICA*, vol. 107, no.52, pp. 22413-22418, 2010.

[5] FuQing Zhao, JianXin Tang, and YaHong Yang, "A new Approach based on Ant Colony Optimization (ACO) to Determine the Supply Chain (SC) Design for a Product Mix," *Journal of Computers*, vol. 7, no.3, pp. 736-742, 2012.

[6] Gonzalez Antonio and Perez Raul, "An Efficient Inductive Genetic Learning Algorithm for Fuzzy Relational Rules," *INTERNATIONAL JOURNAL OF COMPUTATIONAL INTELLIGENCE SYSTEMS*, vol. 5, no.2, pp. 212-230, 2012.

[7] Ahmad Zaryab, Rahmani Keyvan, and D'Souza Roshan M., "Applications of genetic algorithms in process planning: tool sequence selection for 2.5-axis pocket machining," *JOURNAL OF INTELLIGENT MANUFACTURING*, vol. 21, no.4, pp. 461-470, 2010.

[8] Regis Rommel G., "Convergence guarantees for generalized adaptive stochastic search methods for continuous global optimization," *EUROPEAN JOURNAL OF OPERATIONAL RESEARCH*, vol. 207, no.3, pp. 1187-1202, 2010.

[9] Fredriksson Kimmo, "On building minimal automaton for subset matching queries," *INFORMATION PROCESSING LETTERS*, vol. 110, no.24, pp. 1093-1098, 2010.

[10] Lijuan Zhou, Xiaoxu He, and Kang Li, "An Improved Approach for Materialized View Selection Based on Genetic Algorithm," *Journal of Computers*, vol. 7, no.7, pp. 1591-1598, 2012.

[11] Merdan Ziya, Bayirli Mehmet, and Ozturk Mustafa Kemal, "The Simulation of the Two-Dimensional Ising Model on the Creutz Cellular Automaton for the Fractals Obtained by Using the Model of Diffusion-Limited Aggregation," *ZEITSCHRIFT FUR NATURFORSCHUNG SECTION A-A JOURNAL OF PHYSICAL SCIENCES*, vol. 6, no.8, pp. 705-710, 2010.

[12] De Cicco Luca and Mascolo Saverio, "A Mathematical Model of the Skype VoIP Congestion Control Algorithm," I*EEE TRANSACTIONS ON AUTOMATIC CONTROL*, vol. 55, no.3, pp. 790-795, 2010.

[13] Kol'tsova EM, Nenaglyadkin IS, Kolosov AY, and etc., "A cellular automaton for the description of crystal growth from the supersaturated unperturbed and agitated solutions," *RUSSIAN JOURNAL OF PHYSICAL CHEMISTRY*, vol. 74, no.1, pp. S85-S91, 2009.

[14] Yang Z., Cao Z., and Liu, H., "Link supportability analysis of digital channelised satellite communication system using min-max optimisation and variable neighbourhood search algorithm," *IET COMMUNICATIONS*, vol. 4, no.18, pp. 2145-2154, 2010.

[15] Espejo Pedro G., Ventura Sebastian, and Herrera Francisco, "A Survey on the Application of Genetic Programming to Classification," *IEEE TRANSACTIONS ON SYSTEMS MAN AND CYBERNETICS PART C-APPLICATIONS AND REVIEWS*, vol. 40, no.2, pp. 121-144, 2010.

[16] Sivakumar K, Iyengar NGR, and Debb K, "Optimization of composite laminates with cutouts using genetic algorithm, variable metric and complex search methods," *ENGINEERING OPTIMIZATION*, vol. 32, no.5, pp. 635-657, 2000.

[17] Escario Jose B., Jimenez Juan F., and Giron-Sierra Jose M., "Optimisation of autonomous ship manoeuvres applying Ant Colony Optimisation metaheuristic," *EXPERT SYSTEMS WITH APPLICATIONS*, vol. 39, no.11, pp. 10120-10139, 2012.

[18] Gambardella L. M., Montemanni R., and Weyland, D., "Coupling ant colony systems with strong local searches," *EUROPEAN JOURNAL OF OPERATIONAL RESEARCH*, vol. 220, no.3, pp. 831-843, 2012.

[19] Chan M and Szabados B, "On-line production control of tandem systems with finite inter-stage storage, using a

dynamic maximum cycle time algorithm," *INTERNATIONAL JOURNAL OF ADVANCED MANUFACTURING TECHNOLOGY*, vol. 16, no.2, pp. 147-154, 2000.

Shiliang Luo received B.E. degree from Nanchang University and M.A. degree from Guangdong University of Technology, China. He is studying for the degree of Ph.D. at the Guangdong University of Technology, China. His research interests are Cyber-Physical System and Intelligence algorithm.

Lianglun Cheng is a professor of computer science at Guangdong University of Technology, He received B.E. and M.A. degrees from Huazhong University of Science & Technology. He received the Ph.D. degree from Chinese Academy of Sciences. His current research interests include Cyber-Physical System and internet of things. He is a member of China Computer Federation.

Bin Ren received the Ph.D. degree in control theory and control applications from Guangdong University of Technology China. Currently, he is a researcher at Dongguan University of Technology, China. His major research interests include machine vision and image processing. He has published nearly forty papers in related journals.

Quanmin Zhu is a professor in control systems at the Faculty of Computing, Engineering and Mathematical Sciences(CEMS), University of the West of England (UWE), Bristol, UK. His research interests are nonlinear system modeling, identification, control.

The Population-Based Optimization Algorithms for Role Modelling and Path Generation in Group Animation

Hong Liu
School of Information Science and Engineering, Shandong Normal University
Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology
Jinan City, P.R.China
Email: lhsdcn@jn-public.sd.cninfo.net

Yuanyuan Li and Hanchao Yu
School of Information Science and Engineering, Shandong Normal University, Jinan City, P.R.China
Email: lyysdnu@126.com yuhanchao@ict.ac.cn

***Abstract*—Traditional animation by key frame techniques takes animators lots of time and vigour to model and simulate behaviours of crowds. For solving this problem, this paper presents a novel group animation generation approach based on population-based optimization algorithms. It is mainly divided into two parts. First, it puts forward a role modelling approach based on dynamic self-adaptive genetic algorithm and NURBS technology. Second, following the introduction to PSO (Particle Swarm Optimization) algorithm, a group path generative approach is presented. It simulates group behaviours, including cohesion and separation, dynamic object tracking and collision avoidance. Finally, a group of shark modelling and path generation images are exhibited as examples.**

***Index Terms*—group animation, role modelling, genetic algorithm, PSO algorithm, path generation**

I. INTRODUCTION

Group animation has been a main topic in the field of computer animation and game. Traditional key frame techniques took animators lots of time and vigour to model and simulate vivid behaviours of crowds or flocks as each individual's behaviour needs to be scripted carefully to meet the following requirement: motion of the whole group should be harmonious while the individuals in the group look like independent and moving stochastically.

One of the important characteristics of group animation is its ability to reduce the workload on the animators. This is achieved by letting a behavioural model automatically take care of the low-level details of the animation, freeing the animator to concentrate on the big picture. Freeing the animator from low-level animation details is even more important when dealing with crowds.

An animator manually creating a crowd animation is overwhelmed not only by the large number of animated entities, but also by the interactions between them. If all tracks are made by animator one by one, the work will be very heavy while the effect is not satisfied.

Population-based optimization algorithms find near-optimal solutions to the difficult optimization problems by motivation from nature. A common feature of all population-based algorithms is that the population consisting of possible solutions to the problem is modified by applying some operators on the solutions depending on the information of their fitness. Hence, the population is moved towards better solution are as of the search space. Two important classes of population-based optimization algorithms are evolutionary algorithms and swarm intelligence-based algorithms.

Genetic algorithm is a kind of evolutionary algorithms that transforms populations of individual objects into new populations using operations patterned after natural genetic operations and fitness proportionate reproduction. Genetic algorithms begin with an initial population of individuals and then iteratively (1) evaluate the individuals in the population for fitness and (2) perform genetic operations on various individuals in the population to produce a new population.

PSO (Particle Swarm Optimization) algorithm is a swarm intelligence-based algorithm and has a dominance to perform better in simulating group actions. Because it was inspired by the activities of social animals or insects in nature, it shows more smooth and genuine as a basis for group animation,.

This paper presents a novel group animation generation approach for role modelling and path generation in group animation. It puts forward a role modelling approach based on dynamic self-adaptive genetic algorithm and NURBS technology. A group of shark design example is illustrated for showing the modelling process. After then, a group animation path generative approach based on PSO algorithm is introduced It simulates group behaviours, including cohesion and separation, dynamic object tracking and collision avoidance. The generative path can be used as the movement track of the group. In

This paper is supported by the National Natural Science Foundation of China (No.61272094) and the Ph.D. Programs Foundation of Ministry of Education of China (No. 20093704110002), Natural Science Foundation of Shandong Province (No. ZR2010QL01) and Shandong Provincial Key Laboratory Project.

doi:10.4304/jsw.9.1.26-36

this way, the animators will save time and be absorbed in the design of the main roles and scenes.

The remainder of this paper is organized as follows. Section 2 is related work in group animation. Section 3 introduces a group animation role modelling approach based on dynamic self-adaptive genetic algorithm and NURBS technology. In section 4, a group animation path generative approach is presented and showed how to use particle swarm optimisation algorithm to generate group animation paths. The last section summarises the paper and gives an outlook for the future work.

II. Related Works

Virtual groups have been studied since the early days of behavioral animation. The seminal work by Reynolds [1] is considered the first one in the field of behavioral animation. It presented a method to animate large groups of entities called boids, which present behaviors similar to those observed in flocks of birds and schools of fishes. Reynolds started from the premise that the group behavior is just the result of the interaction between the individual behaviors of the group members. Therefore, it would suffice to simulate the reasonably simple boids individually, and the more complex flocking behavior would emerge from the interaction between them.

Tu and Terzopoulos [2] created a realistically rich environment inhabited by artificial fishes. The complexity of the under sea life, including interactions between fishes like predators hunting preys, mating, and schooling, was obtained by modeling the behavior of individual fishes: group behaviors emerged as the individuals interacted.

Going even further in the direction of using more realistic models of the simulated entities, Brogan and Hodgins [3] described an algorithm to control the movements of entities with significant dynamics that travel in groups. By significant dynamics, the authors mean that the work is focused on simulating systems whose dynamics are complex enough to have a strong impact on the motion of the simulated entities.

Researches are being conducted to the use of path planning algorithms associated to generation of realistic movements of the found path. Lavalle [4] introduced the concept of a Rapidly-exploring RandomTree (RRT) as a randomized data structure for path planning problems. Choi et al. [5] proposed a model based on a probabilistic path planning and hierarchical displacement mapping to generate a sequence of realistic movements of a human-like biped figure to move from a given start position to a goal with a set of prescribed motion clips. Metoyer and Hodgins [6] proposed a method for generating reactive path following based on the user's examples of the desired behavior. Zhang et al. [7] presented a framed-quadtree based on reversed d* path planning approach for intelligent mobile robot and Gong et al. [8] introduced a multi-objective particle swarm optimization algorithm for robot path planning

More specifically concerning groups' motion, Rodríguez et al. [9] proposed a model using a road map providing an abstract representation of global environment in formation to achieve different complex group behaviors that cannot be modeled with local information alone. Lien and collaborators [10] proposed ways using roadmaps to simulate a type of flocking behavior called shepherding behavior in which outside agents guide or control members of a flock. Foudil et al. [11] designed a system to simulate pedestrian behaviour in crowds in real time, concentrating particularly on collision avoidance. On-line planning is also referred to as the navigation problem.

Rodrigues [12] and Bicho et. al [13] presented a method for crowd simulation based on a biologically motivated space colonization algorithm. The proposed crowd modelling method is free-of-collision and suited to the interactive control of simulated crowds.

Data-driven models are quite recent in comparison with other methods, and aim to record motion in a preproduction stage or to use information from real life to calibrate the simulation algorithms. One example was proposed by Musse et al. [14] described a model for controlling groups' motions based on automatic tracking algorithms and proposed a new model to quantitatively compare global flow characteristics of two crowds [15].

Although there are many approaches for modeling and path generation in computer animation, only a few researchers try to use population-based optimization algorithms for this purpose. This paper presents a novel group animation modelling and path generation approach based on population-based optimization algorithms.

III. The Role Modeling Based on Dynamic Self-Adaptive Genetic Algorithm and NURBS Technology

For the character of a large scale individuals in group animation, the role modelling in group animation by evolutionary algorithm possesses unexampled advantage. Each individual in group have to be different and each of them have to be similar in group animation. Fortunately, evolutionary algorithm is suitable to solve this kind of problem. It is based on simulating the process of natural selection and reproduction on a computer. This technique depends on the specification of a parameterized model that is general enough to allow a wide variety of possible outcomes of interest to the animator. These outcomes are similar with the seed while each of them are different. It just is accord with request of role modelling. The role modelling based on dynamic self-adaptive genetic algorithm and NURBS technology will be introduced at following section.

A. NURBS Technology

Non-Uniform Rational B-Splines encompass almost every other possible 3D shape definition. A NURBS curve is defined as:

$$C(t)=\frac{\sum_{i=0}^{n}\varpi_i P_i N_{i,k}(t)}{\sum_{i=0}^{n}\varpi_i N_{i,k}(t)} \quad (1)$$

Where P_i are the control points, ϖ_i are the weights of P_i, and $N_{i,k}(t)$ are B-Spline basis functions, i=0,1,2,⋯,n.

The recursive definition of B-Spline basis functions $N_{i,k}(t)$ is:

$$N_{i,0}(t)=\begin{cases}1 & t\in[t_i,t_{i+1}]\\ 0 & t\notin[t_i,t_{i+1}]\end{cases} \quad (2)$$

$$N_{i,k}(t)=\frac{t-t_i}{t_{i+k}-t_i}\times N_{i,k-1}(t)+\frac{t_{i+k+1}-t}{t_{i+k+1}-t_{i+1}}\times N_{i+1,k-1}(t) \quad t\in[t_k,t_{n+1}] \quad (3)$$

In which, t_i are the values of knots, and the knot vector is $T=(t_0,t_1,\cdots,t_{n+k+1})$.

From the definition equation of NURBS curve, it can be seen that the shapes of NURBS curves can be changed by moving control points, altering the weights of control points, and The knot vector is a sequence of parameter values that determines where and how the control points affect the NURBS curve. In this paper, the approach of altering shape is used by moving control points while the structure lines are being adjusted.

There are many creation approaches of NURBS models, such as transshipping to the basic NURBS elements, revolving or lofting to NURBS curves and so on. Therefore, NURBS models can be created by outlining structure lines and then lofting them. In this way, the structure lines of a successful NURBS model are extracted first. Then the extracted structure lines are adjusted. Finally, these structure lines are lofted to generate the other model.

There are both U curves and V curves on NURBS surfaces. U curves are landscape orientation curves while V curves are longitudinal orientation curves on model surface. A NURBS model can be rotten by lofting its U curves or V curves. Therefore, extracting structure curves is to draw out and copy these U and V curves and then adjusted them to form new model.

B. The Coding of Genetic Algorithm

Solving a given problem with genetic algorithm starts with specifying a representation of the candidate solutions. Such candidate solutions are seen as phenotypes that can have very complex structures. There are many coding methods, such as binary coding, grey coding, real coding, symbol coding, tree-structure coding, hybrid coding, and so on. In this paper, the scale factor of structure curves is taken as gene and real coding is used to express scale value. The number of gene bits is decided by the structure curve number of the model.

For example, a model with 7 structure curves can be expressed (0.3) (1.0) (2.2) (1.4) (0.8) (1.9) (1.2), in which (0.3) denotes the scale value of the first curve is 0.3 times of the first curve of the seed.

C. Fitness

Select a current best model by designer, and the fitness of every individual is decided by the similar degree with the best individual. It is calculated according to the radios between the structure curves of an individual with the structure curves of the best individual. The more similar an individual is with the best individual, the higher its fitness value is.

Definition 1 The structure curve radius r_i: The average of the distances between the control points to the center point at the ith structure curve.

Definition 2 The ratio of the current structure curve $Current_i$: The ratio between the radius of the ith structure curve r_i at the current individual and the radius of the first structure curve.

Definition 3 The best ratio of the structure curve $Best_i$: The best ratio between the radius of the ith structure curve r_i at the current individual and the radius of the first structure curve.

$$fitness=\frac{1}{\sum_{i=1}^{n}\frac{Best_i-Current_i}{Best_i}} \quad (4)$$

According to (4), the more similar an individual with the best individual, the higher its fitness value.

D. Self-adaptive Dynamical Adjustment

The performance of genetic algorithm is greatly affected by cross probability P_C and mutation probability P_M. If the unsuitable values of P_C and P_M are used in GA, it is easy to sink into local optimal value early. For solving this problem, an approach of dynamical adjusting to P_C and P_M are presented as following.

First of all, an estimation function for checking whether the current individual has sunk into its local optimal value is defined.

Definition 4 Let x be an individual in current population, $h(x)$ is the fitness value of x, $h_{\max}$ is the fitness value of the best individual in current population, ε is an arbitrary small positive number. The estimation function $k(x)$ is defined as:

$$k(x)=\frac{h(x)}{h^2(x)-(h_{\max}-\varepsilon)^2} \quad (5)$$

Next, a property of the estimation function is proved. Let us differentiate for equation (5) from both side and get:

$$k'(x)=\left(\frac{h(x)}{h^2(x)+(h_{\max}-\varepsilon)^2}\right)'=\frac{h'(x)\left[(h_{\max}-\varepsilon)^2-h^2(x)\right]}{\left(h^2(x)+(h_{\max}-\varepsilon)^2\right)^2} \quad (6)$$

Let $\Omega_1(x^\circ)=\{x\mid h(x)<h(x^\circ)\}$

$\Omega_2(x^\circ)=\{x\mid h(x)>h(x^\circ)\}$

$\Omega_3(h_{\max})=\{x\mid h(x)<h_{\max}\}$

$\Omega_4(h_{\max})=\{x\mid h(x)>h_{\max}\}$

Suppose $x^\circ\in\Omega$ is one local maximum value of $h(x)$. From (5), we get the following property:

When $(h_{\max}-\varepsilon)^2-h^2(x)>0$,

i.e. $h(x)<h_{\max}-\varepsilon$, $k'(x)$ and $h'(x)$ with the same sign, then

(1) If x° is the local maximal value of $h(x)$, then x° also is the local maximal value of $k(x)$, and the attract region of x° is $\Omega_1(x^\circ)\bigcap\Omega_3(h_{\max})$;

(2) If x° is the local minimal value of $h(x)$, then x° also is also is the local maximal value of $k(x)$, and the attract region of x° is $\Omega_2(x^\circ)\bigcap\Omega_3(h_{\max})$。

When $(h_{\max}-\varepsilon)^2-h^2(x)<0$,

i.e. $h(x)>h_{\max}-\varepsilon$, $k'(x)$ and $h'(x)$ with the different sign, then

(1) If x° is the local maximal value of $h(x)$, then x° is the local minimal value of $k(x)$, and the attract region of x° is $\Omega_1(x^\circ)\bigcap\Omega_4(h_{\max})$;

(2) If x° is the local minimal value of $h(x)$, then x° is the local maximal value of $k(x)$, and the attract region of x° is $\Omega_2(x^\circ)\bigcap\Omega_4(h_{\max})$.

From the above consequence, theorem 1 can be gotten. It can be used to estimate whether the current individual is in the global optimum attract region, then dynamically adjust cross probability P_C and mutation probability P_M accordingly.

Theorem 1 Let $h_{\max}-\varepsilon$ be a threshold of the global optimum value (i.e. if $h(x^\circ)>h_{\max}-\varepsilon$, then regard x° as the global optimum value). x^Δ Locates in the global optimum attract region, if and only if $\left[h(x)-h(x^\Delta)\right]\left[k(x)-k(x^\Delta)\right]<0$ is true, $\forall x$ in the adjacent region of x^Δ.

According to theorem 1, we can estimate a current individual x^Δ belongs to the global optimum attract region or the local optimum attract region, and then dynamically adjust P_C and P_M based on the following formula:

$$\begin{cases} P_C=P_C+\alpha\times d\times\dfrac{\left[h(x)-h(x^\Delta)\right]\left[k(x)-k(x^\Delta)\right]}{\left|h(x)-h(x^\Delta)\right|\left|k(x)-k(x^\Delta)\right|} \\ P_M=P_M+\beta\times d\times\dfrac{\left[h(x)-h(x^\Delta)\right]\left[k(x)-k(x^\Delta)\right]}{\left|h(x)-h(x^\Delta)\right|\left|k(x)-k(x^\Delta)\right|} \end{cases} \quad (7)$$

In which, $\alpha=\min\{P_C,1-P_C\}$, $\beta=\min\{P_M,1-P_M\}$, $d=\min\left\{\left|h_{\max}-h(x^\Delta)\right|/(h_{\max}-h_{\min}),\ 1\right\}$, $h_{\min}$ is the fitness value of the worst individual in the population and $h_{\max}$ is the fitness value of the best individual in the population.

The formula 3 is used as following:

If the current individual x^Δ locates in the global optimum attract region, then on the basis of original cross probability P_C, mutation probability P_M and the distance d with the best individual in the population, dynamically decrease the cross probability P_C and mutation probability P_M between 0 and 1, in order to save the individuals located in the global optimum attract region.

If the current individual x^Δ locates in the local optimum attract region, then on the basis of original cross probability P_C, mutation probability P_M and the distance d with the best individual in the population, dynamically increase the cross probability P_C and mutation probability P_M between 0 and 1, in order to avoid sinking into local optimum solution.

The adjusting process is:

(1) For every individual x^Δ in the population, calculate the fitness value $h(x^\Delta)$ and the value of estimate function $k(x^\Delta)$;

(2) $\forall x$ in the adjacent region of x^Δ, calculate the fitness value $h(x)$ and the value of estimate function $k(x)$;

(3) Calculate

$$d=\min\left\{\left|h_{\max}-h(x^\Delta)\right|/(h_{\max}-h_{\min}),\ 1\right\}$$

(4) Let

$$P_C=P_C+\alpha\times d\times\frac{\left[h(x)-h(x^\Delta)\right]\left[k(x)-k(x^\Delta)\right]}{\left|h(x)-h(x^\Delta)\right|\left|k(x)-k(x^\Delta)\right|}$$

(5) Let

$$P_M=P_M+\beta\times d\times\frac{\left[h(x)-h(x^\Delta)\right]\left[k(x)-k(x^\Delta)\right]}{\left|h(x)-h(x^\Delta)\right|\left|k(x)-k(x^\Delta)\right|}$$

The above dynamical adjusting operation can increase the convergence of genetic algorithm and enhance the diversity of the population obviously.

E.The Elitism Strategy

When dynamically adjusting, it is possibly to cause the crossover probability and the variation probability become very large, and thus destroy the outstanding individuals which will appear in the evolution process.

This paper adopts the elitism strategy to retain the outstanding individual. Supposes the population number is n, the strategy is that after every genetic operations, sort the new generated population B by the fitness value of the individual, take front 30 percent invividuals and merge them with the last generation population, get the polulation A. Sorting the individuals in A according to their fitness values, take front 30 percent invividuals in A and compare them with the individuals of the last generation population. If there are k ($k \leqslant 30\%$) individuals belonging to the last generation, randomly eliminate k individuals in A and take the front k individuals merge into A. The elitism strategy make it to be possible to guarantee the current outstanding individuals not to be destroyed by heredity operations. This will be a important guarantee condition for the convergence of the algorithm.

IV. A Design Example to Illustrate the Execution of Genetic Algorithm

In this section, we introduce a shark model design example (Figure 1) to show the modelling process. A complex design can be divided into several part design and then assembled them. For briefly, we only introduce the modelling process of a shark body.

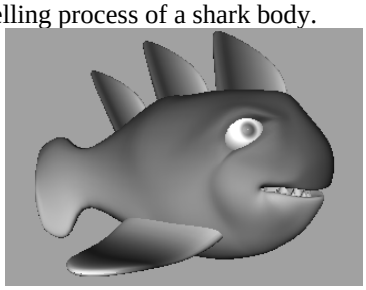


Figure 1. A shark model

Step 1 Initializing the population of chromosomes.

Create a model by animator or import a model from model base, as figure 1 and divided its body model as figure 2.

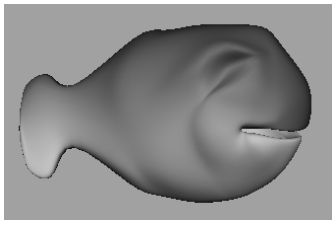


Figure 2. The body of the shark model

(2) Obtain the structure curves number is oparm_num from both U and V orientations by getAttr(Obj.spanU) and getAttr(Obj.spanV) functions.

(3) Draw out the structure curves from both U and V orientations by Duplicate Curve function. There are 16 extracted structure curves at V orientations and they are shown as figure 3.

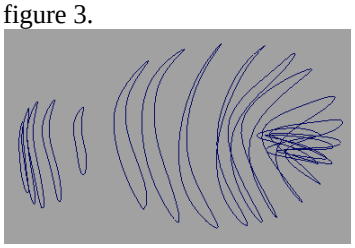


Figure 3. The extracted NURBS curves

(4) Obtain the control point positions of every structure curves and save them in two-dimensional array ep_point[M][N]. There are 8 control points at every structure curve and they are shown as figure 4.

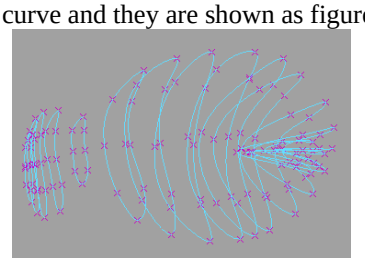


Figure 4. The control points

(5) Reconstitute the structure curves by curve function and the data information of the control points in array ep_point[M][N].

(6) Take a random number between 0 and 1 as scale rate and select a control point randomly at the structure curve, use scale function to scale the structure curves one by one.

(7) Loft the adjusted structure curves to form a new model.

(8) Repeat (5) to (7) until the number of new models to appointed speed size.

Step 2 Count the fitness for each individual in the population according to equation (4).

Step 3 Form a new population according to each individual's fitness based on elitism strategy.

Step 4 Perform crossover, mutation operations on the population.

(1) Crossover

The primary reproductive operation is the crossover operation. The purpose of this operation is to create two new models that contain genetic information inherited from two successful parents. The main crossover ways of real coding based genetic algorithm include signal point and multi-points crossover. A multi-points crossover way is used in this example.

The coding of two parents:

Left: （1.0） （1.13） （0.91） （0.95） （1.08） （0.99） （**1.16**） （0.92） （0.85） （0.92） （1.19） （**0.97**） （0.94） （1.11） （1.12） （1.03）

Right:（1.0）（0.90）（1.10）（0.96）（1.00）（0.98）（**1.00**）（1.14）（1.11）（0.87）（1.09）（**0.87**）（1.12）（1.01）（1.17）（1.06）

Two crossover points (7 and 11) are selected. After crossover, the coding of two children are gotten as following.

Left:（1.0）（1.13）（0.91）（0.95）（1.08）（0.99）（1.00）（0.92）（0.85）（0.92）（1.09）（0.97）（0.94）（1.11）（1.12）（1.03）

Right:（1.0）（0.90）（1.10）（0.96）（1.00）（0.98）（1.16）（1.14）（1.11）（0.87）（1.19）（0.87）（1.12）（1.01）（1.17）（1.06）

The NURBS curves of two parents and two children after crossover can be seen as figure 5 and figure 6.

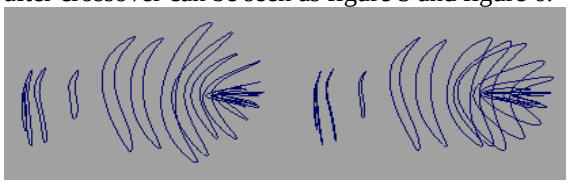


Figure 5. The NURBS curves of two parents

Figure 6. The NURBS curves of two children after crossover

The model of two parents and two children after crossover are shown as figure 7 and figure 8.

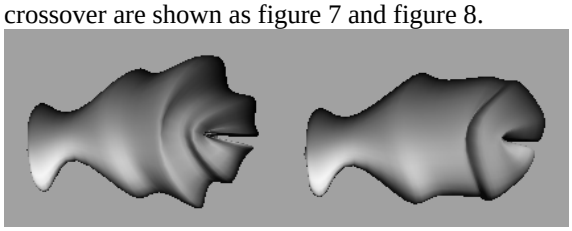


Figure 7. The models of two parents

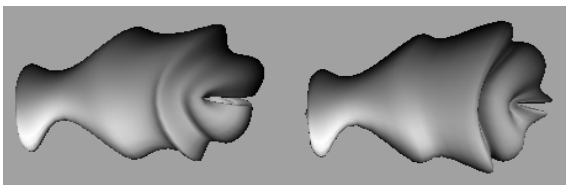


Figure 8. The models of two children after crossover

(2) Mutation

The mutation operation is used to enhance the diversity of trees in the new generation thus opening up new areas of ‘solution space’. It works by random selecting multiple structure curves in a single parent and change their scale radios accordingly.

The coding of two parent：

（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）

Two mutation points (5 and 7) are selected. After mutation, the coding of two children are gotten as following.

（1.0）（1.0）（1.0）（1.0）（1.364）（1.0）（1.069）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）（1.0）

The NURBS curves of the parent and the child after mutation can be seen as figure 9 and figure 10.

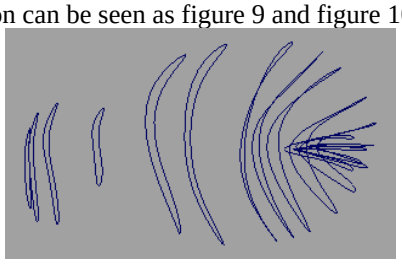


Figure 9. The NURBS curves of parent

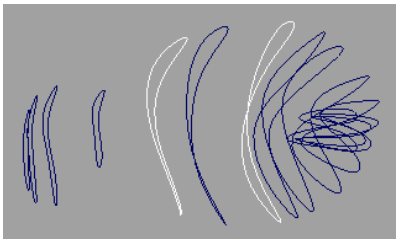


Figure 10. The NURBS curves after mutation

The models of the parent and the child after mutation are shown as figure 11 and figure 12.

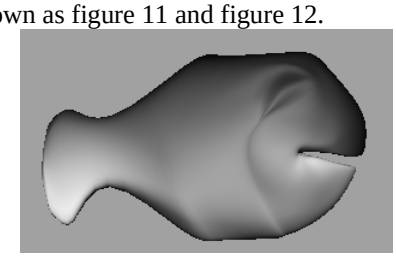


Figure 11. The model of parent

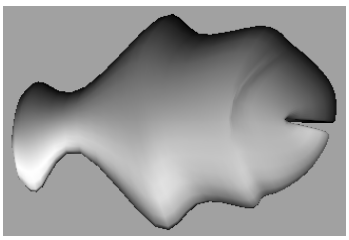


Figure 12. The model after mutation

Step 5 If the procedure doesn’t been stopped by the animator, go to step 2.

This process of selection and crossover, with infrequent mutation, continues for several generations until the animator stop it. Then the detail design will be done by animators with human wisdom.

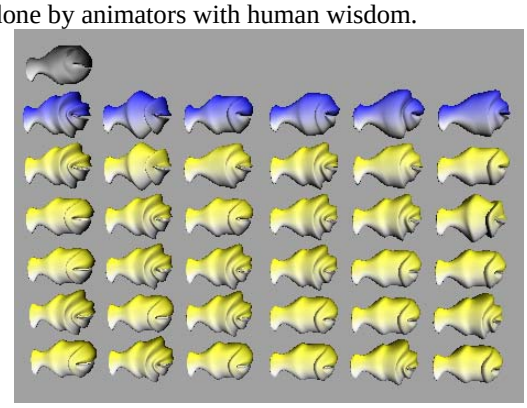


Figure 13. The fish bodes after five generation evolution

Figure 13 shows some generated fish bodes after five generation. The generated components and designed components by animators are classified and saves in a SQL sever based database. These components then are assembled and treated by animators to form a group of roles, and to be used at the following group animation.

V. Group Animation Path Generation Based on PSO Algorithms

A.Particle Swarm Optimization (PSO) Algorithm

Although the size of group is very large, the bird flocks can harmonious achieve the sudden change of direction, group separation and cohesion without collision. This phenomenon inspires many researches in related domain[16,17]. Social animals or insects in nature often exhibit a form of emergent collective behavior known as 'flocking'. The flocking model is a bio-inspired computational model for simulating the animation of a flock of entities. It represents group movement as seen in the bird flocks and the fish schools in nature. In this model, each individual makes its movement decisions on its own according to a small number of simple rules that it reacts to its neighboring members in the flock and the environment it senses. These simple local rules of each individual generate a complex global behavior of the entire flock.

Particle swarm optimization (PSO) was originally introduced by J. Kennedy and R. Eberhart [Kennedy and Eberhart, 1995] in 1995 as an optimization technique. The underlying motivation for the development of PSO algorithm was social behavior of animals such as bird flocking, fish schooling, and swarm theory. Each individual in PSO is assigned with a randomized velocity according to its own and its companions' flying experiences, and the individuals are then flown through hyperspace. In the Standard PSO model, each individual is treated as a volumeless particle in the D-dimensional space, with the position and velocity of ith particle represented as $X_i = (X_{i1}, X_{i2}, \cdots, X_{iD})$ and $V_i = (V_{i1}, V_{i2}, \cdots, V_{iD})$. The particles move according to the following equation:

$$V_{id} = w * V_{id} + c_1 * rand(\cdot) * (P_{id} - x_{id}) + c_2 * Rand(\cdot) * (P_g - X_{id}) \quad (8a)$$

$$X_{id} = X_{id} + V_{id} \quad (8b)$$

where c1 and c2 are positive constant, rand() and Rand() are two random functions in the range of [0,1]. Parameter w is the inertia weight introduced to accelerate the convergence speed of the PSO. Vector $p_i = (p_{i1}, p_{i2}, \cdots, p_{iD})$ is the best previous position (the position giving the best fitness value) of particle i called pbest, and vector $p_g = (p_{g1}, p_{g2}, \cdots, p_{gD})$ is the position of the best particle among all the particles in the population and called gbest.

In PSO algorithm, a particle decides where to move next, considering its own experience is the memory of its best position, and the experience of its most successful neighbour. At each iteration, the particle pbest with the best fitness in the local neighbourhood and the current particle are combined to adjust the velocity alone each dimension, and that velocity is then used to compute a new position for the particle. The portion of the adjustment to the velocity influenced by the individual's previous best position is considered the cognition component, and the portion influenced by the best in the neighbourhood is the social component.

Particle swarms, in common with many population based algorithms, have a dominance to perform better in simulating group actions. Because it was inspired by the activities of social animals or insects in nature, and as a basis for group animation, it shows more smooth and genuine.

The basic group animation consists of four basic steering behaviours:

(1) Cohesion: Steering the individuals in the group to collect to a position;
(2) Separation: Steeling the individuals in the group to separate from one position;
(3) Dynamic object track: Steering group toward the tracking object and keep a suitable distance each other;
(4) Collision avoidance: Steering group remains in close proximity while avoiding collisions with other members of the group and with obstacles in the environment.

The path generation of these basic behaviours based on PSO algorithm will be introduced at the following sections one by one.

B. Cohesion and Separation

In natural world, cohesion and separation are most general behaviours. The acquiring foods together and attacking heterogeneous objects are typical clustering behaviour, and getting away from natural enemy is common separate behaviour. In the animation with large scene, these two behaviours are the actions with high frequency. In our animation environment, an improved

PSO algorithm is used for generating path with more actual effect [18].

In natural biologic collecting, when the individual arriving in target point, it always moves around one position and will not concentre to one point. According to this principle, we enact a threshold for controlling the individuals' movement around target point (see (9)). When the individual arrives in the arrange that takes the target point as circle of center and threshold as radial, it will make stochastic movement in the circle.

$$f = \sqrt{[t_x - (o_x + rand(th))]^2 + [t_y - (o_y + rand(th))]^2 + [t_z - (o_z + rand(th))]^2} \quad (9)$$

Where f is fitness value, t_x,t_y,t_z is the current position of particle, o_x,o_y,o_z is the position of the target point, th is inputted threshold value.

The fitness f is counted by the distance between current position of the particle and one position closed with target point to avoid all particles congregate to one point.

Cohesion Algorithm Based on PSO

Step 1 Initialization: initialize the number of particle
the max number of group overlapping MAX;
the position of target point o_x, o_y, o_z;
threshold value th;
the arrange of each axis of original particle;
accelerate constant c_1, c_2;

Step 2 While（the overlapping number < MAX）do
For every particle
{
(1) Count the fitness value (new pbest) of the new position for every particle;
If new pbest >old pbest
Then pbest=new pbest;
(2) Change gbest according to updated pbest in (1);
(3) Update the speed of every particle, and limited them in V_{max};
(4)Update the position of every particle;
}

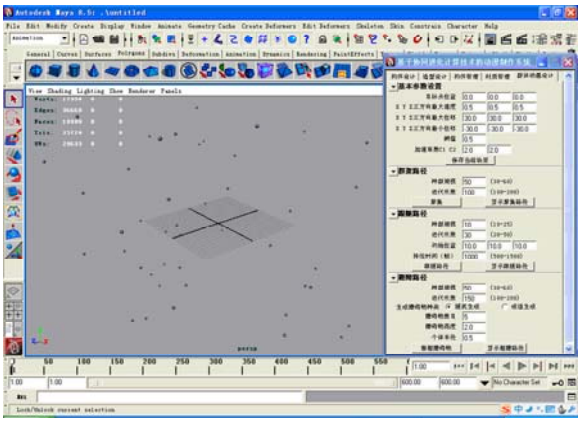


Figure 14. Initial states of the group

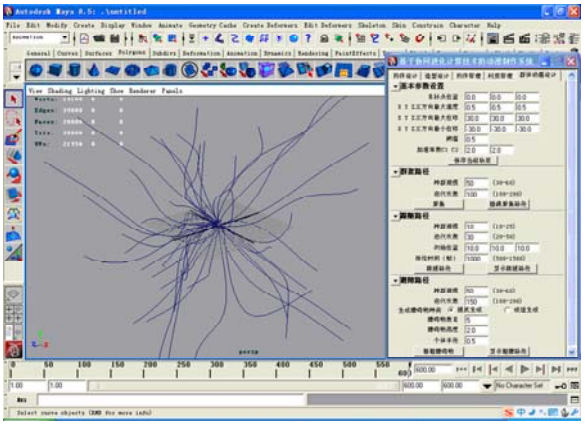


Figure 15. The generative cohesion path

Figure 16. One generated shark cohesion image according to the path in figure 15

Simulated results are as shown in figure 14 and figure 15. Figure 16 is generative shark cohesion according to the path in figure 15. If the different parameters are inputted, various paths with different directions and different types will be generated. The separation takes the opposite fitness to cohesion and is omitted here.

C. Dynamic Object Tracking

Dynamic object tracking behavior among the individuals is also a kind of typical group action in the natural world, such as flight of wide gooses, follow among shoal and so on. Track is an interesting action and can exhibit group intelligence well. The tracking movement in animation can show special effect.

The dynamic object track is implemented by the following process. First of all, erecting initial parameters, and then following the pass points of tracking object, taking tracking object as target position and overlapping MAX times. After that, updating the target position by current position of tracking object,

For each passed point of the tracked object, we take that point as the target position of the individuals of tracking group overlapping MAX times, and then update the target position of the tracking group to the current position of the tracked object, repeat PSO algorithm until the tracked object stop. For every first overlap after updating, the gbest and pbest are initialized as rational larger values for erasing the affect of the last target point.

Dynamic Object Tracking Algorithm Based on PSO

Step 1 Initialization
Iitialize the number of particle
the max number of group overlapping MAX;
the position of target point O_x, O_y, O_z;
threshold value th;
the arrange of each axis of original particle;
accelerate constant C_1, C_2;

Step 2 FOR each passed point of tracked object
WHILE（the overlapping number < MAX）DO
{
IF（the overlap related to this passed point is the first overlap）
THEN { Initialize global best value *gbest* and the every personal best value *pbest*, give them bigger values, such as 10000;}
FOR every particle
{
(1) Count the fitness value (new pbest) of the new position for every particle;
If new pbest >old pbest
Then pbest=new pbest;
(2) Change gbest according to updated pbest in (1);
(3) Update the speed of every particle, and limited them in V_{max};
(4) Update the position of every particle;
}
}

Step 3 Finish the path planning and output the generated pathes.

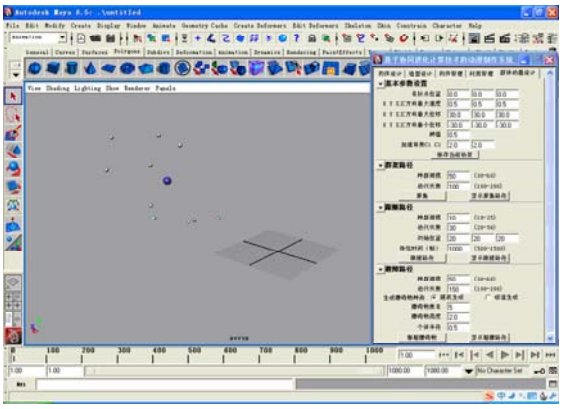


Figure 17. Initial state of dynamic object tracking

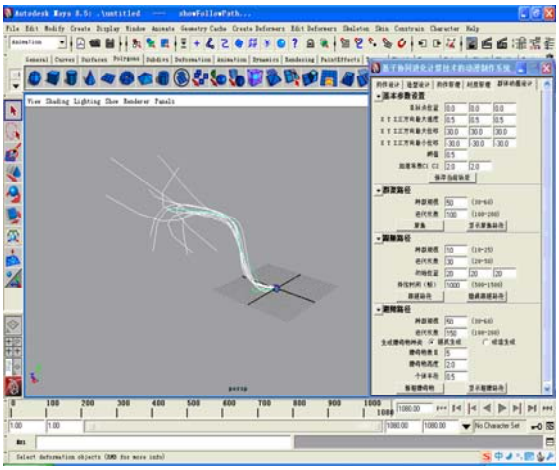


Figure 18. One generated tracking path

Figure 17 and figure 18 are simulated initial state and generative paths while figure 19 is a generated tracking image according to the generated path. If the different start position and target position are set, the different tracking points are produced and various tracking paths will be generated.

Figure 19. One genarated shark tracking image

D. Collision Avoidance

To run as a group, animals must remain in close proximity while avoiding collisions with other members of the group and with obstacles in the environment. Collisions frequently happened in a group action but we have to avoid their occurrence. For escaping collisions in path layout, after the radius and numbers of barriers are erected, two kinds of barriers are generated by randomly and grouping. These barriers locates in the area of the target point and the maximal shift of coordinate x ,y and z. Considering the cost of operations and requirement of real time, the following approach is presented for collision avoidance.

Suppose the radius of the collision object O is r, the current speed of particle i is v(vx,vy,vz) and current location is p(tx,ty,tz). The overlapping of this time can get the estimated next location p'(tx',ty',tz'). Counting the distance d between p' and the center of collision object O. If d< the distance from the center of O to the boundary of collision area，then the collision is possible happened. Therefore, the direction of particle should be changed and recount the next location.

The estimated next location p'(tx',ty',tz') is gotten by the following procedure.

Let vector $\vec{u}$ is the vector from the current position p of the particle i to the center of the collision object O and vector $\vec{k}$ is the vector from the current position p of the particle i to the estimated next position p'. The unit vector $\vec{o}$ should be coplanar with vector $\vec{u}$, $\vec{k}$ and perpendicular to $\vec{u}$. According to the right hand rule and the related rules for cross product, vector $\vec{t}$ and $\vec{m}$ are gotten.

$$\vec{t} = \vec{k} \times \vec{u} \tag{10}$$

$$\vec{m} = \vec{u} \times \vec{t} \tag{11}$$

Let $\vec{o} = \vec{m} / \left|\vec{m}\right|$ and the module of the speed

$\left|\vec{v}\right| = \sqrt{(vx^2 + vy^2 + vz^2)}$. By moving distance $\left|\vec{v}\right|$ from the unit vector $\vec{o}$, the next position p'(tx',ty',tz') is solved.

In figure 20, square frame denotes the collision object, and dashed line denotes the boundary of collision detection while triangle denotes the next position of the particle. We can see from figure 20, the next position of the particle i has entered the area of collision, and the moving direction and the next position should be changed.

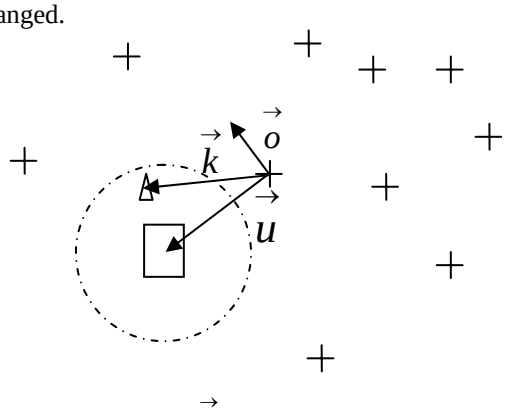


Figure 20. Unit vector $\vec{o}$ and the next position p'(tx',ty',tz')

Collision avoidance algorithm based on PSO

Step 1 Initialization
Initialize the number of particle
the max number of group overlapping MAX;
the position of target point O_x, O_y, O_z;
threshold value th;
the arrange of each axis of original particle;
accelerate constant C_1, C_2;

Step 2 WHILE（the overlapping number < MAX）DO
FOR every particle
{
(1) Count the fitness value (new pbest) of the new position for every particle;
If new pbest >old pbest
Then pbest=new pbest;
(2) Change gbest according to updated pbest in (1);
(3) Update the speed of every particle, and limited them in v_{max};
(4) Count the next position of the particle;
If (the position of the particle has entered the area of collision)
Then
Recount the next position of the particle
according to equation (10) and (11).
}

Step 3 Finish the path planning and output the generated pathes.

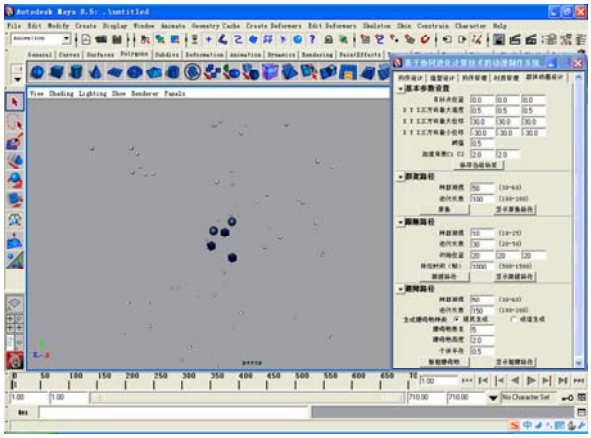


Figure 21. Initial state of collision avoidance

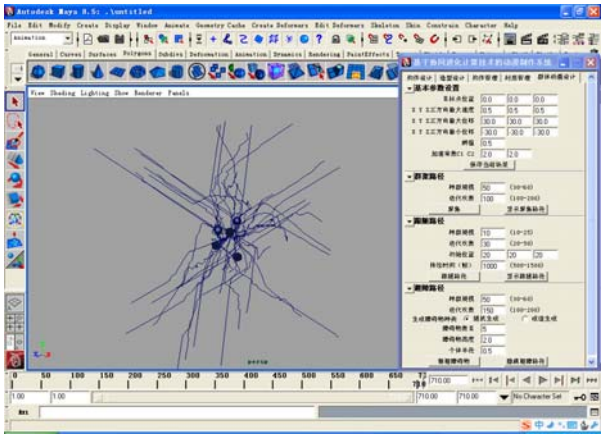


Figure 22. One generated collision avoiding path

Figure 21 and figure 22 are simulated initial state and generated paths according to collision avoidance paths. Figure 23 is a collision avoidance image according to generative path showing in figure 22. It shows that the algorithm can generate the collision avoidance paths successful.

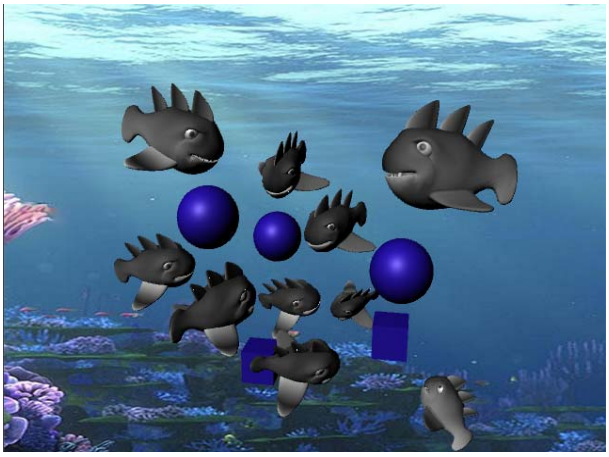


Figure 23. One collision avoidence image according to generative path

V. CONCLUSIONS

In this paper, we propose a role modeling approach based on dynamic self-adaptive genetic algorithm and a group path generating approach based on PSO algorithm for group animation. First, the backgrounds are studied. Second, a role modelling approach based on dynamic self-adaptive genetic algorithm and NURBS technology is put forward and a group of shark design example is illustrated for showing this modelling process. Third, a group path generative approach to simulates group behaviours is presented. The experiment was made in a simulation environment that is able to simulate the role modelling and path generation in animation produce process [19] . An animation named "Fancy Dress Party at the sea floor" has been made in this environment and the algorithms introduced in this paper has been practised .

Although looking simple, the approach emplores a feasible and useful way in an animation generation. It can enhance the fidelity and vitality of computer

animation, and reduce the work intensity of animators remarkably.

Future research will include: i) extending the work in this paper, to model the more complex role; ii) increasing in the system, the population characteristics for the customer classification and evaluation mechanisms for the animator's creation. These improvement will be studied in the very near future.

REFERENCES

[1] C. Reynolds, "Flocks, birds, and schools: a distributed behavioural model," *Computer Graphics*, vol.21, pp.25–34, 1987.

[2] X. Tu, D. Terzopoulos, "Artificial fishes: physics, locomotion, perception, behavior," In: *Proceedings of SIGGRAPH 1994*, pp. 43–50, NY, USA, 1994.

[3] D. C. Brogan, J. K. Hodgins, "Group behaviors for systems with significant dynamics," *Autonomous Robots*, vol. 4, pp. 137-153, 1997.

[4] S. LaValle, "Rapidly-exploring random trees: a new tool for path planning," *Technical Report TR98-11*, Dep. of Computer Science, Iowa State University, 1998.

[5] M. G. Choi, J. Lee, S. Y. Shin. "Planning biped locomotion using motion capture data and probabilistic roadmaps," *ACM Trans. Graph.* vol. 22, pp. 182–203, 2003.

[6] R. A. Metoyer, R.A., J. K. Hodgins, "Reactive pedestrian path following from examples," *The Visual Computer*, vol. 20, pp. 635–649, 2004.

[7] Q. Zhang, J. C. Ma, W. Xie, "A framed-quadtree based on reversed d* path planning approach for intelligent mobile robot," *Journal of Computers*, vol 7, pp. 464-469,2012.

[8] D. W. Gong, J. H. Zhang, Y. Zhang, "multi-objective particle swarm optimization for robot path planning in environment with danger sources," *Journal of Computers*, vol.6, pp. 1554-1561,2011.

[9] S. Rodríguez, J. M. Lien, N. M. Amato, "A framework for planning rotation in environments with moving obstacles," In: *IEEE/RSJ Inter. Conf. on Intelligent Robots and Systems*, pp. 3309-3314, November 2007.

[10] J. M. Lien, S. Rodríguez, J. P. Malric, N. M. Amato, "Shepherding behaviors with multiple shepherds," In: *Proceedings of the IEEE Inter. Conf. on Robotics and Automation*, pp. 3402-3407, 2005.

[11] C. Foudil, D. Noureddine, C. Sanza, Y. Duthen, "Path finding and collision avoidance in crowd simulation," *Journal of Computing and Information Technology*, vol. 3, pp. 217–228, 2009.

[12] R. Rodrigues, M. Paravisi, AdI. Bicho, L. P. Magalhães, C. R. Jung, S. R. Musse, "An interactive model for steering behaviors of groups of characters," *Applied Artificial Intelligence*, vol.24, pp. 594–616, 2010.

[13] A. I. Bicho et. al. "Simulating crowds based on a space colonization algorithm," *Computers & Graphics*, vol.36, pp. 70-79, 2012.

[14] S. R. Musse, C. R.Jung, J.C.S. Jacques, A. Braun, "Using computer vision to simulate the motion of virtual agents.," *Computer Animation and Virtual Worlds*, vol. 18, pp.83–93, 2007.

[15] S. R. Musse, V. J. Cassol, C. R. Jung, "Towards a quantitative approach for comparing crowds," *Computer Animation and Virtual Worlds*, vol. 23, pp. 49-57, 2012.

[16] S. Gao, Z. Y. Zhang, C. G. Cao, "Particle swarm optimization algorithm for the shortest confidence interval problem," *Journal of Computer*, vol. 7, pp.1809-1816, 2012.

[17] S. Song, B. Lu, L. Kong, J. J. Cheng, "A Novel PSO Algorithm Model Based on Population Migration Strategy and its Application,", *Journal of Computer*, vol. 6, pp. 280-287, 2011.

[18] H. Liu, S. J. Xu, "Group animation path generation based on particle swarm optimisation," In: *Proc. of the 14th Int. Conf. on CSCW in Design*, pp. 37-42, Fudan University, Shanghai, China, 2010.

[19] H. Liu, H. C. Yu, Y. Y. Li, Y. L. Sun, "A role modelling approach for crowd animation in a multi-agent cooperative system," In: *Proc. of the 15th Int. Conf. on CSCW in Design*, pp. 304-310, Lausanne, Switzerland, 2011.

Hong Liu was born in 1955, is now a Professor of computer science in the School of Information Science and Engineering, Shandong Normal University. She received PhD degree from the Chinese Academy of Sciences in 1998. Her main research interests include computational intelligence and cooperative design.

Yuanyuan Li was born in 1986. She received M.S. degree from Shandong Normal University, and now is a Ph.D. student in Tongji University. Her main research interests include evolutionary algorithm and group animation.

Hanchao Yu was born in 1986. He received M.S. degree from Shandong Normal University, and now is a Ph.D. student in the Chinese Academy of Sciences. His main research interests include evolutionary algorithm and group animation.

Quality Assessment for Stereoscopic Images by Distortion Separation

Chaozheng Hu, Feng Shao*, Gangyi Jiang, Mei Yu, Fucui Li, Zongju Peng
Faculty of Information Science and Engineering, Ningbo University, 315211, Ningbo, China
Email: shaofeng@nbu.edu.cn

***Abstract*—Quality assessment for stereoscopic images is a challenging issue in three-dimensional research. In this paper, we present an objective quality assessment method for stereoscopic images by distortion separation. In the method, we separate the distortion information for the distorted stereoscopic image (i.e., decompose the distorted stereoscopic image into restored and disturbed stereoscopic images), and use phase-amplitude description model and singular value decomposition model to evaluate them respectively. The experimental results show that compared with other schemes, the proposed method can achieve much higher consistency with the subjective assessments.**

***Index Terms*—stereoscopic image quality assessment, distortion separation, phase-amplitude description, singular value decomposition**

I. INTRODUCTION

With the great advancement of three-dimensional (3D) related technologies [1], 3D video [2] applications have drawn increasing attention in recent years. Since perceptual issue in 3D are completely different with that in 2D case, the necessity for designing 3D image quality assessment (3D-IQA) or stereoscopic image quality assessment (SIQA) approach is increasingly important [3].

In contrast to the 2D case, 3D quality of experience (QoE) needs to consider the various factors that contribute to the overall visual experience in 3D vision [4], e.g., depth perception, visual comfort, etc. Therefore, the direct use of 2D image quality assessment (2D-IQA) in measuring 3D image quality may not be straightforward, because the above perceptual attributes are not considered. A straightforward way of applying the state-of-the-art 2D-IQA methods to 3D-IQA is to evaluate the two views of the stereoscopic image and the estimated disparity map separately, and then combine them into an overall score. Boev *et al*. combined the monoscopic quality component and the stereoscopic quality component for developing a stereo-video quality metric [5]. Gorley *et al*. proposed a Stereo Band Limited Contrast (SBLC) algorithm to evaluate the stereoscopic image quality [6]. You *et al*. investigated the capabilities of some common 2D quality metrics, and integrated the disparity information into quality assessment [7]. Benoit *et al*. presented a linear combination for disparity distortion and the measurement of 2D image quality on both views [8]. However, the quality of stereoscopic image is not a simple combination of the qualities of left and right images, and it is not effective to assess the quality of disparity maps using 2D-IQA methods [9].

Many 3D-IQA methods were proposed by taking binocular properties into account. Maalouf *et al*. computed the cyclopean image from left and right images to simulate the brain perception, and used contrast sensitivity coefficients of cyclopean image as the basis of evaluation [10]. Jin *et al*. grouped the similar blocks from left and right views of stereoscopic image into a 3D stack, and evaluated the quality by 3D-DCT and considering contrast sensitive function and luminance masking [11]. Wang *et al*. proposed a metric by considering the binocular spatial sensitivity to reflect the binocular fusion and suppression properties [12], but the process of the binocular perception were not considered since only a weighted average of left and right views was used. Bensalma *et al*. proposed a Binocular Energy Quality Metric (BEQM) by modeling the simple cells responsible for the local spatial frequency analysis and the complex cells responsible for the generation of the binocular energy [13].

In general, distortion in an image will cause the following two cases: 1) losing some visual information; 2) adding some noticeable artifacts. Different types of quality degradation will have different influence on the perceptual quality. In this paper, we try to separate the distortion from the distorted stereoscopic image, and use different models to evaluate the restored and disturbed stereoscopic images respectively. The rest of the paper is organized as follows. Firstly, the proposed objective quality assessment metric is described in Section II. Then, experimental results are shown in Section III. Finally, conclusions and future work are given.

II. PROPOSED STEREOSCOPIC IMAGE QUALITY ASSESSMENT METRIC

The framework of the proposed quality assessment metric is illustrated in Fig.1. Given the original and distorted stereoscopic images (case of left and right images), the distorted image is first decomposed into a restored and a disturbed images by distortion separation strategy, and phase-amplitude description (PAD) model and singular value decomposition (SVD) model are used to measure their similarities with the original image respectively. Finally, binocular combination is made to get a total quality score.

doi:10.4304/jsw.9.1.37-43

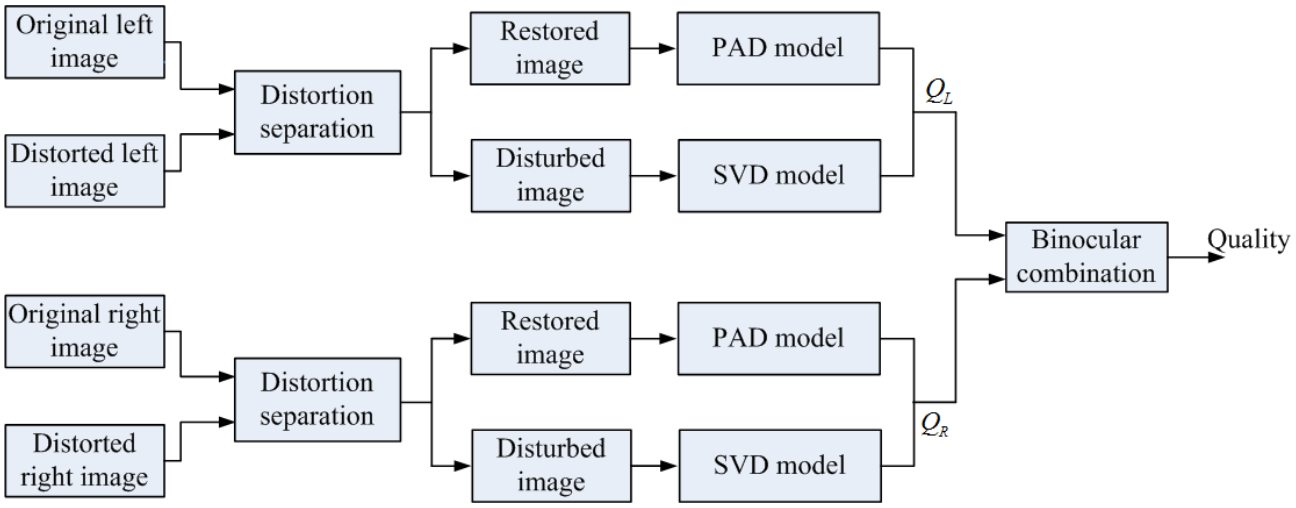


Figure 1. The framework of the proposed quality assessment metric.

A. Distortion Separation From Stereoscopic Image

It is known that distortion in image will cause two cases: 1) losing some visual information; 2) adding some noticeable artifacts. In this work, we classify the types of distortions into two group, information-loss distortion and artifact-additive distortion. Specifically, we separate the distorted image into a restored image and a disturbed image, and measure the detail and redundancy degradation. Firstly, considering that wavelet transform decomposes image into different frequency, we use discrete wavelet transform (DWT) to decompose the original and distorted images into a set of subbands. In this work, we adopt block-based image restoration in wavelet domain. Supposed that $D(\lambda,\theta,i,j)$ (8×8 block in the experiment) denotes the DWT coefficients on different scales and along different orientations of the (i,j)-th block of the distorted image (denoted by spatial scale index λ and orientation index θ), and $O(\lambda,\theta,i,j)$ denotes the corresponding DWT coefficients of the original image. The scale factors are given by [14]

$$k(\lambda,\theta,i,j)=clip(\frac{D(\lambda,\theta,i,j)}{O(\lambda,\theta,i,j)+10^{-30}},0,1) \tag{1}$$

The DWT coefficients of the restored image can be obtained by

$$R(\lambda,\theta,i,j)=\begin{cases}D(\lambda,\theta,i,j), & \theta=1\\ k(\lambda,\theta,i,j)\times O(\lambda,\theta,i,j), & otherwise\end{cases} \tag{2}$$

Since only DWT coefficients in the orientations ($\theta\neq1$) are restored, the detail information of the original image is preserved in the restored image while the added redundancy information is discarded.

The DWT coefficients of the redundancy image is obtained by

$$A(\lambda,\theta,i,j)=D(\lambda,\theta,i,j)-R(\lambda,\theta,i,j) \tag{3}$$

The disturbed image is described by

$$D'(\lambda,\theta,i,j)=O(\lambda,\theta,i,j)+A(\lambda,\theta,i,j) \tag{4}$$

Finally, the restored images and the disturbed images are generated by inverse-transforming their respective DWT coefficients. Fig.2 illustrates the results of the proposed separation method for different distortion types.

B. Quality Assessment Metric

For the restored image, the detail is preserved while the redundancy is discarded. Therefore, structural similarity between the original and restored images is expected to give a reasonable estimation of quality degradation. We get the local phase (LP) and local amplitude (LA) referring to the method in [15]. Then, the phase and magnitude similarities for each pixel in the left image are defined as

$$S_{LP}^{l}(x,y)=\frac{2\times LP^{(org)}(x,y)\times LP^{(res)}(x,y)+C_1}{LP^{(org)}(x,y)^2+LP^{(res)}(x,y)^2+C_1} \tag{5}$$

$$S_{LA}^{l}(x,y)=\frac{2\times LA^{(org)}(x,y)\times LA^{(res)}(x,y)+C_2}{LA^{(org)}(x,y)^2+LA^{(res)}(x,y)^2+C_2} \tag{6}$$

where C_1 and C_2 are constants to avoid the denominator being zero. Finally, the final quality score for the left image is obtained by summing the scores of all pixels

$$Q_{PAD}^{l}=\left(\frac{1}{H\times W}\sum_{y=1}^{H}\sum_{x=1}^{W}S_{LP}^{l}(x,y)\right)\cdot\left(\frac{1}{H\times W}\sum_{y=1}^{H}\sum_{x=1}^{W}S_{LA}^{l}(x,y)\right) \tag{7}$$

For the disturbed image, the redundancy information is added on the original image. Therefore, energy similarity between the original and restored images is used to measure the quality degradation. In this work, we use the singular values as feature basis for the task [16]. The energy change between the original and disturbed images in the singular values is calculated

$$\tau_k=\frac{\left\langle\left|\mathbf{S}_k^{(org)}-\mathbf{S}_k^{(res)}\right|\cdot\mathbf{S}_k^{(org)}\right\rangle}{\left\langle\mathbf{S}_k^{(org)}\cdot\mathbf{S}_k^{(res)}\right\rangle} \tag{8}$$

where $\mathbf{S}_k^{(org)}$ and $\mathbf{S}_k^{(res)}$ denote the singular value vectors of the original and restored images, respectively, and $\langle\cdot\rangle$ denotes the inner product. Finally, the final quality score for the left image is obtained by averaging the changes over all the blocks

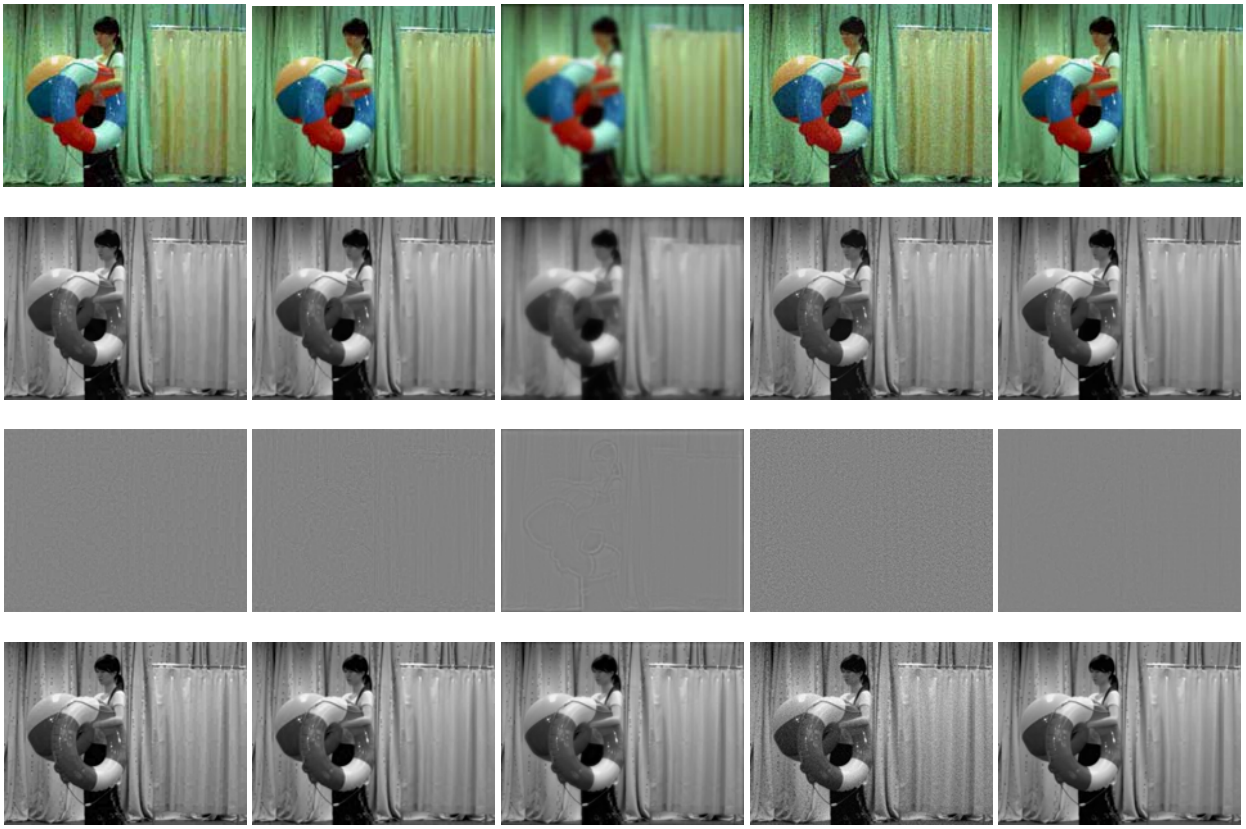


Figure 2. Results of the proposed separation method for different types of distortion, from top to bottom row: the distorted images, the restored images, the redundancy images, and the disturbed images. For left to right: JPEG, JPEG2000, Gaussian Blur, White Noise and H.264.

$$Q_{SVD}^{l} = \frac{1}{N_{\text{block}}} \sum_{k=1}^{N_{\text{block}}} \tau_k \tag{9}$$

Considering that the detail and redundancy losses in the distorted image are superimposed, the above two quality scores Q_{PA}^{l} and Q_{SVD}^{l} are combined into an overall score by a linear weighted sum method, i.e.,

$$\begin{aligned} Q_L &= w_1 \cdot Q_{PAD}^{l} + w_2 \cdot Q_{SVD}^{l} \\ s.t.\ & w_1 + w_2 = 1 \end{aligned} \tag{10}$$

where w_1 and w_2 are parameters used to adjust the relatively importance of redundancy adjunction and detail loss in the quality degradation. In this paper, the parameters can be determined by training. Similarly, the quality score Q_R for the right image can be measured by the same manner.

C. Binocular Combination

After having obtained the quality scores Q_L and Q_R, the next step is to combine the two quality scores into a final score. The direct way is to combine the quality scores Q_L and Q_R by average weighting. However, the weight-averaged method is not effective because binocular combination property is not well considered. In this work, we use two-stage gain control model to combine the two quality scores [17]

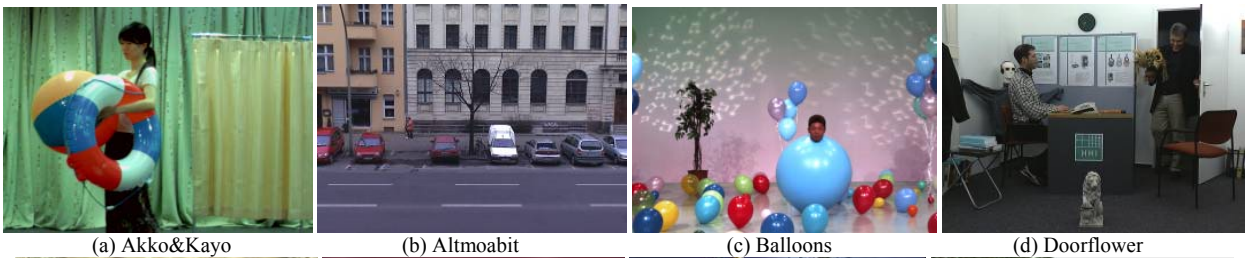
$$Q(L,R) = \frac{\left(Stage1(Q_L) + Stage1(Q_R)\right)^p}{z + \left(Stage1(Q_L) + Stage1(Q_R)\right)^q} \tag{11}$$

where $Stage1(Q_L) = \frac{(Q_L)^m}{s + Q_L + Q_R}$, $Stage1(Q_R) = \frac{(Q_R)^m}{s + Q_L + Q_R}$, and p, q, m, z are model parameters. In the experiment, the same parameter setting with [17] is used.

III. Experimental Results

A. Stereoscopic Image Quality Database

In the experiment, we have used the database presented in [18]. Twenty-six non-expert adult viewers were participated in the subjective evaluation of the database. According to Double Stimulus Continuous Quality Scale (DSCQS) testing method described in ITU-R recommendation BT.500-11, the subjective ratings for the distorted stereoscopic images were obtained on a scale of 0-10. The database includes 12 original stereoscopic image pairs, from which 312 distorted stereoscopic images are generated with five types of distortion: JPEG, JPEG2000, Gaussian Blur, White Noise and H.264. The symmetric distortions are added on left and right images. More specifically, there are 60, 60, 60, 60 and 72 distorted stereoscopic images in the database with JPEG, JPEG2000, Gaussian Blur, White Noise and H.264 distortions, respectively; there are different distortion levels for each distortion type. The corresponding differential mean opinion score (DMOS) values are



(a) Akko&Kayo (b) Altmoabit (c) Balloons (d) Doorflower

(e) Newspaper (f) Kendo (g) Xmas (h) Lovebierd1

Figure 3. Eight selected reference left images in the 3D database [18].

provided. Eight selected reference left images used in the database are shown in Fig.3.

B. Performance Determination

In the experiment, four commonly used performance indicators are employed to further evaluate the metric: Pearson linear correlation coefficient (PLCC), Spearman rank order correlation coefficient (SROCC), Kendall rank-order correlation coefficient (KROCC), and root mean squared error (RMSE), between the objective scores after nonlinear regression and the subject scores. Among these four criteria, SROCC and KROCC are employed to assess prediction monotonicity, and PLCC and RMSE are used to evaluate prediction accuracy. For a perfect match between the objective and subjective scores, PLCC=SROCC=KROCC=1 and RMSE=0. To obtain the relationship between the objective scores and the subjective scores, we use the nonlinear regression with four-parameter logistic function by

$$DMOS_p = \frac{\beta_1 - \beta_2}{1 + \exp(-(x - \beta_3)/\beta_4)} + \beta_2 \qquad (12)$$

where β_1, β_2, β_3 and β_4 are determined by using the subjective scores and the objective scores.

In the experiment, in order to determine the parameters w_1 and w_2, we select a subset of the database to train the parameters by optimizing the PLCC values between the objective and subjective scores. The final parameter determination results is w_1=0.9208, w_2=0.0792. It is obvious that the restored image is more important than the disturbed image in measuring the quality degradation.

C. Overall Assessment Performance

In order to evaluate the performance of the proposed scheme, we compare the evaluation results with two 2D-IQA metrics MSSIM [19], SVD [20], and one SIQA metric (named as Wang-SIQA) [12]. The former two schemes directly estimate the quality of each view separately and generate a weighted average score. The results of PLCC, SROCC, KROCC and RMSE are presented in Table I. From the table we can see that the proposed scheme outperforms the other schemes. For MSSIM and SVD metrics, since they are directly extended from the 2D case and do not take the binocular properties into account, the overall performance is far worse than the proposed scheme. For Wang-SIQA metric, even though it may be effective for some individual distortion types, the overall assessment performance is not very high; the reason is that uniform assessment is adopted for the left and right images, while in the proposed scheme, the similarity measured from the restored image and disturbed image respectively will have a good correspondence with the subjective scores. Fig.4 gives the scatter plots for the MSSIM, SVD and Wang-SIQA metrics. Fig.5 gives the scatter plots for the independent and overall distortion types for the proposed scheme, respectively. The vertical axis denotes the subjective ratings of the perceived distortions and the horizontal axis denotes the predicted objective scores. From the figures, the high accuracy fitting results show the effectiveness of the proposed scheme.

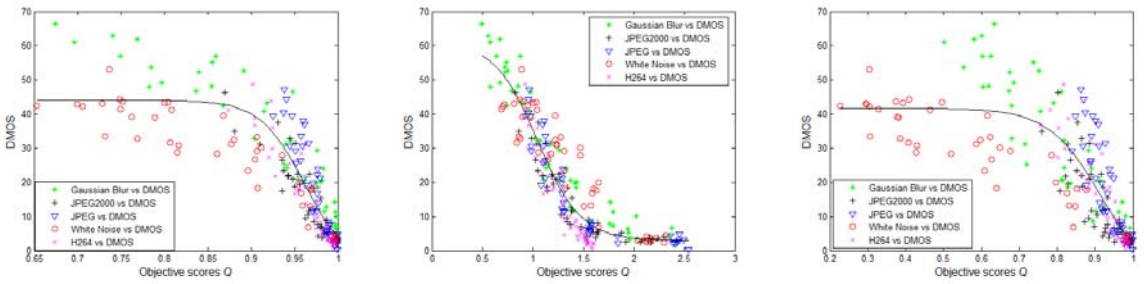
IV. Conclusions

This paper presents a quality assessment method for stereoscopic images by distortion separation. The prominent advantage of the proposed method is that we separate the distortion from the distorted stereoscopic image, and use different singular value decomposition (SVD) model and phase-amplitude description (PAD) model to evaluate the restored and disturbed stereoscopic images respectively. The experimental results show that the proposed method can achieve much higher consistency with the subjective assessments. In this research, only simple image separation model is used for stereoscopic image without considering the binocular characteristics. In the future work, more comprehensive study of various distortions affecting depth perception, visual comfort is needed, and these cues should be fully considered in the separation model.

TABLE 1.

PERFORMANCE COMPARISONS OF DIFFERENT SCHEMES .

Algorithms		Distortion types					
		JPEG	JP2K	GB	WN	H.264	All
PLCC	MSSIM[19]	0.9399	0.9256	0.9525	0.9486	0.9405	0.9028
	SVD[20]	0.9516	0.9523	0.9715	0.9417	0.9639	0.9295
	Wang-SIQA[12]	0.8837	0.8261	0.9221	0.9385	0.9097	0.8564
	Proposed	**0.9840**	**0.9599**	**0.9793**	**0.9564**	**0.9743**	**0.9348**
SROCC	MSSIM[19]	0.9340	0.9248	0.9607	0.9261	0.9314	0.9138
	SVD[20]	0.9443	0.9461	0.9645	0.8993	0.9568	0.9042
	Wang-SIQA[12]	0.8998	0.8737	0.9355	0.9088	0.9002	0.8887
	Proposed	**0.9849**	**0.9692**	**0.9741**	**0.9447**	**0.9637**	**0.9313**
KROCC	MSSIM[19]	0.7509	0.7616	0.8277	0.7535	0.7681	0.7307
	SVD[20]	0.7852	0.8439	0.7899	0.7091	0.8339	0.7271
	Wang-SIQA[12]	0.7044	0.6788	0.7731	0.7394	0.7205	0.6917
	Proposed	**0.9045**	**0.8566**	**0.8742**	**0.8020**	**0.8451**	**0.7709**
RMSE	MSSIM[19]	4.7399	4.2306	6.0480	4.7454	4.3388	7.0088
	SVD[20]	4.2663	3.4077	4.6954	5.0455	3.4038	6.0069
	Wang-SIQA[12]	6.4974	6.2955	7.6666	5.1829	5.3026	8.4101
	Proposed	**2.4706**	**3.1321**	**4.0169**	**4.4295**	**2.8802**	**5.7838**



(a) MSSIM[19] (b) SVD[20] (c) Wang-SIQA[12]

Figure 4. Scatter plots of objective scores vs. subjective scores for MSSIM, SVD and Wang-SIQA schemes.

ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of China (grant 61071120, 61271021, 612712700), and the Natural Science Foundation of Ningbo (grant 2012A610039).

REFERENCES

[1] A. Smolic, P. Kauff, S. Knorr, et al, "Three-dimensional video postproduction and processing," *Proceedings of the IEEE*, vol. 99, no. 4, pp. 607-625, April 2011.

[2] Peng Geng, He Jiang, Zhigang Zhang, et al, "A Video Denoising Method with 3D Surfacelet Transform Based on Block matching and Grouping," *Journal of Computers*, vol. 7, no. 5, pp. 1065-1066, 2012.

[3] H. T. Quan, P. Le Callet, M. Barkowsky, "Video quality assessment: from 2D to 3D – challenges and future trends," in *Proc. of IEEE International Conference on Image Processing*, pp. 4025-4028, Hong Kong, Sep. 2010.

[4] L. Goldmann, T. Ebrahimi, "Towards reliable and reproducible 3D video quality assessment," in *Proc. of SPIE: Three-Dimensional Imaging, Visualization, and Display*, vol. 8043, no. 804302, San Jose, California, USA, April 2011.

[5] A. Boev, A. Gotchev, K. Egiazarian, et al, "Towards compound stereo-video quality metric: a specific encoder-based framework," in *Proc. of IEEE Southwest Symposium on Image Analysis and Interpretation*, pp. 218-222, Denver, Colorado, 2006.

[6] P. Gorley, and N. Holliman, "Stereoscopic image quality metrics and compression," in *Proc. of SPIE: Stereoscopic Displays and Applications XIX*, San Jose, CA, USA, vol. 6803, no. 680305, 2008.

[7] J. You, L. Xing, A. Perkis, at al, "Perceptual quality assessment for stereoscopic images based on 2D image quality metrics and disparity analysis," in *Proc. of*

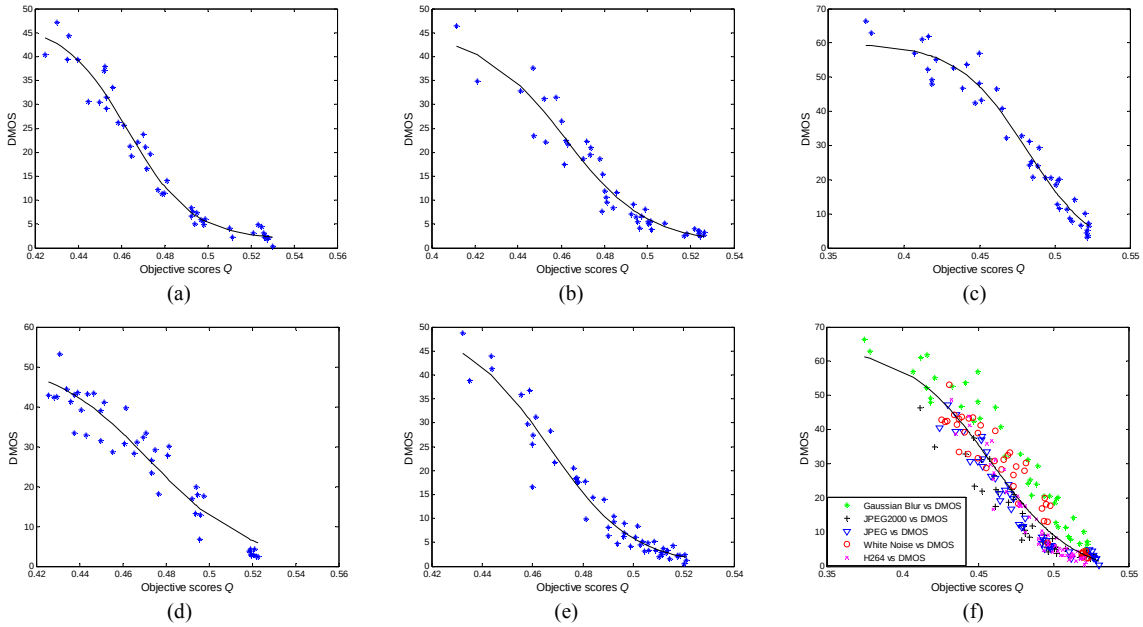


Figure 5. Scatter plots of objective scores vs. subjective scores for the proposed scheme: (a) JPEG; (b) JPEG2000; (c) Gaussian Blur; (d) White Noise; (e) H.264; (f) All distortions.

International Workshop on Video Processing and Quality Metrics for Consumer Electronics, Scottsdale, AZ, USA, 2010

[8] A. Benoit, P. Le Callet, P. Campisi, et al, "Using disparity for quality assessment of stereoscopic images," in *Proc. of IEEE Intentional conference on Image Processing*, pp. 389-392, San Diego, CA, USA, Oct. 2008.

[9] Yiyong Han, Jujun Zhang, Benkang Chang, et al, "Novel Fused Image Quality Measures Based on Structural Similarity," *Journal of Computers*, vol. 7, no. 3, pp. 563-566, 2012.

[10] A. Maalouf, M. C. Larabi, "CYCLOP: A stereo color image quality assessment metric," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1161-1164, Prague, Czech Republic, May 2011.

[11] L. Jin, A. Boev, A. Gotchev, et al, "3D-DCT based perceptual quality assessment of stereo video," in *Proc. of IEEE Intentional conference on Image Processing*, pp. 2521-2524, Brussels, Belgium, Sep. 2011.

[12] X. Wang, S. Kwong, Y. Zhang, "Considering binocular spatial sensitivity in stereoscopic image quality assessment," in *Proc. of IEEE Visual Communications and Image Processing*, Tainan City, Taiwan, Nov. 2011.

[13] R. Bensalma, M. C. Larabi, "A perceptual metric for stereoscopic image quality assessment based on the binocular energy," *Multidimensional Systems and Signal Processing*, to appear, 2012.

[14] S. Li, F. Zhang, L. Ma, et al, "Image quality assessment by separately evaluating detail losses and additive impairments," *IEEE Transactions on Multimedia*, vol. 13, no. 5, pp. 935-949, Oct. 2011.

[15] L. Zhang, L. Zhang, X. Mou, et al, "FSIM: a feature similarity index for image quality assessment," *IEEE Trans. on Image Processing*, vol. 20, no. 8, pp. 2378-2386, Aug. 2011.

[16] Yanfang Hou, Hongmei Feng. "Study of Modulation Recognition Algorithm Based on Wavelet Transform and Neural Network," *Journal of Computers*, vol. 6, no. 7, pp. 1511-1518, 2011.

[17] T. S. Meese, M. A. Georgeson, D. H. Baker, "Binocular contrast vision at and above threshold," *Journal of Vision*, vol. 6, no. 11, pp. 1224-1243, Oct. 2006.

[18] J. Zhou, G. Jiang, X. Mao, et al, "Subjective quality analyses of stereoscopic images in 3DTV system," in *Proc. of IEEE Visual Communications and Image Processing*, Tainan City, Taiwan, Nov. 2011.

[19] Z. Wang, A. C. Bovik, H. R. Sheikh, et al, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, April 2004.

[20] A. Shnayderman, A. Gusev, A. M. Eskicioglu, "An SVD-based grayscale image quality measure for local and global assessment," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 422-429, 2006.

Chaozheng Hu received his B.S.degree from Department of Computer and Information, Anqing Normal College, Anqing, China, in 2011. He is now working towards his M.S. degree in Ningbo University, Ningbo, China. His current research interests include image and video processing and stereoscopic image quality assessment.

Feng Shao received his B.S. and Ph.D degrees from Zhejiang University, Hangzhou, China, in 2002 and 2007, respectively, all in Electronic Science and Technology. He is currently an associate professor in Faculty of Information Science and Engineering, Ningbo University, China. His research interests include video coding, image processing and perception, etc.

Gangyi Jiang received his M.S. degree from Hangzhou University in 1992, and received his Ph.D. degree from Ajou University, Korea, in 2000. He is now a professor in Faculty of Information Science and Engineering, Ningbo University, China. His research interests mainly include video compression, multi-view video coding, etc.

Mei Yu received her M.S. degree from Hangzhou Institute of Electronics Engineering, China, in 1993, and Ph.D. degree form Ajou University, Korea, in 2000. She is now a professor in

Faculty of Information Science and Engineering, Ningbo University, China. Her research interests include video coding and video perception.

Fucui Li received her M.S. degree from Hefei University of Technology, China, in 2004. She is now pursuing the Ph.D degree at Ningbo University, China. Her research interests include video compression and communications, multi-view video coding and error concealing.

Zongju Peng received his B.S. degree in Computer science from Sichuan University, Chengdu, China, in 1998, and Ph.D. degree from Institute of Computing Technology, Chinese Academy of Science in 2010. He is currently an associate professor in Faculty of Information Science and Engineering, Ningbo University, China. His research concentrates on image/video compression.

UDS-FIM: An Efficient Algorithm of Frequent Itemsets Mining over Uncertain Transaction Data Streams

Le Wang [a,b,c], Lin Feng[b,c,*], and Mingfei Wu [b,c]
[a] College of Information Engineering, Ningbo Dahongying University, Ningbo, Zhejiang, China 315175.
[b] School of Computer Science and Technology, Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian, Liaoning, China 116024.
[c] School of Innovation and Experiment, Dalian University of Technology, Liaoning, China 116024.
lelewater@gmail.com; fenglin@dlut.edu.cn;merphy.wmf@gmail.com

***Abstract*—In this paper, we study the problem of finding frequent itemsets from uncertain data streams. To the best of our knowledge, the existing algorithms cannot compress transaction itemsets to a tree as compact as the classical FP-Tree, thus they need much time and memory space to process the tree. To address this issue, we propose an algorithm UDS-FIM and a tree structure UDS-Tree. Firstly, UDS-FIM maintains probability values of each transactions to an array; secondly, compresses each transaction to a UDS-Tree in the same manner as an FP-Tree (so it is as compact as an FP-Tree) and maintains index of probability values of each transaction in the array to the corresponding tail-nodes; lastly, it mines frequent itemsets from the UDS-Tree without additional scan of transactions. The experimental results show that UDS-FIM has achieved a good performance under different experimental conditions in terms of runtime and memory consumption.**

***Index Terms*—frequent itemset, frequent pattern, uncertain dataset, data streams, data mining**

I. INTRODUCTION

In recent years, frequent itemsets mining (FIM) on uncertain datasets [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] has been a topic in data mining with the emergence of uncertain datasets in many applications. For example, the locations of moving objects obtained through RFID or GPS are not precise; data obtained from wireless sensors are not precise. Table 1 shows an example of uncertain transaction dataset, each transaction of which represents that a customer might buy a certain product with a probability. For instance, the first transaction T_1 shows that a customer A might purchase products "C", "D" and "E" with 80%, 85% and 75% chances in near future. These probability values may be obtained by analysing the users' shopping records; for example, the data of transaction T_1 may be obtained by analyzing customer A's shopping history statistically and applying the probability of purchasing a certain product as the corresponding probability values of that item.

TABLE I.
AN EXAMPLE OF UNCERTAIN TRANSACTION DATASET

TID	Transaction itemset
T_1	(C, 0.8), (D, 0.85), (E, 0.75)
T_2	(B, 0.9), (C, 0.8) , (D, 0.6), (F, 0.2)
T_3	(A, 0.15), (B, 0.8) ,(D, 0.4)
T_4	(B, 0.85), (C, 0.6), (D, 0.7)
T_5	(A, 0.6), (B, 0.25), (C, 0.3), (E, 0.5)
T_6	(A, 0.7) , (B, 0.8), (D, 0.25)
T_7	(A, 0.65), (B, 0.7) , (C, 0.5)
T_8	(C, 0.5), (D, 0.65) , (F, 0.6)
T_9	(A, 0.6), (B, 0.82), (C, 0.63)

There have been many studies aimed at FIM on precise static datasets and data streams, such as Apriori [17], FP-Growth [18], H-Mine [19], DST [20], CPS [21], FP-Streaming [22], etc. However, these existing algorithms cannot mine frequent itemsets from uncertain transaction datasets. In the past few years, several algorithms [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] have been proposed for FIM on uncertain transaction datasets, among which [10, 11, 14] are for data streams and the others are for static datasets. The algorithms in [10, 11, 14] maintain the transaction itemsets information to a UF-Tree [8]; however a UF-Tree is not as compact as the original FP-Tree [18] and cannot efficiently maintain transaction itemsets in terms of memory space. Thus these algorithms require a large amount of computational time and memory space to process tree nodes.

In this paper, we propose a tree structure called UDS-Tree for maintaining uncertain transaction itemsets information. We also give a corresponding algorithm called UDS-FIM for mining frequent itemsets from the UDS-Tree without additional scan of transaction datasets.

This work was supported by National Natural Science Foundation of P.R. China (61173163, 51105052) and Liaoning Provincial Natural Science Foundation of China (Grant No. 201102037)
Corresponding Author: Lin Feng; E-mail: lelewater@gmail.com

doi:10.4304/jsw.9.1.44-56

UDS-FIM employs the sliding window model to process data streams. UDS-Tree is a tree as compact as the original FP-Tree. Meanwhile, UDS-FIM removes the obsolete data from the UDS-Tree through scanning a part of the UDS-Tree, instead of scanning the whole tree. The experimental results show that the proposed algorithm has a good performance.

The key contributions of this paper include:

- We propose a new tree structure named UDS-Tree for maintaining uncertain transaction itemsets information;
- We also give an algorithm named UDS-FIM for FIM over uncertain transaction data streams;
- Both sparse and dense datasets, including real-world and synthetic datasets, are used in our experiments to test the performance of the proposed algorithm.

The rest of this paper is organized as follows: Section 2 is the description of the problem and definitions; Section 3 describes related works; Section 4 describes our algorithm UDS-FIM; Section 5 shows the experimental results; Section 6 gives the conclusions.

II. Problem Definitions

In this section, we provide background information about FIM on uncertain transaction data streams. Assume a uncertain transaction data stream *UDS* (i.e. $UDS = \{T_1, T_2, \ldots, T_n, \ldots\}$) contains m distinct items (i.e. $I = \{i_1, i_2, \ldots, i_m\}$), and each transaction itemset t ($t \in UDS$) is represented as $\{x_1, p_1, x_2, p_2, \ldots, x_v, p_v\}$, where $\{x_1, x_2, \ldots, x_v\}$ is a subset of I and the decimal value p_u ($1 \le u \le v$) is called the existential probability of item x_u in the transaction itemset t (denoted as $p(x_u, t)$). An itemset containing k distinct items is called a k-itemset, and its length is k.

Definition 1 ([17]). The *support number* (*SN*) of an itemset X is the number of transaction itemsets containing X in a dataset.

Definition 2 ([8, 13]). The probability of an itemset X in a transaction itemset t is denoted as $p(X, t)$, and is defined by

$$p(X,t) = \prod_{x \in X, x \in t} p(x,t).$$

Definition 3([8, 13]). The *expected support number* (*expSN*) of an itemset X in an uncertain transaction dataset is the sum of its probability values in all transaction itemsets containing X, denoted as $expSN(X)$, and is defined by

$$expSN(X) = \sum_t p(X,t).$$

Definition 4 ([8, 13]). The *minimum expected support threshold minExp* is a predefined percentage of the total number of transactions (which is denoted as n), and then the *minimum expected support number* (*minExpSN*) is defined by

$$minExpSN = n \times minExp.$$

Assume a sliding window contains w batches of data, and each batch of data contains p transaction itemsets (i.e., a window contains $w*p$ transaction itemsets).

Definition 5. Thus, in the sliding window, the *minimum expected support number* (*minExpSN*) is defined by

$$minExpSN = w \times p \times minExp.$$

Definition 6. In a sliding window, an itemset X is called frequent itemset if its expected support number in the window is not less than *minExpSN*.

Frequent itemsets mining on uncertain data streams has two important processes: (1) Updating new data to the tree and removing the obsolete data from the tree; (2) Mining all frequent itemsets of the current sliding window according to the request of user.

III. Related Work

A. Frequent Itemsets Mining over Static Datasets

FP-Growth [18] is a classical pattern-growth algorithm for traditional FIM over precise datasets. Since the publication of FP-Growth, many well-known algorithms have been developed based on it to get better performance, such as FP-Streaming [22], UF-Growth [8] and SUF-Growth [14]; the UDS-FIM algorithm proposed in this paper is also based on FP-Growth for fast FIM on uncertain data streams.

FP-Growth utilizes a 2-step approach for this job: firstly, it finds all frequent 1-itemsets under the condition of k-itemset X ($k \ge 1$); secondly, it generates frequent (k+1)-itemsets using those frequent 1-itemsets and X. It maintains the transaction itemsets to a FP-Tree, thus it finds all frequent 1-itemsets under the condition of X by scanning the FP-Tree. FP-Tree is created with the following rules: (1) itemsets are rearranged in descending order of support numbers of items, and then are added to a FP-Tree; (2) itemsets will share the same node when the corresponding items are same.

The algorithms U-Apriori [13] and UF-Growth [8] are two representatives for FIM on static uncertain datasets. The algorithm U-Apriori is based on the algorithm Apriori [17] which is the first algorithm for FIM on precise transaction datasets and employs the level-wise method. It starts with finding all frequent 1-itemsets with one scan of dataset. Then in each iteration, it first generates candidate (k+1)-itemsets using frequent k-itemsets ($k \ge 1$), and then identifies real frequent (k+1)-itemsets from candidates with one scan of dataset. The iteration goes on until there is no new candidate. U-Apriori has a disadvantage: it generates candidates and requires multiple scans of datasets, so its time performance may become worse with the increase of the number of long transaction itemsets or decrease of the minimum expected support threshold. In 2011, Wang *et al.* [7] proposed the algorithm MBP based on Apriori for FIM on uncertain datasets. The authors proposed one strategy to speed up the calculation of the expected support number of a candidate itemset: MBP stops calculating the expected support number of a candidate itemset if the itemset can be determined to be frequent or infrequent in advance. MBP has a better performance than U-Apriori.

The algorithm UF-Growth [8] is based on FP-Growth [18] for FIM on uncertain datasets. It employs the

pattern-growth method with 2 scans of the dataset. In the first scan, it first finds all frequent 1-itemsets, arranges the frequent 1-itemsets in descending order of support numbers, and then maintains them in a header table. In the second scan, it first removes infrequent items from each transaction itemset, rearranges the remaining items of each transaction itemset in the order of the header table, and then adds the sorted itemset to a tree structure called UF-Tree. After the UF-Tree is created, UF-Growth can recursively create sub header tables and prefix (conditional) UF-Trees in the same manner as the FP-Growth algorithm.

Although UF-Growth needs just two scans of dataset, it still has a disadvantage: it needs a large amount of memory to store UF-Tree because it only merges nodes with the same item and the same probability, when transaction itemsets are added to the UF-Tree. For example, when these two transaction itemsets {A, 0.53, B, 0.70, C, 0.23} and {A, 0.55, B, 0.80, C, 0.23} are added to a UF-Tree by lexicographic order, they will not share the node "A" because the probabilities of item "A" are not equal in these two transactions. To overcome this issue, Leung *et al.* [4] proposed an approximate algorithm based on the algorithm UF-Growth. This approximate algorithm considers that the items with the same *k*-digit value after the decimal point have the same probability. For example, when these two transactions {A, 0.53, B, 0.70, C, 0.23} and {A, 0.55, B, 0.80, C, 0.23} are added to a UF-Tree by lexicographic order, they will share the node "A" if *k* is set as 1 because both probabilities of item "A" are considered to be 0.5; if *k* is set as 2, they will not share the node "A" because the probabilities of "A" in these two transaction are 0.53 and 0.55 respectively. The smaller *k* is set, the less memory the approximate algorithm requires. However, it still cannot build a tree as compact as the original FP-Tree; moreover, it may lose some frequent itemsets.

The algorithm CUFP-Mine [1] outperforms the U-Apriori and UF-Growth when a dataset just is sparse and the predefined threshold is high. It requires a large amount of computational time and memory when transaction itemsets are not short and the threshold is small.

B. Frequent Itemsets Mining over Data Streams

Judging by the mechanism of the window algorithm, three window models can be applied in FIM: sliding window model, landmark window model and damped window model. The window size in the sliding window model is fixed and is specified by user in advance. In the landmark window model, the start point of the window is fixed and is specified by user. The damped window model considers the current data more valuable than old data, so it assigns a weight value for each batch of data or each transaction, and the weight value decreases over time. How to choose the window model depends on the user's interest of the data: the damped window model is employed if the user is interested in historical data and more interested in current data than historical data; the sliding window model is employed if the user is interested in a current fixed-size data. The commonly used approach of mining continuous data streams is the *sliding window model* [2, 14, 20, 21, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32].

Several algorithms base their approaches on the algorithm FP-Streaming [22] which is for FIM over *precise* transaction data streams. FP-Streaming requires two parameters *PreMinsup* and *Minsup* (*PreMinsup* ≤ *Minsup*) that are the user specified minimum support numbers for a batch of data and a window data respectively. The algorithm first finds pre-frequent itemsets whose support numbers are not less than the value *PreMinsup* from each batch in the current window, and then it finds frequent itemsets (whose support numbers are not less than *Minsup*) from all pre-frequent itemsets of all batches in the current window. The FP-Streaming algorithm may lose some frequent itemsets and cannot handle uncertain data.

The algorithms proposed in papers [10, 11, 14] are for FIM over *uncertain* data streams. Based on the algorithms FP-Streaming and UF-Growth, Leung *et al.* [14] proposed two algorithms UF-Streaming and SUF-Growth. UF-Streaming employs the same method as the FP-Streaming: mining frequent itemsets using two minimum support numbers *PreMinsup* and *Minsup*. Thus UF-Streaming may lose some frequent itemsets and it also requires an extra data structure UF-Stream to maintain the pre-frequent itemsets of the current window. SUF-Growth is a precise algorithm and uses only a user specified minimum support number *Minsup*, it directly finds all frequent itemsets with support number that is not less than *Minsup* from a window, and does not lose any frequent itemsets. The algorithm SUF-Growth maintains data of a window to a UF-Tree by the following two rules: (1) each tree node of its UF-Tree contains two probability values and *w* support numbers; (2) when a new batch of data is coming, it first removes the obsolete batch of data from the tree and then adds new batch of data to it. If a user requests the frequent itemsets of the current window, it performs the frequent itemsets mining. Similar to the algorithm UF-Growth, the main weakness of SUF-Growth is that it requires a large amount of memory to store UF-Tree, thus it costs much memory and time to process the UF-Tree. The proposed algorithms in the paper [10, 11] employ the damped window model, but they still use the UF-Tree to maintain uncertain transaction itemsets information.

IV. THE PROPOSED METHOD

The proposed algorithm UDS-FIM mainly consists of three procedures: (1) creating a global UDS-Tree; (2) mining frequent itemsets from the global UDS-Tree; (3) removing the obsolete data from the global UDS-Tree. We describe some structures used by UDS-FIM in Section 4.1, give an example of the construction of a UDS-Tree in Section 4.2, elaborate the algorithm UDS-FIM with an example in Section 4.3, and discuss the method of removing obsolete data from the current window in Section 4.4.

A. Structure of a UDS-Tree

Definition 7. Let itemset $X = \{x_1, x_2, x_3, \ldots, x_u\}$ be a sorted itemset, and the item x_u is called *tail-item* of X. When the itemset X is added into a tree T in accordance with its order, the node on the tree that represents this tail-item is called as a *tail-node*; a node that has no children is called as a *leaf node*; a node that is neither a tail-node nor a leaf-node is called as a *normal node*.

Before a transaction itemset is added into a UDS-Tree, its corresponding probability values are appended to an array (we call it TPA, Transaction Probability Array). For example, Figure 2(a) shows a TPA which maintains the first 2 transaction probability values in Table 1; each element of TPA is called a sub-TPA.

The proposed algorithm UDS-FIM needs two kinds of tree structures: (1) global UDS-Tree, which maintains the transaction itemsets of data streams; (2) prefix UDS-Tree, which is used to maintain transaction itemsets having the shared prefix itemset.

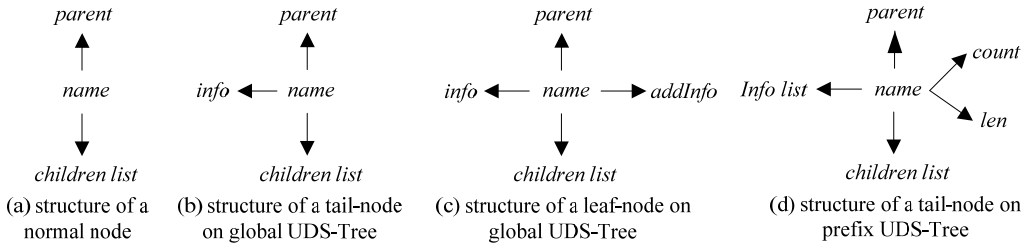


Figure 1. The structures of nodes on a UDS-Tree

The global UDS-Tree contains three kinds of nodes: normal node, tail-node and leaf-node. The structure of nodes is illustrated in Figure 1, where *name* is the item name of each node, *parent* represents the parent node of each node, and *children list* is a list of all the children node of a node. Figure 1(a) shows the structure of a normal node. Figure 1(b) and (c) show the structures of a tail-node and a leaf-node respectively, where field *info* and field *addInfo* include 3 sub-fields:

(1) ***count***: the support number of the node;

(2) ***len***: the length of itemsets;

(3) ***pro_ind***: w lists, containing the indexes of TPA of w batch data respectively (w is the width of the sliding window).

The field *addInfo* is only used when we need to mine the frequent itemsets of a current window, and is removed from the tree after the mining process.

Definition 8. Let T be a prefix tree of the itemset Y. When an itemset X containing itemset Y is added to the tree T, the probability of itemset Y in itemset X, $P(Y, X)$, is defined as the ***base probability*** of itemset X on the tree T.

The prefix UDS-Tree contains two kinds of nodes: normal node and tail-node. The structure of normal node is as same as that of a global UDS-Tree, as shown in Figure 1(a). The structure of tail-node is shown in Figure 1(d), where *info list* is a list of *info* and the *info* includes 3 sub-fields:

(1) ***bp***: w lists maintaining *base probability* values of w batch data respectively (w represents the width of the sliding window);

(2) ***pro_ind***: w lists maintaining the indexes of each TPA of w batch data respectively;

(3) ***item_ind***: a list maintaining the indexes of all items of a path in sub-TPA.

B. Construction of a Global UDS-Tree

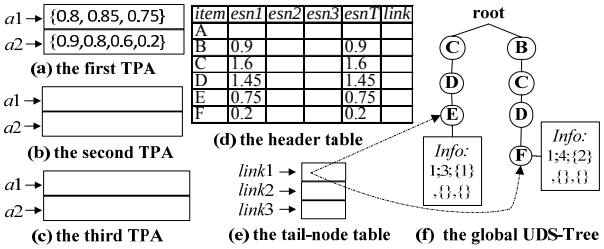


Figure 2. Processing the first batch of data

We illustrate the construction of a global UDS-Tree using the transaction itemsets in Table 1. Assume each window contains 3 batches of data, and each batch contains 2 transaction itemsets.

Before construction the UDS-Tree with the transaction itemsets, first create the following 4 data structures and initialize them as null:

(1) TPA: we need 3 TPAs for maintaining the transaction probability values of 3 batch of data in a current window, as shown in Figure 2(a)-(c);

(2) Header table: the header table contains 6 fields (*item* is the item name; *esn1*, *esn2* and *esn3* are the expected support number of 3 batches data of the current window, respectively; *senT* is the expected support number of the current window; *link* records all nodes of a corresponding item on a tree, but it is not shown in the Figures for simplicity.), as shown in Figure 2(d);

(3) Tail-node table: the tail-node table maintains the tail-nodes of each batch of data in the current window, as shown in Figure 2(e);

(4) Global UDS-Tree: the root of which is initially set as null.

Then process each transaction itemset by the following steps:

Step 1: The probability values of all items in a transaction itemset are stored to a TPA. For example, the TPA in Figure 2(a) maintains the probability values of the first batch of data; *a1* and *a2* in Figure 2(a) correspond to

the probability values of the first transaction and the second transaction of the first batch of data, respectively.

Step 2: The transaction itemset is added to a global UDS-Tree. For example, the global UDS-Tree in Figure 2(f) is the result after adding the first batch of data; the nodes "E" and "F" are 2 tail-nodes; as for the values of the *info* field (such as "1;3;{1};{};{}" of node "E"): the first value represents the support number, the second value is the length of the itemset, and the values in the 3 braces ({}) represent the corresponding indexes in the TPA of each batch of data in the current window (e.g. "1" in the first braches on node "E" represents the first row *a1* of the first TPA in Figure 2(a)).

Step 3: The expected support number and *link* information of each item are maintained to the header table. For example, the header table in Figure 2(d) maintains the header information of the first batch of data (*link* is not shown in the Figures for simplicity).

Step 4: Each new tail-node of each batch of data is maintained to a tail-node table. For example, *link1* of the tail-node table in Figure 2(e) links to all tail-nodes of the first batch of data.

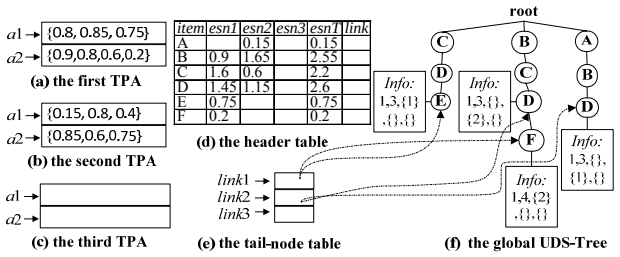


Figure 3. The result of processing the first two batches of data

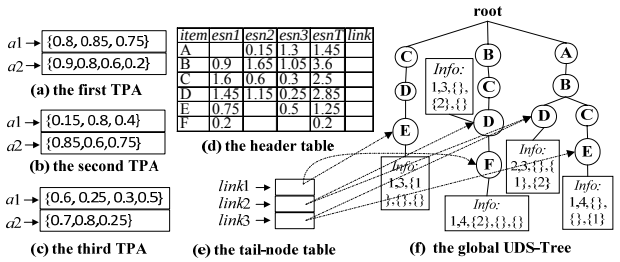


Figure 4. The result of processing the first 3 batches of data

Figure 3 is the result after the first 2 batches of data are processed. When the second transaction ((B, 0.8), (C, 0.5), (D, 0.55)) of the second batch is added to the global UDS-Tree, the node "D" on the path "root-B-C-D-F" become a tail-node, as shown in Figure 3(f).

Figure 4 is the result after the first 3 batches of data are processed. When the second transaction of the third batch of data is added to the global tree, we just update the information on the existing tail-node "D" of the path "root-A-B-D", as shown in Figure 4(f).

When the global UDS-Tree contains 3 batches of data, frequent itemsets mining operation can be performed if frequent itemsets are needed.

Input: A UDS-Tree ***T***, a global header table ***H***, and a minimum expected support number ***minExpSN***.
Output: FIs (frequent itemsets)
(1) Add the information on ***info*** field on each leaf-node to the field ***addInfo***;
(2) **For each** item *x* in *H* (from the last item) **do**
(3) **If**(*x.esnT*≥*minExpSN*) //*x.esnT* is from the header table *H*
(4) Generate an itemset $X = x$;
(5) Copy *X* into FIs;
(6) Create a header table H_x for *X*;
(7) **If**(H_x is not empty)
(8) Create a prefix UDS-Tree T_x for *X*;
(9) **Call SubMining**(T_x, H_x, *X*)
(10) **End if**
(11) **End if**
(12) Pass the information of *addInfo* field to parent nodes;
(13) **End for**
(14) **Return** FIs**.**

SubProcedure **SubMining** (T_x, H_x, *X*)
(15) **For each** item *y* in H_x (from the last item) **do**
(16) Generate an itemset $Y = X \cup y$;
(17) Copy *Y* into FIs;
(18) Create a header table H_y for *Y*;
(19) **If**(H_y is not empty)
(20) Create a prefix UDS-Tree T_y for *Y*;
(21) **Call SubMining**(T_y, H_y, *Y*)
(22) **End if**
(23) Pass the information of *info list* field to parent nodes;
(24) **End for**

Figure 5. Mining frequent itemsets from a global UDS-Tree

C. Mining Frequent Itemsets from the Current Window

1) The mining algorithm

The algorithm UDS-FIM employs the pattern-growth approach like the algorithm FP-Growth for mining frequent itemsets. The main differences between UDS-FIM and FP-Growth lie in their tree structures and the information maintained in their header tables. The detailed mining algorithm is shown in Figure 5.

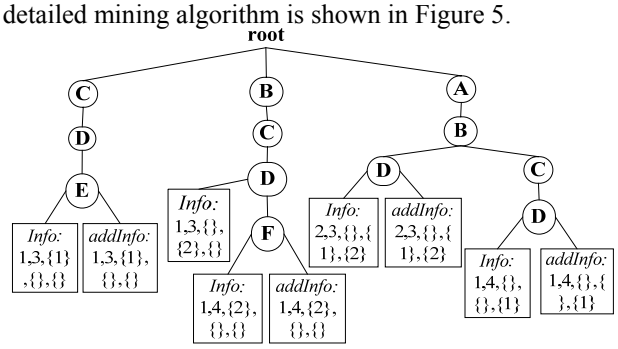


Figure 6. Adding a field addInfo on each leaf-node

Because the probability information on the global UDS-Tree is used not only for the current window, but also for subsequent windows, it cannot be modified when the frequent itemsets is being mining. But the algorithm UDS-FIM needs to modify the probability information when it mines frequent itemsets. So we add a field on each leaf-node to maintain the total probability information of its path (name this field as *addInfo*, as in line 1 in Figure 5); see Figure 6.

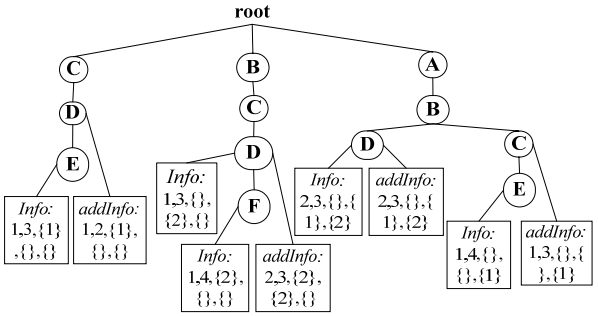


Figure 7. After passing field addInfo on leaf-nodes "E" and "F" to parent nodes

After the *addInfo* field on each node (we denote it as *AI*) is processed, it is passed to its parent node according to the following procedures if the parent node is not root (and if the parent node is root, just set *AI* as null.):

(1) If the parent node contains an *addInfo* field (we denote it as *PAI*), add the support number to *PAI* and copy *pro_ind* of *AI* to the existing *PAI*; otherwise pass *AI* to the parent node and perform the next procedure.

(2) If the parent node contains field *info*, add the support number in *info* to the field *addInfo* and copy *pro_ind* of *info* to the *addInfo* field. For example, Figure 7 is the result after passing *addInfo* on leaf-nodes "E" and "F" in Figure 6 to corresponding parent node.

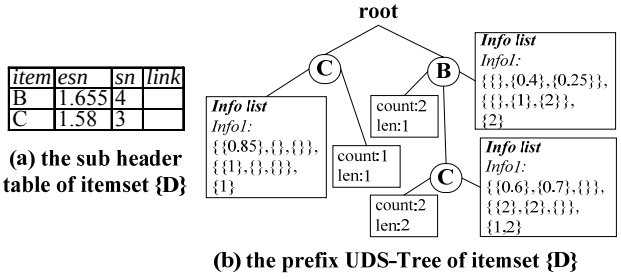


Figure 8. The prefix UDS-Tree of itemset {D}

The structure of a prefix UDS-Tree is different from that of a global UDS-Tree. We illustrate steps of creating a prefix UDS-Tree by an example. When the item "D" in the header table in Figure 4(d) is processed, all nodes "D" contains the field *addInfo*, as shown in Figure 7. There are 3 branches containing node "D". First, a sub header table for the itemset {D} is created by scanning these 3 branches and their probability information on 3 nodes "D". Figure 8(a) shows the sub header table of the itemset {D} which only contains items whose *esn* (expected support number) are not less than 1.5. Second, a prefix UDS-Tree needs to be created because there is more than one item in the sub header table. The prefix UDS-Tree is created by the following steps:

Step 1: Retrieve the first path "root-C-D" containing the node "D" and its probability information *addInfo*, and process the itemset {C} on this path by the following Substeps:

Substep1.1: Insert the itemset {C} to a prefix UDS-Tree which root is initially set as null;

Substep1.2: Append the probability information to the tail-node of the itemset {C}; the result is the path "root-C" in Figure 8(b). "{{1},{},{}}" on the tail-node "C" maintains the *pro_ind* information; "{{0.85},{},{}}" maintains the *bp* information, e.g., "0.85" is the probability of the itemset {D} in the first transaction of the first batch; "{1}" maintains the *item_ind* information, e.g., "1" shows that item "C" is the first element in the corresponding transactions.

Step 2: Retrieve the second path "root-B-C-D" and its probability information *addInfo*, and process the itemset {BC} on this path by the following Substeps:

Substep2.1: Insert the itemset {BC} to the prefix UDS-Tree;

Substep2.2: Append the probability information which is obtained from *addInfo* to the tail-node "C" of the itemset {BC}; the result is the path "root-B-C" in Figure 8(b). On the node "C" of the path "root-B-C", "{{2},{2},{}}" maintains the *pro_ind* information (two "{2}" represent the second row of the first TPA and the second TPA respectively); "{{0.6},{0.7},{}}" maintains the *bp* information, e.g., "0.6" and "0.7" are the probability values of the itemset {D} in the second transaction of the first batch and the second batch, respectively; "{1,2}" maintains the *item_ind* information, e.g., "1" and "2" represent that items "B" and "C" is the first and second element in corresponding transaction respectively.

Step 3: Retrieve the third path "root-A-B-D" and its probability information *addInfo*, and process the itemset {AB} on this path by the following Substeps:

Substep3.1: Remove the item "A" that is not in the sub header table from the itemset;

Substep3.2: Insert the itemset {B} to the prefix UDS-Tree and maintains its probability information on its tail-node "B"; the result is the path "root-B" in Figure 8(b).

2) An example of mining frequent itemsets

The global tree in Figure 4(f) is used as an example here to illustrate the detailed process of mining frequent itemsets. The minimum expected support number is set to 1.5. The following are the detailed steps:

Step 1: Add the probability information on field *info* of each leaf-node to the field *addInfo* of each leaf-node, as shown in Figure 6;

Step 2: Orderly process the items "F" and "E" in the global header table in Figure 4(d) by the following Substeps:

Substep2.1: Because expected support numbers of items "F" and "E" are less than 1.5, the field *addInfo* on nodes "F" and "E" are passed to their parent node, the result is shown in Figure 7.

Step 3: Process the item "D" in the global header table in Figure 4(d) by the following Substeps:

Substep 3.1: Append item "D" to a *base-itemset* (which is initialized as null; and each new base-itemset is a frequent itemset), because the expected support number of item "D" is not less than 1.5;

Substep 3.2: Create a sub header table for the base-itemset {D} by scanning those paths containing node "D"; the sub header table is shown in Figure 8(a) ;

Substep 3.3: Create a prefix UDS-Tree for the base-itemset {D} by scanning those paths containing node "D" because the sub header table contains more than one items; the prefix tree is shown in Figure 8(b);

Substep 3.4: Mining the prefix tree in Figure 8(b):

Firstly process the item "C" in the header table in Figure 8(a). (1) Append the item "C" to the current base-itemset and get a new frequent itemset {DC}; (2) Create a sub header table for the current base-itemset {DC} by scanning the paths containing node "C" in Figure 8(b); and the sub header table is null; (3) Remove the item "C" from the current base-itemset.

Secondly process the item "B" in Figure 8(a) and get a new frequent itemset {DB}; do not need to create a prefix tree because the new sub header table is null.

Substep 3.5: Remove the item "D" from the current base-itemset.

Substep 3.6: Pass the field *addInfo* on nodes "D" to its parent node.

Step 4: Process the item "C" in the global header table in Figure 4(d) by the following Substeps:

Substep 4.1: Append the item "C" to the current base-itemset and get a new frequent itemset {C};

Substep 4.2: Create a sub header table for the base-itemset {C}; the result of the sub header table is null.

Substep 4.3: Pass the field *addInfo* on nodes "C" to its parent node.

Step 5: Process the remaining items in header table in Figure 4(d), and get one new frequent itemset {B}.

The first window of the dataset in Table 1 contains 5 frequent itemsets: {D}, {DC}, {DB}, {C} and {B}.

D. Removing Obsolete Data

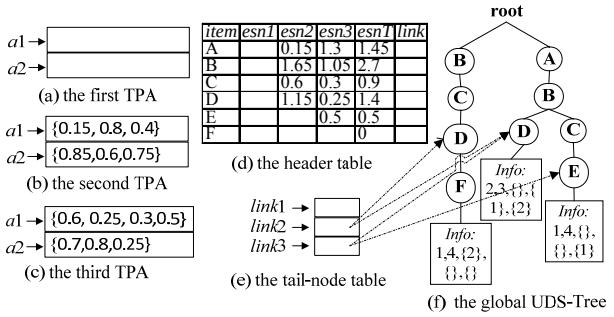


Figure 9. After removing the first batch of data

The tail-node table (see in Figure 4(e)) maintains all tail-nodes of each batch of the current window. When obsolete batch of data need removing, the useless nodes can be removed from the global UDS-Tree by scanning all tail-nodes of the obsolete batch of data.

For example, as shown in Figure 4(f), when the first batch of data are removed from the tree, there are two tail-nodes: the node "E" on path "root-C-D-E" and the node "F" on path "root-B-C-D-F". The path "root-C-D-E" can be removed because the node "E" on this path has no children and there is no other tail-node on this path. When processing the node "F", just one node "F" is removed because its parent node is a tail-node. After removing the obsolete data from the global tree, clear the first TPA and *link1* on the tail-node table for the coming data. After removing the first batch of data, the result is shown in Figure 9.

V. EXPERIMENTS

In this section, we evaluate the performance of the proposed algorithm UDS-FIM. In our experiments, we also implemented a variant of the algorithm MBP to mine uncertain data stream and denote the revision algorithm as UDS-MBP. We compare the algorithm UDS-FIM with the state-of-the-art algorithms SUF-Growth and UDS-MBP on both types of datasets: the sparse transaction datasets and dense transaction datasets. These three algorithms were written in Java programming language. The configuration of the testing platform is as follows: Windows 7 operating system (64bit), 4G memory, Intel(R) Core (TM) i3-2100 CPU @ 3.10 GHz; Java heap size is 2G.

Table 2 shows the characteristics of 4 datasets used in our experiments. "|D|" represents the number of transactions; "|I|" represents the total number of distinct items; "ML" represents the mean length of all transaction itemsets; "SD" represents the degree of sparsely or density. The real-world datasets *connect* and *kosarak* were obtained from FIMI Repository [33]. The dataset *connect* is a well-known dense dataset whose degree of density is 33.33%; moreover, the length of each transaction itemset is very long, i.e., 43. The dataset *kosarak* is a sparse dataset whose degree of sparsely is 0.02%; it contains 990K transaction itemsets and is a large dataset. The synthetic datasets *T10I4D100k*, and *T20I6D100K* came from the IBM Data Generator [17]. Since these four original datasets do not provide probability values for each item of each transaction itemset, as suggested by literatures [4, 8, 15], we assign a randomly generated existential probability of range (0, 1] to each item of each transaction itemset. The runnable programs and testing datasets can be downloaded from the Google Code repository at http://code.google.com/p/uds-tree/downloads/list.

TABLE II.
DATASET CHARACTERISTICS

Dataset	|D|	|I|	ML	SD (%)	Type
connect	67,557	129	43	33.33	dense
kosarak	990,002	41271	8	0.02	sparse
T10I4D100K	100,000	870	10	1.16	sparse
T20I6D100K	100,000	980	20	2.03	sparse

TABLE III.
EXPERIMENTAL PARAMETERS

Parameters	***Description***
min_exp	minimum expected support threshold
w	window size: number of batches in a window (#)
p	batch size: number of transactions in a batch (K)

The algorithms UDS-FIM, SUF-Growth and UDS-MBP can mine all frequent itemsets from a dataset, so the main performance measures used in this paper are *running time* and *memory size*. The experimental parameters are listed in Table 3, and the parameter values are chosen according to the characteristics of the datasets.

A. Evaluation on varied minimum expected support threshold

In this section, we illustrate the performance of the proposed algorithm under varied *minimum expected support threshold* while the window size and batch size are fixed.

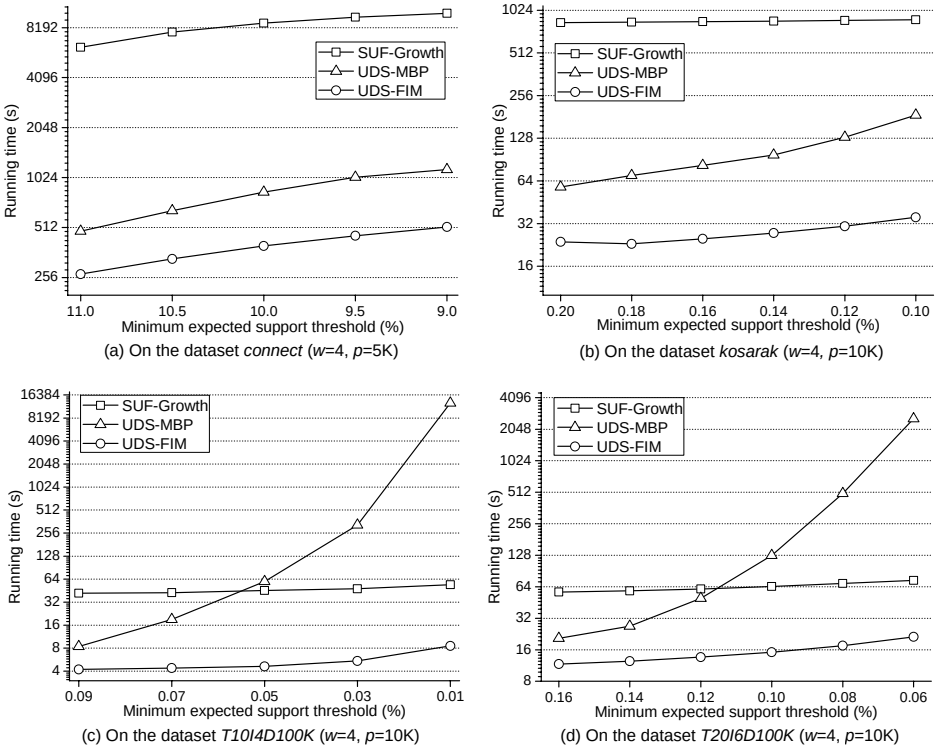
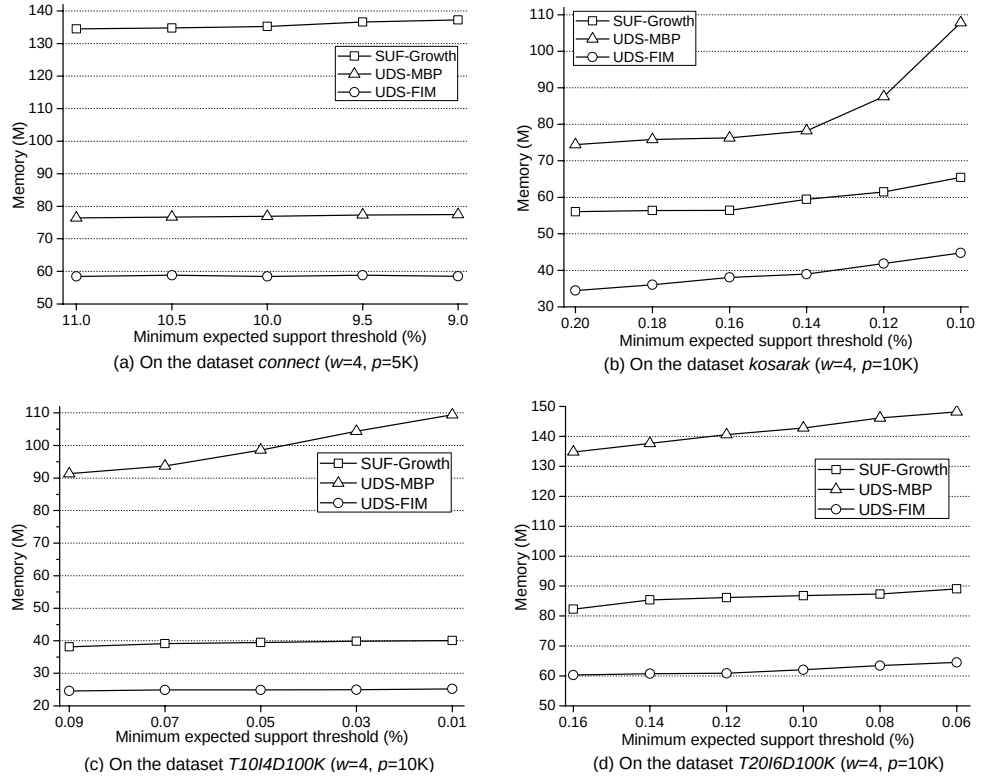


Figure 10. Runtime under varied minimum expected support threshold

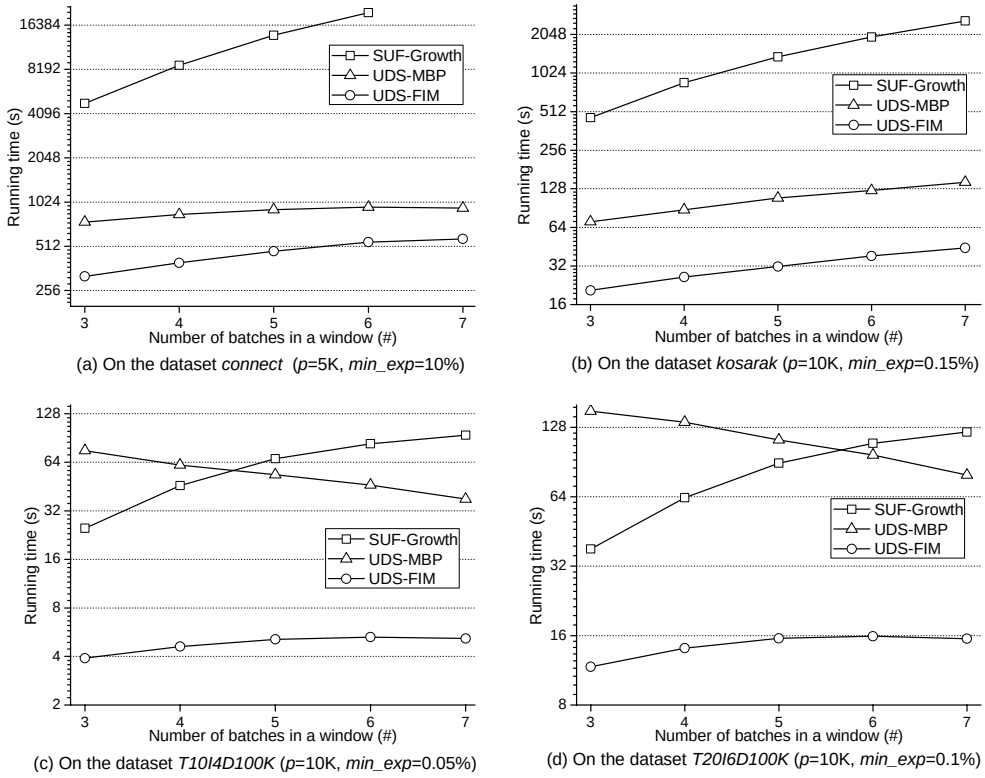
Because the dataset *connect* is more dense than the other three datasets, the number of transactions in each batch data is set as 5000 for *connect*, and it is set as 10000 for the other three datasets; the datasets *connect*, *kosarakt*, *T10I4D100K* and *T20I6D100K* are divided into 13, 99, 10 and 10 batches, respectively. On these four datasets, mining operation was performed on 10, 96, 7 and 7 consecutive windows respectively. Figure 10 shows runtime comparison of the algorithms UDS-FIM, SUF-Growth and UDS-MBP; Figure 11 compares the memory usage on four datasets under different minimum expected support thresholds. In this case, UDS-FIM has achieved the best performance among three algorithms. The reason is that the number of tree nodes generated by UDS-FIM is less than that by SUF-Growth (especially on real-world datasets) and that UDS-MBP generates too many candidates; for example, SUF-Growth generates 43732G tree nodes while UDS-FIM generates 443G tree nodes, and UDS-MBP generates 314086 candidates (on *connect* with *w*=4, *p*=5000, *min_exp*=9%). As the minimum expected support threshold decreases, the number of candidate itemsets generated by UDS-MBP sharply

increases on synthetic datasets. This leads to the sharp increase of running time of UDS-MBP, as shown in Figure 10.



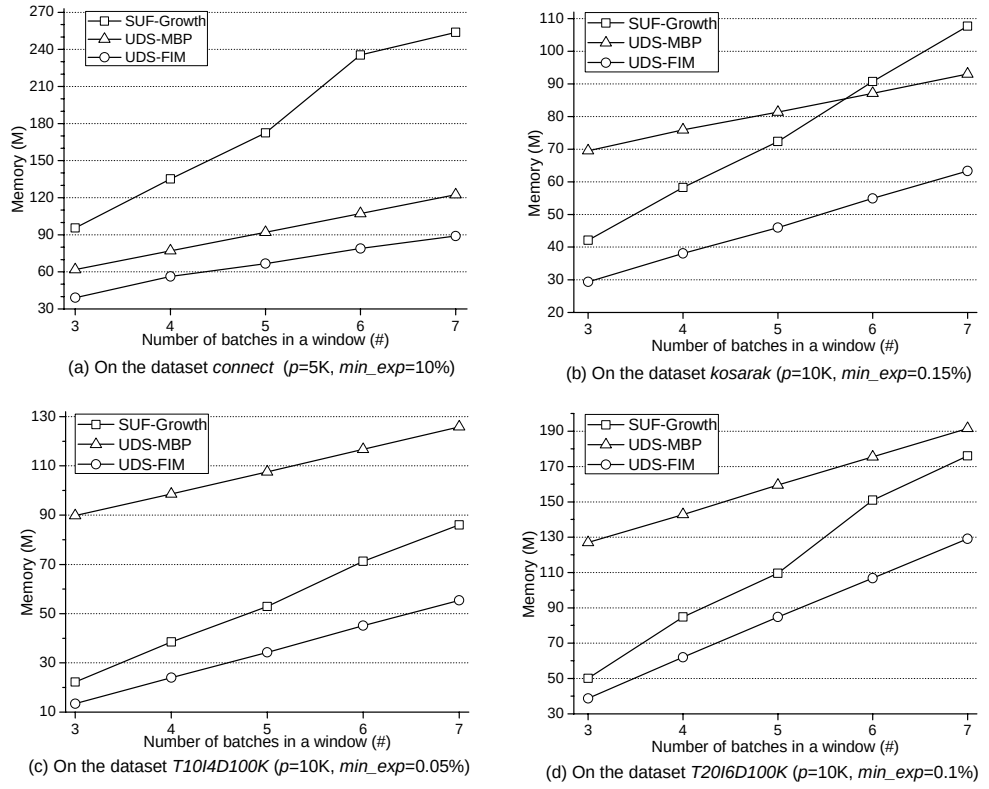
(a) On the dataset *connect* (*w*=4, *p*=5K)
(b) On the dataset *kosarak* (*w*=4, *p*=10K)
(c) On the dataset *T10I4D100K* (*w*=4, *p*=10K)
(d) On the dataset *T20I6D100K* (*w*=4, *p*=10K)

Figure 11. Memory under varied minimum expected support threshold



(a) On the dataset *connect* (*p*=5K, *min_exp*=10%)
(b) On the dataset *kosarak* (*p*=10K, *min_exp*=0.15%)
(c) On the dataset *T10I4D100K* (*p*=10K, *min_exp*=0.05%)
(d) On the dataset *T20I6D100K* (*p*=10K, *min_exp*=0.1%)

Figure 12. Runtime under varied window size



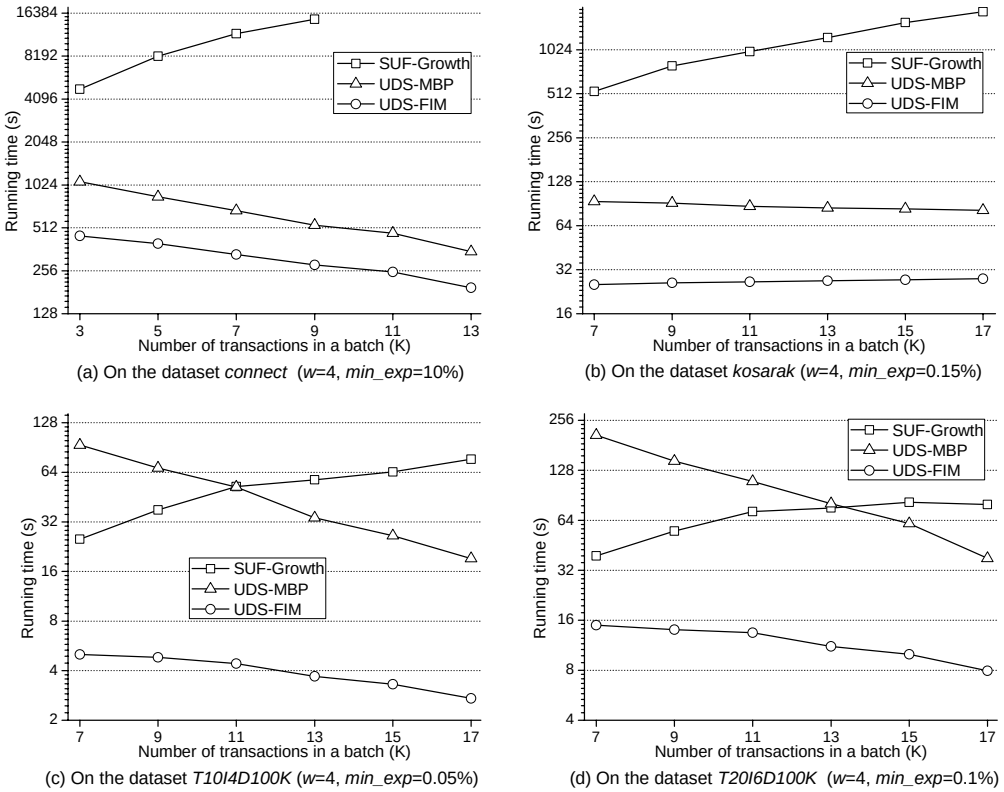
(a) On the dataset *connect* (*p*=5K, *min_exp*=10%)

(b) On the dataset *kosarak* (*p*=10K, *min_exp*=0.15%)

(c) On the dataset *T10I4D100K* (*p*=10K, *min_exp*=0.05%)

(d) On the dataset *T20I6D100K* (*p*=10K, *min_exp*=0.1%)

Figure 13. Memory under varied window size



(a) On the dataset *connect* (*w*=4, *min_exp*=10%)

(b) On the dataset *kosarak* (*w*=4, *min_exp*=0.15%)

(c) On the dataset *T10I4D100K* (*w*=4, *min_exp*=0.05%)

(d) On the dataset *T20I6D100K* (*w*=4, *min_exp*=0.1%)

Figure 14. Evaluation under varied batch size

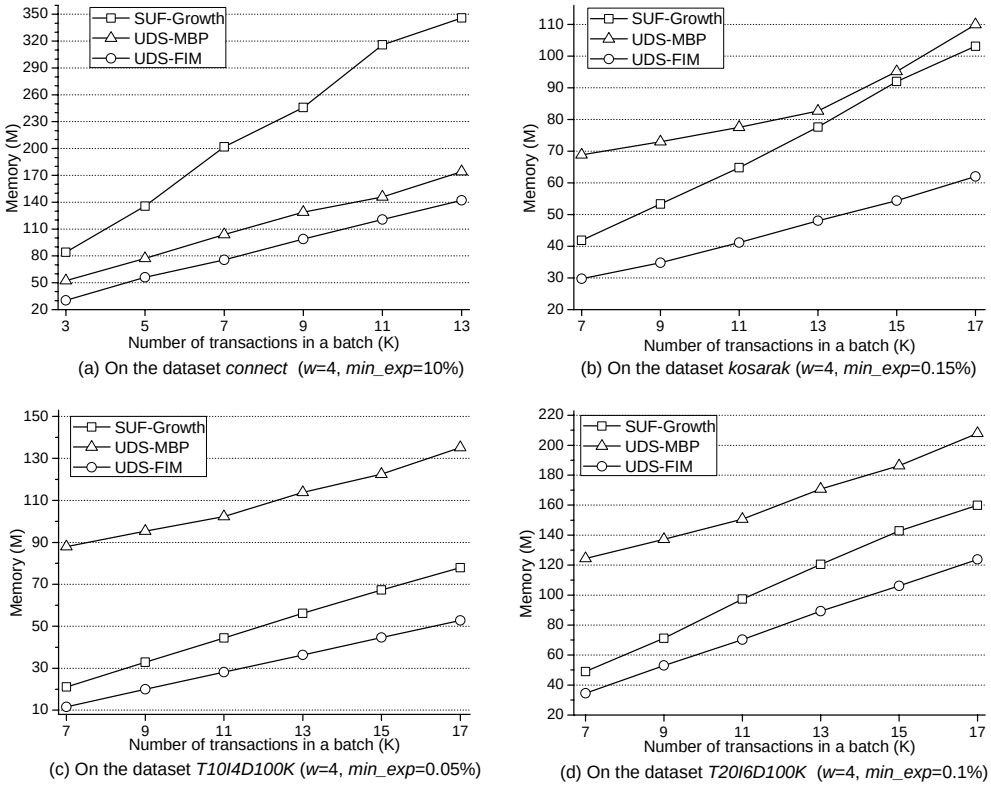


Figure 15. Memory under varied batch size

B. Evaluation on Varied Window Size

In this section, we evaluate the performance of the proposed algorithm under varied number of batches in a window while the parameters *p* and *min_exp* are fixed. A mining operation was performed on each window.

Figures 12-13 show the performance (runtime and memory consumption) of UDS-FIM, SUF-Growth and UDS-MBP using the four datasets respectively when the window size is changed.

From Figure 12, we can see that the performance of the proposed algorithm UDS-FIM beats SUF-Growth and UDS-MBP in terms of running time. The main reason is that UDS-FIM generates less number of tree nodes than SUF-Tree, and it does not generate candidates as UDS-MBP, so UDS-FIM consumes less time to process tree nodes under the same circumstances. (Note that Figure 12 (c, d) indicate an interesting feature: on synthetic datasets, the number of candidates generated by UDS-MBP decreases with the increase of the window size, so the running time of UDS-MBP decreases when the window size increases; however it still can not outperform UDS-FIM).

Moreover, Figures 12 shows that the running time of UDS-FIM is more stable with the increase of the window size on sparse datasets, as shown in Figure 11 (c-d). As the window size increases, the number of transaction itemsets in each window increases, thus the memory consumption of three algorithms increases with the increase of the window size.

Figure13 shows that UDS-FIM has better performance than SUF-Growth and UDS-MBP in terms of memory. This is because that UDS-FIM more efficiently compresses transaction itemsets to a tree than SUF-Growth; moreover, it does not generate candidates and maintains data of a window like UDS-MBP.

C. Evaluation on Varied Batch Size

In this section, we evaluate the performance of the proposed algorithm under varied number of transactions in a batch while the parameters *w* and *min_exp* are fixed.

As the batch size increases, the times of mining operation decreases fast. For example, the mining operation is performed 19 times with *p* =3K while 2 times with *p*=13K on the dataset *connect*; it is 138 times with *p*=7K while 55 times with *p*=17K on the dataset *kosarak*. Thus the total running time (processing a whole dataset) of the algorithms UDS-FIM and UDS-MBP decrease on the datasets *connect*, *T10I4D100K* and *T20I6D100K* though the running time of processing one window increases with the increase of the batch size, as shown in Figure 14 (a, c, d). Note that SUF-Growth generates a bigger tree (too many tree nodes) with the increase of the batch size, its running time of processing one window sharply increases; this leads to increase of its total running time though the times of its mining operations decreases, as shown Figure 14.

With the increase of the batch size, the memory usage increases, as shown Figure 15. However, UDS-FIM still has achieves the best performance among three algorithms in terms of runtime and memory usage.

VI. CONCLUSIONS

In this paper, we propose an efficient algorithm named UDS-FIM for mining frequent itemsets over uncertain

transaction data streams based on sliding window method, and also propose a data structure named UDS-Tree for maintaining uncertain transaction itemsets. Unlike the existing algorithms on the discussed problem, whose tree structures are not as compact as FP-Tree structure, the data structure (UDS-Tree) in our proposed algorithm is a tree as compact as the original FP-Tree. The algorithm UDS-FIM firstly maintains probability information of transaction itemsets to an array; then it maintains transaction itemsets to a UDS-Tree and maintains indexes of transaction itemsets in the array to the corresponding tail-nodes. It mines frequent itemsets with just one scan of database. The experimental results show that the performance of UDS-FIM is better than that of SUF-Growth under different experimental conditions, including varied minimum utility thresholds, varied window size, and varied batch size, on both real-world and synthetic datasets.

In this paper, we just employed the sliding window model, but the proposed tree structure UDS-Tree can be applied to the landmark window model and the damped window model for frequent itemsets mining over uncertain data streams. Meanwhile, the proposed algorithm can be adopted for parallel computing. After the header table and the global tree are constructed, the items in the header table can be processed by parallel.

REFERENCES

[1] C.W. Lin and T.P. Hong, "A new mining approach for uncertain databases using CUFP trees," *Expert Systems with Applications*, Vol.39, no.4, pp.4084-4093, 2011.

[2] G. Liao, L. Wu, C. Wan, and N. Xiong, A practice probability frequent pattern mining method over transactional uncertain data streams, in *8th International Conference on Ubiquitous Intelligence and Computing*. 2011, pp.563-575.

[3] C.C. Aggarwal and P.S. Yu, "A survey of uncertain data algorithms and applications," *IEEE Transactions on Knowledge and Data Engineering*, Vol.21, no.5, pp.609-623, 2009.

[4] C.K. Leung, M.A.F. Mateo and D.A. Brajczuk, A tree-based approach for frequent pattern mining from uncertain data, in *12th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2008)*. 2008, pp.653-661.

[5] X. Sun, L. Lim and S. Wang, "An approximation algorithm of mining frequent itemsets from uncertain dataset," *International Journal of Advancements in Computing Technology*, Vol.4, no.3, pp.42-49, 2012.

[6] T. Calders, C. Garboni and B. Goethals, Approximation of frequentness probability of itemsets in uncertain data, in *IEEE International Conference on Data Mining (ICDM 2010)*. 2010, pp.749-754.

[7] L. Wang, D.W. Cheung, R. Cheng, S. Lee, and X. Yang, "Efficient Mining of Frequent Itemsets on Large Uncertain Databases," *IEEE Transactions on Knowledge and Data Engineering*, no.99(PrePrints), 2011.

[8] C.K. Leung, C.L. Carmichael and B. Hao, Efficient mining of frequent patterns from uncertain data, in *International Conference on Data Mining Workshops (ICDM Workshops 2007)*. 2007, pp.489-494.

[9] Q. Zhang, F. Li and K. Yi, Finding frequent items in probabilistic data, in *International Conference on Management of Data (ACM SIGMOD)*. 2008, pp.819-831.

[10] C.K. Leung and F. Jiang, Frequent itemset mining of uncertain data streams using the damped window model, in *26th Annual ACM Symposium on Applied Computing (SAC 2011)*. 2011, pp.950-955.

[11] C.K. Leung and F. Jiang, Frequent pattern mining from time-fading streams of uncertain data, in *13th International Conference on Data Warehousing and Knowledge Discovery (DaWaK 2011)*. 2011, pp.252-264.

[12] C.C. Aggarwal, Y. Li, J. Wang, and J. Wang, Frequent pattern mining with uncertain data, in *15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2009)*. 2009, pp.29-37.

[13] C. Chui, B. Kao and E. Hung, Mining frequent itemsets from uncertain data, in *11th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2007)*. 2007, pp.47-58.

[14] C.K.S. Leung and B. Hao, Mining of frequent itemsets from streams of uncertain data, in *International Conference on Data Engineering*. 2009, pp.1663-1670.

[15] L. Sun, R. Cheng, D.W. Cheung, and J. Cheng, Mining uncertain data with probabilistic guarantees, in *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2010)*. 2010, pp.273-282.

[16] T. Bernecker, H.P. Kriegel, M. Renz, F. Verhein, and A. Zuefle, Probabilistic frequent itemset mining in uncertain databases, in *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (kDD 2009)*. 2009, pp.119-127.

[17] R. Agrawal and R. Srikant, Fast algorithms for mining association rules in large databases, in *International Conference on Very Large Data Bases (VLDB 1994)*. 1994, pp.487-487.

[18] J. Han, J. Pei and Y. Yin, Mining frequent patterns without candidate generation, in *International Conference on Management of Data (ACM SIGMOD)*. 2000, pp.1-12.

[19] J. Pei, et al., "H-Mine: Fast and space-preserving frequent pattern mining in a large databases," *IIE Transactions (Institute of Industrial Engineers)*, Vol.39, no.6, pp.593-605, 2007.

[20] C.K.S. Leung and Q.I. Khan, DSTree: A tree structure for the mining of frequent sets from data streams, in *IEEE International Conference on Data Mining (ICDM 2007)*. 2007, pp.928-932.

[21] S.K. Tanbeer, C.F. Ahmed, B. Jeong, and Y. Lee, "Sliding window-based frequent pattern mining over data streams," *Information Sciences*, Vol.179, no.22, pp.3843-3865, 2009.

[22] C. Giannella, J. Han, J. Pei, X. Yan, and P.S. Yu, "Mining frequent patterns in data streams at multiple time granularities," *Next generation data mining*, Vol.2003, no.212, pp.191-212, 2003.

[23] M. Deypir and M.H. Sadreddini, "A dynamic layout of sliding window for frequent itemset mining over data streams," *Journal of Systems and Software*, Vol.85, no.3, pp.746-759, 2012.

[24] M.S. Khan, F. Coenen, D. Reid, R. Patel, and L. Archer, "A sliding windows based dual support framework for discovering emerging trends from temporal data," *Knowledge-Based Systems*, Vol.23, no.4, pp.316-322, 2010.

[25] C. Li and K. Jea, "An adaptive approximation method to discover frequent itemsets over sliding-window-based data streams," *Expert Systems with Applications*, Vol.38, no.10, pp.13386-13404, 2011.

[26] C. Chu, V.S. Tseng and T. Liang, "An efficient algorithm for mining temporal high utility itemsets from data streams," *Journal of Systems and Software*, Vol.81, no.7,

pp.1105-1117, 2008.
[27] M. Deypir and M.H. Sadreddini, "Eclat: An efficient sliding window based frequent pattern mining method for data streams," *Intelligent Data Analysis*, Vol.15, no.4, pp.571-587, 2011.
[28] J.H. Chang and W.S. Lee, "estWin: Online data stream mining of recent frequent itemsets by sliding window method," *Journal of Information Science*, Vol.31, no.2, pp.76-90, 2005.
[29] B. Li, Fining frequent itemsets from uncertain transaction streams, in *2009 International Conference on Artificial Intelligence and Computational Intelligence (AICI 2009)*. 2009, pp.331-335.
[30] Y. Kim, E. Park and U. Kim, Mining approximate Frequent itemsets over data streams using window sliding techniques, in *International Conference on Database Theory and Application (DTA 2009)*. 2009, pp.49-56.
[31] H. Li and S. Lee, "Mining frequent itemsets over data streams using efficient window sliding techniques," *Expert Systems with Applications*, Vol.36, no.2 PART 1, pp.1466-1477, 2009.
[32] P.S.M. Tsai, "Mining top-k frequent closed itemsets over data streams using the sliding window model," *Expert Systems with Applications*, Vol.37, no.10, pp.6968-6973, 2010.
[33] B. Goethals. Frequent itemset mining dataset repository, http://fimi.cs.helsinki.fi/data/. Accessed 2011.

Research on Multi-Tenant Distributed Indexing for SaaS Application

Heng Li
College of Computer Science/Chongqing University, Chongqing, China
Email: lihengcq@gmail.com

Dan Yang and Xiaohong Zhang
College of Computer Science/Chongqing University, Chongqing, China
Email: {dyang, xhzhang}@cqu.edu.cn

***Abstract*—Multi-tenant is the key feature for SaaS application, however, the traditional indexing mechanism has failed in multi-tenant shared scheme database. This paper proposed a multi-tenant distributed indexing mechanism. We create a global index first and then create the local index by MapReduce framework based on Hadoop. We also proposed the process of index update and index merging. Experimental results show that our multi-tenant distributed indexing mechanism has a good acceleration capability in creating index and high efficiency in retrieval, and provide good isolation for tenants to protect data safe.**

***Index Terms*—multi-tenant, indexing, distribute, mapreduce**

I. INTRODUCTION

In recent years, multi-tenant database schema which should make a good balance between efficiency and customized[1] has become a hot topic for SaaS[2][3]application. Several works have been presented on design and implement multi-tenant database schema, such as "chunk folding" [4] 、"pivot table" [5] 、"xml table" [6] 、"meta data driven" [7] and so on, each technique has its own characteristics and applicable scenarios [8]. However, the research on index of multi-tenant database is still relatively lacking. The traditional indexing mechanism has failed in these schemas for the three reasons below:

(1)The traditional index [9][10] is created on the ordinary data table column attributes which doesn't involve multi-tenant situation. When different tenants search for result, the date obtained by the traditional index contains too much other information which has nothing to do with the tenants, it is a waste storage space, while making a safety hazard for tenant's own data cannot be isolated.

(2)The multi-tenant database needs to be extended according to the tenants' requirements, each schema has its own method. For example, "chunk folding" store the customized date in each chunk, "pivot tables" distinguish and store the customized date in int and string column, in "meta data driven" schema, different types of data will be stored in a varchar type field, tenants get the definition of metadata first, and then navigate to the extended data. Regardless of which kind of schema, it contains large custom property data which belonging to different logical column in the same column, the traditional indexing mechanism has failed, and cannot support combined index for multiple columns attribute.

(3)The date of each tenant is relative small and very large for the whole multi-tenant database. In shared schema model, it will consume a lot of time and take up a lot of unnecessary disk space if we create a unified data index in the traditional way, and the retrieval efficiency is low for the large index file.

To solve this problem, researchers proposed some solutions. In Force.com [11] Weismann used universal Table [12] to store tenant's business data and stored the logic index data in some pivot tables. It solved the problem of homogeneous index column data object in SaaS environment, but the article didn't diccuss more about data synchronization problems between perspective tables and sparse tables, and the platform didn't open its index maintenance strategy. In paper [13][14]it proposed a cracking mechanism in mangoDB database. It is a query-driven method, it dynamically adjust the order of the tuple in each query in accordance with the the avl tree. To transaction-based multi-tenant application, each update must respond in a timely manner, so this query-driven method has obvious defects. Kong lanju etc[15]proposed a multi-tenant index model in "key-value" schema, this model extend the multi-tenant database and add a indexing mechanism based on metadata. The model is built in a single relational database, it didn't explain the mechanism in large concurrent which will lead overload to single machine. In conclude, Stefan Aulbach proposed in his paper: the ideal database system for SaaS has not yet been developed, there left many problems to be solved [16].

This paper proposed a multi-tenant distributed indexing mechanism for SaaS application in cloud computing environment. Firstly, we create a global index and then create the local index by MapReduce[17] framework. It makes a good isolation for each tenant. Experiment showed that our mechanism has a good

doi:10.4304/jsw.9.1.57-62

acceleration ability in creating index, tenants can search their own data quickly and exactly.

II. System Architecture

Figure 1 illustrates our proposed multi-tenant distribute indexing architecture. There are five main components in our design, including filter, source extractor, indexing module, search module and the distributed cloud storage system HDFS[18].

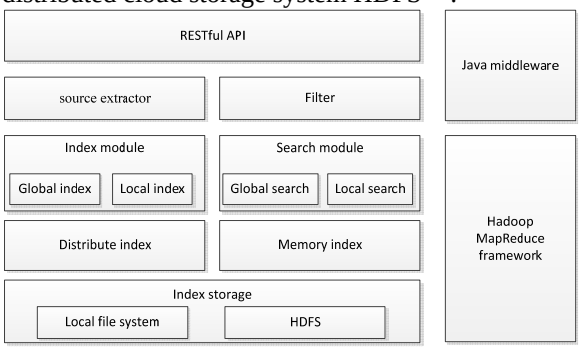


Figure 1. System architecture.

Our architecture has the following features:

(1) multi-tenant awareness and isolation

As Figure 2 shows, in the phase of creating global index, the source extractor get the query result from multi-tenant database by SQL, change the result set into JSON sequence, generate key-value pairs with the tenantid as output format. Then, put the key-value pairs to their own index server cluster by computing the key through distribute hash algorithm. This step implements the initial isolation of tenants' index data.

Physical SQL:
mysql>select p.projectid as id, p.projectname as name ,p.createdate as date, p.manager as manager, d.value as desc from project p, customer_objects o, key_value d where o.object_name='project' and o.object_type='field' and d.objectid=o.objectid and p.tenantid=o.tenantid and p.tenantid=1

Logic SQL:
mysql>select id,name,createdate,manager,desc from project where tenantid=1

Query result:

id	name	createdate	manager	desc
1	SeCloud	2012-04-01	Admin	It is for cloud computing
2	3DCampus	2012-04-03	Janney	A 3D map for visual campus
3	ImageCut	2012-05-03	Pluto	New method to cut image
4	openStack	2012-07-03	Block	infrastructure for Cloud computing

Transform:

Key	Value
tenant1	Id=0 {"name":"seCloud","createdate":"20120401","manager":"admin","desc":"it is for cloud computing"} Id=1 {"name":"3DCampus","createdate":"20120403","manager":"Janney","desc":" A 3D map for visual campus"} Id=2 {"name":" ImageCut","createdate":"20120503","manager":"Pluto","desc":" New method to cut image"} Id=3{"name":" openStack","createdate":"20120703","manager":"Block","desc"," infrastructure for Cloud computing"}

Figure 2. Source extraction

In the phase of creating local index, we get the tenantid and field out from the JSON document and joined them together as one field, then stored in the inverted index[19] which is illustrated in Figure 3, this is the secondary isolation.

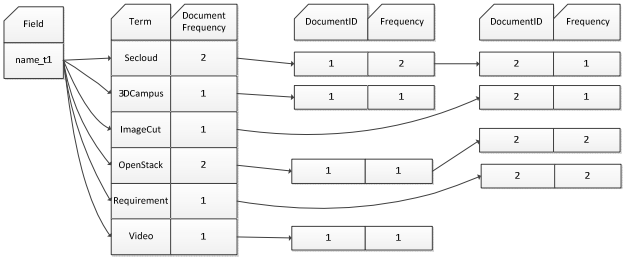


Figure 3. Inverted index

When tenant request for search, the filter obtained the tenantid from context, locate to the index server cluster by tenantid. In the phase of local search, T={t1,t2,t3…..t|t|} is the feature dictionary of system, U={u1,u2,u3…u|u|} is the tenants' collection, F={f1,f2,f3…..f|f|} is the fields' collection, D=(d1,d2,d3….d|d|) is the documents' collection, the index can be represented as a collection of I={<f,t,d>|r(f,t,d,u)>0}, r(f,t,d,u) is discriminant function, it returns a positive value when t is the feature item of d which joined f and u as a field. Suppose local search as S={f,t,d,u},

$$D(t)=\Phi(t,S)=\{d|(t,d)\in I\} \quad (1)$$

D(t) is the document collection of retrieve vocabulary, Φ is retrieval functions of local search. We use r as discriminant function, and isolate the tenants' search quest by (f,t,d,u).

(2) Index cluster grouping

Different tenants have different index cluster groups. In each group, there is one server used as namenode, and the left severs are datanodes. When index data increases, we can increase the compute nodes of the cluster group to improve performance. Meanwhile, the Master/Slave model in each cluster group ensure the availability of Indexing Service in the case of internal nodes crash.

(3) Restful Api style

REST is proposed in a doctoral thesis in 2000, it is suitable to use in the complex network environment. Our proposed architecture used Restful interface to implement data access and exchange both in the phase of creating index and returning the search result, and it has the following characteristics: Since the stateless of communication itself, it allows different servers to handle different requests in a series of requests to improve server's scalability. It can simplify the software requirements by using browser as a client. REST dependence is smaller than other mechanisms superimposed on top of the HTTP protocol, and it don't need additional resource discovery mechanism. It has a better compatibility in the software technology evolution period.

(4) MapReduce Framework

We create local index by MapReduce framework. MapReduce is a computing framework which process and generate large data sets in map function, the programmers design the processing of every data block, and in reduce function, and there will be a reduction of the intermediate results. Users only need to specify the map and reduce functions to write distributed parallel programs. When running on the MapReduce program

on cluster, the programmer need not worry about how to input data block, allocation and scheduling, at the same time the system will also handle the failure problem of some cluster nodes and the communication of inter-node. MapReduce applications get a list of key-value pairs as an input. The Map method processes each key-value pair in the input list separately, and outputs one or more key-value pairs as a result. map(key, value)-> [(key, value)]. The Reduce method aggregates the output of the Map method. It gets a key and a list of all values assigned to this key as an input, performs user defined aggregation on it and outputs one or more key-value pairs.reduce(key, [value]) ->[(key, value)]. Parallelization in the MapReduce framework is achieved by executing multiple Map and Reduce tasks concurrently on different machines in the cluster.

III. System Architecture

A. Create Index

As figure.4 (a) shows, we use consistency hash function on the machine node and the index data to implement unified computing, mapping them in a circle address space (0~232-1). After source extractor output the key-value pairs:<tenantid,queryResult>, we calculate the location of each pair by hash function on tenantid, find out which master node it belongs to, read each line of the value and generate the collection of original documents, then build a global B+ tree index(Figure 5 shows), at last, we upload the documents to the master node, save the global index file and original documents as key-value pairs to HDFS which the tenant corresponding.

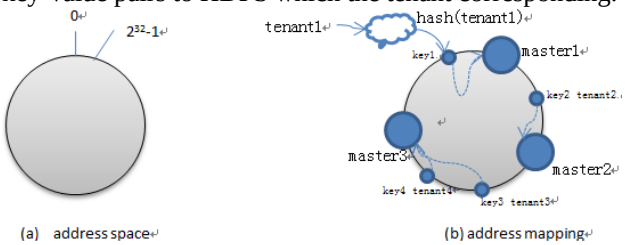


Figure 4. address space and mapping

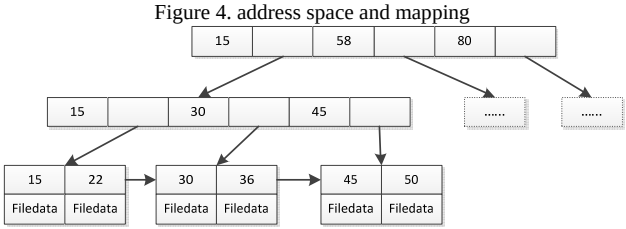


Figure 5.Global B+ tree

Algorithm 1. CreatGlobalIndex
Input:<tenantid,queryResult>
Output:documents collection
Begin
1. Get collection of Key as S
2. for key in S // Iteration
   get the distribution area R by hash function on key
   get the MasterNodeLocation by Inverse operation on R
3. get the value by key
4. for value in V //second iteration,split the query results
   docs=readline(value)
   build B+ tree globalindex with docs
   save<globalindex,docs> to HDFS
5. for doc in docs // third iteration,split docs to singal doc
   upload doc to MasterNodeLocation
   end for
   end for
  end for
END

B. Create Local Index

The master node in the cluster contains namenode and is responsible for distributing task called JobTracker. The slave node contains datanode and is responsible for job runs called TaskTracker. There are four steps below:

Step1. Master node divided the input files into N blocks, and send them to N slaves, meanwhile, the JobTracker send the CreatLocalInvertedIndexMap 、CreatLocalInvertedIndexReduce function to each slaves.

Step2.Each slave machine run CreatLocalInvertedIndexMap, resolve the input document, output <tenantid+field,term>as key-value pairs.

Step3.After sort the pairs in step2, each reducer runs the CreatLocalInvertedIndexReduce function, resolve the input pairs, joins tenantid and filed as luence field, use the terms as luence index value, then put the luence field and luence value in a luence document model. At last, output<tenantid, LuceneDocumentWrapper > as key-value pairs.

Step4.In hadoop's jobconf, we set the customized class LuceneOutputFormat as the output format, call luence index module to generate inverted index, save the temporary index to the local path of reduce node, after all reduce node finish, merge each index file for a complete index file and copy it to HDFS.

Algorithm 2 MRCreateLocalInvertedIndex
Input:documents collection
Output:index file
BEGIN
1.Init MapReduce,set and distribute mapreduce task
2.map(LongWritable key, Text text, OutputCollector<Text, Text> output, Reporter reporter) //CreatLocalInvertedIndexMap task
  get Fields by resolve input document
  get Terms by resolve input document
  for term in Terms // Iteration
    set key1=tenantid join field
    set value1=term
    output(key1,value1)
  end for
3.reduce(Text key, Iterator<Text> value, OutputCollector<Text, LuceneDocumentWrapper> output, Reporter reporter) //CreatLocalInvertedIndexReduce
  create luencedoc as luence document model
  while iter.hasNext() // Iteration
  get term from value
  luencedoc.add(key,term) //put key and term into luence document model
   set key3= tenantid which obtained from key
   set value3=format(luencedoc)

output(key3,value3) //reduce output

4.get value in step3 and call luence index module to generate inverted index

save the temporary index to the local path of reduce node

If all reduce nodes finish

Optimization index and close

merge each index file for a complete index file

copy the index file to HDFS

END

C. Search Process

Step1.When filter obtained the search request, insert ed it into the user's queue, then get the tenantid as key fro m the context, set the search request sentence as value, pu t them into hash table: hashtable<Key:tenantid,Value:List <SearchQuery>>. By this means, different tenants' search request is assigned to the corresponding master node.

Step2.When master node get the search request, it identify fields and keywords by lexical analysis and create a syntax tree by Syntax analysis, in figure 6.

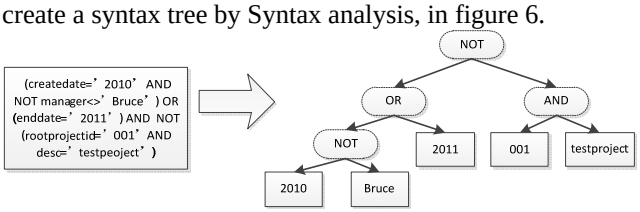


Figure 6. Request sentence and syntax tree

Step3.Master node get the local index file from HDFS, obtain the document linked list by search in the local index, then computing relevency between query sentence q and document d through formula(2) below, return the linked list collection by the order of relevency.

$$score(q,d) = \frac{\vec{V_q} \cdot \vec{V_d}}{|\vec{V_q}||\vec{V_d}|} = \frac{\sum_{i=1}^{n} w_{i,q} w_{i,d}}{\sqrt{\sum_{i=1}^{n} w_{i,q}^2}\sqrt{\sum_{i=1}^{n} w_{i,d}^2}} \quad (2)$$

Wi,q is the weight of the word i in document d

Step4.Master node get the global index and original documents, search the linked list collection in the global index, return the corresponding original documents.

Algorithm 3 GetSerachResult

Input:search request sentence

Output:result documents

BEGIN

1.get the tenantid from context

set hashtable=<Key:tenantid,Value:List<SearchQuery>>

Distribute search request to master node

2.init D

3.do lexical analysis and syntax analysis with SearchQuery

4.join tenantid and field, create search object

5.get inverted index from hdfs to memory

6.for t in SearchQuery // Iteration

get docs from inverted index with t

and docs to D

7.do boolean operations on D,merge the result

8.computing the relevency by formula(2),return the documentid

9.get the original documents through search doucumentid in global index

10.return result documents

END

D. Index Update

Usually, indexing is a relatively time consuming process, espasially when data set is very large but there is less new record, it is too costly to rebuild the entire index. In this paper, we choose main index plus incremental index way to achieve index update. Firstly, we create a synchronization table in the multi-tenant database, Figure 7(a) shows, then we set a refresh interval time, when source extractor get the new data, it also update the operation_id in the synchronization table. At last, source extractor send the new data to master node and inform that it is an incremental update, master node create an incremental update index in the memory as Figure 7(b) shows.

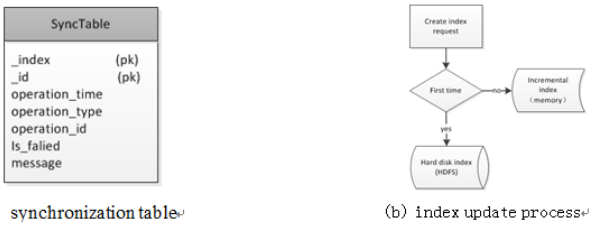


Figure 7. Index update

E. Index Merge

When the memory is not enough for growing index, we need to merge the index in memory and hard disk. Figure 8 shows the mode of index merge.

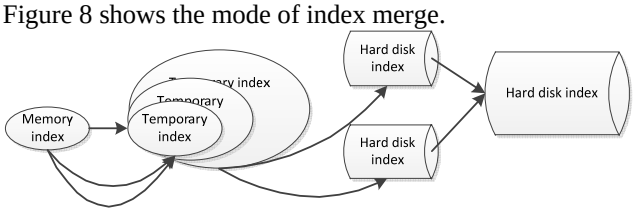


Figure 8. Index merge

Algorithm 4 MergeIndex

BEGIN

1. set a Threshold
   if memory> Threshold
   add memory index to merge queue,create temporary index
2. set interval time t1,t2
   if t>t1 save the temporary index to hard disk and clean the temporary index
   if t>t2 merge index in hard disk

END

IV. Experiment

The environment we conducted experiments on contained 3 clusters, each cluster composed of 4 dual processors nodes , each node has 1 GB of main memory. The index data of tenants 1-10 are distributed in three groups in the cluster. In each cluster, there was one namenode and the left were datanodes. The operating system was Linux Ubuntu 12. We write java client on multiple hosts simultaneously to simulate multi-tenant session, each client using multiple threads to achieve

concurrent users, each session runned in its own thread and got the target database by connection pool. Since there is no standard data set for this task, we construct a base schema of a particular business domain application from the data schema in TPC-W database[20].We append a tenantid column so that it can be shared by multiple tenants as "Common tables", we choose the "meta data driven" schema to store the customized data. The purpose of our experiment is testing the index creation and search capabilities in our multi-tenant distributed indexing mechanism.

A. Acceleration Capability Test

We simulate 3 tenants obtained the documents collection from database , each document is a json sequence which contained 22 key-value pairs. Table 1 shows the documents collection.

TABLE1.
DOCUMENT SIZE

	samples	features
Tenant1	30000	22
Tenant2	120000	22
Tenant3	240000	22

TABLE 2.
RUN TIMES FOR CREATING INDEX

	Tenant1	Tenant2	Tenant3
1node	71s	252s	481s
2nodes	60s	195s	310s
3nodes	35s	122s	212s

From the experiment results (Tables 2 and Figure 9(a)) it is possible to see that the time of each job decrease with the node increase, It means that we can significantly improve the indexing processing capabilities on the same scale data by increase the node. It should also be noted that the real time is less than the record time. This is because the background tasks of the mapreduce framework are relatively slow to start, so each separate mapreduce job that is started slows down the process. In conclude, to different tenants, when the index data is small, the acceleration capability can be ignored, so we can reduce the computing node to save cost, when the index data is large, we can improve the efficiency of indexing by increasing compute nodes

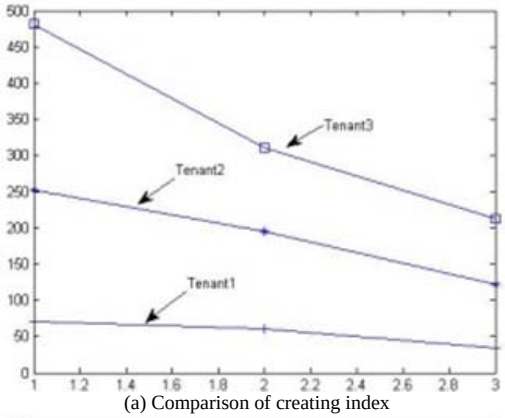
B. Search Capabilities Test

In the first experiment, we create three index in different size:73.7M,287.1M,538.8M. Now we simulate 3 tenants request for search, each tenant contained 100 users who send concurrent request. We test 7 types of requests :S1-S7.Table 3 record the average time of per user.

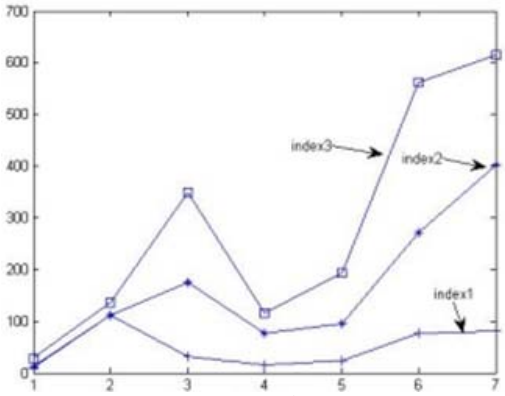
S1:get all document collections
S2:search value from all documents
S3:search in a range : 1<c_id<10000
S4:search by field value:Field=c_phone
S5:combination query1:c_id=111 AND c_phone= 7448718095072587
S6: combination query2:c_zip=prifix(9364) AND NOT c_id<10000 AND c_discount<0.4
S7:combination query 3:(1000<c_id<10000 AND NOT c_zip=prifix(9018)) OR (10000<c_id<20000 AND c_phone=prefix(7448))

TABLE 3.
RUN TIMES FOR RETRIEVAL

	S1	S2	S3	S4	S5	S6	S7
tenant1	10ms	111ms	31ms	15ms	23ms	77ms	81ms
tenant2	12ms	112ms	175ms	77ms	96ms	272ms	403ms
tenant3	28ms	137ms	350ms	115ms	194ms	562ms	615ms



(a) Comparison of creating index



(b) Comparison of retrieval

Figure 9.Experiment result

From Table.3 and Figure 9(b) we can see that it responsed fast in the case of concurrent retrieval, the result returned in milliseconds. Though the retrieval time is different in different request type, the impact on the end user is very weak. To improve retrieval efficiency, it is better to be avoided retrieve in the global scope, and should add the field as filter. We can also concluded that the index file size is an important factor affecting the efficiency of retrieval. If some individual tenants have a huge index data, we can add caching mechanism in the retrieval phase, or split the index file and add distributed retrieval algorithm to improve efficiency.

V. CONCLUSIONS

This paper proposed a Multi-Tenant distributed indexing mechanism for SaaS application, which has a good acceleration capability in creating index and high efficiency in retrieval, and provide good isolation for tenants to protect data safe. In future work, we will go on researching on caching mechanism and distributed

retrieval algorithm, for further optimize performance and reduce costs.

ACKNOWLEDGMENT

This work is supported by State Natural Sciences Foundation Projects of China under Grant (60975015), Chongqing science research project funding under Grant (CSTC2009AC2057).

REFERENCES

[1] F.Burno."Exeuting an IP Protection Strategy in a SaaS Environment", http://www.slideshare.net/Rinky25/saas-environment, Jul. 22, 2011.
[2] M. Dokas, R. J.Wallace, R. Marinescu, S. Imran, and F. S.Foping. Towards a Novel Early Warning Service for State Agencies: A Feasibility Study. In Information Technologies in Environmental Engineering, pages 162–175. Springer Berlin Heidelberg, 2009.
[3] F. S. Foping, I. M. Dokas, J. Feehan, and S. Imran. On Using Software as a Service to Deploy an Early Warning Service. In International Conference on Enterprise Information Systems and Web Technologies, pages 161–168, Orlando,Florida, USA, 2009. ISRST.
[4] S. Aulbach, T. Grust, D. Jacobs, A. Kemper, and J. Rittinger. Multi-tenant databases for software as a service: schema-mapping techniques. In SIGMOD '08: Proceedings of the 2008 ACM SIGMOD international conference on Management of data, pages 1195-1206, New York, NY, USA, 2008. ACM.
[5] R. Agrawal, A. Somani, and Y. Xu. Storage and querying of e-commerce data. In VLDB '01: Proceedings of the 27th International Conference on Very Large Data Bases, pages 149{158. Morgan Kaufmann Publishers Inc., 2001.
[6] D. Florescu and D. Kossmann. Storing and querying XML data using an RDMBS. IEEE Data Eng. Bull, 22(3):27-34,1999.
[7] Li heng, Yang dan, Zhang xiaohong, A new meta-data driven data-sharing storage model for SaaS, International Journal of Computer Science Issues, Volume 9, Issue 6,2012
[8] S.Aulbach, T.Grust, D.Jaeobs, A.KemPer and M.Selbold, A Comparison of Flexible Schemas for Software as a Service, SIGMOD, 2009.
[9] Fuqing Zhao, An Improved PSO Algorithm with Decline Disturbance Index, Journal of Computers, 2011, 691-697
[10] Aiguo Li, RSR-tree: A Dynamic Multi-dimensional Index Structure, Journal of Computers,2011,2552-2558
[11] Salesforce AppExchange. http://www.salesforce.com
[12] The Foree.com Multitenant Architecture, Understanding the Design of Salesforee.com's Internet Application Development Platform.
[13] Kersten M, Manegold S. Cracking the database sore Proceedings of the CIDR.Asilomar,CA,USA,2005:213-224
[14] Idreos S,KerstenM,Manegold S.Databasecracking Proceedings of the CIDR.Asilomar,CA,USA,2007:68-78
[15] Kong LanJu, Li QingZhong,Research on Index of Multi-Tenant Based on Key-Values for SaaS Application. chinese journal of computers. 2010 vol32 No.12
[16] S. Aulbach, D. Jacobs, A. Kemper, and M. Seibold, "A comparison of flexible schemas for software as a service," in Proceedings of the 35th SIGMOD international conference on Management of data, ser. SIGMOD '09. New York, NY, USA: ACM, 2009, pp. 881–888.
[17] Dean J, Ghemawat S. Map/Reduce: Simplied Data Processing on Large Clusters[C].In:OSDI 2004, San Francisco,2004,137-150
[18] S. Ghemawat, H. Gobioff, S.-T. Leung, The google file system, SIGOPS Operating Systems Review 37 (2003) 29–43.
[19] Shaojun Zhong, A Design of the Inverted Index Based on Web Document Comprehending, Journal of Computers,2011,664-670.
[20] http://www.tpc.org/tpcw/

Heng Li is a lecture in Chongqing University. Currently, he is a PhD student in College of Computer Science of Chongqing University. His interests are in cloud computing, data mining & machine learning.

Dan Yang is a professor of Chongqing University. Current research interests: data mining, computer vision, machine learning, enterprise informatization.

Xiaohong Zhang is a professor of Chongqing University.

Hybrid Intelligent Recommending System for Process Parameters in Differential Pressure Vacuum Casting

Zhuangya Zhang
Rapid Manufacturing Engineering Center, Shanghai University, Shanghai , China
Email: zhangzhuangya@126.com

Haiguang Zhang, Yuanyuan Liu and Qingxi Hu
Rapid Manufacturing Engineering Center, Shanghai University, Shanghai , China
Email: haiguangdd@shu.edu.cn, yuanyuan_liu@ shu.edu.cn, huqingxi@ shu.edu.cn

***Abstract*—The determination of process parameters in Differential Pressure Vacuum Casting (DPVC) process depends on the technologist's experience, and thus the optimized ones are usually determined through repeated molding trial and repairing process. However, this can result in problems of long production period and high cost. So, combining case based reasoning (CBR), neural network 、agent model and fuzzy inference, a hybrid intelligent model is proposed herein to solve this problem. First, the CBR strategy is adopted for setting the initial process parameters by simulating the technologist's reaction where technologists determines the optimized parameters by referencing highly similar case from past experience. If the CBR fails, the neural network reasoning (NNR) strategy is applied to determine the initial process parameters by imitating technologist's "experience reasoning" process; if no similar case exists, the agent model reasoning (AMR) strategy is applied to determine the initial parameters. Finally, a fuzzy inference (FI) based on expert knowledge is developed for revising defects and optimizing process parameters during the molding trial process until the part quality can meet the requirements. Based on the intelligent model, the corresponding software system is developed, and the experiment results show that the system is effective and can be applied to practical production.**

***Index Terms*—Differential pressure vacuum casting, Case based reasoning, Agent model, Fuzzy inference**

I. Introduction

Under the production condition of advanced manufacturing, rapid tooling technology which is based on rapid prototyping has become the researchers' focus recently because it has high capability of shortening the manufacturing period and meeting the individual requirements [1],[2]. DPVC technology is one of the rapid tooling technologies and belongs to the range of forming process in lower pressure. It involves uniformly mixing two kinds of materials and defoaming step, then they are poured into enclosed mould under pressure, and finally the finish product can be obtained after sizing process by heating. Determining the process parameters of DPVC is a complicated task and involves lots of experiences [3,4]. During the forming process, the mixed material experience lots of physical and chemical action, such as polymerization, crosslinking and solidification. This thus increases the difficulty for controlling the actual process. Analytical relation can't be easily established between process parameters and finish products and thus limits the application of traditional optimization methods. Because of these constraints, for a long time, the process parameters are obtained by technicians through try and error method.

Recent years, with the rise of artificial intelligent technology, many scholars and manufacturer in this industry have done lots of research for optimizing process parameters. With the aid of these technologies, Y.J.Lee[5], Y.K.Shen[6], AthanasiosBikas[7] have adopted the analysis software of mould flow and done orthogonal tests of multiple factors for obtaining the main effort of each factor which involved utilizing ANOVA method to probe the efforts between process parameters and quality of finished product. The results of numerical emulation and experiment can give the advice for determining the process parameters. However, for the limitation of test scale, this method can't reflect all the possible cases, thus may lose the optimized solution. Several researchers proposed neural network [8,9], support vector machine [10], Grey theory[11], Kriging model[12,13] and gaussian process[14] to optimize process parameters. But the built models are limited to specific products and can't represent the general products.

Other scholars have introduced the artificial intelligent technology to optimize process parameters. C.K.Kong [15] has developed a process parameters determination system on the base of case reasoning. K.Shelesh-Nezhad [16] mainly discussed the correction technique in the

Manuscript received April 4, 2013; revised July 12, 2013; accepted August 11, 2013.
Corresponding author: Haiguang Zhang, haiguangdd@shu.edu.cn.

doi:10.4304/jsw.9.1.63-69

process of case reasoning. He [17], Lau [18] proposed NN model to determine the process parameters in the plastic industry. Tan and Yuen [19] proposed the method of multi-objective optimization to correct the defect products. However, with the constraint of size of the case library, CBR technology can't ensure the process parameters can give the right advice for producing the acceptable products. The single defect correction system requires the experienced technicians to set up initial process parameters. Because of these restraints, the above mentioned researches are limited to the exploration of theory and these methods have not been adopted for industrial practice.

In this paper, based on the actual system features of DPVC process and combining CBR, NNR, AMR and FI, a hybrid recommending system for process parameters in DPVC has been built to effectively emulate the repeated molding process when determining the parameters and obtain the optimized parameters.

II. Hybrid Intelligent Model

Following the idea of repeated molding and repair by technologist to obtain optimized process parameters, a hybrid intelligent model is constructed by combining CBR, NNR, AMR and FI, shown in Fig.1.

III. Process Parameters Recommending

A. Case-based Reasoning Strategy

The core idea of the CBR is, based on relevant case information, to find similar solution for new cases and based on case differences, to adjust the solution differences. The CBR implementing procedures are shown in Fig.2.

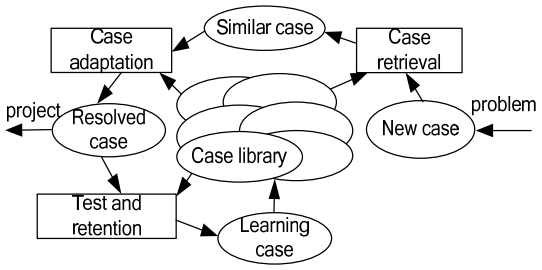


Fig. 2 Implementing procedures of CBR

The case description contains characteristics of product C, materials performance M, and solution (P), as shown in Eq. (1).

$$case = [(C, M), P] = \left\{ [(c_1, c_2, \ldots, c_n), (m_1, m_2, \ldots, m_n)] \ , (p_1, p_2, \ldots, p_n) \right\} \quad (1)$$

where p_i denotes process parameter vector, i=1...n ,; P represents the vector space of the process parameters; m_i denotes material performance

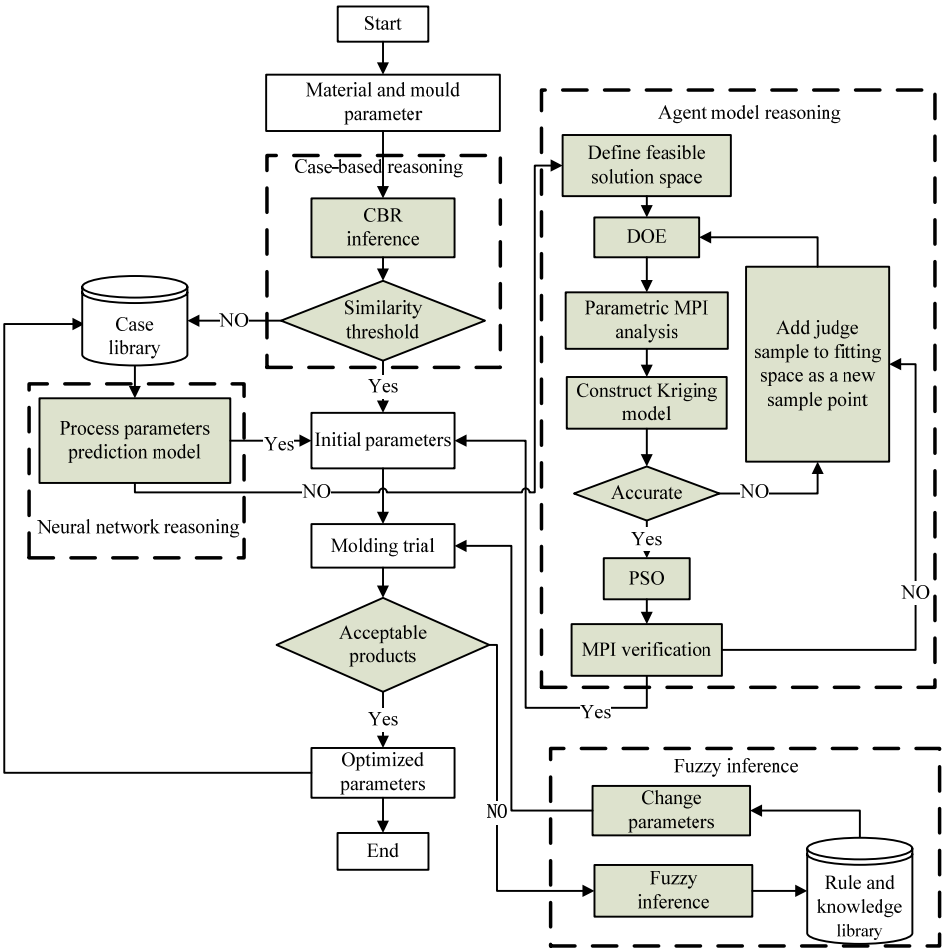


Fig. 1 The framework of intelligent model

parameter vector, i=1...n ; M represents vector space of material performance parameters; c_i denotes vector of product characteristics, i=1...n ; C denotes vector space of product characteristics.

The similarity of target case and source case can be calculated following Eq.(2):

$$Sam(i,j) = \sum_{i=1}^{n}[W_i \times S_c(i)] \times \sum_{j=1}^{n}[V_j \times S_M(j)] \qquad (2)$$

where W_i and V_j represent weight coefficient and similarity of material performance, respectively; $S_c(i)$ and $S_M(j)$, calculated following Eq. (3), are the product similarity of characteristic between target and source cases.

$$S = \frac{1}{1+\lambda \times \left| x_{obj} - x_{src} \right|} \qquad (3)$$

where x_{obj} denotes attribute factor value of the target case; x_{src} denotes attribute factor value of corresponding source case; λ denotes sensitivity coefficient, through which local similarity can be adjusted. The materials used in DPVC belong to reaction molding materials, so process parameters vary widely between different materials. Furthermore, for the same kind of material, the characteristics of mold cavity determine the process parameters. In this paper, mould cavity characteristics (cavity volume, average thickness, the complexity of the cavity) are used as the input and process parameters (differential pressure, mold temperature, materials temperature) used after having manufactured qualified products as output.

In DPVC process, we set the thresholds of hierarchical similarity as 0.95 and 0.80, respectively, as shown in Table 1

TABLE I.
SAMPLE SIMILARITY AND HANDLING METHODS

Case No.	Similarity Range	Corresponding Operation
Sample1	$0.95 \le Sam(i,j)$	Directly employ the process parameters of corresponding case
Sample2	$0.80 \le Sam(i,j) \le 0.95$	Artificially adjust process parameters through molding trial process
Sample3	$Sam(i,j) \le 0.80$	If case-based reasoning fails, employ IPM

B. Neural Network Reasoning Strategy

The efficiency and performance of case-based recommending strategy for reasoning process parameters depend largely on the coverage of case library, case retrieval and case adaptation. And in many applications solely CBR recommending strategy is not sufficient to guarantee the good performance of the system. Therefore, the CBR recommending strategy needs to be supplemented. Base on general regression neural network, a forecasting model is established between product characteristics and process parameters to predict the process parameters.

The product eigen value of random variables x is $x_{\text{new}}=(c_{1new},c_{2new},...c_{nnew})$, random variables y denotes regression with respect to the product characteristics x_{new} . $f=(x_{new},y)$ denotes joint probability density function between random variables x and random variable. $y_{new}=(p_{1new}, p_{2new},\ldots, p_{nnew})$ represents predicted vector, and y_{new} can be calculated using Eq.(4).

$$y_{new}=\mathrm{E}(y/x_{new})=\frac{\int_{-\infty}^{\infty} y f(x_{new},y)\mathrm{d}y}{\int_{-\infty}^{\infty} f(x_{new},y)\mathrm{d}y} \qquad (4)$$

Density function $\hat{f}=(x_{new},y)$ can be obtained by characteristics of the product parameter vector x_i and process parameter vector y_i (i=1...n) from case library though Eq. (5):

$$\hat{f}=(x_{new},y) = \frac{1}{n(2\pi)^{\frac{q+1}{2}}\sigma^{q+1}}\sum_{i=1}^{n}\exp[-\frac{(x_{new}-x_i)^{\mathrm{T}}(x_{new}-x_i)}{2\sigma^2}]\exp[-\frac{(x_{new}-y_i)^2}{2\sigma^2}] \qquad (5)$$

In Eq. (5), n is the number of same material cases in the case library; q is the dimension of the product characteristics x_i vector, i=1...n ; σ is the width of the gaussian function coefficient. Substituting $f=(x_{new},y)$ with $\hat{f}=(x_{new},y)$ gives the predictive value of the process parameters.

$$y_{new}=\frac{\sum_{i=1}^{n} Y_i \exp[-\frac{(x_{new}-x_i)^{\mathrm{T}}(x_{new}-x_i)}{2\sigma^2}]}{\sum_{i=1}^{n}\exp[-\frac{(x_{new}-x_i)^{\mathrm{T}}(x_{new}-x_i)}{2\sigma^2}]} \qquad (6)$$

The general regression neural network structure is shown in Fig. 3

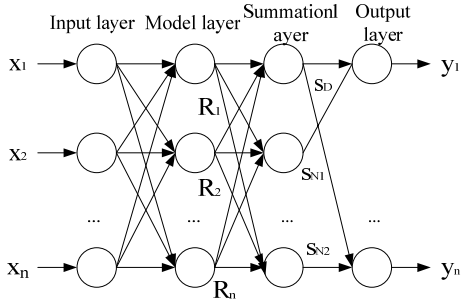


Fig.3 Structure of the general regression network

Training samples in the general regression neural network are all from actual successful processing cases. Of course, at the beginning, because of the limited number of samples and data singularity, the library can not contain all kinds of moulds, so network training is ineffective, and still needs repeated molding trials. But with the every ideal casting process parameters adding to the library, robustness of the training sample data will be getting better and better, the effect of the training will be more and more accurate, and the recommended process parameters will be much closer to the optimized ones.

C. Agent Model Reasoning Strategy

If the case library doesn't contain any information about the new products, then the strategy of imitating technologist's "repeated molding trial" process is employed. Based on the Kriging model and particle swarm optimization algorithm, optimization model of process parameter is established to solve the problem of new products design and optimization.

$$\begin{cases} \min(\text{or}\max) y=f(x)=(f_1(x),f_2(x),...,f_k(x)) \\ x=(p_1,p_2,...,p_n)\in X \\ y=(f_1(x),f_2(x),...,f_n(x))\in Y \\ s.t. \quad e_i(x)\le 0, i=1,2,...,m \end{cases} \tag{7}$$

Unlike the process parameter prediction model in section B, x is process parameter vector, X is process parameter space; y is indication vector of product quality, Y is indicator vector space of the product quality; $f(x)$ is the relationship function between the quality indicators and process parameters; $e_i(x)$ is molding process restrictions from molding machinery, material ,etc.

Employ experimental design method to obtain samples from the space of process parameter, and MPI strategy to analyze the sample set $S=[x_1,x_2,...,x_m]^{\mathrm{T}}$ and response set $Y_s=(y_1,y_2,...,y_n)$. Kriging model $f(x)$ is used to structure agent model between quality indicators and process parameters.

Kriging model: $$y_e(x)=F(\beta_{:,e},x_{\text{new}})+z_e(x) \tag{8}$$

$$F(\beta_{:,e},x)=\beta_{1,e}f_1(x)+...+\beta_{p,e}f_p(x) \tag{9}$$

where $\beta_{:,e}$ denotes regression coefficients, $y_e(x)$ is represented by a linear combination of already known training samples Y_s.

$$\hat{y}_e(x)=c^T Y_s \tag{10}$$

This equation can meet unbiased estimate $E(\hat{y}_e(x)-y_e(x))=0$ and the estimated variance minimum condition $\min \mathrm{E}((\hat{y}_e(x)-y_e(x))^2)$. Thus the combination coefficients c^T can be obtained, and Kriging model constructed. Furthermore, partical swarm optimization algorithm is employed to find the optimal process parameters in solution space. The particle swarm optimization process is shown in Fig.4.

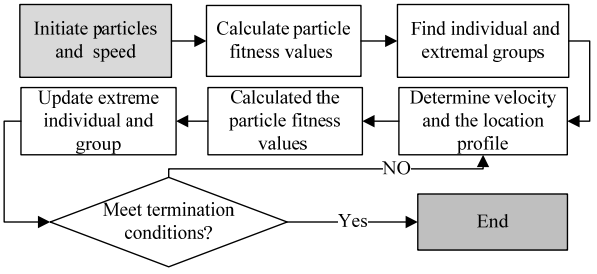


Fig. 4 Procedures of the particle swarm algorithm

IV. Defect Correction and Process Optimization

Aiming at eliminating the defects of products after molding trial, knowledge-based fuzzy inference system is established to intelligently reivse the defects. The

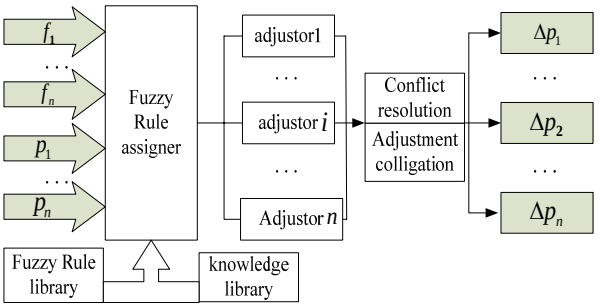


Fig. 5 Defect revision and process parameters optimization framework

defect revising and optimization framework for process parameters is shown in Fig. 5.

There may be more than one defect in molding trial. In order to revise the defects f_i (i=1,2,…, m), multiple process parameters p_i, $i=1...n$, should be adjusted. The adjusting value of Δp_i is affected most by the degree of defect and the current process parameters of last molding trial process. Therefore current value of process parameters and defect levels are used as inputs in fuzzy inference system, adjustment of process parameters as the output. Thus all adjustment of all process parameters can be obtained.

Designing fuzzy rules is based on if-then rules:if x is X and y is Y then z is Z. x is language variable, representing "defect level" , and X is characterization of defect levels, which is divided into { No defects, Slight, Moderate, Serious },and scaled into the interval [1,4]; Y is the characterization of the current process parameters, and it is divided into {Tiny, Middle, Big}, and scaled into the interval [1,3]; Z is characterization of the adjustment of the process parameters, and it is divided into { Smaller, Slightly Smaller, Constant, Slightly Larger, Larger }, and scaled into the interval [-1,1]. Conventional triangular membership functions are used for fuzzification of inputs.

The Max - min Composition operation from Mamdani reasoning is used for fuzzy reasoning, and the method of gravity center is used for parameter revision's reverse justification processing. The center of the area enclosed by the membership function curve and the abscissa is used as the value of the final output of the fuzzy inference.

V. System Implementation

Based on the above-mentioned model and methodology, an intelligent recommending system for process parameters, which is built on the platform of Microsoft VisualC++, is thus developed. Taking advantage of standard communication interface protocol-TCP/IP, the communication between the proposed system and the controller of the master

machine can be realized. The developed system is mainly composed of these functional modules: the module of extracting information, the module of managing database, the module of CBR, the model of NNR, the model of AMR, the module of FBR, the module of reasoning and explanation, the module of user interaction and the module of communication with controller, shown in Fig. 6.

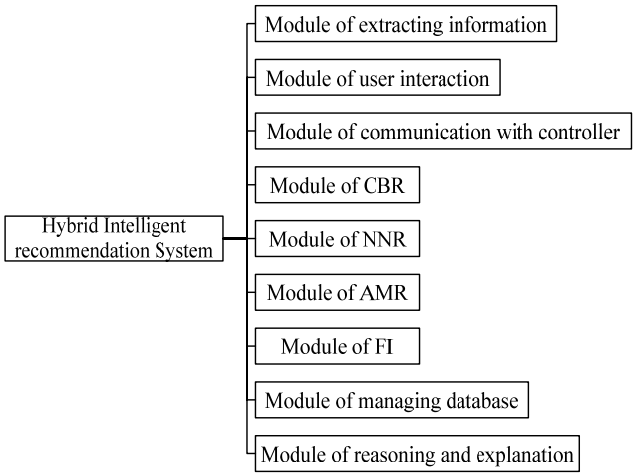


Figure 6 The functional modules of the system

(1) Module of extracting information: based on the STL file, obtain the geometrical characteristic from the mould cave;
(2) Module of user interaction: after having obtained the similar case through searching, the user can perform the operation of judging and selection;
(3) Module of communication with controller: pass the reasoning result to the controller through communication protocol for mould trial;
(4) Module of CBR: through the retrieving, matching and revising process, intelligently recommend process parameters;
(5) Module of NNR: by learning cases with the same material from the case library, establish the prediction model between characteristic of the product and process parameters for intelligent recommending;
(6) Module of AMR: combining the knowledge library with MPI, the relation model between process parameters and the quality of the product can be established for intelligent recommending;
(7) Module of FI: through the feedback and model of fuzzy inference reasoning process, adjust the corresponding the value of the process parameters;
(8) Module of managing database: manage the database, including case library, rule and knowledge library, to make the operation easy for the users, and extend the case library and realize the self-learning function for the system by saving the successful cases;
(9) Module of reasoning and explanation: explain the procedures and result of reasoning process parameters to the technicians for the judgment;

The system interface is shown in Fig 7.

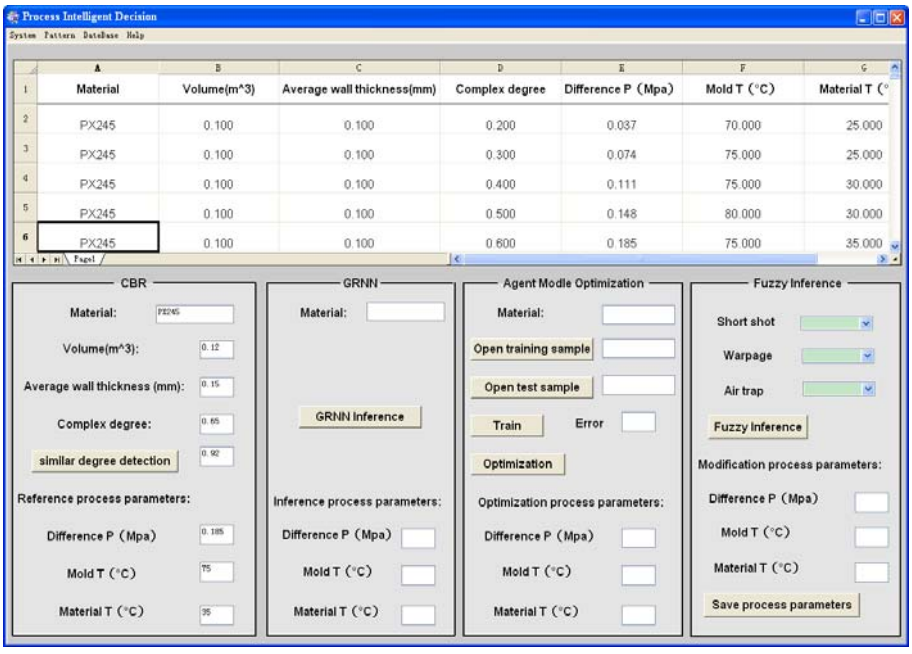


Fig. 7 Interface of intelligent recommending system for process parameters

VI. System Application

In order to test the performance of the proposed recommending system, the cover of headlight of a certain brand of motorcycle and one kind of shoe are employed herein. The product prototypes and corresponding moulds are shown in Fig. 8 and Fig. 9. The experiment is conducted in V450N-VD vacuum casting machine, designed and manufactured solely by Rapid Manufacturing Engineering Center, Shanghai University, China.

Fig. 8 Prototype and mould of the cover

Fig. 9 Prototype and mould of the shoes

Through retrieving the already existing cases, the overall similarity of the shoe is 0.73 which is less than 0.80. This indicates that CBR fails. Through NNR for reasoning process parameters, we can obtain the set of process parameters: difference pressure is 0.0075Mpa, mold temperature 70 °C and material temperature 20 °C. After manufacturing using these parameters, the quality of the shoe is shown in Fig.10.

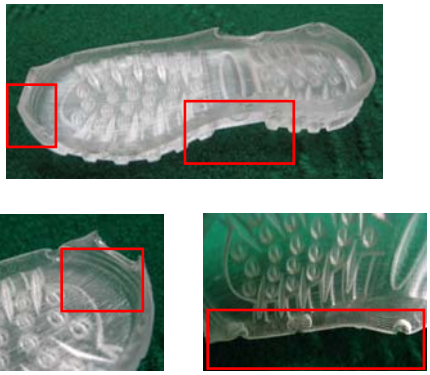


Figure 10. The initial process parameters molding trial

We find that the defects of insufficient casting and air bubble exist. Using fuzzy inference for revising defects and optimizing process parameters, the adjusted process parameters are: difference pressure is 0.009 Mpa, mold temperature75 °C, and material temperature 30 °C. After manufacturing using these parameters, the quality effect of shoe is shown in Fig.11 which shows defects of insufficient casting have disappeared and air bubble have decreased, suggesting good product quality.

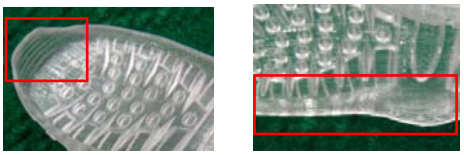


Fig. 11 The initial process parameters molding trial

For the cover of headlight, technologists have tried molding trial three times, but the final product still have obvious air bubble and insufficient casting defects, as shown in Fig.12. Because similar case with the same material UP5170 can't be found in the case, so case reasoning and neural network reasoning strategies fails.

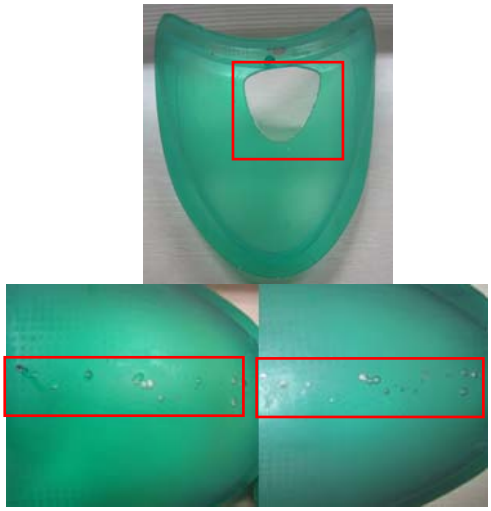


Figure 12.molded by molding personnel

Therefore, AMR for optimizing process parameters recommending strategy is used to obtain initial process parameters where difference pressure is 0.008 Mpa, mold temperature 70 °C and material temperature 25 °C. During the first mould trial process, the final product doesn't exhibit defects of insufficient casting and air bubble, shown in Fig.13. The product quality is obviously better than before.

Figure 13.molded by molding personnel

VII. CONCLUSION

The traditional determination method for process parameters in DPVC depends on technologists' experience through repeated molding trial and repair process to obtain the optimized ones. However, this may give rise to the problem of prolonging production period and thus increasing the cost in actual production process. Therefore, a hybrid intelligent model is constructed herein, employing CBR, NNR, AMR and FI, to intelligently recommend process parameters for DPVC. The actual production cases show that, compared with traditional method, this intelligent recommending system can shorten the production period, reduce the cost and improve the stability of product quality. Besides, it can provide a new thought for solving similar problems in other occasions.

ACKNOWLEDGMENT

The project is supported by the National Science Foundation for Post-doctoral Scientists of China (Grant No. 2011M500755) and Shanghai Key Laboratory of Manufacturing Automation and Robotics(Grant No. ZZ0803).

REFERENCES

[1] LIU Hongjun,LI Yamin, and CAO Chi, "Development trends and demand analysis of rapid tooling technology," *Mould Industry*, vol.36, pp.63–66. May 2010.

[2] WOHLERS T, *Wohlers report 2012*, Wohlers Associates. USA,2012, pp.33–39.

[3] Oertel G. *Polyurethane Handbook*, NewYork: Hanser Publishers, 1985, pp.69–73.

[4] Min K, Hwang Y, and Choi G, "Effect of Reactive Polyurethane on Toughness of Unsaturated Polyester resin," *ApplPolym Sci*, vol.84, pp.735–740, April 2002.

[5] Y.J. Lee, C.H.Chung,and Y.T.Jhan,"Mold-flow Analysis for Manufacturing FRP Structures in Vacuum Assisted Resin Transfer Molding," *Conference Proceedings, Japan Society of Naval Architects and Ocean Engineers*, vol.21-23, pp. 345–348, November 2006.

[6] Y.K.Shen, J.J.Liu,C.T.Hartnett ,and C.Y. Chiu , "Comparison of The Results For Semisolid And Plastic Injection Molding process," *Heat Mass Transfer*,vol. 29, pp.97–105, October 2002.

[7] Athanasios Bikas, Nikos Pantelelis, Andreas Kanarachos, "Computational tools for the optimal design of the injection molding process," *Materials Processing Technology*, vol.122, pp.112–126, March 2002.

[8] Shen C Y, Wang L X , and Li Q, "Optimization of injection molding process parameters using combination of artificial neural network and genetic algorithm method,"*Journal of Materials Processing Technology*, vol.183, pp.412–418, March 2007.

[9] HUANG F, GU J, XU J, "The optimum method on injection molding condition based on RBF network and ant colony algorithm," *Proceedings of the first ACM/SIGEVO Summit on Genetic and Evolutionary Computation. Shanghai*, pp.835–838, June 2009.

[10] Zhou J , Turng L S , Kramschuster A, "Single and multiobjective optimization for injection molding using numerical simulation with surrogate models and genetic algorithms," *International Polymer Processing*, vol.21, pp.509–520, 2006.

[11] Yao Tao,Wang Pengcheng, "Optitimized Design of injection Molding Process Parameters Based on Grey Relational Analysis,"*Journal of InnerMongolia University of Technology*, vol.23, pp.273–277, 2004.

[12] Gao Yuehua, Wang Xicheng, "An effective warpage optimization method in injection molding based on the Kriging model,"*The International Journal of Advanced Manufacturing Technology*, vol.37, pp.953–960, June 2008.

[13] Gao Yuehua, Wang Xicheng, "Warpage optimization and influence factor analysis of injection molding,"*Journal of Chemical Industry and Engineering*, vol.58, pp.1575–1580, June 2007.

[14] Zhou J , Turng L S, "Process optimization of injection molding using an adaptive surrogate model with Gaussian process approach," *Polymer Engineering and Science*, vol.47, pp. 684–694, Mar 2007.

[15] C.K.Kong,G.F.Smith,"Application of Case Based Reasoning in Injection Molding," *Materials Processing Technology*, vol.63, pp.463–467, January 1997.

[16] K.Shelesh-Nezhad, E.Siores, "An intelligent system for plastic injection molding process design,"*Materials Processing Technology*, vol.63, pp.458–462, January 1997.

[17] He W, Zhang Y F , Lee K S , Fuh J Y H , and Nee A Y C, "Automated process parameter resetting for injection molding: a fuzzy-neuro approach," *Intelligent Manufacturing* , vol.9, pp.17–27, January 1998.

[18] Lau H C W , Wong T T , and Pun K F, "Neural-fuzzy modeling of plastic injection molding machine for intelligent control1," *Expert Systems with Applications* , vol.17, pp. 33–43,1999.

[19] Tan K H , Yuen M M F, A fuzzy multi-objective approach for minimization of injection molding defects , *Polymer Engineering and Science* , vol.40, pp. 956–971, 2000.

Zhuangya Zhang is a Ph.D. student in shanghai University, Shanghai, China. He received his master degree from Henan University of science and technology in 2010. His current main research interests include intelligent system, expert system and rapid prototyping papid tools.

Haiguang Zhang is a lecturer in Shanghai University, Shanghai, China. She received her Ph.D. degree from the Shanghai University in 2011. Currently, Her main research interests include intelligent system, expert system and rapid prototyping tool.

Yuanyuan Liu is a associate professor in shanghai University, Shanghai, China. She received her Ph.D. degree from the shanghai jiaotong university, in 2008. Currently, Her main research interests include The control system design theory and Engineering application.

Qingxi Hu is a professor at shanghai University Shanghai, China. He received his Ph.D. degree from the Hua zhong University of science and technology in 1997. Currently, His main research interests include rapid prototyping tools, expert system and intelligent system, etc.

Distributed Service Discovery Algorithm Based on Ant Colony Algorithm

Chijun Zhang
College of Management Science and Information Engineering, Jilin University of Finance and Economics, Changchun, China
Key Laboratory of Logistics Industry Economy and Intelligent Logistics at Universities of Jilin Province , Changchun, China
Email: cjzhang6@163.com

Guanyu Mu*
College of Management Science and Information Engineering, Jilin University of Finance and Economics, Changchun, China
Email: guangyumu@126.com

He Chen
College of Communication Engineering, Jilin University, Changchun, China

Tiezheng Sun, Liyan Pang
College of Management Science and Information Engineering, Jilin University of Finance and Economics, Changchun, China

***Abstract*—UDDI is a universal description, discovery and integration protocol. As a public registry of Web service, it is designed to store information about each company and its service. Traditional centralized service discovery structure of UDDI service registration center does not apply to large-scale service discovery. When all the services register to a center, the service bottleneck, failure of single point and the poor scalability defects will occur. In addition, traditional service matching mechanisms are mainly based on keywords method which lacks of semantic description and makes the service publisher and demanders cannot reach a common semantic understanding. This will lead to the problems of semantic conflicts and low accuracy that seriously affects the precision and recall of service matching. To address these shortcomings of the centralized service discovery structure of UDDI, we propose a distributed semantic service registration center which is in the construction of loosely coupled P2P network enabled the progressive massive search. In the P2P distributed network, there can be a large number of nodes to store the registration information which is suitable for large-scale service because of the adaptivity, scalability and good fault tolerance characteristics. In order to reduce the number of concurrent transmitted packets, the advanced ant colony algorithm is introduced to forward packets by probabilistic choice. The results comparison with the traditional algorithm is given through the simulation experiments and it has shown that the proposed method has good performance for the distributed service discovery**

***Index Terms*—UDDI, P2P distributed network, Semantic, Ant colony algorithm**

I. INTRODUCTION

The emergence of e-commerce is an important change of combining business and the information technology together. At the same time, the service-oriented is another breakthrough which provides a variety of opportunities to find new customers, supply flow and new service for business entities [1-3]. Web service architecture is accomplished through a series of open protocols and specifications. The most important three protocols are SOAP (service-oriented architecture), WSDL (Web Service Definition Language) and UDDI (universal description, discovery and integration). UDDI is the key technologies for service publishing. It provides universal description, discovery and integration of Web service and the Web service lookup operation can be implemented with the combination of UDDI and WSDL. The core components of UDDI is the UDDI business registry,which describe the business entities and their Web service in XML file. The information provided by the UDDI business registration consists of three parts of the white, yellow and green pages respectively [4-7].

Traditional UDDI service registry center utilizes the centralized service discovery model where all service is concentrated in one server. The lookup method of this structure is simple and the speed is relative fast. However, the drawbacks are the existence of a single point of failure, performance bottlenecks, and not suitable for large-scale service discovery [8-11]. On the other hand, UDDI service description is commonly in form of the WSDL documents that does not support non-functional semantic description and attributes of service quality, which is not suitable for the semantic extension of service description [12-16]. Requirements of service demanders cannot be well described in the WSDL documents and it only supports simple keyword comparison for the technical details as well.

doi:10.4304/jsw.9.1.70-75

To overcome the disadvantages of the centralized structure of UDDI, the P2P distributed network is proposed in many researches [17, 18]. In the P2P network, there can be a large number of nodes storing the registration information and it is suitable for large-scale service due to the adaptivity, scalability and good fault tolerance characteristics. However, information searching algorithm of the fully distributed unstructured P2P network has certain blindness due to the low routing efficiency and poor scalability. For large-scale distributed service, the service discovery efficiency is not very high. The current solutions are of the following aspects. METEOR-S proposed the creation of a shared ontology [19]. Each UDDI service registration center in the P2P network maps the registered service on it to one or more ontology concepts and then use the shared ontology to organize the P2P topology. Chen etc. proposed to use DNS to manage P2P nodes[20]. However, these proposed methods are mostly tightly coupled.

As a capable language that can express the service capabilities, adopting semantic description for service registry architecture can provide good intelligence [21, 22]. Registration center of UDDI service introduces semantic annotations so that services and ontology concepts can be associated together. Utilizing ontology concept identifications which are already associated with Web service in the semantic routing table so that it is not to deal with the UDDI server but the service on UDDI server when conducting the route searching processes. At the same time, the concept ID and server ID are bundled in the routing table can solve the problem of mapping between service and servers.

In this paper, an improved distributed service discovery algorithm based on agent and the ant colony algorithm was proposed for the Internet on the basis of constructing the semantic routing. For the service discovery mechanisms in the P2P network, ontology-based knowledge was introduced for publishing and discovering the web services in the service registry. Concepts and relations in ontology were superimposed to the network to construct the service request routing to improve the service discovery and query capabilities. Through the analysis of Comparative experiments with the Spay and Wait protocol, the proposed algorithm has shown better performance in many aspects.

The article is organized as follows. Section 2 provides the main theory of the advanced semantic routing method based on ant colony algorithm. The evaluation results are illustrated in section 3 by comparing the proposed algorithm with the Spay and Wait protocol. Section 4 is our concluding remarks.

II. Algorithms

A. Figures and Tables

The basis of the algorithm is to construct the semantic routing table. The identifications of a routing table on the regular network are constituted by IP addresses, while the semantic routing table consists of the identifications of the concepts from the ontology knowledge base. Semantic routing table is shown in Table 1. Concept represents the concept in the ontology which is associated with the specific service. Next hop represents the next server of the local server which leads to reach the server where the concept Ci is located. Hop count is on behalf of the total number of the hops to the destination server when node Nj serves as the next hop. Pheromone represents the pheromone left by the ants.

TABLE 1:

THE SEMANTIC ROUTING TABLE

Concept	Next hop	Hop count	Pheromone
Ci	Nj	m	phi
Ci	Nk	n	ph**j**
Cj	Ni	k	phk
Ck	Nj	…	…
…	…	…	…

B. Improve the Ant Colony Algorithm

It has the advantage of high convergence rate and has attracted a lot of scholars engaged in the study of the theory and application of it.

Ant colony algorithm is a kind of modern swarm intelligence algorithm inspired by the behavior of ants foraging process. It has the advantage of high convergence rate. In the ant colony algorithm, each path has the distribution of ant pheromone. Note that the pheromone is a kind of special chemical odor left on the path in the process of ants moving.

P2P service discovery is not to find a target node, but to find all nodes where the target services locate as much as possible. Therefore, this paper proposed an advanced protocol algorithm (ASW) based on the Spray and Wait protocol and ant colony algorithm.

In the proposed algorithm, packets transmitted by the P2P service discovery agent are corresponding to the ants. The agent searches for the appropriate service agent based on semantic routing table, which means to search for the ontology concepts associated with the appropriate services. The concepts of qualifying the searching conditions in the routing table may be multiple and the pheromone will be the basis for probability of selecting. When found the appropriate service, the agent will update the routing tables and pheromone along the path, through which the semantic routing table can be dynamically maintained. A service may correspond to more than one ontology concept and the searching algorithm is applicable.

C. Routing

The delivery of messages is represented by the ant walking. First, the agent queries the ontology concept ID associated with the services to be searched in the routing table. If there is no appropriate ID, k nodes will be randomly selected for packet forwarding. If multiple

concept IDs are filtered out, the probability of reaching the target node according to the routing list will be calculated according to the pheromone. The probability selection formula is as follows.

$$p_{ij}^{k}=\begin{cases}\dfrac{[\tau_{ij}(t)]^{\alpha}[1/d_{ij}]^{\beta}}{\sum_{s\in allowed_k}[\tau_{is}(t)]^{\alpha}[1/d_{is}]^{\beta}} & j\in allowed_k(i)\\ 0 & \text{Others}\end{cases} \quad (1)$$

p_{ij}^{k} is the probability value under the condition that the k-th ant at the i-th node sets the j-th node as the destination; $\tau_{ij}(t)$ is the pheromone dispersed on the path of the i-th and j-th node at time t; $allowed_k(i)$ is the non-visited nodes when the k-th ant is at the i-th node; the distribution of α and β represents the degree of importance for pheromone and visibility.

The greater $\tau_{ij}(t)$ is and the shorter the distance between node i and node j is, the probability of the path ij being selected will be greater.

K nodes around will be selected to transmit the package according to the value of p_{ij}^{k}.

D. Update of the Pheromone

After finding the target service, the agent needs to update the density of the pheromone on the passing paths as the routing basis of other agents. $\tau_{ij}(t)$ will be updated at each iteration, as shown in the formula below.

$$\tau_{ij}(t+\Delta t)\leftarrow\sum_{k=1}^{m}\Delta\tau_{ij}^{k} \quad (2)$$

M is the number of ants and $\Delta\tau_{ij}^{k}$ is the incremental of the pheromone at the k-th interation. The calucation formular of $\Delta\tau_{ij}^{k}$ is as follows.

$$\Delta\tau_{ij}^{k}=\begin{cases}\dfrac{Q}{L_k} & if\ (i,j)\in tour\ \ done\ \ by\ \ ant\ \ k\\ 0 & otherwise\end{cases} \quad (3)$$

Lk is the total length of paths after the k-th ant completing travelling around. Q is a constant to control the increasing speed of $\Delta\tau_{ij}^{k}$.

At the same time, pheromone on each route of the routing table regularly volatilizes. The pheromone will volatile to none if haven't been update for a long time which means the services associated with ontology concepts of the target node may be canceled or the target node has exited the network. The pheromone evaporation formula is as follows.

$\tau_{ij}(t+\Delta t)\leftarrow\rho\tau_{ij}(t)$, Where $\rho\in(0,1)$. (4)

E. Life Time Control

In order to control the packets (ants) roaming around network, a life cycle TTL is set for every packet. When a packet is produced, TTL of it is set to an initial value and it decreases by1 when forwarded once only if the next node is not the destination. If the next node is the target node, then TTL stays unchanged. These measures are conducive to the messages (ants) to search more service. When TTL is 0, the ants automatically die.

F. Maintaining the Semantics Routing Table

In the beginning, when each server node is registered to the P2P network, the ontology concepts which are associated with the local server should be broadcasted to the neighbors to construct the initiate routing table. Every concept forms a routing entry. The next hop is the local server and the number of the hop is 1. The pheromone is set to the initiate pheromone value. After the ants roaming and finding the target node where target service located, the update process including the hops, next hop and the pheromone will be adopted.

III. EXPERIMENT

The simulator ONE is utilized to provide the opportunity network environment. The parameter settings for the ant colony algorithm are as follows. Alpha which stands for the importance degree of pheromone is 1. Beta which stands for the importance degree of the heuristic factor is 5. Q which is the pheromone increasing strength coefficient is 100. Rho which is the pheromone evaporation coefficient is 0.5. The Simulation duration is set to 200s, 300s and 500s.

For the protocol need to select k rounding nodes as the next hop target nodes, we set k=1, k=3 and k=6 to during the experimental measures respectively. The comparative experiment was done by comparing with the Spay and Wait protocol (SW) marked as SW.

The results analysis was done by collecting the simulation performance reports. The number of the sending packets is shown in Table2.

TABLE 2:

CONFLUENCE OF THE ARRIVING RATES FOR THE SENDING PACKAGES

time	**0.2**	**0.3**	**0.5**
k=6	28	48	73
SW	6	10	17
k=3	26	38	65
k=1	1	1	3

According to Table 2, Figure 1 can be made. From the figure, the number of the sending packets increases in turn of k=1, k=3 and k=6 when utilizing the proposed routing algorithm based on ant colony algorithm, While the number of packets produced by the SW algorithm is between the number of k = 1 and k = 3.

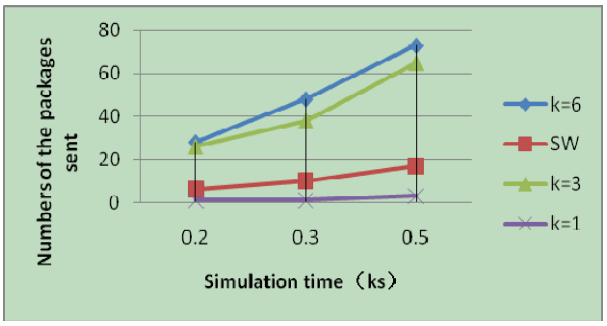


Figure 1: Confluence of the arriving rates for the sending packages

The number of messages reaching the destination is shown in Table 3.

TABLE 3:
CONFLUENCE OF THE NUMBER OF MESSAGES REACHING THE DESTINATION

time	0.2	0.3	0.5
k=6	3	7	11
SW	6	10	17
k=3	3	5	8
k=1	1	1	3

Figure 2 can be made according to Table 3. From the figure, the number of the messages reaching the destination increases in turn of k=1, k=3 and k=6 when utilizing the proposed routing algorithm based on ant colony algorithm. The number of packets reaching the destinations produced by the SW algorithm is the most.

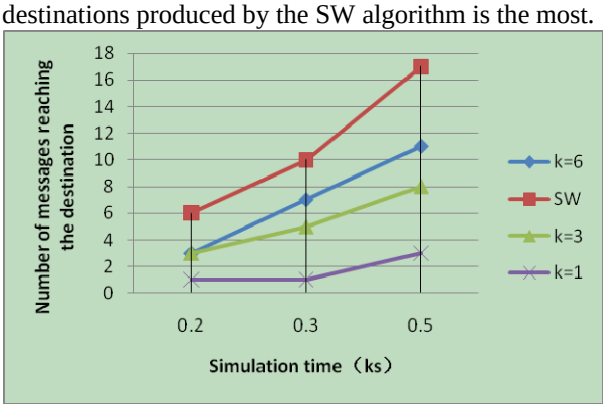


Figure 2: Confluence of the number of messages reaching the destination

The arrival rates of the packets are shown in Table 4.

TABLE 4:
CONFLUENCE OF THE ARRIVAL RATES OF THE SENDING PACKETS

time	0.2	0.3	0.5
k=6	0.5	0.7	0.6471
SW	1	1	1
k=3	0.5	0.5	0.4706
k=1	0.1667	0.1	0.1765

Figure 3 is made according to Table 4. It can be found that the arrival rates of the sending packets increases in turn of k=1, k=3 and k=6 when utilizing the proposed routing algorithm based on ant colony algorithm. The arrival rate of the sending packets produced by the SW algorithm is the greatest.

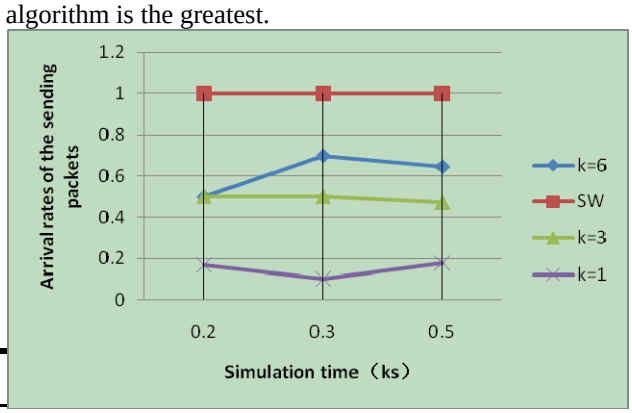


Figure 3: Confluence of the arrival rates of the sending packets

The average delay is shown in Table 5.

TABLE 5:
CONFLUENCE OF THE AVERAGE DELAY

time	0.2	0.3	0.5
k=6	8.5333	12.3857	16
SW	4.2667	3.83	3.4824
k=3	7.2333	8.38	7.2625
k=1	2.7	2.7	2.6333

Figure 4 can be made according to Table 5. It can be found that the average delay increases in turn of k=1, k=3 and k=6 for the proposed routing algorithm based on ant colony algorithm. The average delay produced by the SW algorithm is between the results of k=1 and k=3.

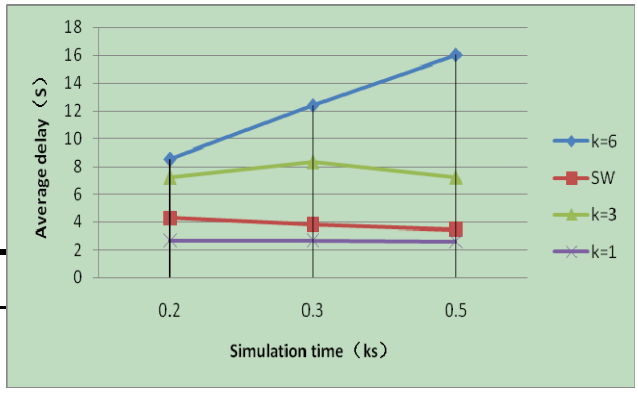


Figure 4: Confluence of the average delay

The return rate is shown in Table 6.

TABLE 6:

CONFLUENCE OF THE RETURN RATE

time	0.2	0.3	0.5
k=6	0.2	0.8	0.8
k=3	0	0.2	0.8
k=1	0	0.2	0.2
SW	0.6	0.6	0.6

Figure 5 can be made according to the Table 6. It can be found that the return rate increases in turn of k=1, k=3 and k=6 for the proposed routing algorithm based on ant colony algorithm. The return rate produced by the SW algorithm mostly does not change with the simulation time.

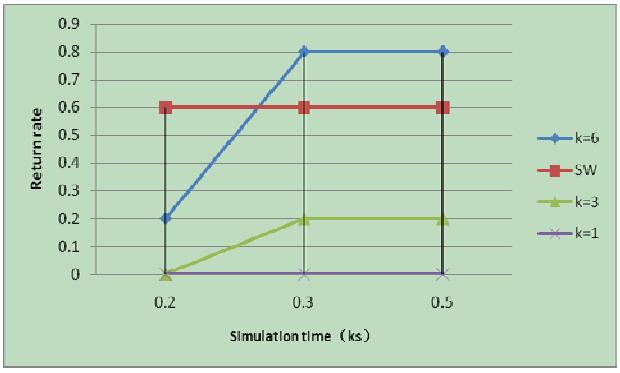


Figure 5: Confluence of the return rate

IV. CONCLUSIONS

On the basis of the semantic routing algorithms, this study proposes a novel distributed service discovery algorithm based on the ant colony algorithm by introducing the probability selection mechanism. The messages choose the next hop by the probabilistic choice in accordance with the distribution of the pheromone. Through the simulation procedures, the proposed algorithm has shown the superiority at the return rate of messages and so on, compared with traditional SW protocol.

ACKNOWLEDGMENT

The authors are grateful to the support of the Science Technology Research Foundation of Jilin Province Education Department under Grant no. 2012184, the Science Technology Research Foundation of Jilin Province Education Department under Grant no. 2012185, no. 2012189, And National Natural Science Foundation of China (NSFC) under Grant no. 61272412, and Jilin province science and technology development plan item under Grant no. 20110303.

REFERENCES

[1] M. Younas, et al., An efficient composition of Web services with active network support, Expert Syst Appl, vol. 31, no. 4, 2006, pp. 859-869.
[2] M. Zur Muehlen, et al., Developing web services choreography standards—the case of REST vs. SOAP, Decis Support Syst, vol. 40, no. 1, 2005, pp. 9-29.
[3] Y. Cardinale, et al., Web service selection for transactional composition, Procedia Computer Science, vol. 1, no. 1, 2010, pp. 2689-2698.
[4] B. Gengler, UDDI Has Problems, Computer Fraud & Security, vol. 2001, no. 8, 2001, pp. 5-6.
[5] M.B. Juric, et al., WSDL and UDDI extensions for version support in web services, J Syst Software, vol. 82, no. 8, 2009, pp. 1326-1343.
[6] M.B. Juric, et al., WSDL and UDDI extensions for version support in web services, J Syst Software, vol. 82, no. 8, 2009, pp. 1326-1343.
[7] J.A. Shuler, XML, UDDI, and SOAP: the “Verbs” and “Nouns” of “Semantic Electronic Government Information”: edited by John A. Shuler, The Journal of Academic Librarianship, vol. 27, no. 6, 2001, pp. 467-469.
[8] Q. Tao, et al., A novel prediction approach for trustworthy QoS of web services, Expert Syst Appl, vol. 39, no. 3, 2012, pp. 3676-3681.
[9] J. Kouki, et al., An Agent-Based Approach for Binding Synchronization of Web Services, Procedia Computer Science, vol. 10, no. 0, 2012, pp. 921-926.
[10] C. Makris, et al., Efficient and adaptive discovery techniques of Web Services handling large data sets, J Syst Software, vol. 79, no. 4, 2006, pp. 480-495.
[11] S. Pastore, The service discovery methods issue: A web services UDDI specification framework integrated in a grid environment, J Netw Comput Appl, vol. 31, no. 2, 2008, pp. 93-107.
[12] N. Gibbins, et al., Agent-based Semantic Web Services, Web Semantics: Science, Services and Agents on the World Wide Web, vol. 1, no. 2, 2004, pp. 141-154.
[13] M.L. Sbodio, et al., Discovering Semantic Web services using SPARQL and intelligent agents, Web Semantics: Science, Services and Agents on the World Wide Web, vol. 8, no. 4, 2010, pp. 310-328.
[14] J.M. García, et al., Improving semantic web services discovery using SPARQL-based repository filtering, Web Semantics: Science, Services and Agents on the World Wide Web, no. 0.
[15] M. Sabou, et al., Learning domain ontologies for semantic Web service descriptions, Web Semantics: Science, Services and Agents on the World Wide Web, vol. 3, no. 4, 2005, pp. 340-365.
[16] M. Sabou and J. Pan, Towards semantically enhanced Web service repositories, Web Semantics: Science, Services and Agents on the World Wide Web, vol. 5, no. 2, 2007, pp. 142-150.
[17] G.J. Fakas and B. Karakostas, A peer to peer (P2P) architecture for dynamic workflow management, Inform Software Tech, vol. 46, no. 6, 2004, pp. 423-431.
[18] D. Ghosal, et al., P2P contracts: a framework for resource and service exchange, Future Gener Comp Sy, vol. 21, no. 3, 2005, pp. 333-347.
[19] S.K.S.A. K, A scalable P2P infrastructure of registries for semantic publication and discovery of Web service, Journal of Information Technology and Management, vol. 6, no. 1, 2005, pp. 17-39.
[20] X.B.C.Y. DW, A P2P based Web service discovery mechanism with bounding deployment and publication,

Chinese Journal of Computers, vol. 28, no. 4, 2005, pp. 615-626.

[21] H.N. Talantikite, et al., Semantic annotations for web services discovery and composition, Computer Standards & Interfaces, vol. 31, no. 6, 2009, pp. 1108-1117.

[22] W. Kim, et al., WSCPC: An architecture using semantic web services for collaborative product commerce, Comput Ind, vol. 57, no. 8–9, 2006, pp. 787-796.

\

Chijun Zhang, born in 1972, Vice Professor and Ph.D. Member of Key Laboratory of Logistics Industry Economy and Intelligent Logistics at Universities of Jilin Province. Her current interests include things of internet, wireless network and semantic theory.

Guanyu Mu, born in 1971, Vice Professor and Ph.D. Her current interests include the information manage.

He Chen, M.S. candidate. Her current research interests include multi-agent theory.

Tiezheng Sun, born in 1981, Ph.D candidate. His interests include Nondestructive testing and on-line detection.

Liyan Pang, born in 1975, M.S. Her current interests include Business Information Management.

A Risk Model of Requirements Change Impact Analysis

Marfizah Abdul Rahman, Rozilawati Razali and Dalbir Singh
Centre of Software Technology and Management, Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, 43600, UKM Bangi, Selangor, Malaysia
Email: marfizah@gmail.com, rozila@ftsm.ukm.my, dalbir@ftsm.ukm.my

***Abstract*—Software systems are critical assets to organisations as they support important business processes and workflow. To maintain the value of these assets, the requirements of software systems must evolve whenever there are changes in business needs. A key problem to organisations is implementing requirements change to the existing software systems. Such initiatives need proper analyses so that their effects could be determined before resources are spent. Impact analysis is therefore an important step in requirements change management. As a project, any change implementation involves risks. It is thus necessary for impact analysis to consider risk factors for implementing requirements change. However to date, the risk factors concerning requirement change are not much explored. This paper aims to identify the risk factors for implementing requirements change. The risk factors were identified through two qualitative approaches, namely a review of related work and a focus group study. The former involved fifty published articles and the latter concerned five domain experts. The collected risk factors from both studies were analysed by using content analysis. The risk factors form a risk model for analysing impacts of implementing requirements change. The model helps practitioners to assess the viability of requirements change requests.**

***Index Terms*—requirements change management, risk factor, impact analysis**

I. INTRODUCTION

Software is dynamic and changes rapidly in order to respond to various business needs. There are many causes of software changes. One of them is due to addition and modification of requirements. Requirements change takes place in both development and maintenance phases [1]. One fourth of requirements change occur during maintenance phase [2]. As compared to development, requirements change that happens during maintenance is more costly since the software has been put into operation and used by its users [3].

Users issue requirements change through change request forms, which information is used during impact analysis. Impact analysis analyses current environment and foresees the possible effects on the existing software when implementing the requested change. The results of impact analysis guide the Change Control Board (CCB) to decide whether the requested change should be implemented. Any approved change request is indeed a software project where its scope, cost and schedule for implementation are defined. Impact analysis therefore needs to be accurate in order to avoid the failure of such projects.

As a software project, it is necessary for CCB to assess risks during impact analysis for requirements change [3]. Risk is an event that triggers unwanted conditions that could bring harm and loss to a project. Risks are managed through a set of action plans [4]. Risk assessment in particular involves risk identification, risk analysis and risk prioritisation [5]. Despite its importance, it is uncertain how to incorporate risk assessment during impact analysis for requirements change.

The key aspect of risk assessment is the categorisation of risk factors. The aim of this paper is to explore the risk factors that should be analysed during impact analysis concerning projects involving requirements change. The individual risks are collated from theoretical and empirical work as a conceptual model that shows the interrelationships among several categories of risk factors. The model acts as a guide for assessing risks in implementing requirements change. The paper is organised as follows: Section 2 provides the related work on the subject matter. Section 3 briefly explains the methodology used. Section 4 presents and elaborates the proposed model. Finally, Section 5 concludes the paper with a summary that outlines the main findings and future work.

II. RELATED WORK

Requirements change has been a critical issue in software development projects. One particular issue in requirements change is how to deal with the requirements change before implementing them. A proper process of managing requirements change can ensure the successful implementation of the change. The critical step in managing requirements change is to decide either to accept or reject the requested change [6,7]. Such a difficult decision has to be made by a dedicated technical committee, namely Change Control Board (CCB) through impact analysis [8,9]. During impact analysis, the affected elements will be analysed [10]. To date, it is

doi:10.4304/jsw.9.1.76-81

uncertain how CCB should analyse the impacts of those elements and subsequently decide the way forward [11].

Users issue changes in requirements through change request forms. A change request form contains change attributes such as reasons, types and sources of change, which are necessary for project team to understand the request [12]. Requirements change normally affects software and hardware of the current system. When considering a change request, source code [13,14], documentation [15], tools [16] and architecture [14] of the existing software are examined to assess the impacts. The change in software normally causes some changes in hardware and vice-versa. The changes in hardware include memory usage [17], performance [3] and platform [18]. The change is complex if it involves a new software or hardware technology that has not been used in prior projects [19,20].

Requirements change also concerns human aspects. Project team is responsible to analyse the change request forms received from users. To ensure the feasibility of the change, assessing the project team's capability such as skill, knowledge, experience and motivation during impact analysis is important [21]. On the other hand, user involvement is necessary so that the users are aware of the systems' operations after the change [22]. Furthermore, the users can also provide information about the current system and clarify the change that they requested [23].

Although requirements change provides an opportunity for a software system to improve its value, it triggers risk. Improper implementation of requirements change can cause late delivery, cost overrun, low product quality and sometimes failure to the entire software project [24]. Therefore, it is important to analyse the risk factors in implementing the requirements change through impact analysis [3]. The risk factors are indeed the affected and affecting elements of the change. The analysis of the these elements helps to reduce the ripple effects and unforeseen outcomes before the change is implemented [3].

Requirements change initiatives are considered as software projects and thus, risk factors concerning projects also apply to them. Inexperienced, lack of knowledge and skill among project team members are widely known project risks [19]. In addition, lack of commitment from team members towards the project and ineffective communication between team members and users also impede project success [20]. Besides project team and users, a project is also risky if it fails to gain support and commitment from the top management [20]; [25]. Furthermore, the number of third party involved [20] and degree of dependency on them also contribute to project risks [25].

Both technical and non-technical elements mentioned above influence the schedule and cost to implement a requirements change. A study shows that optimising the schedule can result in significant time saving to implement the change [26]. There are four factors related to cost in requirements change, namely the number of project team members and consultants as well as project duration, size and scope [27]. Inaccurate judgment of the affected and affecting elements may cause in inadequate allocation of time and cost for implementing the change [19,20].

The review above indicates that there are various elements that are deemed necessary when managing requirements change. As the elements contribute to the success or failure of a requirements change project, they are considered as risks. The identified risk however are scattered and treated discretely. It is unclear how these risks influence each other and can be classified as risk factors of implementing requirements change.

III. METHODOLOGY

The purpose of this study was to identify the risk factors of implementing requirements change. The identified risk factors could help CCB to assess the impacts of the requested requirements change and decide whether the project team should implement it. In order to ensure the identified risk factors are holistic and practical, the study employed both theoretical and empirical approaches. The former concerned a review of previous studies whereas the latter involved a focus group interview with practitioners from software industry. Fig. 1 illustrates the research design, which contains the main activities involved in the study.

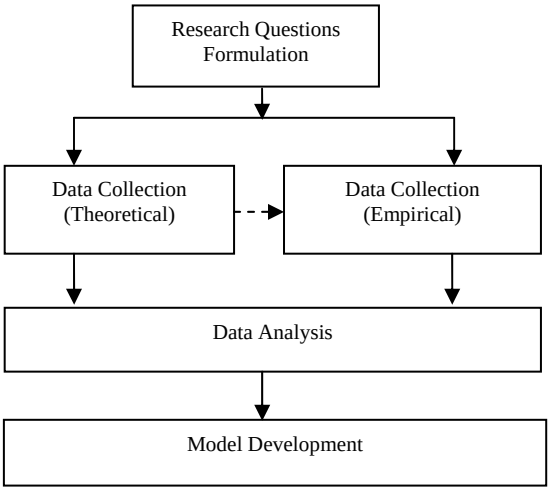


Figure 1. Research design

The following paragraphs explain each activity briefly:

- Formulate Research Questions

In general, the study aimed to answer the following research questions. The questions were generated based on a preliminary study made on the subject matter.

What are the risk factors involved in implementing requirements change? How do these factors relate to each other during impact analysis of requirements change implementation?

- Collect Theoretical Data – A Review

The objective of the review was to determine the risk elements concerning requirements change implementation as a software development project, which should be analysed during impact analysis. The keywords used in searching the articles therefore included "change impact analysis", "software change impact analysis", "requirements change impact analysis", "requirements change", "software change", "software risk" and "software development risk". There was about one hundred articles found but only fifty were selected for further analysis. The other fifty articles were rejected, as they are not relevant to the study. The searching was performed on several prominent online databases. The articles were from year 1995 until 2012 that covered both journals and conference proceedings. The findings of the review can be found in the earlier study [28].

- Collect Empirical Data – A Focus Group Interview

In order to confirm the risk elements found in the literature, a focus group interview with several domain experts and practitioners from the industry was conducted. Focus group is a planned discussion to gather information of interest in a permissive and non-threatening environment [29]. The approach was selected because it captures ideas and background regarding process and product through first degree contact and direct access to participants [30].

The focus group employed the approach suggested by [31]. The interview used semi-structured questions, which were constructed based on the risk elements found in the review. The questions also adopted the factors proposed by [32,33]. Prior to the real session, a pilot study was conducted with five software developers. The purpose of the pilot study was to validate the accuracy and completeness of the questions as well as the feasibility of the session. The feedback received from the pilot study was used to improve the planning of the real session.

Predefined selection criteria of informants were set in order to ensure the gathered data would be meaningful. The potential informants must possess more than ten years of experience in software development and must be involved in requirements change management process. To fulfill this requirement, the study employed purposive sampling [34]. The study identified and invited eight informants to the session. A formal invitation letter was sent to them, which contains information regarding the focus group session such as purpose, impact of the study, date, time and venue. Only five informants agreed to attend and thus the response rate was 62%. All of them were government servants. Table 1 provides brief background information about the informants.

The focus group session took about two hours and was video-recorded. Before the session commenced, the author explained the procedure and acquired participation agreement from the informants through consent forms.

TABLE I.
INFORMANTS' BACKGROUND

Agency	System	Informant	Designation
A	A1	I1	Head of project
	A2	I2	Head of unit
B	B1	I3	Head of project
	B2	I4	Head of unit
C	C1	I5	Head of unit

- Analyse Data and Construct the Model

The collected data from both theoretical and empirical work were transcribed and analysed by using content analysis. Content analysis is a research technique for making replicable and valid inferences from text to the contexts of their use, in a way of providing knowledge, new insights, a presentation of facts and a practical guide to action [35]. The first step was to identify the significant risk elements based on frequency analysis. The elements were grouped into several distinct risk factors. Table 2 tabulates the significant risk factors concerning requirements change management found in the review and the focus group interview respectively. Each risk factor constitutes the corresponding risk elements. Most elements were present in both work (marked with /). Nine elements (marked with X in "Theoretical-Review" column) emerged only from the empirical work. Since the experts in the focus group strongly advocated these items, they therefore were included in the model. The numbers in brackets represent the number of informants mentioned about the elements. For example, 4/5 means four out of five informants agreed on the element. In terms of importance, the informants ranked the risk factors from the most important to the least as follows: Project Team, Identification of Change, Software, Hardware, User, Top Management, Planning of Change Implementation, Strategic Planning, Technology Standard and Third Party. The risk factors were categorised into four main components, namely People, Process, Product (Existing) and Organisation. The second step was to connect the risk factors systematically and conceptualise them as a model. The detailed description of the model is included in the next section.

IV. THE MODEL

Figure 2 below illustrates a risk model of requirements change impact analysis. The model contains four essential components: People, Process, Product (Existing) and Organisation. Each component consists of several risk factors and the corresponding risk elements that need to be considered holistically during impact analysis for implementing requirements change. The risk factors are interconnected during the process. The arrows between the risk factors in the model indicate the relationships that they have on each other.

TABLE II.
RISK ELEMENTS AND FACTORS FOR REQUIREMENTS CHANGE

Component	Risk Factors and Elements	Theoritical -Review	Empirical -Focus Group (Frequency)
People	User		
	Involvement	/	/ (5/5)
	Knowledge	/	/ (5/5)
	Commitment	/	/ (4/5)
	Communication	/	/ (5/5)
	Readiness	X	/ (3/5)
	Cooperation	/	/ (3/5)
	Project Team		
	Skill	/	/ (5/5)
	Knowledge	/	/ (5/5)
	Experience	/	/ (2/5)
	Motivation	/	/ (2/5)
	Commitment	/	/ (5/5)
	Communication	/	/ (5/5)
	Top Management		
	Support	/	/ (5/5)
	Commitment	/	/ (5/5)
	Third Party		
	Number of third party involved	/	/ (2/5)
	Dependency to external agents	/	/ (4/5)
Process	Identification of Change		
	Reasons	/	/ (5/5)
	Type	/	/ (3/5)
	Source	/	/ (4/5)
	Planning		
	Effort	/	/ (5/5)
	Scheduling	/	/ (5/5)
	Cost	/	/ (3/5)
Product (Existing)	Software		
	Source code	/	/ (3/5)
	Software architecture	/	/ (5/5)
	Tools	/	/ (4/5)
	Documentation	/	/ (2/5)
	Integration	X	/ (3/5)
	Interface	X	/ (3/5)
	Hardware		
	Memory space	/	/ (3/5)
	CPU Performance	/	/ (2/5)
	Platform	/	/ (2/5)
	Integration	X	/ (3/5)
	Interface	X	/ (3/5)
Organisation	Technology Standard		
	Software	X	/ (4/5)
	Hardware	X	/ (4/5)
	Strategic Planning		
	Policy	X	/ (4/5)
	Goal	X	/ (4/5)

The *People* component consists of user, project team, top management and third party. Normally, the user issues a change request through a change request form. The project team is responsible to review and analyse the change request and estimate the change. To ensure comprehensive analysis and estimation, the project team should possess appropriate skills, knowledge and experience about the system. In addition, the project team's motivation and commitment during impact analysis are also essential. The project team also needs to communicate effectively with the user. Due to incomplete and ambiguous information in the change request form, the project team often requires further elaboration from the user. User involvement is therefore important. The user must understand the change that he or she raises. He or she also must cooperate and commit when analysing the impacts. Changes normally cause resistance among users. Consequently, it is necessary to measure users' readiness before implementing the change.

After identifying and understanding the requested change from the user, the project team has to estimate the change. When estimating the effort, cost and schedule of the change, the project team requires commitment and support from the top management. The effort may need to be adjusted based on the approved cost and permitted schedule by the top management. The number of third party involved in the project and the degree of dependency towards them also influence the planning of change implementation.

The *Process* component contains two main activities concerning impact analysis, namely identification of change and planning of change implementation. The identification of change is based on the information included in the change request form. It is important to identify the reason, type and source of the change in order to analyse the urgency and impacts that they would bring to the existing product. On the other hand, the latter concerns the planning of effort, schedule and cost based on the involvement of third party and top management, project team's capability, existing hardware and software capacity as well as organisational settings.

The *Product* component encompasses the existing hardware and software. Software comprises source code, software architecture, tools and documentation. Based on the information stated in the change request form, source code is analysed to determine the possible affected parts by the change. Changes to source code normally require software architecture and current documentation to be updated. Moreover, changes in a particular software component can affect the hardware especially the memory space, CPU performance and platform.

Subsequently, changes to hardware may entail certain software configuration. A large system may integrate and interface with other systems. The integration and interface happen at the software and hardware levels. Any changes made to these components require modification to their dependencies. Through the product analysis, the estimation of the affected elements can be determined.

The *Organisation* component contains the organisational technology standards and strategic planning. Technology standards refer to specific hardware and software criterion specified by the organisation, which have to be adhered to in any software development and maintenance projects. Each organisation possesses strategic plans such as policies that outline its roadmap and strategies to be taken in order to fulfil its vision and mission. To ensure software development strategies align with organisational strategies, any change implementation must be checked against both the technology standards and strategic plans set by the organisation. These requirements are considered when planning the effort, cost and schedule of change implementation.

V. Conclusion And Future Work

This paper has discussed the risk factors together with the corresponding risk elements concerning requirements change, which should be considered during impact analysis. They were gathered through a literature review and a focus group interview involving experts. The risk elements and factors form a risk model that could guide practitioners in assessing the risks of implementing requirements change. Rather than relying on conventional wisdom, practitioners could currently execute the impact analysis more guided and systematically.

The study was broad-brush and qualitative. The findings should therefore be refined and strengthen further by confirming the risk elements and factors quantitatively through a large scale survey. In addition, the quantitative analysis enables the generation of specific metrics for measuring the risk elements and factors. The model could then be extended as a risk measurement model for requirements change initiatives.

Acknowledgement

This work was funded by Universiti Kebangsaan Malaysia (UKM-GUP-2012-005).

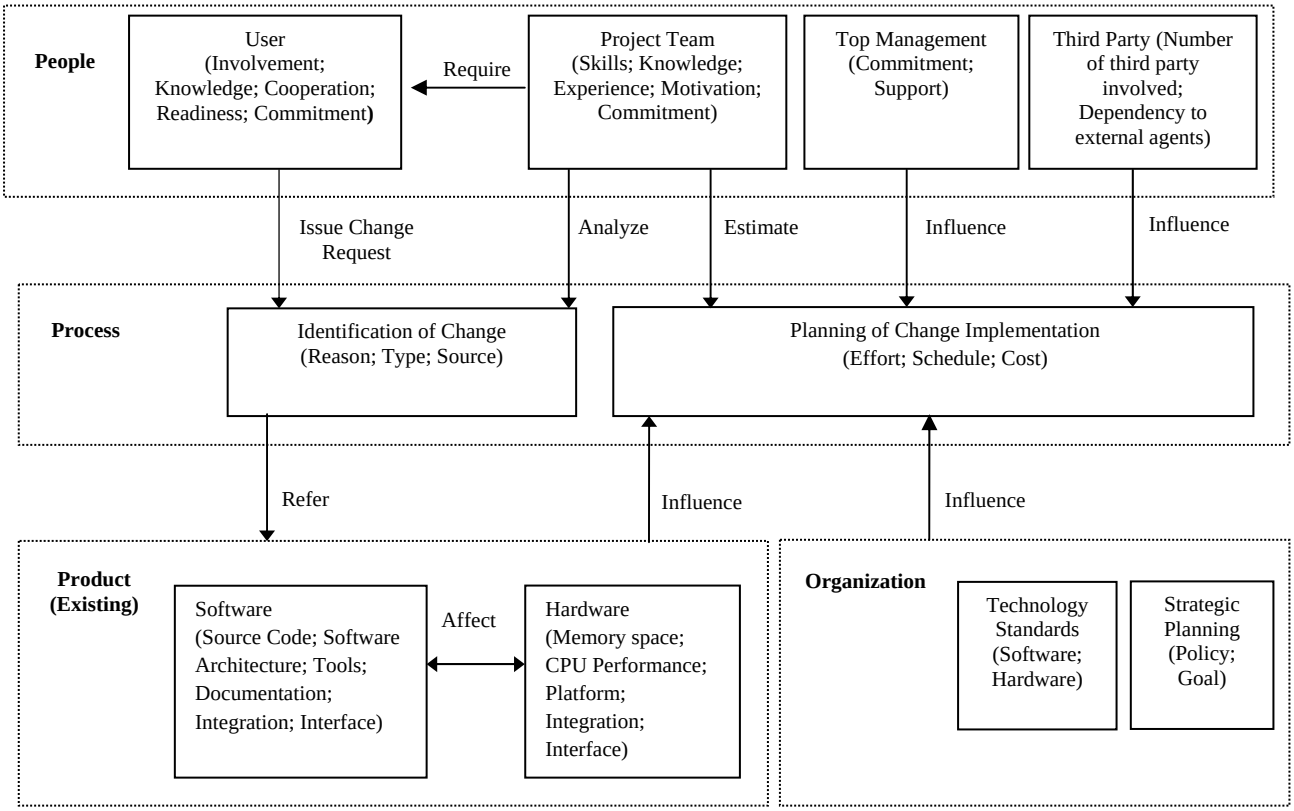


Figure 2. A Risk Model of Requirements Change Impact Analysis

REFERENCES

[1] M. K. Gungor, E. Elbasi, and J. W. Fawcett, "New change impact factor estimation in software," *Turk J Elec Eng Comp Sci*, vol. 20, no. 1, pp. 1–14, 2012.

[2] M. W. Bhatti, F. Hayat, and S. Ahmed, "An Investigation of Changing Requirements with respect to Development Phases of a Software Project," *Inf. Syst.*, pp. 323–327, 2010.

[3] B. J. Williams and P. B. J. Williams, "Change Risk Assessment : Understanding Risks Involved in Changing Software Requirements," *2006 Int. Conf. Softw. Eng. Res. Pract.*, 2006.

[4] T. Abdullah, A. Mateen, and T. Mustafa, "Risk Analysis of Various Phases of Software Development Models," *Eur. J. Sci. Res.*, vol. 40, no. 3, pp. 369–376, 2010.

[5] B. W. Boehm, "Software Risk Management : Principles and Practices," *IEEE Softw.*, vol. 8, no. 1, pp. 32–41, 1991.

[6] J. A. Wickboldt, A. Bianchin, R. C. Lunardi, G. Andreis, W. Luis, C. B. Both, L. Z. Granville, L. P. Gaspary, D. Trastour, and C. Bartolini, "Improving IT Change Management Processes with Automated Risk Assessment," *Ifip Int. Fed. Inf. Process.*, pp. 71–84, 2009.

[7] H. O. Ali, M. Z. A. Rozan, and A. M. Sharif, "Identifying challenges of change impact analysis for software projects," *Int. Conf. Innov. Manag. Technol. Res.*, pp. 407–411, May 2012.

[8] M. W. Bhatti, F. Hayat, and S. Ahmed, "A Methodology to Manage the Changing Requirements of a Software Project," *Inf. Syst.*, pp. 319–322, 2010.

[9] B. B. Chua and J. Verner, "Examining Requirements Change Rework Effort: A Study," *Int. J. Softw. Eng.*, vol. 1, no. 3, pp. 48–64, Jul. 2010.

[10] S. Park and D. Hwan Bae, "An Approach to Analyzing the Software Process Change Impact Using Process Slicing and Simulation," *J. Syst. Softw.*, vol. 84, pp. 528 – 543, 2011.

[11] B. Alenljung and A. Persson, "Portraying the practice of decision-making in requirements engineering: a case of large scale bespoke development," *Requir. Eng.*, vol. 13, no. 4, pp. 257–279, Aug. 2008.

[12] N. Nurmuliani, D. Zowghi, and S. P. Williams, "Requirements Volatility and Its Impact on Change Effort : Evidence-based Research in Software Development Projects," *AWRE 2006*, 2006.

[13] H. Kaiya, K. Hara, K. Kobayashi, A. Osada, and K. Kaijiri, "Exploring How to Support Software Revision in Software Non-intensive Projects Using Existing Techniques," *IEEE 35th Annu. Comput. Softw. Appl. Conf. Work.*, pp. 327–334, Jul. 2011.

[14] U. Vora, "Change Impact Analysis and Software Evolution Specification for Continually Evolving Systems," *2010 Fifth Int. Conf. Softw. Eng. Adv.*, pp. 238 – 243, 2010.

[15] T. M. Pigoski, "Software Maintenance," in in *The Guide to the Software Engineering Body of Knowledge (SWEBOK)*, no. May, 2001, pp. 1–16.

[16] N. F. Schneidewind, "Predicting risk as a function of risk factors," *Innov. Syst. Softw. Eng.*, vol. 1, pp. 63–70, Mar. 2005.

[17] N. F. Schneidewind, "Investigation of the Risk to Software Reliability and Maintainability of Requirements Changes," *Proceedings. IEEE Int. Conf. Softw. Maint.*, pp. 127–136, 2001.

[18] N. Nurmuliani, D. Zowghi, and S. P. Williams, "Using card sorting technique to classify requirements change," *Proceedings. 12th IEEE Int. Requir. Eng. Conf. 2004.*, pp. 224–232, 2004.

[19] W.-M. Han and S.-J. Huang, "An empirical analysis of risk components and performance on software projects," *J. Syst. Softw.*, vol. 80, pp. 42–50, 2007.

[20] L. Wallace and M. Keil, "Software project risks and their effect on outcomes," *Commun. ACM*, vol. 47, no. 4, pp. 68–73, Apr. 2004.

[21] B. B. Chua, "Rework Requirement Changes in Software Maintenance," *Int. Conf. Softw. Eng. Adv.*, pp. 252 – 258, 2010.

[22] J. F. Hoorn, E. A. Konijn, H. van Vliet, and G. van der Ver, "Requirement Change: Fear Dictate the Must Haves; Desires the Won't Have," *J. Def. Softw. Eng.*, vol. 80, pp. 328–355, 2007.

[23] Z. Jiayi, L. Yunjuan, and G. Yuesheng, "The Requirements change Analysis for Different level users," *Int. Symp. Intell. Inf. Technol. Appl. Work.*, pp. 987–989, 2008.

[24] S. Foo and A. Muruganantham, "Software risk assessment model," *IEEE*, pp. 536 – 544, 2000.

[25] R. Schmidt, K. Lyytinen, M. Keil, and P. Cule, "Identifying Software Project Risk: An International Delphi Study," *Jounal Manag. Inf. Syst.*, vol. 17, no. 4, pp. 5–36, 2001.

[26] R. Reboucas, J. Sauve, A. Moura, C. Bartolini, and D. Trastour, "A decision support tool to optimize scheduling of IT changes," *10th IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, pp. 343 – 352, 2007.

[27] R. Lagerstrom, L. M. von Wurtemberg, H. Holm, and O. Luczak, "Identifying factors affecting software development cost and productivity," *Softw. Qual. J.*, pp. 1 – 23, 2011.

[28] M. A. Rahman, R. Razali, and D. Singh, "A Conceptual Model of Impact Analysis for Requirements Change," *AWERProcedia Inf. Technol. Comput. Sci.*, vol. 03, pp. 763–770, 2013.

[29] R. A. Krueger and M. A. Caser, *A Practical Guide for Applied Research*, Fourth Edi. Thousand Oaks CA: Sage Publications., 2009.

[30] C. Canada and M. Rd, "Studying Software Engineers : Data Collection Techniques for Software Field Studies," *Empir. Softw. Eng.*, vol. 10, pp. 311–341, 2005.

[31] J. Kontio, J. Bragge, and L. Lehtola, "The Focus Group Method as an Empirical Tool in Software Engineering," *Springer*, no. 2004, pp. 271–280, 2008.

[32] G. Stark, A. Skillicorn, and 1st Lt Ryan Ameele, "An Examination of the Effects of Requirements Changes on Software Releases," *J. Def. Softw. Eng.*, no. December, pp. 11–16, 1998.

[33] P. Rovegard, L. Angelis, and C. Wohlin, "An Empirical Study on Views of Importance of Change Impact Analysis Issues," *IEEE Trans. Softw. Eng.*, vol. 34, no. 4, pp. 516–530, 2008.

[34] M. A. Babar, L. Bass, and I. Gorton, "Factors Influencing Industrial Practices of Software Architecture Evaluation : An Empirical Investigation," *Springer-Verlag Berlin Heidelb.*, pp. 90–107, 2007.

[35] K. H. Krippendorff, *Content Analysis: An Introduction to Its Methodology*, Second Edi. London: Sage Publications, Inc, 2004.

Yet Another Java Based Discrete-Event Simulation Library

Brahim Belattar
University Colonel El Hadj Lakhdar/ Department of computer Science, Batna 05000, Algeria
Email: brahim.belattar@univ-batna.dz

Abdelhabib Bourouis
University Larbi Ben M'Hidi/ Department of computer Science, Oum El Bouaghi 04000, Algeria
Email: a.bourouis@univ-oeb.dz

***Abstract*—JAPROSIM is a well designed library, free and open source that adopts the popular process-interaction worldview. It is implemented in Java programming language allowing deep access to its powerful features and can serve as a basis for the development of dedicated object-oriented simulation environments. The paper presents architecture and major components of the library. The process-interaction world view adopted by JAPROSIM is discussed. A modeling example is given in order to highlight JAPROSIM capabilities. Important features of JAPROSIM are summarized and suggestions for improving our work are given.**

***Index Terms*—Discrete Event Simulation, Object-Oriented Simulation, JAPROSIM, Process-Interaction Worldview, Java-based modeling and simulation.**

I. Introduction

The formalism used by a simulation language to conceptualize a domain or system is called its "worldview". Three worldviews are commonly used to model the dynamics of discrete-event systems: Event-Scheduling, Process-Interaction and Activity Scanning. The process-interaction worldview is often convenient for describing the queuing nature of higher-level stochastic systems. Simulation models can be implemented in a variety of languages. From an external point of view, the principal component of simulation software is the simulation language (SL) which allows description of simulation models and their dynamic behavior [1].

Today, Object Oriented Modeling (OOM) is largely recognized as an excellent approach that deals with large and complex systems through abstraction, modularity, encapsulation, layering and reuse. A conceptual model is obtained by decomposing a real system in a set of objects in interaction. Each object represents a real world entity that encapsulates state and behavior. A class is a template for creating objects that share common related characteristics. Object-Oriented Simulation (OOS) benefits from all the powerful features of the OOM especially model conceptualization which is one of the early steps in a simulation study.

JAPROSIM is an object-oriented simulation library, free and open source that adopts the popular process-interaction worldview. The library is implemented in Java programming language allowing deep access to its powerful features. The library is divided into packages to organize the collection of classes into important functional areas. It is easy to build discrete event simulation models using JAPROSIM, either for experimented programmers in Java or for simulation experts with elementary programming knowledge. JAPROSIM can serve as a basis for the development of dedicated object-oriented simulation environments. Furthermore, since Java has been commonly adopted as a teaching language in Computer Science area, JAPROSIM may also serves as an academic material for teaching discrete event modeling and simulation [2].

The rest of the paper is organized as follows: In section 2, we present an overview of related work. Architecture and major components of the library are presented in section 3. In section 4 we discuss the process-interaction worldview adopted by JAPROSIM. A modeling example is given in section 5 in order to highlight JAPROSIM capabilities. In Sections 6 and 7 we summarize important features of JAPROSIM and provide suggestions for future improvements of our work.

II. Related Work

A large research effort has been devoted to enrich mainstream languages as C, C++, Java, Python with simulation capabilities [3]. The most common choice is to provide the additional simulation functionality through a software library. Independently of the architectural level at which they are provided (application, library, language), the simulation capabilities embody a world view for their users. The world view is essentially the set of concepts that constitute the basic elements available to the modeler to compose and to specify the simulation. The diverse world views are functionally equivalent, but differ in expressive power and in terms of computational efficiency. The idea of building process-oriented

Corresponding author: Brahim Belattar Email: brahim.belattar@univ-batna.dz

doi:10.4304/jsw.9.1.82-88

simulations using a general purpose object-oriented programming language is not original and several tools were developed in this way. For example, both of CSIM++ [4] and YANSL [5] are based on C++, while PsimJ [6], JSIM [7] are based on Java. Discrete Event Simulation tools written in Java, like PsimJ and SSJ [8] are well designed and freeware libraries but not open source. Silk [9] is also well designed but is a commercial tool.

There is also a large collection of free open source libraries, we may consider for instance:

- JavaSim [10] is a set of Java packages for building discrete event process-based simulation, similar to that in Simula and C++SIM.
- Simjava [11] is a process based discrete event simulation package for Java, similar to Jade's Sim++, with animation facilities.
- jDisco [12] is a Java package for the simulation of sys-tems that contains both continuous and discrete-event processes.
- DESMO-J [13] is a framework which supports both event and process worldviews.
- SimKit [14] is a component framework for discrete event simulation, influenced by MODSIM II and based on the event graph modeling.

SimJava and JSim are among the first implementations of the thread-based class of simulators. These early efforts pay particular attention to web-based simulation and to the Java Applet deployment model. Many simulators aim at replicating the functionality and design of Simula in Java. For example, DesmoJ supports advanced process-oriented modeling features. These include capacity-constrained resources, conditional waiting and special process relationships as producer/consumer and asymmetric master/slave. SSJ is designed for performance, flexibility and extensibility. It offers its users the possibility to choose between many alternatives for most of the internal algorithms and data structures of the simulator [3].

JAPROSIM is not a java version of any existing simulation language as Simjava or JavaSim. There are, however, unique aspects in JAPROSIM that lead to fundamental distinctions between our work and others. For example, JAPROSIM embeds a hidden mechanism for automatic collection of statistics. This approach enables a clean separation between implementing the dynamics of the model and gathering data, so traditional performance measurements are automatically computed. The model can thus be created without any concern over which statistics are to be estimated, and the model classes themselves will not contain any code involved with statistics. This leads in more code source clarity. Nevertheless, users could, if needed, implement specific statistics collection using different classes offered by the JAPROSIM statistics package. This feature makes the key difference between JAPROSIM and the other discrete event simulation libraries written in Java. Exception is made for SimKit which already offers this possibility, but which uses a different modeling approach based on event graphs [2].

III. The JAPROSIM Library

The JAva PRocess Oriented SIMulation (JAPROSIM) library is part of an ongoing project that aims at providing an advanced visual interactive simulation and modeling environment for Discrete Event Systems (DES) [2]. The library is currently divided into six main packages:

- kernel: a set of classes dealing with active entities, scheduler, queues and resources.
- random: contains classes for uniform random stream generation.
- distributions: contains a rich set of classes for useful probability distributions.
- statistics: contains classes representing intelligent statistical variables.
- gui: a set of graphical user interface classes to use for project parameterization, trace and simulation results presentation.
- Utilities: a set of useful classes for express model development.

We will focus on the simulation kernel and the random and statistics.

A. The Kernel Package

The kernel package is at the heart of JAPROSIM. It is made up of classes dealing with active entities, scheduler, queues and resources. A UML class diagram of the kernel is given below.

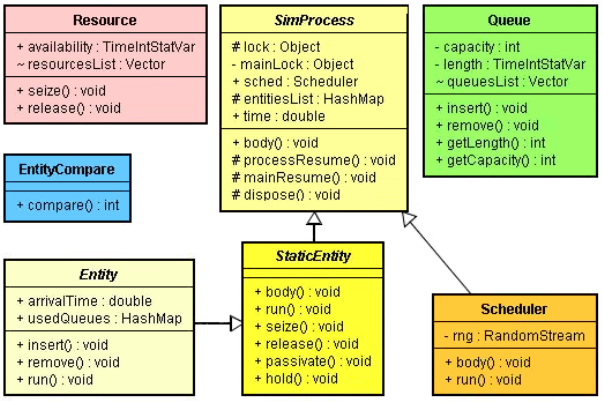


Figure 1. The Kernel class diagram.

The coroutine like mechanism is implemented trough SimProcess, Scheduler, StaticEntity and Entity classes. A coroutine program is a collection of coroutines which run in quasi-parallel with one another. Each coroutine is an object with its own execution state, so that it may be suspended and resumed. Our aim in the design of JAPROSIM was putting a great emphasis into following the semantic of SIMULA but the design itself is not close to it. The advantage of this approach is that design is simpler without explicit coroutine class support and the semantics of facilities that are well-known and thoroughly tested through many years use of SIMULA are completely supported. Native support for multithreaded execution is a fundamental aspect to the implementation of a natural process-oriented modeling

capability in Java. Every active entity's life cycle is executed in a single separate thread.

B. The Random and Statistics Packages

Random number generators (RNGs) are the basic tools of stochastic modeling. The random package provides the RandomStream interface which represents a base reference for creating Random Number Generators. Each RNG must rewrite the *RandU01()* method which normally returns a uniformly distributed number (a Java double) in the interval [0, 1]. JAPROSIM provides a set of well known good RNGs see [15] and [16], as Park-Miller, McLaren-Marsaglia and RandMrg in which the backbone generator is the combined multiple recursive generator (CMRG) proposed in [17]. The *setSeed(long[] seed)* method is used to specify seeds instead of default values.

The user can define its own RNG by implementing the RandomStream interface. To be used with JAPROSIM, an instance of the user-defined RNG must be assigned to the Scheduler's static public attribute rng. A prosperous set of discrete and continuous Random Variate Generators (RVGs) is offered by the distribution sub-package. This set covers typically most practical distributions to be used in discrete event simulation. However, the user could supply it with additional RVGs.

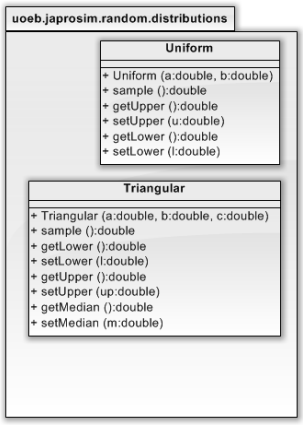


Figure 2. The distribution sub-package.

The statistics package provides two useful classes. *DoubleStatVar* class dealing with time-independent statistical variables (having double values) as response time and waiting time in a queue. It implements the mechanisms for keeping track of observational-based statistics and must be updated every time its value change using the *update()* method. *TimeIntStatVar* class is used for time-dependent statistics (with integer values) such as a queue length or number of customers in a system. Typically, the user instantiates the desired class, then puts and updates it in the appropriate code locations. The placement of statistical variables and their update is a source of several pitfalls. For this reason we have enhanced automatic placement and update of those variables for the most known and useful performance measures.

IV. PROCESS-INTERACTION WORLDVIEW IN JAPROSIM

The origins of the process-interaction worldview can be traced to the authors of SIMULA. It provides a way to represent a system's behavior from the active entities point of view. A system is modeled as a set of active entities in interaction. Interaction is a consequence of competition and/or cooperation for the acquisition of critical resources. A process-oriented model is a description of the sequence of processing steps these entities experience as they flow through the system. Each active entity's life cycle consists of a sequence of events, activities and delays. A routine implementing an active entity requires special mechanisms for interrupting, suspending and resuming its execution at a later simulated time under the control of an internal event scheduler. This can be achieved using special programming languages that offer at least a SIMULA's coroutine like mechanism, thus programming languages offering multithreading like Java are suitable.

In JAPROSIM, active entities are transient entities moving through the system (dynamic entities). An entity's life cycle is a sequence of active and passive phases. On one hand, an active phase is characterized by the execution of the relevant process. Normally this corresponds to the events during which system state changes without progression of simulation time. On the other hand, passive phases are characterized by activities and delays. So the relevant process is suspended while simulation time advances. Events are the criterion of scheduling which explain the use of a future event list (FEL). After a process is suspended, the scheduler resumes and decides of which is the next process to reactivate according to the system state and the FEL. The scheduler is a special process that coordinates the execution of a simulation model. Processes are executed in pseudo-parallel and only one (which has the imminent simulation time) is running at any instance of real time. Simulation processes may execute concurrently at any instance of simulation time. Hence the scheduler executes in alternation with other simulation processes.

This shared behavior is modeled through the *SimProcess* abstract class which extends the Java Thread class. The method *processResume(Entity e)* is called by the scheduler to reactivate a simulation process and *mainResume()* is called by a simulation process to reactivate the scheduler. Each simulation process has its own lock object. Locks are used in combination with *wait()* and *notify()* to synchronize implementation threads instead of the Java deprecated methods *suspend()* and *resume()*. A thread which calls any of the previous methods will block on its own lock after notifying the appropriate one. *Schedule(Entity e)* is a synchronized method offered by the *SimProcess* class which could be called by the scheduler or by a newly created simulation process for an appropriate insertion into the FEL. At the end of its life cycle, a simulation process calls automatically the *dispose()* method to reactivate the

scheduler without blocking itself. So the corresponding thread could be terminated. This leads to free occupied memory and improve simulation performance. Otherwise this may cause a Java runtime error as we experienced with an academic version of the commercial package Silk.

Specific behavior of a simulation process is normally described using the dedicated abstract method *body()*. It must be rewritten to be an ordered sequence of method invocations terminated by an implicit automatic call to *dispose()*. The behavior of the scheduler is also described using this method. Since *SimProcess* is abstract, it is intended to be extended. A new class is created to model simulation processes. The *Entity* class provides the basis for defining classes that obey to the process-oriented simulation worldview. This class is declared to be abstract, so instances of *Entity* can not be created directly. Instead, modelers define their own classes that extend *Entity* and describe the dynamic behavior of the corresponding system components in terms of the process-oriented methods inherited in particular from those classes.

Each class derived from *Entity* runs in its own thread of execution, a capability inherited from *SimProcess*. The *Entity* class provides the implementation of the *run()* method which in turn invokes *body()*. The user is required to supply the *body()* method. Four remarkable methods are offered: *insert(), remove(), seize(), hold()* and *release()*. They could be used to model familiar queuing scenarios. The *passivate()* method is used to wait until a specific system state is reached (ex: waiting for a resource to be free). Since the thread will be suspended and inserted into the passive list (PL) after a call to *passivate()*, this call is typically used within a *while()* loop. Each time the scheduler takes control; it starts reactivating suspended threads in the PL first, then dealing with the FEL. So such a reactivated thread would have the opportunity to return back to the PL, if there is no expected evolution in the system state.

The abstract class *StaticEntity* is used to model the behavior of active entities that have not the ability to move. Typical examples of those entities are “intelligent resources”. *StaticEntity* derives directly from *SimProcess*. Since The *Entity* class is used to model dynamic entities, it derives from *StaticEntity* and defines two new methods *insert()* and *remove()*. The other methods: *seize(), hold(), release()* and *passivate()* discussed previously are defined in the *StaticEntity* and hence inherited by *Entity*.

The scheduler proceeds in two phases. First, it reactivates each thread in the PL. So the reactivated thread checks for expected changes in the system state and may return back to the PL as it may continue executing the rest of its operations. Secondly, the scheduler picks the imminent simulation process from the FEL and reactivates the corresponding thread. These two phases are repeated as long as the simulation experiment termination condition isn’t verified. The *Scheduler* class has an attribute *rng* which is an instance of a random number generator and could be customized by the user. The *EntityCompare* class implements the Java Comparator interface and is used to implement priority queuing mechanism.

The *Resource* class represents a passive entity characterized by a capacity. Generally, a simulation process seizes some units of a resource to accomplish a service and releases them later. The *hold()* method of the *StaticEntity* class is used to specify the service duration. The *Queue* class models a space for waiting which may be limited. It provides an ordered list where entities (or other user-defined types) can reside. Typically, an entity is inserted into a queue by having it activate the *insert(Queue q)* method of the *Entity* class. There is no implicit conditional status delay logic associated with queues, which means that the entity's thread of execution is not suspended pending some system status evolution.

Modeling conditional status delays is the realm of the *while()* and *passivate()* constructs. As a consequence, an entity can reside simultaneously in any number of queues. This feature can be particularly convenient in collecting certain types of system statistics related to waiting times or queue lengths. Another important distinction is that the removal of an entity from a queue could be independent of the ordering of the queue at the time of removal. Users are required to explicitly identify the entity to be removed at the time of removal. Typically this is accomplished by having the corresponding entity activate the *remove(Queue q)* method of the *Entity* class. While entities are generally inserted and removed from queues using the *insert(Queue q)* and *remove(Queue q)* methods of the *Entity* class, the same tasks can be accomplished using the *insert(Entity e)* and *remove(Entity e)* methods defined in the *Queue* class.

V. USING THE JAPROSIM LIBRARY

In order to promote understanding JAPROSIM capabilities, we present an example which illustrates a simplified simulation model of a TV inspection and adjustment process as described in [18]. It gives a good impression of the wide applicability of simulation in production and logistics.

In this model, an arriving TV is first inspected at an inspection station. If a TV is found to be functioning improperly, it is routed to an adjustment station. After adjustment, the TV is sent back to the inspection station where it is again inspected. TVs passing inspection, whether to the first time or after one or more routings through the adjustment station, are sent to a packing area. A probabilistic branching is used when a TV passes the inspection station. It specifies that 15% of the TVs inspected are sent to the adjustment station and 85% are sent to the packing area. The inter-arrival time between TVs to the system, the inspection delay and the adjustment delay are all modeled as uniform variates.

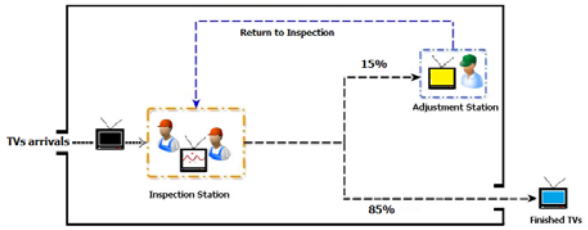


Figure 3. TVs Inspection and Adjustment.

From the description given, we can easily identify two resources which represent the two stations of the system modeled. The first resource represents the inspector and has a capacity of two units. The second resource represents the adjustor and has a capacity of one unit. Since we have one input arrivals, we distinguish one active entity in the model. A class diagram of the JAPROSIM simulation model for this example is shown below:

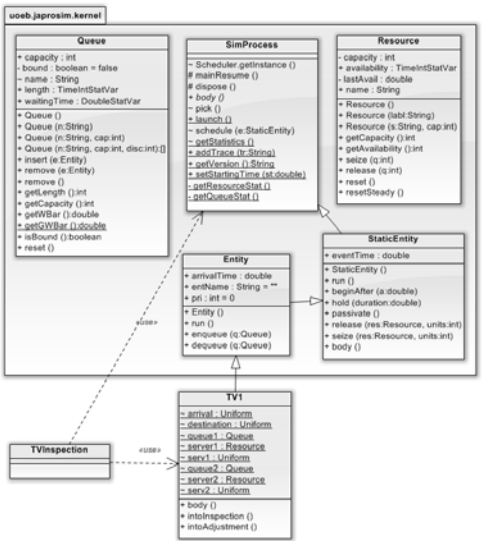


Figure 4. A class diagram of the simulation model.

It is important to note that with JAPROSIM, a simulation model is simply a Java source program which merges process interaction modeling features provided by the library simulation packages with powerful features of the Java programming language. From the class diagram given in Figure 11, it appears that the JAPROSIM simulation model uses two classes named respectively *TV1* and *TVInspection*.

The java source code of *TV1 class* is given below:

```
1.  import uoeb.japrosim.kernel.*;
2.  import uoeb.japrosim.random.distributions.*;
3.  public class TV1 extends Entity {
4.  static Uniform arrival = new Uniform(3.5, 7.5);
5.  static Uniform destination = new Uniform(0.0, 1.0);
6.  static Queue queue1 = new Queue("INSP QUEUE");
7.  static Resource server1 = new Resource("Inspection", 2);
8.  static Uniform inspectdelay = new Uniform(6, 12);
9.  static Queue queue2 = new Queue("ADJT QUEUE");
10. static Resource server2 = new Resource("Adjustment", 1);
11. static Uniform adjstdelay = new Uniform(20, 40);
12. public void body() {
13. new TV1().beginAfter(arrival.sample());
14. intoInspection();
15. }
16. public void intoInspection() {
17. queue1.insert(this);
18. while (server1.getAvailability() < 1) {
19. passivate();
20. }
21. seize(server1, 1);
22. queue1.remove(this);
23. hold(inspectdelay.sample());
24. release(server1, 1);
25. if (destination.sample()<=0.15) {
26. intoAdjustment();
27. }
28. }
29. public void intoAdjustment() {
30. queue2.insert(this);
31. while (server2.getAvailability() < 1) {
32. passivate();
33. }
34. seize(server2, 1);
35. queue2.remove(this);
36. hold(adjstdelay.sample());
37. release(server2, 1);
38. intoInspection();
39. }
40. }
```

Figure 5. Source code of The TV1 class.

We can easily distinguish four parts in this source code. The first part (from line 4 to line 11) serves to set the parameters of the model. We can see that the inspection delay, the adjustment delay and the inter-arrival time are defined as uniform variates with specific arguments. We have also to define the inspector and adjustor resources and their associated queues. The variable destination is defined as a uniform variate and is used to decide if a TV just inspected is to be routed to the adjustment station or to exit the system.

The second part (from line 12 to line 15) serves to route the active entity to the inspection station and to create next TVs arrivals with respect to the inter-arrival time between TVs. The third part (from line 16 to line 28) represents the classical scheme of resource allocation. A TV arriving at the inspection station is inserted in the associated queue. When a resource unit is free, it is allocated to a waiting TV with respect to the queue priority. An inspection delay associated to this TV is sampled, and the TV will hold the resource unit seized until the associated delay is elapsed. The resource unit is then released and can be allocated to other waiting TVs. Line 28 serves to decide if the TV just inspected is to be routed to the adjustment station or to exit the system.

The fourth part (from line 29 to line 39) models the adjustor resource allocation scheme. A TV arriving at the adjustment station is inserted in the associated queue. When the adjustor resource is free, it is allocated to a waiting TV with respect to the queue priority. An adjustment delay associated to this TV is sampled, and the TV will hold the adjustor resource seized until the associated delay is elapsed. The adjustor resource is then released and the TV is sent back to the inspection station.

To run the simulation model, we need another class which contains the *main()* method. This class is called *TVInspection* and its java source code is:

```
1  import uoeb.japrosim.kernel.*;
2  import uoeb.japrosim.random.distributions.*;
3  public class TVInspection {
4          public static void main(String[] args) {
5                  SimProcess.time = 0.0;
6                  SimProcess.sched.start();
7                  new TV1().beginAfter(0.0);
8          }
9  }
```

Figure 6. Source code of the TVInspection class.

When running the simulation model, the JAPROSIM window is first displayed. It consists of an experimentation frame where simulation parameters are to be set. Parameters like the number of replications, the simulation duration, the RNG used must be specified here by the user. A button Run/Stop allows user to start simulation, stop and resume it at any time during execution. Two other buttons are used for presentation of simulation results and trace execution.

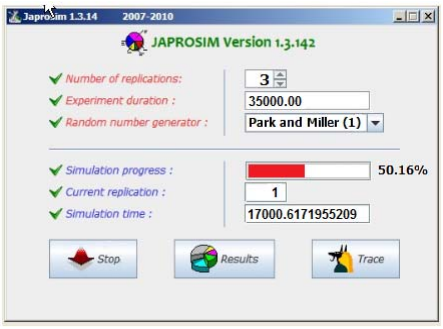


Figure 7. JAPROSIM experimentation frame.

At the end of each simulation run, the simulation results can be viewed in a textual form or in a graphical one. Textual simulation results are expressed as statistical quantities which resume resources and queues utilization during a run. On the other hand, the graphical form uses plots, bar charts or pie charts.

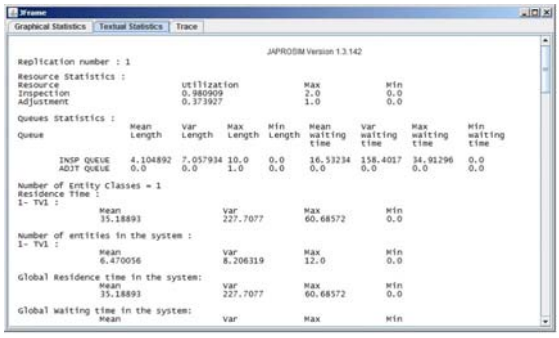


Figure 8. Statistical results.

In addition to statistical results, JAPROSIM allows graphical presentation of selected performance measures.

Figure 9. Graphical Simulation results.

Example of such a presentation is given in Fig. 9. It shows the utilization of the resources used in the simulation model during each replication.

VI. Summary of Japrosim Important Features

The example presented reveal many advantages of the object-orientation of JAPROSIM and the process-interaction worldview adopted. The relationship between the simulation model and the real system is more obvious and therefore easier to teach and to understand. The java source code of the simulation model is easy to understand and users can learn far more than if they have to experiment with sophisticated commercial simulation packages in which important details of the simulation implementation are hidden and thus never understood.

Furthermore, we can observe in the source code of the classes used in the JAPROSIM simulation models, that no class of the statistics package is explicitly used. In addition, no Java constructs are clearly used to do so. This is the key feature of JAPROSIM that all well known and useful performance measures are implicitly and automatically handled. The user doesn't worry about how many, or what kind of statistical variables to use, nor where to place and update them. Explicit statistical variable handling by the user may lead to undetectable programming errors and pitfalls. This is why JAPROSIM is said to be easy and safe to use for all users, including those who aren't qualified Java programmers.

The automatic handling mechanism of statistical variables is embedded in the library. The *SimProcess* class declares a protected static entitiesList which is a Java HashMap to collect the residence time of each simulation entity class (a Java class that extends the JAPROSIM *Entity* class). The key for the HashMap is the class name and values are *DoubleStatVar*. In the *Entity* constructor, each time a new *entity* class is created, the above HashMap is updated. In the *run()* method of the *Entity* Class and after the call to the *body()* method, the residence time is updated using the simulation time and the arrivalTime attributes.

Each Queue object possesses a statistical variable to hold waiting time. This variable is updated trough *insert()*/*remove()* methods. The number of entities in a queue is handled by a length time-dependent statistical variable. The resource availability is also a time-dependant variable. It is used to compute resource utilization. The *Queue* class has a static Java Vector to register all queues used in the simulation model. In the same way, the *Resource* class also has an analogous list to keep track of all used resources. Those lists have a package visibility; hence they could be accessed by all the simulation processes. They are updated each time a new resource or queue instance is created.

VII. Conclusion

In this paper we have presented the JAPROSIM simulation library. It is written in Java and was deliberately kept simple, easy to use and extensible. From the example presented, many advantages of the object-orientation of JAPROSIM and the process-interaction worldview adopted have been exhibited. Today, JAPROSIM is a fully functional library which has been tested thoroughly. At the time of writing, major

enhancements made from the previous versions are: automatic detection of the steady state of the system modeled and graphical viewing of simulation outputs. JAPROSIM is distributed since several years as an Open Source project. The source code is available freely (http://sourceforge.net/projects/japrosim/) along with some documentation. Future improvements will focus on increasing the JAPROSIM performances, integrating a graphical model building facility, providing animations of simulation models and using xml standards for web-based simulation and interoperability with other tools.

ACKNOWLEDGMENT

This work was supported in part by the Algerian Government under a CNEPRU Grant B*01320110026.

REFERENCES

[1] Korichi Ahmed, Belattar Brahim, "Towards a Web Based Simulation Groupware: Experiment with BSCW", WSEAS transactions on Business and Economics, Issue 1, Volume 5, pp. 9-15, January 2008.

[2] A. Bourouis, B. Belattar: "JAPROSIM: A Java Framework for Discrete Event Simulation", in Journal of Object Technology, vol. 7, no. 1, January-February 2008, pp. 103-119, http//www.jot.fm/issues/issue_2008_01/article3/

[3] Antonio Cuomo, Massimiliano Rak, Umberto Villano: "Process-oriented Discrete-event Simulation in Java with Continuations - Quantitative Performance Evaluation", In Proceedings of the 2nd International Conference on Simulation and Modeling Methodologies, Technologies and Applications, pp. 87-96, 2012, Rome, Italy, 28 - 31 July, 2012.

[4] H. Schwetman, "Object-Oriented simulation modeling with C++/CSIM17", In Proceedings of the 1995 Winter Simulation Conference, ed. C. Alexopoulos, K. Kang, W. R. Lilegdon, and D. Goldsman, pp. 529-533, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, December 1995.

[5] J. A. Joines, S. D. Roberts: "Design of object oriented simulations in C++", In Proceedings of the 1996 Winter Simulation Conference, ed. J. Charnes, D. Morrice, D. Brunner, and J. Swain, pp. 65-72, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, December 1996.

[6] J. M. Garrido, *Object-oriented Discrete Event Simulation with Java*. Kluwer/Plenum, NY, September 2001.

[7] J. A. Miller, Y. Ge, and J. Tao, "Component Based Simulation Environments: JSIM as a Case Study Using Java Beans", In Proceedings of the 1998 Winter Simulation Conference, ed. D. J. Medeiros, E. F. Watson, J. S. Carson and M. S. Manivannan, pp. 373-381, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, December 1998.

[8] P. L'Ecuyer, L. Melian, and J. Vaucher, "SSJ: A framework for stochastic simulation in Java", In Proceedings of the 2002 Winter Simulation Conference, ed. E. Yücesan, C.-H. Chen, J. L. Snowdon, and J. M. Charnes, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, pp. 234–242, December 2002.

[9] R. A. Kilgore, "Silk, Java and Object-Oriented simulation", Proceedings of the 2000 Winter Simulation Conference, ed. J. A. Joines, R. R. Barton, K. Kang, and P. A. Fishwick, pp. 246-252, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, December 2000.

[10] M. C. Little, "The JavaSim User's Manual", Department of Computing Science, University of Newcastle upon Tyne, 1999.

[11] F. Howell and R. McNab, "simjava: a discrete event simulation package for Java with applications in computer systems modelling", First International Conference on Web-based Modelling and Simulation, San Diego CA, Society for Computer Simulation, January 1998.

[12] K. Helsgaun, "Discrete Event Simulation in Java", DATALOGISK SKRIFTER (writings on computer science), Roskilde University, 2000.

[13] B. Page, T. Lechler and S. Claassen, "Objektorientierte Simulation in Java mitdem Framework DESMO-J" ("Object-Oriented Simulation in Java with the Framework DESMO-J", in German). Libri Book on Demand, Hamburg, 2000. University of Hamburg, Faculty of Informatics.

[14] A. Buss, "Component Based Simulation Modeling with SimKit", Proceedings of the 2002 Winter Simulation Conference, ed. E. Yücesan, C.-H. Chen, J. L. Snowdon, and J. M. Charnes, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, pp. 243-249, December 2002.

[15] P. L'ecuyer, "Uniform Random Number Generator", In Proceedings of the 1998 Winter Simulation Conference, ed. D. J. Medeiros, E. F. Watson, J. S. Carson, and M. S. Manivannan, pp. 97-104, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, December 1998.

[16] P. L'ecuyer, F. Panneton, "Fast Random Number Generators Based on Linear Recurrences Modulo 2: Overview and Comparison", In Proceedings of the 2005 Winter Simulation Conference, ed. M. E. Kuhl, N. M. Steiger, F. B. Armstrong, and J. A. Joines, pp. 110-119, Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, December 2005.

[17] P. L'ecuyer, Good parameters and implementations for combined multiple recursive random number generators. *Operations Research*, vol. 47(1), pp 159–164, 1999.

[18] C. D. Pegden, R. E. Shannon, and R. P. Sadowski, *Introduction to Simulation Using SIMAN*. New York McGraw-Hill Inc., 1990.

Brahim Belattar is a professor at the University of Batna since 1992. He has also taught at the University of Constantine from 1982 to 1985. He received his BS degree in Computer science from the University of Constantine in 1981 and his MS and PhD degrees from the University Claude Bernard of Lyon (French) respectively in 1986 and 1991. His research interests include simulation, databases, semantic web and AI.

Abdelhabib Bourouis is a lecturer at the University of Oum el Bouaghi since 2003. He received his BS degree in Computer science from the University of Constantine in 1999 and his MS and PhD degrees from the University of Batna respectively in 2003 and 2009. His research interests include Artificial intelligence, performance evaluation, parallel and distributed simulation.

Survey of Community Structure Segmentation in Complex Networks

Tingrui Pei
College of Information Engineering, Xiangtan University, Xiangtan, China
Key Laboratory of Intelligent Computing & Information Processing of Ministry of Education,Xiangtan University, Xiangtan, China
Email: peitr@163.com

Hongzhi Zhang
College of Information Engineering, Xiangtan University, Xiangtan, China
Key Laboratory of Intelligent Computing & Information Processing of Ministry of Education,Xiangtan University, Xiangtan, China
Email: zhz317387928@163.com

Zhetao Li*
College of Information Engineering, Xiangtan University, Xiangtan, China
Key Laboratory of Intelligent Computing & Information Processing of Ministry of Education,Xiangtan University, Xiangtan, China
School of Computer, National University of Defense Technology, Changsha, China
Email: chu5044130@sohu.com

Youngjune Choi
Department of Information and Computer Engineering, Ajou University, Suwon, Korea
Email: choiyj@ajou.ac.kr

***Abstract*—Community structure analysis is a hot research spot in social networks and complex networks. In order to summarize recent research progress, this paper reviews the background, the motivation, the advantages and disadvantages of existing works related to community structure discovering. A comprehensive outline was obtained by analysis of different clustering algorithms**.

***Index Terms*—Social networks, Community structure, Segmentation analysis**

I. INTRODUCTION

Social network is to reflect the relationship between the nodes which are in the intra-group or in the inter-group. It uses nodes to represent individuals in the network, and attachment between nodes to represent the relationship among individuals, the community to represent groups which share the same characteristic. Thus, what we define for social network is that to project the complex relationship in society to nodes and attachment in network.

In the past decade, there has been a surge of interest in both empirical studies of networks [1], and development of mathematical and computational tools for extracting insight from network data [2-5]. The best-studied form of large-scale structure in networks is modular or community structure [6, 7]. The main reason is that community structure may correspond to functional units within a networked system. An example of this kind of link between structure and function drives much of the present excitement about networks: In a metabolic network, a community might correspond to a circuit. In a social network, a community might correspond to a group of people brought together by a common interest. Discovery of communities also has great significance in recognition terrorist organization or prevention infectious diseases and so on.

Although, scholars have made outstanding achievements in the past years, the existing research results are still not enough to discover the relationship between the function and structure in complex network. Besides, there are no uniform optimal community concept and measurement criteria on dividing the community, so it is difficult to have a recognized measure to identify the quality of the discovered communities.

II. CLASSIFICATION ALGORITHMS

At present, the complex network clustering algorithms can be divided into the following 3 types:

The first type: Based on optimization methods, it transforms the complex network clustering problem into a

*Corresponding author: Zhetao Li , Email: chu5044130@sohu.com

doi:10.4304/jsw.9.1.89-93

quadratic optimization problem, through the calculation of the matrix characteristic vector to optimize the predefined "cut" function, such as: spectrum divide method, etc.

The second type: Based on heuristic methods, it transforms the complex network clustering problem into predefined heuristic planning design problems, such as: GN algorithm, CPM algorithm, and so on.

The third type: other clustering methods, such as: the method based on similarity, etc.

III. Based on the Optimization Clustering Method

The two principal methods based on optimization clustering method are Spectrum method and local optimal method. Spectrum method is the application of "cut" function which is minimizing predefined by quadratic optimization technology. The lowest "cut" division is considered to be the best network division. Local optimal algorithm includes three basic parts: the objective function, the optimal solution and the candidate search strategy. The differences existing in the different algorithm are the objective function and the search strategy of the optimum solution.

(1) Traditional spectrum divide method [8] based on the Laplace matrix. This algorithm based on the node that is in the same club is approximately equal to division the structure of community in each element that is in the eigenvectors of non-zero eigenvalues. In most cases, the actual Laplace matrix is a sparse matrix, so it can be fast calculated the characteristic vector though the Lanczos method, which has advantage of high speed and accuracy.

The biggest disadvantage of traditional spectrum method is that it only divides the community into two communities once. To have a network divided into more communities, one has to repeat the algorithm many times. As to this problem, Wu and Huberman put forward the rapid resistance spectrum segmentation method [9] based on the network voltage spectrum. The basic idea is: if one treats two nodes which are not in the same club considered as source nodes (voltage is 1) and the end node (whose voltage is 0), treats each side as a resistance whose value is 1,then, they will have a similar voltage value in the same community. This algorithm has low complexity ($O(m+n)$), but it needs to know the number of the communities in advance.

In order to overcome the defects, Capocci proposed another spectrum divide algorithm [10] on the foundation of traditional spectrum method and on standard matrix $N = K^{-1}A$. Using standardized transformation conversion, the maximum eigenvalue of the matrix N is always more than 1, and the corresponding feature vector is called the first the ordinary characteristic vector. In a community structure with obvious network, if the number of community is K, then the first ordinary eigenvalue of the matrix N will be K-1 which is very close to 1, while the other values are obviously different from 1. Besides, in this K-1 eigenvalue vector, the nodes in the same club will be much closed. Therefore, in the network with obvious structure, the elements distribution in the vector is the obvious form of steps, and the level of the ladder is equal to the number of community K, so the spectrum divide algorithm can get a good effect.

(2) K-L algorithm [11], fast Newman algorithm [12] and GA algorithm [13] in chapter 3 is typical clustering algorithm methods which based on local search optimization technology. This kind of algorithm includes three basic parts: the objective function, the candidate of the search strategy and optimal solution search strategy. Almost all of them have the same candidate solution search strategy, but the target function and the optimal solution search strategy are different.

In the process of K-L algorithm, it only accepts better candidate solution, so the solution that finds can always be the local optimal but not the global. The biggest limitation of K-L algorithm is that it needs prior experience to produce good initial cluster structure, otherwise the bad initial solution may lead to slow convergence speed and the worse of the final solution.

In order to improve the algorithm rate, in 2004, Newman put forward the FN [12] algorithm, which is mainly realized by maximizations module degrees Q. The function Q is defined as follows:

$$Q = \sum_{s=1}^{K} [\frac{m_s}{m} - (\frac{d_s}{2m})^2] \quad (1)$$

The complexity of the algorithm is $O(mn)$, m, n is representing the all number edges and nodes in network respectively, but FN algorithm compared with GN algorithm has less accuracy.

Through the same goal with FN, Guimera and Amaral put forward clustering algorithm GA [13] based on the simulated annealing algorithm. This algorithm has jumped out local optimal solution, and has the ability of finding optimal solutions, so its cluster precision is high. However, because of its sensitive to input parameter, different parameter setting often leads to bigger difference clustering results and running time.

Take optimization method to identify the network structure totally depends on optimizing targets, so "biased" goal function will cause "biased" solution. But, the vast majority of optimization algorithm is based on the maximized Q value to do cluster analysis. However, the research found that Q function is biased itself. It can't characterize the optimal cluster structure accurately, which means this algorithm may not find all network cluster structures which are real properly.

IV. Heuristic Clustering methods

GN algorithm [6], improved GN algorithm [4, 14], CPM algorithm [15] and PAK algorithm [16] are classic heuristic complex network clustering algorithm. The common characteristics of this kind is: for most network, to design heuristic algorithm on certain intuitive hypothesis, they can find the optimal solution or time optimal solution quickly, but they can't ensure that it can get satisfactory solution to all input network from theory.

In 2002, Girvan and Newman put forward GN algorithm, using repeatedly recognition and cluster strategy clustering complex network which delete the

connections in between [6]. It mainly base on the theory that the intra-group's betweenness should be bigger than inter-group eventually once can build a hierarchical clustering tree to realize community division. The biggest drawback of GN algorithm is the low calculation speed, which is suitable for small and medium-sized network. But, it doesn't need prior conditions, and possess high accuracy.

In 2003, Tyler introduced the basic statistical methods into GN algorithm, and put forward approximate algorithm GN [4]. The monte carlo algorithm estimates part of the approximate number of node betweenness, rather than calculates all the exact number of node betweenness. Obviously, this algorithm improves the speed, but reduces the cluster precision.

Considering that the GN algorithm's low efficiency is caused by excessive spending count edge betweenness, Radicchi propose connection clustering coefficient to replace the edge betweenness [14] in 2004. Based on the theory that cluster of connections between connected clustering coefficients should be less than that in connected clustering coefficient to divide community. The complexity of the algorithm is $O(m^3 / n^2)$, in which m is an iteration time, and n is total node. The biggest limitation of this algorithm is that it is not suitable for network with little processing circuit or no circuit.

At present, overlap community structure is not considered in most algorithms, however, has more practical significance in most applications. For example, in the semantic web, polysemous are allow to be appeared in network cluster with different meaning. In 2005, Palla put forward CPM algorithm [15] which can identify overlap network structure. The fundamental assumption of the algorithm is: network constituted by more neighbor cluster of k-group, and the next-to two k groups share k-1 nodes at least, with each k group only belonging to a cluster, but the k-groups belonging to different network may share some nodes. This algorithm is the first one which can calculate the overlap community structure. In actual application, parameter k is difficult to be determined, the selection of different k value often gets greater difference between network cluster structure, so it difficult to judge quality.

In order to solve the problem of excavation overlap community structure, Gregory, put forward PAK algorithm [16] in 2010 to find overlapping community. This method is based on the advanced modular design and use the professional label algorithm as its basic theory. It is the best overlap community found algorithm at present, as it can recover the overlap community effectively and is suit for large-scale and intensive network, but it also has higher complexity.

V . Other Clustering Method

Besides the two principal methods mentioned above, there are other complex network clustering methods, for example: hierarchical clustering method based on similarity, in which the similarity of nodes is defined based on the structure of network topology, similar coefficient based on structure congruent [17], similarity based on the random walk [18], joint center [19] and node number based on the sharing neighbor [20], etc.

VI. The Comparison between the Clustering Algorithms

TABLE I.
HEURISTIC CLUSTERING ALGORITHM

Algorithm	Complexity	Accuracy	Applicable condition
GN algorithm	high	high	Medium and small network
Akin-GN algorithm	low	low	Complex network
Improve GN algorithm	low	high	More contour network
CPM algorithm	low	low	Network have obvious hierarchical structure
PAK algorithm	low	high	Mass and intensive network

The heuristic algorithm it is generally to designing algorithm rules based on the intuitive assumption, so from the table 2, it can generally draw an ideal accuracy, and its algorithm complexity is also improved compared with optimization algorithm. But, it is because the intuitive assumption that its usable range is reduced and optimization algorithm present the conditions more obviously. Hence, seeking for universal characteristics of the complexity of network or the nature of community is also a challenge to heuristic algorithm.

TABLE II.
BASED ON THE OPTIMIZATION CLUSTERING ALGORITHM

Algorithm	Complexity	Accuracy	Applicable condition
Laplace Matrix algorithm	low	high	Two community network
Resistance - voltage spectrum segmentation method	low	high	known the number of community
The standard of the spectrum matrix method	low	high	Network have obvious hierarchical structure
K-L algorithm	high	high	Good initial cluster structure
FN algorithm	low	low	Complex network
GA algorithm	high	high	Network have obvious hierarchical structure

Table 1 show when the complexity and the accuracy of the algorithm are assured, the usable range will greatly cut or need more prior experience. But for a wide useable algorithm, its complexity and accuracy will become a pair of contradictory. The reason may be that optimization algorithms are not able to fully understand the relationship between community structure and the complex network itself, thus leading to the "deviation"

for the objective function, which eventually leads to the restrictions of the accuracy and applicability. So, how to find the reasonable target function is a challenge to optimize clustering algorithms.

VII . Comparison of Accuracy and Stability

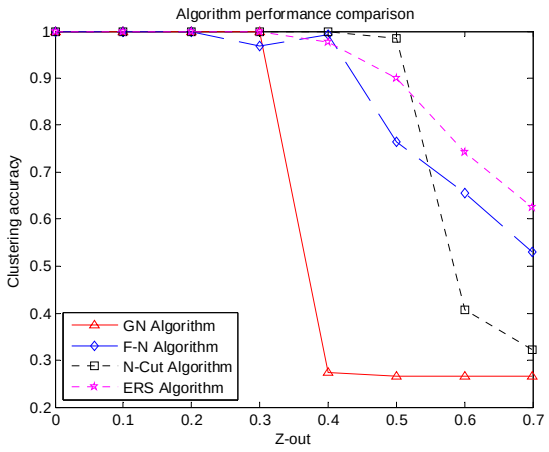


Figure 1. Algorithm performance comparisons..

Most of the existing algorithm of complex network clustering can be divided into two categories: Optimization based methods and heuristic methods. This paper shows their advantages and disadvantages respectively through the analysis of two kinds of social networks community partition algorithm. In this experiment, we use the network which is put forward by Newman and Girvan. This network is regarded as a standard network when testing the performance of the algorithm. Each graph was constructed with 128 vertices, which divided into four communities of 32 vertices each, and the node degree can be adjusted freely. Change of the node degrees would affect the artificial networks hierarchy structure, thus the networks can test the performance of community partition algorithm better. In the experiment, we compared the performance by testing GN, FN, N-Cut and ERS algorithm.

At first, it is a truth for a community that the nodes internal degree is larger than the nodes external degree necessarily in the networks, which means that out-degree can reflect the close degree of internal nodes in the networks. Thus it is concluded that the entire network was of the degree of obvious of hierarchy. The larger of the out-degree of the network, the less obvious structure of the network was. This paper uses Z-out as a variable to divide community. We can see it clearly in Fig.1 that the bigger the value of Z-out, the less accuracy it will be. Also, it shows all algorithms perform high accuracy when Z-out is less than 0.3, but the accuracy of the algorithms begins to fall as the Z-out grows. When the Z-out is less than 0.3, GN algorithm drops faster than any other algorithms, while ERS and N-Cut algorithm still perform high accuracy. As we can see that Z-out=0.5 is a turning point. All algorithms perform a lower accuracy when Z-out is bigger than 0.5, but the ERS algorithm still keeps stable relatively. So ERS has a high stability than other algorithms, and it is more suitable for complex network.

VIII . Conclusion

The complex network clustering is one of the most important complex network analysis methods, and has a broad prospect of application. This paper mainly focuses on the existing complex network clustering algorithms. According to the basic solution strategy, the existing complex network clustering algorithms are divided into two categories: optimization-based method and heuristic-based method; From analyzing the basic principles and relative merits of the existing methods, it shows that encouraging results have been achieved in decade years, but the complex network clustering problem is far from been well resolved. It is embodied in the following respects:

The first problem is that what is the inevitable relationship between the network cluster structure and the else complex phenomenon of the network? Namely, from the network "inner" attributes, can we promote an optimization objective function, an objective reflect and characterizations of the cluster structure.

Secondly, most of the existing discover algorithm for complex networks consider the complexity and precision, or due to the needs of transcendental experience, its scope of application is greatly limited. Therefore, how to design a clustering algorithm which is fast, high precision and no supervision is also a burning question.

Lastly, along with the development of social development and expansion in application field, network clustering problem are diversified. The existing algorithm has been difficult to satisfy present demand, so developing the new clustering algorithm for the special network is necessary. The typical problem during the process includes the division of the overlapped community, dynamic complex network of clustering, distributed network clustering and so on [21-25]. In addition, the unmetered theory and technology has also become one of the major problems in current complex network clustering.

It is believed that these three aspects will be the developing direction of the complex network research in future.

Acknowledgment

This research was supported by National Natural Science Foundation of China with Grant No. 61173036, Hunan Province College Key Laboratory Open Foundation Project with Grant No. 2009GK3016 and Science and Technology Planning Project of Hunan Provincial Science & Technology Department with Grant No.2011GK3200.

References

[1] Newman M E J. The structure and function of complex networks[J]. SIAM review, 2003, 45(2): 167-256.
[2] Boccaletti S, Latora V, Moreno Y, et al. Complex networks: Structure and dynamics[J]. Physics reports, 2006, 424(4): 175-308.
[3] Newman M. Networks: an introduction[M]. Oxford University Press, 2009.

[4] Tyler J R, Wilkinson D M, Huberman B A. E-mail as spectroscopy: Automated discovery of community structure within organizations[J]. The Information Society, 2005, 21(2): 143-153.
[5] Costa L F, Rodrigues F A, Travieso G, et al. Characterization of complex networks: A survey of measurements[J]. Advances in Physics, 2007, 56(1): 167-242.
[6] Girvan M, Newman M E J. Community structure in social and biological networks[J]. Proceedings of the National Academy of Sciences, 2002, 99(12): 7821-7826.
[7] Fortunato S. Community detection in graphs[J]. Physics Reports, 2010, 486(3): 75-174.
[8] Pothen A, Simon H D, Liou K P. Partitioning sparse matrices with eigenvectors of graphs[J]. SIAM Journal on Matrix Analysis and Applications, 1990, 11(3): 430-452.
[9] Wu F, Huberman B A. Finding communities in linear time: a physics approach[J]. The European Physical Journal B-Condensed Matter and Complex Systems, 2004, 38(2): 331-338.
[10] Capocci A, Servedio V D P, Caldarelli G, et al. Detecting communities in large networks[J]. Physica A: Statistical Mechanics and its Applications, 2005, 352(2): 669-676.
[11] Newman M E J. Detecting community structure in networks[J]. The European Physical Journal B-Condensed Matter and Complex Systems, 2004, 38(2): 321-330.
[12] Newman M E J. Fast algorithm for detecting community structure in networks[J]. Physical review E, 2004, 69(6): 066133.
[13] Guimera R, Amaral L A N. Functional cartography of complex metabolic networks[J]. Nature, 2005, 433(7028): 895-900.
[14] Radicchi F, Castellano C, Cecconi F, et al. Defining and identifying communities in networks[J]. Proceedings of the National Academy of Sciences of the United States of America, 2004, 101(9): 2658-2663.
[15] Palla G, Derényi I, Farkas I, et al. Uncovering the overlapping community structure of complex networks in nature and society[J]. Nature, 2005, 435(7043): 814-818.
[16] Liu X, Murata T. Advanced modularity-specialized label propagation algorithm for detecting communities in networks[J]. Physica A: Statistical Mechanics and its Applications, 2010, 389(7): 1493-1500.
[17] Wasserman, Stanley, and Joseph Galaskiewicz, eds. Advances in social network analysis: Research in the social and behavioral sciences. Sage, 1994.
[18] Pons P, Latapy M. Computing communities in large networks using random walks[M]//Computer and Information Sciences-ISCIS 2005. Springer Berlin Heidelberg, 2005: 284-293.
[19] Yang B, Liu J. Discovering global network communities based on local centralities[J]. ACM Transactions on the Web (TWEB), 2008, 2(1): 9.
[20] Sun P G, Gao L, Shan Han S. Identification of overlapping and non-overlapping community structure by fuzzy clustering in complex networks[J]. Information Sciences, 2011, 181(6): 1060-1071.
[21] Gan X, Wang J. The synchronization problem on a class of supply chain complex network[J]. Journal of Computers, 2013, 8(2): 267-271.
[22] Ma R, Deng G, Wang X. A cooperative and heuristic community detecting algorithm[J]. Journal of Computers, 2012, 7(1): 135-140.
[23] Wang Y, Gao L. Detecting protein complexes by an improved affinity propagation algorithm in protein-protein interaction networks[J]. Journal of Computers, 2012, 7(7): 1761-1768.
[24] De Lay N, Gottesman S. A complex network of small non-coding RNAs regulate motility in Escherichia coli[J]. Molecular microbiology, 2012, 86(3): 524-538.
[25] Barthwal R, Misra S, Obaidat M S. Finding overlapping communities in a complex network of social linkages and Internet of things[J]. The Journal of Supercomputing, 2013: 1-24.

Tingrui Pei, born in 1970. PhD, professor, Doctor Supervisor. He is graduated from Beijing University of Posts and Telecommunications, His main research interests include wireless sensor network (WSN) and Multimedia communication.

He is a professor of Dept. Information and Communication Engineering Xiangtan University.

Zhetao Li, born in 1980. PhD,Associate professor, Master Supervisor. His main research interests include internet of things (IOT), compressive sensing, social computing. He is Associate professor of Dept. Information and Communication Engineering Xiangtan University.

Hongzhi, Zhang born in 1987. Master graduate student. His main research interests include internet of social computing and complex large-scale data information processing.

A Public-Key Cryptosystem Based On Stochastic Petri Net

Zuohua Ding[a], Hui Zhou[a], Hui Shen[a], Qi-wei Ge[b]
[a] Lab of ICSE, Zhejiang Sci-Tech University, Hangzhou, Zhejiang, 310018, China
Email: zouhuading@hotmail.com
[b] Faculty of Education, Yamaguchi University, 1677-1 Yoshida, Yamaguchi 753-8513, Japan
Email: gqw@yamaguchi-u.ac.jp

***Abstract*— In this paper, we present a new method to build public-key Cryptosystem. The method is based on the state explosion problem occurred in the computing of average number of tokens in the places of Stochastic Petri Net (SPN). The reachable markings in the coverability tree of SPN are used as the encryption keys. Accordingly, multiple encryption keys can be generated, thus we can perform multiple encryption to get as strong security as we expect. The decryption is realized through solving a group of ordinary differential equations from Continuous Petri Net (CPN), which has the same underlying Petri net as that of SPN. The decipherment difficulty for attackers is in exponential order. The contribution of this paper is that we can use continuous mathematics to design cryptosystems besides discrete mathematics.**

***Index Terms*— Public-key cryptosystem, Stochastic Petri net, Continuous Petri net, Multiple encryption.**

I. INTRODUCTION

The Internet has become so widespread that any one can obtain and provide information easily through the public network. To guarantee the safe communications, the utilization of cryptography becomes very important in order to avoid the leak of secret information or dishonest alternation of the information.

There are two types of cryptography: private-key and public-key cryptosystems. Private-key cryptosystem uses a common private key to encrypt and decrypt messages, and can process encryption and decryption very fast, but it faces a problem to distribute the private key through the public network without leaking of the secrecy [22] [23]. Public-key cryptosystem successfully solves this problem by preparing a pair of keys (public and private keys) in the way that it opens the public key to the public and keeps the private key in secret [19].

Currently, there are a few public-key cryptosystems, such as RSA [21], ElGamal [4], and the elliptic curve cryptography [18]. Since the security(encryption or decryption) of RSA is $O(exp(c(logn)(loglogn))^{1/2})$ (c is a constant, and n is a large factoring number), which is subexponential order rather than an exponential order, we may classify these crytosystems as subexponential cryptosystems.

This work is partially supported by the NSF under Grant No. 61170015 and No.61210004.

Recently, Ge and Okamoto [7] proposed a new public-key cryptography, namely PNPKC, and Ge et al. [8] proposed a Multiple-Encryption Public-Key Cryptography, namely MEPKC. Both Cryptography use elementary T-invariants of Petri nets as the public keys. The security is e^m, where m is the number of transitions of the Petri net. If the encryption is performed in k stages, then the security will be $(e^m)^k$. Such kind of crytosystems can be called exponential cryptosystems.

So far, the public-key cryptosystems are designed with discrete mathematics. In this paper we propose a new public-key cryptography by using continuous mathematics. The encryption part is based on the well known state explosion problem of stochastic Petri nets(SPN), i.e. the state space will increase exponentially as the number of places or the number of initial marking values increases, even through many reduction skills have been proposed to combat this problem such as [13] [26]. The decryption part is based on a group of ordinary differential equations, which can be easily solved by using Runge-Kutta algorithm [9].

The encryption key is composed of a reachable marking in the coverability tree of SPN and the average number of tokens in the places of SPN. A brief description is in the following: The sender randomly select a group of initial markings from a well designed range to generate the coverability tree of a SPN, and compute the average number of tokens of SPN by some software such as SPNP and GreatSPN. By combing this reachable marking and the average number of tokens together in some way, we will get the encryption key. This key is a number that has integral part and decimal fraction part.

The uniqueness of reachable markings guarantee that the encryption key is unique. The key is hidden in a knapsack problem, which is NP-complete. Multiple encryption keys can be generated, thus we can perform multiple encryption to get as strong security as we expect. Hence, we open a key generator to the public.

For the attacker to decrypt, he/she has three difficulties: 1) To compute all the average numbers of tokens of the Petri nets that have initial marking from the given range. If we carefully design the maximum value of the range, then it is hard for attackers to solve all the average number of tokens even using some software. 2) From these average numbers of tokens, the attacker needs to

doi:10.4304/jsw.9.1.94-103

determine which one matches the decimal fraction, and thus to determine the initial marking value selected by the sender. 3) The attacker needs to generate the coverability tree based on this initial marking value, and to determine which reachable marking in the tree has been selected by the sender, in other words, to determine the integral part of of the key.

For the receiver to decrypt the ciphertext, he/she also needs to solve all the average number of tokens of the Petri nets that have initial marking values in the given range. However, the receiver can get these average numbers of tokens by solving a set of ordinary differential equations, which is simple. In the equations, the initial values correspond to the initial markings. The set of equations comes from Continuous Petri Net (CPN), of which the underlying Petri net is the same as that of SPN. CPN is defined recently by David and Alla [2] [3] attempting to deal with the state explosion problem of discrete Petri net by removing the integrality constraints. The solutions of the equations are called state measures in the places. In this paper, we have proved that the state measures in the places equal the average numbers of tokens in the places.

Analysis shows that the security for our method is $v^{2I}O(na^{P(k,n)}b^{Q(k,n)})$, $a > 1, b > 1$, where v is the length of the range of initial marking values, I is the number of places that can be set the initial markings from the range, n is the number of places of the Petri net, k is the maximum number of tokens in the initial markings, and $P(k,n), Q(k,n)$ are two polynomials of k, and n. If applying r-stage encryption, the security can reach $v^{2Ir}O(n^r a^{rP(k,n)} b^{rQ(k,n)})$.

We are not claiming that our public-key encryptosystem is superior to the existing encryptosystems. It is our attempt to design the public-key encryptosystem from a different angle, and give some suggestions in this field.

The rest of the paper is organized as the following: Section 2 briefly introduces the method to compute the average number of tokens of SPN and gives the computational complexity. Section 3 presents a method to compute the state measures of CPN and analyzes the computational complexity. Section 4 proves that the average numbers of tokens of SPN equal the state measures of CPN. Section 5 discusses the security of our SPN based public-key cryptograph. In Section 6, we use a concrete example to illustrate how to use our method to design a public-key cryptograph. Section 7 discusses a related work. The last section, section 8 concludes the paper by simply describing how to combine our system with other encryption system for digital signature, and indicating our future work.

II. The Method To Compute The Average Number of Tokens of SPN and Its Computational Complexity

A. Stochastic Petri Nets(SPN)

The following definition comes from [14].

Definition 2.1: A *continuous stochastic Petri net* is a tuple $SPN = (P, T, A, M_0, \lambda)$, where (P, T, A, M_0) is a underlying untimed Petri net: $P = \{p_1, p_2, \ldots, p_n\}$ is the set of places, $T = \{t_1, t_2, \ldots, t_m\}$ is the set of transitions, $A \subset (P \times T) \cup (T \times P)$ is the set of arcs, and M_0 is the initial marking. $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ is a set of average firing rates of transitions satisfying exponential distributions:

$$\forall t \in T,\ F_t(x) = P\{X_t \leq x\} = 1 - e^{-\lambda_t x}$$

where x represents time, X_t is a continuous random variable representing the time delay for transition t, λ_t is the average firing rate associated with transition t.

A Markov process is a stochastic process that satisfies the *Markovian property*

$$P\{X(\tau) \leq x | X(t), t \in [0, \theta]\} = P\{X(\tau) \leq x | X(\theta) = y\}$$

for any $\tau > \theta$. Markov processes with a discrete state space are called Markov chains. If the parameter t is continuous, the process is a continuous-time Markov chain (CTMC). The time spent in states of a CTMC is a random variable with nonnegative exponential probability density function(pdf).

In practice, a CTMC is described through either a state transition rate diagram or a transition rate matrix, denoted by Q. The state transition rate diagram is a labelled directed graph whose vertices are labelled with the CTMC states, and whose arcs are labelled with the rate of the exponential distribution associated with the transition from a state to another.

If we have the reachable graph (or coverability tree) of SPN, then replacing the firing transition t associated with the arc by average firing rate λ_t (or marking related λ_t), we will get the CTMC that is isomorphic to SPN. Actually we have the following result [15].

Theorem 2.2: Any SPN with finite places and finite transitions is isomorphic to a Continuous Time Markov Chain.

This result enables us to compute average number of tokens in places of SPN.

B. Method To Compute The Average Number of Tokens In Places of SPN

Average number of tokens in places is an important parameter in system performance analysis. It can be solved through the following steps [15].

(1) Constructing transition rate matrix $Q = [q_{ij}]$

The transition rate matrix can be constructed from the coverability tree of SPN. For the elements a_{ij} outside the main diagonal: if there is an arc from state M_i to state M_j, then the value is the rate of the exponential distribution associated with the transition from M_i to M_j; if there is no arc connected, then this element is 0. For the element a_{ii} on the main diagonal, its value is the opposite of the sum of firing rates outputted from state M_i.

(2) Finding the steady state probability $X = (x_1, x_2, \ldots, x_l)$, where l is the number of all reachable markings in the coverability tree of SPN.

This can be obtained by solving the equation group

$$\begin{cases} XQ = 0, \\ \sum_i x_i = 1, \qquad 1 \le i \le l. \end{cases}$$

where Q is a l dimension square matrix.

(3) Constructing place state table

Based on the coverability tree of SPN, we list all the reachable markings. Every reachable marking is a n-dimension vector, which is a row in the table. Thus the table has l rows and n columns.

(4) Obtaining the token probability density function (pdf)

That is to find in the steady state the probability of the number of tokens contained in a place. For a $p \in P$, letting $P[M(p) = i]$ denote the probability of i tokens contained in place p, then the token pdf can be obtained as

$$P[M(p) = i] = \sum_j P[M_j],$$

where $M_j \in R(M_0)$ and $M_j(p) = i$.

(5) Finding the average number of tokens in places

For any $p \in P$, in the steady state, $u_i = \sum_j j \times P[M(p_i) = j]$ is the average number of tokens in place p for any reachable marking.

C. The complexity of finding the average number of tokens in the places

Currently, the best algorithm to solve the equation group

$$\begin{cases} XQ = 0, \\ \sum_i x_i = 1, \qquad 1 \le i \le l. \end{cases}$$

is from Harrow et al. [10] and the complexity is $O(l)$. l depends on n, k and can be estimated as the following. Let k be the maximum number of tokens in the initial markings. Since the size of the reachability graph increases exponentially with both the number of places and the number of tokens in the initial marking, we may assume that $l = a^{p(k,n)}$, $a > 1$, where $p(k, n)$ is a polynomial of k and n. Thus, the complexity to solve this equation group is $O(a^{p(k,n)})$.

From step (3) of Section 2.2, the complexity to find the average number of tokens in a single place is $O(a^{p(k,n)}) + O(a^{p(k,n)}) = O(a^{p(k,n)})$. Hence to find average number of tokens in n places, the complexity is $n \times (O(a^{p(k,n)}) + O(a^{p(k,n)})) = O(na^{p(k,n)})$.

III. The Method To Compute The State Measures of CPN and Its Computational Complexity

Since the size of reachable markings in the coverability tree increases exponentially with both the number of places and the number of tokens in the initial marking. As a result, we will not be able to compute the steady state probability for very large models. We will use some relaxation technique to overcome this difficulty. This relaxation leads to a continuous-time formalism: Continuous Petri Net (CPN).

A. Continuous Petri Net

Definition 3.1: A *Continuous Petri Net* is a tuple $CPN =< P, T, A, M_0, \lambda >$, where (P, T, A) is a underlying Petri net MP: $P = \{p_1, p_2, \ldots, p_n\}$ is the set of places, $T = \{t_1, t_2, \ldots, t_m\}$ is the set of transitions, $A \subset (P \times T) \cup (T \times P)$ is the set of arcs, and M_0 is the initial marking. $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ is a set of average firing rates of transitions.

In the definition, the average firing rate λ_t is actually the reciprocal of firing delay of transition t. In a CPN, the marking of a place is no longer an integer but a nonnegative real number.

Definition 3.2: Let $I = [0, \infty)$ be the time interval and let $m_i : I \to [0, \infty), i = 1, 2, \ldots, n$ be a set of mappings that associated with place p_i. A marking of a Continuous Petri Net $CPN =< P, T, A, v >$ is a mapping

$m : I \to [0, \infty)^n$,

$m(\tau) = (m_1(\tau), m_2(\tau), \ldots, m_n(\tau))$.

Definition 3.3: (State Measure) Given any time moment $t \in [0, \infty)$, the marking value in a place is called the State Measure of this place, denoted as $m(t)$. State measures take nonnegative real numbers as their values.

A transition is enabled if all the input places have nonzero markings. Only enabled transitions can be fired. So, if some marking is moved into a place, we say that the state measure in this place is increasing; if some marking is moved out from a place, we say that the state measure in this place is decreasing. The change rate of state measure can be calculated as the following.

Let p_1 and p_2 be the input places of a transition t and their markings are $m_1(\tau)$ and $m_2(\tau)$, respectively. Let λ_t be the firing rate associated with t, then following the definition of Continuous Petri net defined by David and Alla [2] [3], the marking moving out from p_1 and p_2 is defined by $\lambda_t \times min\{m_1(\tau), m_2(\tau)\}$. If t has only one input p_1, then marking $\lambda_t \times m_1(\tau)$ will be moved out from p_1.

We consider the following type of Petri net as the underlying Petri net of SPN and CPN. It is a subclass of normal Petri net net, namely Message Passing Petri net, or MP for short.

Definition 3.4: A Petri net P is MP if

- P has finitely many places;
- the places of P are partitioned into two disjoint partitions C and B;
- each place from C has one or two input transitions and one or two output transitions, but can not have two input transitions and two output transitions at the same time;
- each place from B has one input transition and one output transition;
- each transition has one input place from C and one output place from C; and
- each transition has either
  1) no input places from B and no output places from B;
  2) no input places from B and one output place from B;

3) one input place from B and no output places from B; or
4) one input place from B and one output place from B.

Here C stands for "Internal States", while B stands for "Buffer".

In a MP, the Internal States and the directly connected transitions form one or several place/transition cycles, namely process net. Hence a MP can also be described as process nets that interact to each other through Buffer B.

With such kind of Petri net structure, the state space still increases exponentially as the number of tokens in the Internal States or Buffer increases.

B. Solving State Measures From Ordinary Differential Equation Model

Based on the semantics defined above, the state measure at each place can be calculated from a differential equation. We have the following cases.

1) One place to one place. As Fig.1 shows, place p will get marking from place p_1. Let the marking at place p and p_1 be m and m_1, respectively. Assume that the firing rates at transition t_1 and t are d_1 and d, respectively. Then the state measure m can be represented as

$$m'(\tau) = d_1 \times m_1(\tau) - d \times m(\tau). \quad (1)$$

If at least one of t_1 and t is not enabled, then $m_1(\tau) = 0$ or/and $m(t) = 0$. Hence the above equation is still true in these situations.

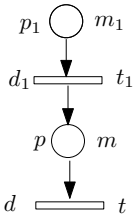


Figure 1. One place to one place model.

2) Two place to one place. As Fig. 2 shows, place p will get marking from place p_1 and p_2. Let the markings at place p_1, p_2 and p be m_1, m_2 and m, respectively. Assume that the firing rates at transition t_1 and t are d_1 and d, respectively. Then the state measure m can be represented as

$$m'(\tau) = d_1 \times min\{m_1(\tau), m_2(\tau)\} - d \times m(\tau). \quad (2)$$

If t_1 is not enabled, then $m_1(\tau) = 0$ or/and $m_2(\tau) = 0$. If t is not enabled, then $m(\tau) = 0$. Hence the above equation also covers these situations.

3) One place to two places. As Fig. 3 shows, place p will get marking from place p_1, but will send some marking out together with place p_2. Let the markings at place p_1, p_2 and p be m_1, m_2 and m, respectively. Assume that the firing rates at transition t_1 and t are d_1 and d, respectively. Then the state measure m can be represented as

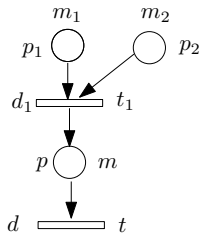


Figure 2. Two places to one place model.

$$m'(\tau) = d_1 \times m_1(\tau) - d \times min\{m(\tau), m_2(\tau)\}. \quad (3)$$

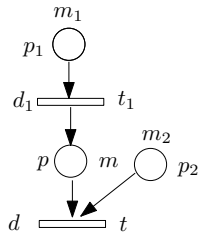


Figure 3. One place to two places model.

If t is not enabled, then either $m(\tau) = 0$ or $m_2(\tau) = 0$, or both. Hence the above equation is still true.

4) Two places to two places. As Fig. 4 shows, transition t_1 has two input places m_1 and m_2 and transition t has two input places m and m_3. Assume the firing rates at transition t_1 and t are d_1 and d, respectively. Then the marking m can be represented as

$$m'(\tau) = d_1 \times min\{m_1(\tau), m_2(\tau)\} - d \times min\{m(\tau), m_3(\tau)\}. \quad (4)$$

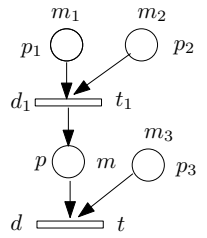


Figure 4. Two places to two places model.

From the differential equation model, we see that state measures are uniquely determined by the system structure and the firing rates.

C. The Computational Complexity

To get the state measures of all the places, we need to solve the initial value problem of ordinary differential equations.

Generally speaking, it is hard to find explicit analytic solutions for nonlinear ordinary differential equations, thus most of the time, we turn to find numerical solutions

instead. We may use function $ode45$ in Matlab to solve our equations. Function $ode45$ is the implementation of combined fourth and fifth-order Runge-Kutta method. $ode45$ is designed to handle the following general problem

$$\frac{dx}{dt} = f(t, x),\ x(t_0) = x_0,$$

where t is the independent variable and x is a vector of dependent variables to be found.

Numerical solutions may give us computational errors due to the algorithm and the machine. In our situation, the computation error can come from two sources: truncation error (because a truncated Taylor Series is used in the computation), and rounding error (because a finite number of binary digits is used inside the machine).

For the truncation error, since the fourth-order Runge-Kutta method has local truncation error $O(h^5)$ and the fifth-order Runge-Kutta method has local truncation error $O(h^6)$, where h is the step size, thus the global truncation error of $ode45$ is $O(h^5)$ [9]. Noticing that the fifth-order Runge-Kutta method can automatically adjust the step size, thus $ode45$ can approximate to the given accuracy by setting $opts$ with command $odeset$. For the rounding error, since implicit Runge-Kutta method has stable area [9], and the algorithm is guaranteed to converge in the stable area. Thus the rounding error of the perturbation can not increase and will decrease to 0 in the iteration process [1].

For the complexity of Runge-Kutta method, if the accuracy is lower than 0.00001, then Runge-Kutta method is more efficient than Newton method. We know that the complexity for Newton method in general is $O(mn^3)$, where n is the number of variables and m is the iteration, which is usually $O(n)$ and never exceeds $O(n^2)$ [25]. Hence, the complexity for Runge-Kutta method in general is $O(n^4)$ and never exceeds $O(n^5)$.

Thus solving the state measure needs time $O(n^5)$, where n is the number of places.

IV. Average Numbers of Tokens of SPN = State Measures of CPN

SPN and CPN describe the events of the system, execution time of events, and the relations between events. In both models, the average execution time of events represent the firing rates of the corresponding transitions. The difference is located in: 1) In SPN, the average number of tokens are obtained by computing Markov chain, while in CPN, the state measures are obtained by solving ordinary differential equations; 2) The computational complexity for SPN is exponential while the computational complexity for CPN is polynomial.

The following result gives us the relation of SPN and CPN.

Theorem 4.1: If SPN and CPN are modeling the same system, then the average number of tokens in places of SPN equal the state measures in places of CPN.

Proof 4.2: Our proof is on the basis of [12]. We consider three situations.

(1) Net with single input

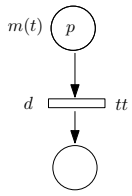


Figure 5. A transition with single input.

Fig. 5 shows a transition with a single input. In the figure, p is the input place of transition tt, $m(t)$ represents the state measure of p at time t, d is the average firing rate of tt, W is the time delay of tt. Assume that p has initial value k_1 at time t_0. In SPN, a transition needs time from enabled to firing, and this time is represented by a random variable W, which is subjected to an exponential distribution function: $F_{tt}(\Delta t) = P[W \leq \Delta t] = 1 - e^{-d\Delta t}$, $\Delta t > 0$. Assume that after Δt time, the average number of tokens of p is k_1', then

$$k_1' = E[m(p)] = k_1 P[W > \Delta t] = k_1 e^{-d\Delta t}.$$

In CPN, for this net, we have equation $x' = -dx$ and $x(t_0) = k_1$. Solving this equation, we get $m(t_0 + \Delta t) = k_1 e^{-d\Delta t}$.

Thus in this case, our result is correct.

(2) Net with two inputs

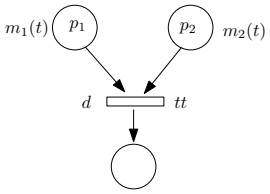


Figure 6. A transition with two inputs.

Fig. 6 shows a transition with two input places. In the figure, p_1 and p_2 are two input places of transition tt, $m_1(t)$ and $m_2(t)$ represent state measures of p_1 and p_2 at time t, respectively. d is the average firing rate of tt, W is the delay of tt. Assume that p_1 has initial value k_1 at time t_0 and p_2 has initial value k_2 at time t_0.

In SPN, let k_1' and k_2' be the new average numbers of tokens of p_1 and p_2 after time Δt, respectively. Then

$$\begin{aligned} k_1' &= E[m(p_1)] \\ &= k_1 - min\{k_1, k_2\} P[W \leq \Delta t] \\ &= k_1 - min\{k_1, k_2\}(1 - P[W > \Delta t]) \\ &= k_1 - min\{k_1, k_2\}(1 - e^{-d\Delta t}). \end{aligned}$$

In CPN, for this net, we have equations:

$$x_1' = -d \times min\{x_1, x_2\},\ x_2' = -d \times min\{x_1, x_2\}$$

with the initial values: $x_1(t_0) = k_1, x_2(t_0) = k_2$. Since $min\{x_1, x_2\}$ is nondeterministic at every time t, it is hard to give analytic solution. With numerical solution, we may partition Δt into several small intervals Δt_i, such that on each such interval, $min\{x_1, x_2\}$ will take a fixed

value. Now we solve the equations on interval Δt_1 as the follows.

i) If $x_1(t_0) < x_2(t_0)$, or $k_1 < k_2$, then $x_1' = -dmin\{x_1, x_2\} = -dx_1$, and $k_1' = x_1(t_0 + \Delta t_1) = k_1 e^{-d\Delta t_1}$.

ii) If $x_1(t_0) \geq x_2(t_0)$, or $k_1 \geq k_2$, then $x_1' = -dx_2$, $x_2' = -dx_2$, then $x_2(t_0 + \Delta t_1) = k_2 e^{-d\Delta t_1}$. Since in the steady state, the output markings from p_1 and p_2 are equal, and the output marking from p_2 is $k_2 - k_2 e^{-d\Delta t_1} = k_2(1 - e^{-d\Delta t_1})$, so the output marking from p_1 should be $k_2(1 - e^{-d\Delta t_1})$. Thus $k_1' = k_1 - k_2(1 - e^{-d\Delta t_1})$.

Combining i) and ii), we get $k_1' = k_1 - min\{k_1, k_2\}(1 - e^{-d\Delta t_1})$, which is the same as the average marking of SPN. We will get similar results on other intervals. Hence in this case, our result is also correct.

(3) Now consider the general cases for Fig. 1, Fig.2, Fig.3, and Fig.4. In SPN, for $\forall t \in T$, its marking flow rate, i.e. average marking moving to the output place in unit time, is $R(t,s) = W(t,s) \times \sum_{M \in E} P(M) \times \lambda$, where E is the set of all reachable markings that make t enable, λ is the average firing rate of t, $W(t,s)$ is the weight attached to the arc from transition t to place s. From the proof of (1) and (2), we know that $R(t,s) = d \times m$, or $R(t,s) = d \times min\{m_1, m_2\}$, where m, m_1, m_2 are the input places of tt, and d is the average firing rate.

Hence for the place m in Fig. 1, Fig.2, Fig.3, and Fig.4, at time t, *the average number of markings of a place = average number of markings to this place - average number of markings out this place*, i.e., $\int_0^t (d_1 m_1 - dm)dt$ for Fig. 1; $\int_0^t (d_1 min\{m_1, m_2\} - dm)dt$ for Fig.2; $\int_0^t (d_1 m_1 - dmin\{m_2, m\})dt$ for Fig.3; $\int_0^t (d_1 min\{m_1, m_2\} - dmin\{m_3, m\})dt$ for Fig.4. These expressions are actually the solutions of Equation (1), Equation (2), Equation (3), and Equation (4) in Section 3.2, respectively. Hence, *the average number of tokens of m in SPN = state measure value of m in CPN*.

Hence, we complete the proof.

V. Public-Key Cryptosystem

A. Public Key and Private Key

1) Public Key: Let $\langle \sum, H \rangle$ be a public key, where $\sum = (P, T, A, M_0, \lambda)$ is a bounded Stochastic Petri Net that has an MP as the underlying Petri net. H is a Hash fucntion which will be defined in the following.

For any $p_i \in P$, let $M_0(p_i)$ represent the initial marking value for place p_i with the range $n_1 \leq M_0(p_i) \leq n_2$, $n_1, n_2 \in N^+$, $i = 1, \ldots, n$. Assume that the sender randomly selects the initial markings $M_0^+(p_i)$ from these range. Define

$$M_0'(p_i) = \begin{cases} H_1(M_0^+(p_i)), & M_0(p_i) \neq 0; \\ 0, & M_0(p_i) = 0. \end{cases}$$

Here H_1 is usually a linear function depending on the size of SPN, the maximum number of tokens in the initial markings, and the memory size. Let $CT(\sum(M_0'))$ be the coverability tree of the net. Define V by $V = H(M_0^+(p_i), J_i, U) = V_2 + V_3 = R_1 J_i^T + 10^{-p} R_2 U^T$, where

- J_i is the row vector of n dimension of $CT(\sum(M_0'))$; J_i^T is the transpose of J_i; R_1 is a n dimension vector with positive integers; $V_2 = H_2(J_i) = R_1 J_i^T$, where H_2 is 1-1 mapping; R_2 is a randomly selected n dimension vector with positive integers.
- $V_3 = H_3(U) = 10^{-p} R_2 U^T$, where $U = (u_1, u_2, \ldots, u_n)$, u_i is the average number of tokens in place p_i of SPN, that can be solved by the sender. $p(\in N)$ is an integer depending on the selection of R_2 and $M_0(p_i), n_1 \leq M_0(p_i) \leq n_2$, which can determine as the following. The receiver calculates the maximum value of all $R_2 U^T$ by solving the equation groups as discussed in Section 3.3. Let M be the maximum. Then take $p = min\{q \in N | 10^q \geq M\}$. This p can guarantee that the number $10^{-p} max\{R_2 U^T\}$ is a decimal fraction, thus the number $V_3 = H_3(U) = 10^{-p} R_2 U^T = g$ from the sender is also a decimal fraction. The receiver then computes all the V_3, and finds which V_3 is the most closest one to this g. The initial markings for this closest V_3 are exactly the initial markings selected by the sender. However, the attacker does not know how to generate p. In order to get p, the attacker has to has to try every possible initial marking, and calculate all possible V_3 from $CT(\sum(M_0'))$. The complexity for the attacker will be in multiple exponential.

2) Private Key: The private key is designed as $< E, \overline{H_2} >$, where E is a set of equations consisting of the following six types of ordinary differential equations generated from Petri net MP:

- Type 1 [Internal]. $m_i' = \tilde{d}_{i-1} m_{i-1} - \tilde{d}_i m_i$. Here m_i and m_{i-1} are the states of the same process net.
- Type 2 [Input-before]. $m_i' = \tilde{d}_{i-1} min\{m_{i-1}, x_k\} - \tilde{d}_i m_i$. Here m_i and m_{i-1} are the states of the same process net. m_k is the input to this process net from buffer.
- Type 3 [Input-after]. $m_i' = \tilde{d}_{i-1} m_{i-1} - \tilde{d}_i min\{m_i, m_k\}$. Here m_i and m_{i-1} are the states of the same process net. m_k is the input to this process net from buffer.
- Type 4 [Input-before-after]. $m_i' = \tilde{d}_{i-1} min\{m_{i-1}, m_k\} - \tilde{d}_i min\{m_i, m_l\}$. Here m_i and m_{i-1} are the states of the same process net. m_k and m_l are the inputs to this process net from buffer.
- Type 5 [Asynchronous]. $m_k' = \tilde{d}_i m_i - \tilde{d}_{i'} min\{m_{i'}, m_k\}$. Here m_i and $m_{i'}$ are the states of two different service nets respectively. m_k is the message between these two service nets.
- Type 6 [Synchronous]. $m_k' = \tilde{d}_i min\{m_i, m_l\} - \tilde{d}_{i'} min\{m_{i'}, m_k\}$. Here m_i and $m_{i'}$ are the states of two different service nets respectively. m_k and m_l are the messages between these two service nets, where m_l is usually indicates the request that can be calculated by Type 5 and m_k is the reply.

$\overline{H_2} : V_2 \to J_i$ is a mapping which can be determined based on the reachable marking set of coverability tree through the formula $V_2 = R_1 J_i^T$.

We claim that it is almost impossible to derive private key from public key. The reason is as the following. If we design the k(the maximum number of tokens in the initial markings) and the range of H_1 big enough, the attacker needs to try all possible initial markings to determine $M_0^+(p_i)$, and then further to determine $CT(\sum(M_0'))$ and all the J_i, and finally to determine the J_i in the private key. The whole process is multiple exponentially hard.

B. Encryption and Decryption

1) Steps of Encryption: There are five steps in the encryption.

(1) For a plaintext P, the sender generates cipertext C_1' using symmetric cryptosystems such as AES and 3DES.

(2) Randomly select the initial value $M_0^+(p_i)$ of $p_i, i = 1, 2, \ldots, I$ from the range $n_1 \le M_0(p_i) \le n_2$, $n_1, n_2 \in N^+$. Following the method to calculate the average number of tokens of SPN in the steady state and using some software such as SPNP or GreatSPN, we can compute $U = (u_1, u_2, \ldots, u_n)$.

(3) Compute $M_0'(p_i)$, and then get the coverability tree $CT(\sum(M_0'))$ of $SPN\sum(M_0')$. Randomly select a row vector J_i which corresponds to the node i in $CT(\sum(M_0'))$. Based on the function $V_2 = H_2(J_i) = R_1 J_i^T$ in the public key, we compute V_2 and thus obtain the value of $V = V_2 + V_3$, which is a number with integral part and decimal part.

(4) The cipertext $C_1 = (C_1', V)$ is obtained which can be regarded as the result of the first stage encryption.

(5) Multiple encryption: Regarding C_1 as the plaintext, randomly choose a row vector different from the first time vector from the coverability tree $CT(\sum(M_0'))$. Repeating the steps (1)-(4), eventually after r stages, we will get the cipertext $C_r = (C_r', V_r)$.

2) Steps of Decryption: There are four steps in the decryption.

(1) After receiving the cipertext $C_r = (C_r', V_r)$, based on the initial marking range $n_1 \le M_0(p_i) \le n_2$, $n_1, n_2 \in N^+$ and the semantics of CPN, we can build an ordinary differential equation group. Applying Runge-Kutta algorithm, we calculate many values of $V_3 = H_3(U) = 10^{-p} R_2 U^T$ at different initial marking values. Then we find the most closest V_3 to the decimal fraction from the sender. The initial markings $M_0(p_i)$ for this most closest V_3 are the initial markings selected by the sender.

(2) Based on the value of $M_0^+(p_i)$, and

$$M_0'(p_i) = \begin{cases} H_1(M_0^+(p_i)), & M_0(p_i) \ne 0; \\ 0, & M_0(p_i) = 0. \end{cases}$$

in the public key, we can determine the coverability tree $CT(\sum(M_0'))$ of $SPN\sum(M_0')$ from the sender.

(3) Building the mapping $\overline{H}_2 : V_2 \to J_i$, where $V_2 = H_2(J_i) = R_1 J_i^T$, and J_i is the row vector of $CT(\sum(M_0'))$. Find the V_2 that matches the integral part of V_r, thus from mapping $\overline{H}_2$, we can determine the row vector J_i selected by sender.

(4) Using J_i for the decryption to C_r', we will get the $r-1$ stage cipertext $C_{r-1} = (C_{r-1}', V_{r-1})$. Repeat the above steps until we get the plaintext P.

C. Security Measure

1) The Decryption Complexities For The Attacker and For The Receiver: In order to decipher the text, the attacker must know the initial marking values selected by the sender. Normally people will use the method in section 2.2 to compute average number of tokens for SPN. The time complexity to compute one time average number of tokens is $O(na^{P(k,n)})$, $a > 1$, here k is the maximum number of tokens in the initial markings, $P(k,n)$ is a polynomial of k and n. Since each of those places $p_i, i = 1, 2, \ldots, I$ that can be assigned the initial markings from the range $n_1 \le M_0(p_i) \le n_2$ has $n_2 - n_1 + 1$ possibilities to take the initial values, thus the computing complexity to get all possible v_3 is $(n_2 - n_1 + 1)^I O(na^{P(k,n)})$, $a > 1$. Since the number of states will increase exponentially as the number of places and the number of initial markings of places increase, we assume time to calculate the states is $O(b^{Q(k,n)})$, where $Q(k,n)$ is a polynomial of k and n, and $b > 1$. There are $(n_2 - n_1 + 1)^I$ possibilities for the sender to select the initial markings. Since every selected initial marking $M_0^+(p_i)$ corresponds a coverable tree $CT(\sum(M_0'))$, thus there are also $(n_2 - n_1 + 1)^I$ possibilities to select trees. Hence, for one time decryption, the complexity is $(n_2 - n_1 + 1)^I \times O(b^{Q(k,n)}) \times (n_2 - n_1 + 1)^I \times O(na^{P(k,n)}) = (n_2 - n_1 + 1)^{2I} \times O(na^{P(k,n)} b^{Q(k,n)})$, $a > 1, b > 1$.

However, the receiver only needs to solve a group of ordinary differential equation group and the complexity is $O(n^5)$. When the initial markings are changed, the initial values to the ordinary differential equation group will be changed, but the complexity to solve the equation group still stays the same. Thus to determine the initial marking of places selected by sender, the receiver at most needs to solve the equation group $(n_2 - n_1 + 1)^I$ times, so the complexity for the decryption is $(n_2 - n_1 + 1)^I O(n^5)$.

2) The Complexity for Multiple Encryption: In order to increase the decryption difficulty, we may adopt multi-stage encryption. The corresponding complexity is as the following.

(1) Since in every stage the selected row vectors J_i are different, then the complexity to decipher r-stage encryption plain text is $(n_2 - n_1 + 1)^{2rI}$ $O(n^r a^{rP(k,n)} b^{rQ(k,n)})$, $a > 1, b > 1$.

(2) We may increase the process nets in the Petri net, i.e. to increase the index I in the expression $(n_2 - n_1 + 1)^I O(na^{P(k,n)} b^{Q(k,n)})$, then as the number of process nets increase, the complexity will increase exponentially.

(3) We may increase the the maximum number k of tokens in the initial marking, accordingly, the state space will expand quickly and attackers can not compress this expanding state space caused by the increasing number of tokens.

In summary, the computing time for an attacker to compute the average number of tokens is exponential, thus it is hard to get the coverability tree selected by sender. On the other hand, in our public key, based on the knapsack problem (NP-complete problem [6]), we have designed a Hash function $V_2 = H_2(J_i) = R_1 J_i^T$. Thus the attacking to our encryption is also a NP-complete problem.

VI. An Example To Design A Public-Key Cryptosystem

A. Preparing Public Key and Private Key

(1) Choose a bounded Petri net as shown in Fig. 7. Fig. 8(a)(b) can be used for multiple encryption, where (a) is to increase the number of process nets and (b) is to increase the Internal States in the process net. In Fig. 7, $M_0(p_2) = M_0(p_4) = M_0(p_5) = M_0(p_6) = 0$, and the firing rates for the transitions t_1, t_2, t_3 and t_4 are 1. $M_0(p_1)$ and $M_0(p_3)$ are in the range: $1 \leq M_0(p_1) \leq M_0(p_3) \leq 10, M_0(p_1), M_0(p_3) \in N^+$.

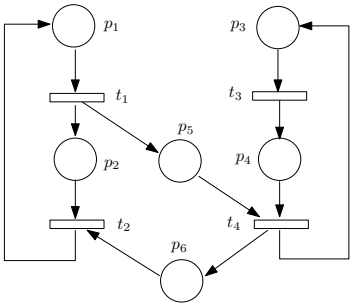


Figure 7. Petri net for encryption.

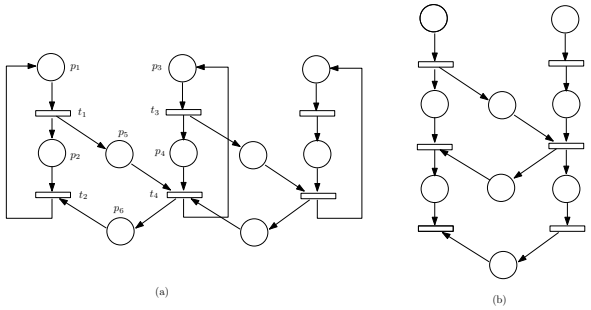


Figure 8. Extended Petri net for multiple encryption.

(2) Design Hash function H.

i) Define new initial markings:

$$M_0'(p_i) = V_1 = \begin{cases} H_1(M_0^+(p_i)), & M_0(p_i) \neq 0; \\ 0, & M_0(p_i) = 0. \end{cases} = \begin{cases} 2(M_0(p_i)), & M_0(p_i) \neq 0; \\ 0, & M_0(p_i) = 0. \end{cases}$$

Note that here we design $H_1(M_0^+(p_i)) = 2(M_0(p_i))$ only for the convenience, and H_1 in the real time is designed based on the ability to decipher the text, memory and the calculation speed.

ii) Randomly select $R_1 = (1, 5, 13, 17, 7, 23)$ for $V_2 = H_2(J_i) = R_1 J_i^T$.

iii) Randomly select $R_2 = (1, 2, 3, 4, 5, 6)$. Based on the formula $V_3 = H_3(U) = 10^{-p} R_2 U^T$, we determine p by calculating the maximum value of $R_2 U^T$. Let $M_0(p_1) = M_0(p_3) = 10$, $M_0(p_2) = M_0(p_4) = M_0(p_5) = M_0(p_6) = 0$, we build the following set of equations:

$$\begin{cases} m_1' = min\{m_2, m_6\} - m_1, \\ m_2' = m_1 - min\{m_2, m_6\}, \\ m_3' = min\{m_4, m_5\} - m_3, \\ m_4' = m_3 - min\{m_4, m_5\}, \\ m_5' = m_1 - min\{m_4, m_5\}, \\ m_6' = min\{m_4, m_5\} - min\{m_2, m_6\}, \end{cases}$$

with the initial values: $m_1(0) = m_3(0) = 10$, $m_2(0) = m_4(0) = m_5(0) = m_6(0) = 0$. Using Matlab, we get $U = (3.3333, 6.6667, 3.3325, 6.6675, 3.3342, 3.3325)$. Thus, $R_2 U^T = 90.0002$. Since $p = min\{q \in N | 10^q \geq 90.0002\} = 2$, we get $V_3 = H_3(U) = 10^{-2} \times (1, 2, 3, 4, 5, 6) U^T$.

Thus the Hash function H would be

$$\begin{aligned} V &= H(M_0^+(p_i), J_i, U) = V_2 + V_3 \\ &= R_1 J_i^T + 10^{-p} R_2 U^T \\ &= (1, 5, 13, 17, 7, 23) J_i^T + 10^{-2} \times (1, 2, 3, 4, 5, 6) U^T. \end{aligned}$$

(3) Private key. First to determine E, which is a set of ordinary differential equations as the following:

$$\begin{cases} m_1' = min\{m_2, m_6\} - m_1, \\ m_2' = m_1 - min\{m_2, m_6\}, \\ m_3' = min\{m_4, m_5\} - m_3, \\ m_4' = m_3 - min\{m_4, m_5\}, \\ m_5' = m_1 - min\{m_4, m_5\}, \\ m_6' = min\{m_4, m_5\} - min\{m_2, m_6\}, \end{cases}$$

with the initial values: $1 \leq m_1(0), m_3(0) \leq 10$, $m_2(0) = m_4(0) = m_5(0) = m_6(0) = 0$. Next to determine $\bar{H}_2$, which is to determine J_i.

We need to solve the above differential equations covering all the cases that m_1 and m_3 take values from 1 to 10. Without loss of generality, we only calculate the solutions of the differential equation group for the range $1 \leq M_0(p_1), M_0(p_3) \leq 2$. If $M_0(p_1) = M_0(p_3) = 1$, $V_3 \approx 0.09$; If $M_0(p_1) = 1, M_0(p_3) = 2$, $V_3 \approx 0.13$; If $M_0(p_1) = 2, M_0(p_3) = 1$, $V_3 \approx 0.16$; If $M_0(p_1) = 2, M_0(p_3) = 2$, $V_3 \approx 0.18$. Since the decimal fraction of V_3 from sender is 0.092, by comparing with all the cases of V_3 here, we choose the most closest one $V_3 \approx 0.09$. From this value, we imply that the sender uses $M_0(p_1) = M_0(p_3) = 1$ as the initial markings.

Since

$$M_0'(s_i) = V_1 = \begin{cases} 2(M_0^+(s_i)), & M_0(s_i) \neq 0; \\ 0, & M_0(s_i) = 0. \end{cases}$$

we determine the coverability tree in the situation $M_0(s_1) = M_0(s_3) = 2$, which is shown in Fig. 9.

Since there are 18 reachable markings in the tree, we will have 18 row vectors. Based on the formula $V_2 =$

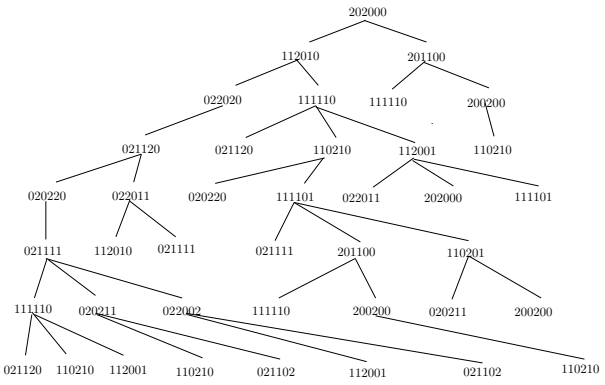


Figure 9. Part of the coverability tree.

$H_2(J_i) = R_1 J_i^T = (1, 5, 13, 17, 7, 23) J_i^T$, we define the mapping $\overline{H}_2 : V_2 \to J_i$ by Table I.

TABLE I.
INVERSE FUNCTION $\overline{H}_2 : V_2 \to J_i$

V_2	J_1	J_2	J_3	J_4	J_5	J_6
28	2	0	2	0	0	0
32	2	0	1	1	0	0
36	2	0	0	2	0	0
39	1	1	2	0	1	0
43	1	1	1	1	1	0
47	1	1	0	2	1	0
50	0	2	2	0	2	0
54	0	2	1	1	2	0
55	1	1	2	0	0	1
58	0	2	0	2	2	0
59	1	1	1	1	0	1
63	1	1	0	2	0	1
66	0	2	2	0	1	1
70	0	2	1	1	1	1
74	0	2	0	2	1	1
82	0	2	2	0	0	2
86	0	2	1	1	0	2
90	0	2	0	2	0	2

B. Encryption

The encryption contains the following steps:

(1) With AES, the sender transforms plaintext P to cipertext C_1'.

(2) Randomly select $M_0(p_1) = M_0(p_3) = 1$. By using the method in Section 2.2 and software SPNP or GreatSPN to calculate the average number of tokens of SPN, we get $U = (u_1, u_2, \ldots, u_m) = (0.3077, 0.6922, 0.3076, 0.6923, 0.3846, 0.3076)$. Thus $V_3 = H_3(U) = 10^{-2} \times (1, 2, 3, 4, 5, 6) U^T \approx 0.092$.

(3) Since

$$M_0'(p_i) = V_1 = \begin{cases} 2(M_0^+(p_i)), & M_0(p_i) \neq 0; \\ 0, & M_0(p_i) = 0. \end{cases} = \begin{cases} 2, & M_0(p_i) \neq 0; \\ 0, & M_0(p_i) = 0. \end{cases}$$

we build the the coverability tree of $SPN \sum(M_0^+)$ as shown in Fig. 9. In the figure we only given part of the tree. In the tree, the sender randomly choose row vector $(0, 2, 2, 0, 1, 1)$ as the encryption vector J_i. Since $V_2 = H_2(J_i) = R_1 J_i^T = (1, 5, 13, 17, 7, 23)(0, 2, 2, 0, 1, 1)^T = 66$, we get $V = V_2 + V_3 \approx 66 + 0.092 = 66.092$.

(4) Finally, we get the cipertext $(C_1', V) = (C_1', 66.092)$.

Note: For the computing convenience, we only choose $M_0(p_1) = M_0(p_3) = 1$, and only perform one time encryption.

C. Decryption

After getting the cipertext $C_1 = (C_1', 66.092)$, the receiver knows that the integral part of V is 66. By checking the table of function $\overline{H}_2$, we find that the sender has chosen the vector $J_{13} = (0, 2, 2, 0, 1, 1)$ for encryption. Using J_{13} as the decryption key of AES, we will get the plaintext P.

VII. RELATED WORK

RSA [21] is the most extensively used public-key crytosystem, and its security relies on the difficulty of factoring the large integer problem. Its complexities of encryption, decryption and attacking are the same: $O(exp(c(logn)(loglogn))^{1/2})$, c is a constant and n is a large factoring number. This expression is subexponential, not exponential. In our public-key crytosystem, we first use private key cryptosystem such as AES or 3DES to encrypt the plaintext, which belongs to a NP-problem [22]. Then based on the knapsack problem, we design a Hash function: $V = H(M_0^+(p_i), J_i, U) = V_2 + V_3 = R_1 J_i^T + 10^{-p} R_2 U^T$, where the computing of J_i from V, R_1, and R_2 also belongs to a NP-complete problem [6]. Thus the security of our method is higher than that of RSA after one time encryption. If applying r-stage encryption, the security can reach $(n_2 - n_1 + 1)^{2rI} O(n^r a^{rP(k,n)} b^{rQ(k,n)})$.

PGP [5] is a protocol for email text encryption. Its core part is RSA. When encrypting, PGP first compresses plain text, and then encrypts the compressed plaintext with session key, finally encrypts the session key with RSA. Our technique is also based on session key. However, PGP is based on RSA, while ours is based on NP-complete problem, thus our security is higher than PGP. Also because PGP is based on RSA, the encryption is slow. Since our encryption requires computing average number of tokens in places of SPN, and decryption is to solve a group of differential equations, our encryption and decryption are comparably faster.

MEPKC [8] is designed based on elementary T-invariants of the Petri net. Petri nets are used as a key-generator and elementary T-invariants are used as the encryption keys. After r-stage encryption, the security is $(e^m)^r$, which is still an exponential expression. In MEPKC, the sender needs to construct a small Petri net such that the net contains as many as possible elementary T-invariants, where elementary T-invariants are used as the entryption keys. In our technique, we use the reachable markings of coverability tree to generate key, and the coverability tree is comparably easy to get from SPN, so our encryption is faster than MEPKC.

VIII. CONCLUSION

We have developed a new public-key cryptosystm based on the difficulty to solve average number of tokens in places of SPN for a given range of initial marking values, and used CPN to perform the decryption. The reachable markings in coverability tree of SPN are used as the encryption key, and the plaintext can be encrypted in multiple stages. Comparing with the traditional public-key cryptosystms such as RSA, PGP, our technique has higher security. Moreover, the encryption and the decryption are easier.

Usually both the public key and the private key in the public-key cryptosystem can be used to encrypt plaintext, such as RSA, ECC, etc. However, in our technique, only public key can be used for the encryption, so our technique can not be used for digital signature. To overcome this shortcoming, we may combine our system with those public-key cryptosystems that are qualified for digital signature. Now we use DSA as the example to illustrate the encryption and decryption process. Assume that the sender A(with DSA) sends the plaintext P to the receiver B(with our technique). The public key and private key of A are K_{eA} and K_{dA}, and public key and private key of B are K_{eB} and K_{dB}, respectively. A first uses its own private key K_{dA} to encrypt the plaintext P, and the result is $S = E(P, K_{dA})$; then A uses the public key K_{eB} of B to encrypt S, and the result is $C = E(S, K_{eB})$; finally A sends C to B. After B receives C, B uses its own private key K_{dB} to decrypt C, and obtain $S = D(C, K_{dB})$; then uses the public key K_{eA} of A to decrypt S, and obtain $P = D(S, K_{eA})$. Thus the secret and the reality are promised. In this way, our technique can also be used for digital signature.

In order to increase the attack difficulty, we may design more complicated hash function H in the public key. We may also combine our cryptosystem with other cryptosystems to increase the security. One may notice that while our technique increase the decryption difficulty for attackers, it also increase the computing work for the receivers. Two issues will be solved in the future: 1) How to store all reachable markings in the coverability tree of SPN; 2) How to estimate security if the key itself gets brute force attack.

REFERENCES

[1] U. M. Ascher, L. R. Petzold, *Computer methods for ordinary differential equations and differential-algebraic equations*, Society for Industrial & Applied Mathematis, Philadelphia, PA, USA, 1998.

[2] R. David and H. Alla, Continuous Petri nets, *Proceedings of* 8^{th} *European Workshop on Application and Theory of Petri nets*, Zaragoza, Spain, pp.275-294, 1987.

[3] R. David and H. Alla, Autonomous and timed continuous Petri nets, *Proceedings of* 11^{th} *Intl Conference on Application and Theory of Petri nets*, Paris, France, pp.367-381, 1990.

[4] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions in Information Theroey*, vol.IT-31, no.4, pp.469-472, 1985.

[5] S. Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly & Associates, 1994.

[6] M. R. Garey, D. S. Johson, *Computers and Intractability (A Guide to the Theory of NP-Completeness)*, W. H. Freeman and Company, New York,1991.

[7] Q. W. Ge, T. Okamoto, A Petri net based public-key cryptography: PNPKC, *IEICE. Trans. Fundamentals*, vol.E-84-A(6), pp.1532-1535, 2001.

[8] Q. Ge, C. Shigenaga, and R. Wu, A Petri net based new conception of publickey crytography, *Proceedings of ICFS'02*, pp.37-42, 2002.

[9] E. Hairer, S.P. Nϕrsett, G. Wanner, *Solving Ordinary Differential Equations(I)(II)*, Nonstiff Problems, Second Edition, Springer-Verlag, 1993.

[10] A. W. Harrow, A. Hassidim, S. Lloyd, Quantum algorithm for solving linear systems of equations, *Phys. Rev. Lett.*, vol.103, no. 15, pp.150502-150506, 2009.

[11] W. Henderson, D. Lucic, P. G. Taylor, A net level performance analysis of Stochastic Petri Nets, *J. Austral. Math. Soc. Ser. B*, vol.31, 176-187, 1989.

[12] K. Hiraishi, Performance evaluation of workflows using continuous Petri nets with interval firing speeds, *Petri Nets'08*, *LNCS*, vol.5062, pp.231-250, 2008.

[13] C. Lin, D. C. Marinescu, Stochastic high-level Petri nets and applications, *IEEE Transactions on Computers*, vol.37, no.7, pp.815-825, 1988.

[14] M. K. Molloy, Performance analysis using stochastic Petri nets, *IEEE Transactions on Computers*, vol. C-31, no.9, pp.913-917, 1982.

[15] M. K. Molloy, On the integration of delay and throughput measures in distributed processing models. Ph.D. dissertation, Univ. of California, Los Angeles, 1981.

[16] M. A. Marsan, A. Bobbio, S. Donatelli, Petri nets in performance analysis: An introduction, *Petri Nets'98*, *LNCS*, vol.1491, pp.211-256, 1998.

[17] B. B. Nich, S. E. Tavores, Modelling and analyzing cryptographic protocols using Petri nets, *Advance in Cryptology-LNCS*, vol.718, pp.275-295, 1992.

[18] T. Okamoto and S. Uchiyamaa, Recent topics of public-key cryptography: 1. On the security of elliptic curve cryptosystems, *IPSJ Magazine*, vol.39, no.12, pp.1252-1257, 1998.

[19] T. Okamoto, E. Fujisaki, and S. Uchiyamaa, Recent topics of public-key cryptography: Provably secure and practical public-key encryption, *IPSJ Magazine*, vol.40, no.2, pp.170-177, 1999.

[20] L. Recalde, S. Haddad, M. Silva, Continuous Petri nets: expressive power and decidability issues, *ATVA'07*, *LNCS*, vol.4762, pp.362-377, 2007.

[21] R. L. Rivest, A. Shamir, L. Adleman, A method of obtaining digital signatures and Public-Key cryptosystems, *Comm. of ACM*, vol.21, no.2, pp.120-126, 1978.

[22] A. Salomaa, *Public-Key Cryptograpghy*, Springer-Verlag, Berlin, Heidelberg, 1990.

[23] T. Shitayama, A survey of block ciper AES and a view of the future, *IPSJ Magazine*, vol. 40, no.2, pp.139-145, 1999.

[24] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press Inc., 1995.

[25] S. A. Teukolsky, W. H. Press, W. T. Vetterling, *Numerical recipes in C++ (2nd edition)*, Cambridge Univ Press, 1993.

[26] S. Tu, S. M. Shatz, and T. Murata, Applying Petri net reduction to support Ada tasking deadlock analysis, *Proceedings of the* 11^{th} *International Conference on Distributed Computing Systems*, pp.96-103, Paris, France, 1990.

Estimation of Distribution Algorithms for Knapsack Problem

Shang Gao
School of Computer Science and Technology, Jiangsu University of Science and Technology, Zhenjiang 212003, China
Email: gao_shang@just.edu.cn

Ling Qiu
Artificial Intelligence of Key Laboratory of Sichuan Province, Sichuan University of Science and Engineering ,Zigong 643000,China

Cungen Cao
Key Laboratory of Intelligent Information Processing, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China
Email: cgcao@ict.ac.cn

***Abstract*—Estimation of distribution algorithms (EDAs) is a new kind of evolution algorithm. In EDAs , through the statistics of the information of selected individuals in current group, the probability of the individual distribution in next generation is given and the next generation of group is formed by random sampling. A wide range of mathematical model of the knapsack problem are proposed. In this paper, the EDAs is applied to solve the knapsack problem. The influence of several strategies, such as numbers of population and better population selection proportions are analyzed. Simulation results show that the EDAs is reliable and effective for solving the knapsack problem. The Maltab code is given also. It can easily be modified for any combinatorial problem for which we have no good specialized algorithm.**

***Index Terms*—estimation distribution algorithm, knapsack problem, genetic algorithm**

I. INTRODUCTION

The knapsack problem or rucksack problem is a problem in combinatorial optimization: Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a given limit and the total value is as large as possible. It derives its name from the problem faced by someone who is constrained by a fixed-size knapsack and must fill it with the most valuable items. The 0/1 knapsack problem is proven to be NP-complete. It is traditionally solved by the dynamic programming algorithm, which is accepted as the most practical way to solve this problem. With the advent of parallel processors, many researchers concentrated their efforts on development of approximation algorithms for NP-complete problems based on the application of parallel processors. For the 0/1 Knapsack problem, such works were reported by Peters and Rudolf [1], and Gopalakrishnan et al. [2]. Another relevant branch of research was related to design of systolic arrays for dynamic programming problems. This approach was considered in works of Li et al. [3], Lipton et al. [4] and others. A different model for the parallel computation of the Knapsack problem with weights given by real numbers was considered by A. Yao [5]. Currently, the method solving knapsack problem are accurate methods (such as dynamic programming, the recursive method, backtracking, branch and bound method [6]), approximation algorithms (such as the greedy method [6], Lagrange method, etc.) and intelligent optimization algorithms (such as simulated annealing algorithm[7], genetic algorithms [7] genetic annealing evolutionary algorithm [8], ant colony algorithm [9, 10]), particle swarm optimization algorithm [11], DNA [12]）. A new version of MOEA/D with uniform design for solving multiobjective 0/1 knapsack problems is proposed in reference [13].

Estimation of distribution algorithms (EDAs) are stochastic optimization techniques that explore the space of potential solutions by building and sampling explicit probabilistic models of promising candidate solutions. This explicit use of probablistic models in optimization offers some significant advantages over other types of metaheuristics. EDAs were successfully applied to optimization of large spin glass instances in two-dimensional and three-dimensional lattices, military antenna design, multiobjective knapsack, groundwater remediation design, aminoacid alphabet reduction for protein structure prediction, identification of clusters of genes with similar expression profiles, economic dispatch, forest management, portfolio management, cancer chemotherapy optimization, environmental monitoring network design, and others. In this paper, a new method for knapsack problem is put forward based on estimation of distribution algorithms and better population selection proportions are analyzed. Estimation of distribution

doi:10.4304/jsw.9.1.104-110

algorithms (EDAs) is a new area of evolutionary computation. In EDAs there is neither crossover nor mutation operator. New population is generated by sampling the probability distribution, which is estimated from a database containing selected individuals of previous generation.

Since Estimation of distribution algorithms (EDAs) were proposed by Baluja in 1994 [14], EDAs quickly become an important branch of evolutionary algorithms because they have better mathematical foundation than other evolutionary algorithms. On the basis of statistical learning theory, EDAs use some individuals selected from the population at the current evolutionary generation to build a probability model and then produces offspring for the next generation by sampling the probability model in a probabilistic way. A lot of investigations in [15-22] show that EDAs have good optimization performance in both combinatorial problems and numeric optimization problems. Until now there are many studies about EDAs, but EDAs mainly consist of several types: Population based incremental learning (PBIL) [14], univariate marginal distribution algorithm (UMDA), compact genetic algorithm (CGA), mutual-information-maximizing input clustering algorithm (MIMIC) , bivariate marginal distribution algorithm (BMDA), factorized distribution algorithm (FDA), Bayesian optimization algorithm (BOA), extended compact genetic algorithm (ECGA) and estimation of Bayesian network algorithm (EBNA). UMDA works well only in the solution of linear problems with independent variables, so it requires extension as well as application of local heuristics for combinatorial optimizations. PBIL uses vector probabilities instead of population and has good performance for solving problems with independent variables in binary search space. CGA independently deals with each variable and needs less memory than simple genetic algorithm. MIMIC searches the best permutation of the variables at each generation to find the probability distribution through using Kullback-Leibler distance. BMDA is mainly based on the construction of a dependency graph, which is acyclic but does not necessarily have to be a connected graph. FDA integrates evolutionary algorithms with simulated annealing. This method requires additively decomposed function and the factorization of the joint probability distribution remains same for all iterations. BOA applies Bayesian network and Bayesian Dirichlet metric to estimate joint probability distributions, thus, it can take advantage of the prior information about the problem. ECGA factorizes the joint probability distribution as a product of marginal distributions of variable size. EBNA employs Bayesian network for the factorization of the joint probability distribution and BIC score.

II. The Mode of Knapsack Problem

The most common problem being solved is the 0-1 knapsack problem, which restricts the number x_i of copies of each kind of item to zero or one.

Let there be n items, x_1 to x_n where x_i has a value p_i and weight c_i. The maximum weight that we can carry in the bag is C. It is common to assume that all values and weights are nonnegative. To simplify the representation, we also assume that the items are listed in increasing order of weight.

$$\begin{aligned} &\max \sum_{i=1}^{n} p_i x_i \\ &s.t. \quad \sum_{i=1}^{n} c_i x_i \le C \\ &x_i \in \{0,1\}, (i = 1,2,\cdots,n) \end{aligned} \tag{1}$$

Maximize the sum of the values of the items in the knapsack so that the sum of the weights must be less than the knapsack's capacity.

The knapsack problem is one of the most studied problems in combinatorial optimization, with many real-life applications. For this reason, many special cases and generalizations have been examined.

One common variant is that each item can be chosen multiple times. The **bounded knapsack problem** specifies, for each item i, an upper bound u_i (which may be a positive integer, or infinity) on the number of times item i can be selected:

$$\begin{aligned} &\max \sum_{i=1}^{n} p_i x_i \\ &s.t. \quad \sum_{i=1}^{n} c_i x_i \le C \\ &0 \le x_i \le u_i \end{aligned} \tag{2}$$

x_i integral for all i.

The **unbounded knapsack problem** (sometimes called the **integer knapsack problem**) does not put any upper bounds on the number of times an item may be selected:

$$\begin{aligned} &\max \sum_{i=1}^{n} p_i x_i \\ &s.t. \quad \sum_{i=1}^{n} c_i x_i \le C \\ &x_i \ge 0 \end{aligned} \tag{3}$$

x_i integral for all i.

The unbounded variant was shown to be NP-complete in 1975 by Lueker.

If the items are subdivided into *k* classes denoted N_i, and exactly one item must be taken from each class, we get the **multiple-choice knapsack problem**:

$$\begin{aligned} &\max \sum_{i=1}^{k} \sum_{j \in N_i} p_{ij} x_{ij} \\ &s.t. \quad \sum_{i=1}^{k} \sum_{j \in N_i} c_{ij} x_{ij} \le C \\ &\quad \sum_{j \in N_i} x_{ij} = 1 \qquad 1 \le i \le k \\ &\quad x_{ij} \in \{0,1\} \end{aligned} \tag{4}$$

If for each item the profits and weights are identical, we get the subset sum problem (often the corresponding decision problem is given instead):

$$\begin{aligned} &\max \sum_{i=1}^{n} p_i x_i \\ &s.t. \quad \sum_{i=1}^{n} p_i x_i \le C \\ &\quad x_i \in \{0,1\}, (i = 1,2,\cdots,n) \end{aligned} \tag{5}$$

If we have *n* items and *m* knapsacks with capacities C_i, we get the **multiple knapsack problem**:

$$\begin{aligned} &\max \sum_{i=1}^{m} \sum_{j=1_i}^{n} p_{ij} x_{ij} \\ &s.t. \quad \sum_{i=1}^{n} c_j x_{ij} \le C_i \qquad 1 \le i \le m \\ &\quad \sum_{i=1}^{m} x_{ij} \le 1 \qquad 1 \le j \le n \\ &\quad x_{ij} \in \{0,1\} \end{aligned} \tag{6}$$

As a special case of the multiple knapsack problem, when the profits are equal to weights and all bins have the same capacity, we can have **multiple subset sum problem**: **Quadratic knapsack problem**:

$$\begin{aligned} &\max \sum_{i=1}^{n} p_i x_i + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} p_{ij} x_i x_j \\ &s.t. \quad \sum_{i=1}^{n} c_i x_i \le C \\ &\quad x_i \in \{0,1\} \end{aligned} \tag{7}$$

If there is more than one constraint (for example, both a volume limit and a weight limit, where the volume and weight of each item are not related), we get the **multiply constrained knapsack problem**, **multi-dimensional knapsack problem**, or *m*-**dimensional knapsack problem**. (Note, "dimension" here does not refer to the shape of any items.) This has 0-1, bounded, and unbounded variants; the unbounded one is shown below.

$$\begin{aligned} &\max \sum_{i=1}^{n} p_i x_i \\ &s.t. \quad \sum_{j=1}^{n} c_{ij} x_j \le C_i \qquad 1 \le i \le m \\ &\quad x_i \ge 0 \qquad 1 \le i \le n \end{aligned} \tag{8}$$

x_i integral for all i.

If all the profits are 1, we can try to minimize the number of items which exactly fill the knapsack:

$$\begin{aligned} &\min \sum_{i=1}^{n} x_i \\ &s.t. \quad \sum_{i=1}^{n} c_i x_i = C \\ &\quad x_i \in \{0,1\}, (i = 1,2,\cdots,n) \end{aligned} \tag{9}$$

We call these problems Knapsack-like problems.

If we have a number of containers (of the same size), and we wish to pack all *n* items in as few containers as possible, we get the bin packing problem, which is modeled by having indicator variables $y_i = 1 \Leftrightarrow$ container *i* is being used:

$$\begin{aligned} &\min \sum_{i=1}^{n} y_i \\ &s.t. \quad \sum_{j=1}^{n} c_j x_{ij} \le C y_i \qquad 1 \le i \le n \\ &\quad \sum_{i=1}^{n} x_{ij} = 1 \qquad 1 \le j \le n \\ &\quad y_i \in \{0,1\} \qquad 1 \le i \le n \\ &\quad x_{ij} \in \{0,1\} \end{aligned} \tag{10}$$

The cutting stock problem is identical to the bin packing problem, but since practical instances usually have far fewer types of items, another formulation is often used. Item j is needed B_j times, each "pattern" of items which fit into a single knapsack have a variable, x_i (there are m patterns), and pattern i uses item j b_{ij} times:

$$\begin{aligned} &\min x\sum_{i=1}^{m} x_i \\ &s.t. \quad \sum_{i=1}^{m} b_{ij} x_i \le B_j \qquad 1 \le j \le n \\ &\sum_{i=1}^{n} x_{ij} = 1 \qquad 1 \le j \le n \\ &x_i \in \{0,1,\cdots,n\} \qquad 1 \le i \le m \end{aligned} \tag{11}$$

If, to the multiple choice knapsack problem, we add the constraint that each subset is of size n and remove the restriction on total weight, we get the assignment problem, which is also the problem of finding a maximal bipartite matching:

$$\begin{aligned} &\max \sum_{i=1}^{k} \sum_{j=1_i}^{n} p_{ij} x_{ij} \\ &s.t. \quad \sum_{i=1}^{n} x_{ij} = \le 1 \qquad 1 \le j \le n \\ &\sum_{j=1}^{n} x_{ij} = 1 \qquad 1 \le i \le n \\ &x_{ij} \in \{0,1\} \qquad 1 \le i \le k, j \in N_i \end{aligned} \tag{12}$$

In the Maximum Density Knapsack variant there is an initial weight c_0, and we maximize the density of selected of items which do not violate the capacity constraint:

$$\begin{aligned} &\max \frac{\sum_{i=1}^{n} p_i x_i}{c_0 + \sum_{i=1}^{n} c_i x_i} \\ &s.t. \quad \sum_{i=1}^{n} c_i x_i \le C \\ &x_i \in \{0,1\} \end{aligned} \tag{13}$$

III. Basic Estimation of Distribution Algorithms

Estimation of distribution algorithms (EDAs), sometimes called probabilistic model-building genetic algorithms (PMBGAs), are stochastic optimization methods that guide the search for the optimum by building and sampling explicit probabilistic models of promising candidate solutions[12]. Optimization is viewed as a series of incremental updates of a probabilistic model, starting with the model encoding the uniform distribution over admissible solutions and ending with the model that generates only the global optima [13].

EDAs belong to the class of evolutionary algorithms. The main difference between EDAs and most conventional evolutionary algorithms is that evolutionary algorithms generate new candidate solutions using an implicit distribution defined by one or more variation operators, whereas EDAs use an explicit probability distribution encoded by a Bayesian network, a multivariate normal distribution, or another model class. In EDAs the new population of individuals is generated without using neither crossover nor mutation operators. Instead, the new individuals are sampled starting from a probability distribution estimated from the database containing only selected individuals from the previous generation. Figure 1 illustrates the flowchart of EDA.

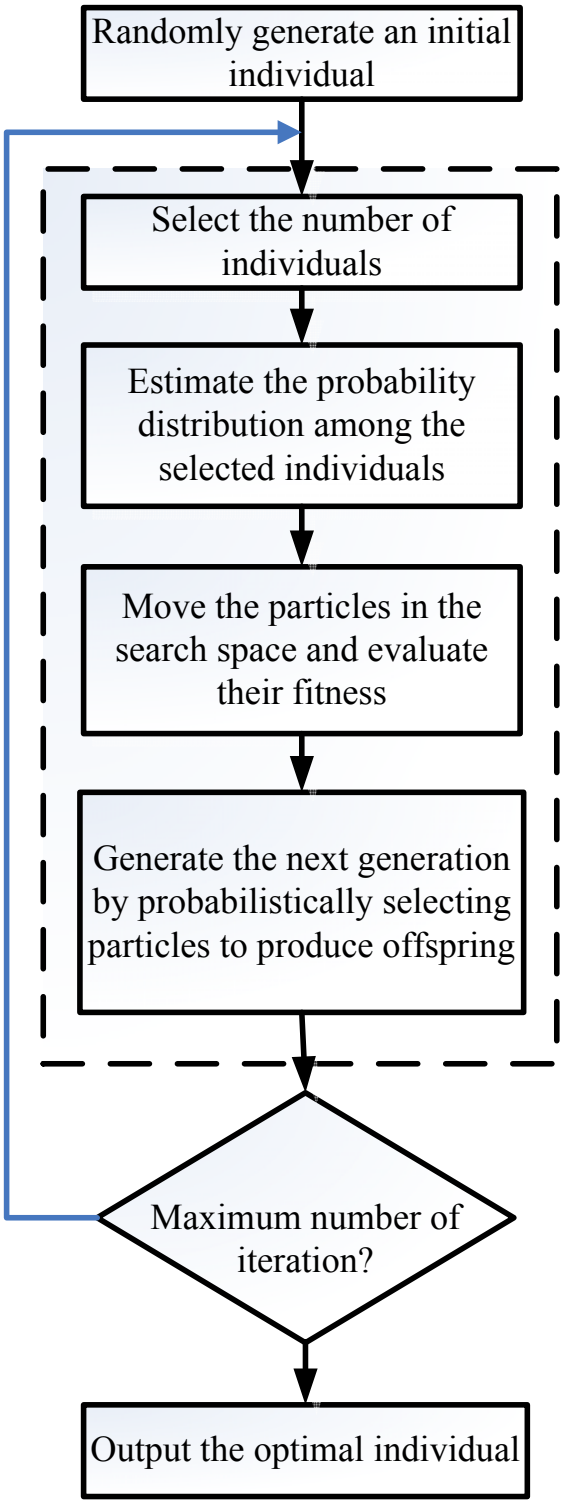


Figure 1. Illustrates the flowchart of EDA.

The general procedure of an EDA is outlined in the following[16]:

Step 1 t = 0;

Step 2 initialize model M(0) to represent uniform distribution over admissible solutions

Step 3 while (termination criteria not met)

Step 3.1 P = generate N>0 candidate solutions by sampling M(t)

Step 3.2 F = evaluate all candidate solutions in P

Step 3.3 M(t+1) = adjust_model(P,F,M(t))

Step 3.4 t = t + 1

Using explicit probabilistic models in optimization allowed EDAs to feasibly solve optimization problems that were notoriously difficult for most conventional evolutionary algorithms and traditional optimization techniques, such as problems with high levels of epistasis. Nonetheless, the advantage of EDAs is also that these algorithms provide an optimization practitioner with a series of probabilistic models that reveal a lot of information about the problem being solved. This information can in turn be used to design problem-specific neighborhood operators for local search, to bias future runs of EDAs on a similar problem, or to create an efficient computational model of the problem.

IV. Solving 0/1 Knapsack Problem by EDAs

Firstly, we transform (1)(constrained problem) into a single unconstrained problem.

$$\min f = -\sum_{i=1}^{n} p_i x_i + M\left\{\min\left\{0,\left[C-\sum_{i=1}^{n} c_i x_i\right]\right\}\right\}^2 \qquad (14)$$

where $M > 0$ is a large number.

The other knapsack problem models can also transform. For example, we transform (13)(constrained problem) into a single unconstrained problem.

$$\min f = -\frac{\sum_{i=1}^{n} p_i x_i}{c_0 + \sum_{i=1}^{n} c_i x_i} + M\left\{\min\left\{0,\left[C-\sum_{i=1}^{n} c_i x_i\right]\right\}\right\}^2 \qquad (15)$$

The estimation of distribution algorithms for 0/1knapsack problem is as follows:

Step 1 Using the uniform design technique, for each variable are the probability of random values within $(p_1, p_2, \cdots, p_n)^T = (0.5, 0.5, \cdots, 0.5)^T$. Generate N individuals constitute the initial population.

Step 2 Assess the fitness of all individuals in the initial population, and retain the best solution.

Step 3 Order the population by fitness in descending sorting, and choose the optimal m individuals (m ≤ N).

Step 4 Build a probability vector $(p_1, p_2, \cdots, p_n)^T$ based on the statistical information extracted from the selected m solutions in the current population.

Step 5 Sample N new solutions from this build probability models $(p_1, p_2, \cdots, p_n)^T$.

Step 6 If the given stopping condition (up to the required number of iterations nmax) is not met, go to step 2.

The estimation of distribution algorithms' time complexity is estimated as follows: The time to calculate the fitness operation is the longest, so the time complexity of algorithm is about $O(N.n_{max})$.

The estimation of distribution algorithms for other knapsack problem models is similar to above algorithm.

V. Numerical Example

We solve a typical knapsack problem of literature [9]. n = 10, C = 269 g, $\{p_1, p_2, \ldots, p_{10}\}=\{55,10,47,5,4,50,8,61,85,87\}$, and $\{c_1, c_2, \ldots, c_{10}\}=\{95,4,60,32,23,72,80,62,65,46\}$.

The program of EDAs is implemented by MATLAB. The MATLAB implementation is given below:

```
%EDA_Knapsack.m
%EDAs for Knapsack Problem
clear all
n=10;
p=[55 10 47 5 4 50 8 61 85 87]';
c=[95 4 60 32 23 72 80 62 65 46]';
G=269;
M=1;
N=1000;
m=0.4*N;
r=[0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5]';
for nn=1:20
   for j=1:N
      X(j,:)=Xrand(r,n);
   end
   for j=1:N
      fknapsack(j)=objknapsack(n,c,p,X(j,:),G,M);
      ffknapsack(j)=X(j,:)*p;
   end
   SX=X;
   SX(:,n+1)=fknapsack';
   B=sortrows(SX,n+1);
   fmin=B(1,n+1);
   xmin=B(1,1:n);
   for k=1:m
      SelectX(k,1:n)= B(k,1:n);
   end
   r=sum(SelectX)/m;
   for i=1:N
      if ffknapsack(i)>295
        ffknapsack(i)=0;
      end
   end
```

```
    opf(nn)=max(ffknapsack);
    meanf(nn)=mean(ffknapsack);
end
opf
meanf
plot(1:20,opf,'-.',1:20,meanf,'-')
legend('Best values','Average values');
xlabel('The time of iteration')
ylabel('The value of knapsack')
```

Xrand.m is is given below:

```
function y=Xrand(r,n)
for i=1:n
   if rand<=r(i)
      y(i)=1;
   else
      y(i)=0;
   end
end
```

Objknapsack.m is is given below:

```
function f=objknapsack(n,c,p,x,G,M)
f=-x*p+M*(min(0,G-x*c))^2;
```

When N = 100, m = 0.4 * N, the procession of value is shown in Figure 1. The main parameters affecting the performance of the EDA are the number N of the population and selected population number m.

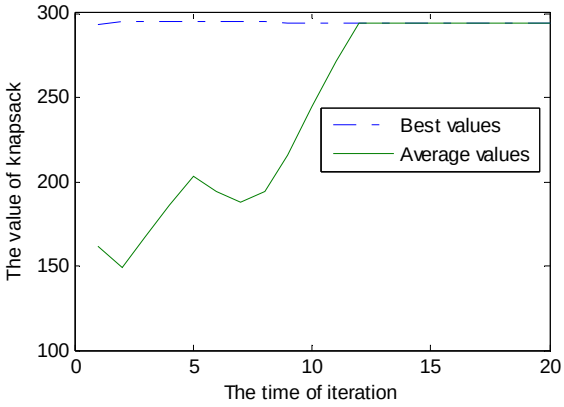


Figure 2. Figure2. The iterative process of the best values and the average values

When m=N/2, it test 100 times, and the statistics are shown in Table 1. When N = 100, sometimes the algorithm goes into the local optimal solution and not to reach the global optimum value 295, so we can't give statistics. Seen from Table 1, N is smaller, the effect is not good. N is greater, the effect is better. Of course, the greater the time is needed. We set N to moderate, such as N of 800.

TABLE I.
COMPARISON RESULTS OF N

N	Average number of iterations	Minimum number of iterations	Maximum number of iterations
100	-	-	-
200	3.3	1	10
300	2.82	1	6
400	2.53	1	6
500	2.13	1	5
600	1.99	1	5
700	1.71	1	5
800	1.69	1	5
900	1.59	1	4
1000	1.56	1	4

When N = 800, it test 100 times, and the statistics are shown in Table 2. From Table 2, if the ratio of m/N is the greater, the effect is the worse. Of course, the ratio m/N is too small, it is easy to fall into local minima. So the ratio of m/ N is 10% -30%, the results were quite good.

TABLE II.
COMPARISON RESULTS OF M/N

N	Average number of iterations	Minimum number of iterations	Maximum number of iterations
2.5%	—	—	—
5%	1.42	1	2
10%	1.37	1	2
20%	1.53	1	3
30%	1.56	1	3
40%	1.60	1	4
50%	1.69	1	5
60%	1.71	1	5

VI. CONCLUSIONS

The estimation of distribution algorithms can not only solve the knapsack problem, but also the algorithm can be applied for integer programming problem. Estimation of distribution algorithms can be slightly modified to solve similar nonlinear mixed integer programming problem. The estimation of distribution algorithms can be further improved, such as adding the crossover operators and mutation operators, so the performance may be better.

ACKNOWLEDGMENT

This work was supported by the Open Project Program of Key Laboratory of Intelligent Computing & Information Processing (Xiangtan University), Ministry of Education (No. 2011ICIP05), Artificial Intelligence of Key Laboratory of Sichuan Province(2012RYJ04), Jiangsu 333 Project , Qing Lan Project. and the National Natural Science Foundation of China under Grant 51008143.

REFERENCES

[1] J. Peters, L. Rudolph. Parallel Approximation Schemes for Subset Sum and Knapsack Problems. In 22nd Annual

Allerton Conference on Communication, Control and Computing, 1984, pp.671-680.
[2] P.S. Gopalakrishnan, I.V. Ramakrishnan, L.N. Kanal. Parallel Approximate Algorithms for the 0-1 Knapsack Problem. In Proceedings of the International Conference on Parallel Processing, 1986, pp 444-451.
[3] Guo-jie Li, Benjamin W.Wah. Systolic Processing for Dynamic Programming Problems. In Proceedings of the International Conference on Parallel Processing, 1985, pp.434-441.
[4] Richard J. Lipton, Daniel Lopresti. Delta Transformations to Simplify VLSI Processor Arrays for Serial Dynamic Programming. In Proceedings of the International Conference on Parallel Processing, 1986, pp.917-920.
[5] Andrew Chi-Chin Yao. On the Parallel Computation for the Knapsack Problem. In 13th Annual ACM Symposium on Theory of Computing, 1981, pp. 123-127.
[6] Wang Xiaodong. Algorithm design and analysis. Beijing: Electronic Industry Press,2001, pp.92-168.(In Chinese)
[7] Wang Ling. Intelligent optimization algorithm and its application, Beijing: Tsinghua University Press,2001:17-59. (In Chinese)
[8] Jin huimin,Ma Liang. Genetic annealing evolutionary algorithm applied to the knapsack problem. Journal of University Of Shanghai for Science And Technology, 2004, vol.26, no.6, pp.561-564. (In Chinese)
[9] Ma Liang,Wang Longde. Ant optimization algorithm for knapsack problem, Computer Applications . 2001, 21(8), pp. 4-5. (In Chinese)
[10] Yu Yongxin,Zhang Xinrong. Optimization algorithm for multiple-choice knapsack problem based on ant colony system. Computer engineering, 2003, 29(20), pp.75-76, 84. (In Chinese)
[11] Gao Shang, Yang Jingyu. Solving Knapsack Problem by Hybrid Particle Swarm Optimization Algorithm. Engineering science,2006,.8(11), pp. 94-98. (In Chinese)
[12] Ye Lian, Zhang Min. Solution to the 0-1 knapsack problem based on DNA encoding and computing method. Journal of Computers, 2013, 8(3), p 669-675.
[13] Tan Yan-Yan, Jiao Yong-Chang. MOEA/D with uniform design for solving multiobjective knapsack problems. Journal of Computers, 2013, 8(2),pp.302-307.
[14] Shumeet Baluja. Population based incremental learning: A method for integrating genetic search based function optimization and competitive learning. Technical Report, No. CMU-CS-94-163, Carnegie Mellon University, Pittsburgh, Pennsylvania, 1994.
[15] Zhou shude, Sun zengqi. A Survey on Estimation of Distribution Algorithm. Acta Automatica Ainica, 2007,33(2), pp.113-124. (In Chinese)
[16] H. Muhliebe, G. Paass. From recombination of genes to the estimation of distributions I. binary parameters. In Lecture notes in computer science. Berlin, Germany: Springer Verlag, 1996 ,vol.1141, pp.178-187.
[17] M. Pelikan, D. E. Godberg, E. C. Paz. Linkage problem, distribution estimation, and Bayesian networks. Evolutionary Computation. 2000, 8(3), pp.311-340.
[18] T K Paul, H. Iba. Linear and combinatorial optimizations by estimation of distribution algorithms. In 9th MPS Symposium on Evolutionary Computation, IPSJ, Japan, 2002.
[19] Haina Rong, Yuquan Li. A Novel Estimation of Distribution Algorithm with Multiple Probability Models. AISS: Advances in Information Sciences and Service Sciences, 4(17), pp. 308- 315, 2012.
[20] Guolin Yu. Multi-objective estimation of Estimation of Distribution Algorithm based on the Simulated binary Crossover. JCIT: Journal of Convergence Information Technology, 7(3), pp. 110-116, 2012.
[21] Rui Zhang. A Rule-Based Estimation of Distribution Algorithm for Solving Job Shop. JCIT: Journal of Convergence Information Technology, 6(8), pp. 220-227, 2011.
[22] Rong Haina, Cheng Jixiang, Li Yuquan. Radar emitter signal analysis with estimation of distribution algorithms. Journal of Networks, 2013, 8(1), p 108-115.

Shang Gao was born in 1972, and received his M.S. degree in 1996 and Ph.D degree in 2006. He now works in school of computer science and technology, Jiangsu University of Science and Technology. He is a professor and He is engage mainly in systems engineering and soft computing.

Ling Qiu was born in 1980, and received his M.S. degree in mathematics in 2008. She now works in Artificial Intelligence of Key Laboratory of Sichuan Province, Sichuan University of Science and Engineering. She is engage mainly in soft computing.

Cungen Cao was born in 1964, and received his M.S. degree in 1989 and Ph.D. degree in 1993 both in mathematics from the Institute of Mathematics, the Chinese Academy of Sciences. Now he is a professor of the Institute of Computing Technology, the Chinese Academy of Sciences. His research area is large scale knowledge processing.

A Framework to Assess Legacy Software Systems

Basem Y. Alkazemi
Department of Computer Science, Umm Al-Qura University, Makkah, Saudi Arabia
Email: bykazemi@uqu.edu.sa

***Abstract*—Enterprise organizations require flexible software systems that can handle emerging market needs from time to time, chiefly to ensure the organization has a competitive edge in the market. On the other hand, several organizations still possess legacy software systems, which have definite functionalities but may limit their development progress to comply with emerging e-business needs. Off-the-shelf systems might be one possible option if a decision for replacement is made. Equally, improving the architecture of a legacy system can be a valid option to consider as well. The decision on which approach to follow when dealing with a legacy software system must be made based on a thorough investigation of the nature of the system. This paper develops a conceptual framework to analyse legacy software systems in order to support CEOs in making informed decisions about the appropriate approaches to follow in order to keep their organizations functional and competitive.**

***Index Terms*—legacy system, software architecture, decision making**

I. Introduction

Legacy software systems still represent valuable assets to many organizations, even with the pioneering of new technologies and wisdom. One of the main aspects that forces an organization to maintain its legacy system in business is the highly customized functionality provided by the system, which cannot be easily implemented in many brand-new enterprise solutions. However, such reluctance to put new systems in place might negatively affect the evolution of the organization in terms of its compliance with the latest business needs (e.g. e-commerce models). Therefore, CEOs must be able to make informed decisions on how their organizations can proceed towards satisfying new business requirements. This paper presents our analysis of the Student Information System (SIS) at Umm Al-Qura University (UQU) [1] in order to identify its appropriateness to stay in business and to subsequently help the CEOs at UQU to make a decision about the most suitable strategy to follow in order to keep the organization functional in a business context.

The remainder of this paper is organized as follows: section 2 describes the key background work in the field of assessing legacy systems. Section 3 presents the proposed framework for assessing legacy systems. Section 4 describes the case study with which we conducted the experimentations. Section 5 presents the application of our framework to assess the legacy system we selected as the case study. A discussion about the results obtained from analysing the legacy system and the implications of these results are given in section 6. Finally, section 7 presents the conclusions of the paper and suggests avenues for future work.

II. Background Work

The term "legacy system" in this paper refers to a running system that still meets a considerable percentage of an organization's business needs in terms of functional aspects but does not comply with emerging architectural standards. Although this view might somewhat differ from common definitions in the literature, such as that of McGee [2], our definition considers more specifically the architectural aspects of the legacy system, in addition to other factors such as support, functionality, and technology. Based on the architectural style adopted by an organization, we can classify the system in terms of whether it is a legacy system or not regardless of the functional aspects, as we assume that all systems available in an organization are being utilized; otherwise, they would be shut down. For example, desktop applications that are based on a client–server architectural pattern can be considered legacy systems if they are still in use among large enterprise organizations such as universities. The reason for this is that client–server solutions have many limitations with respect to extensibility and the adaptation of new emerging e-business requirements. Thus, a system can be considered a legacy system in one context but not in another smaller one (e.g. for student projects).

Summerville [4] identifies two main dimensions for assessing legacy systems, namely environment and application. Environment assessment is concerned with certain vendor- and technology-related aspects. Application assessment, however, examines the internal non-functional attributes of the system itself. A more refined version of this assessment framework is proposed by Ransom et al. [5], who consider the technical, business, and organizational infrastructure aspects of the system. Grace et al. [6] established the SMART methodology for analysing legacy software systems in order to migrate to an SOA-compatible [6] environment. Their analysis is mainly concerned with identifying potential business logics from legacy systems in order to refactor and expose these as service components. Seacord et al. [7] identified three main dimensions for assessing legacy systems, namely technical, programmatical, and organizational considerations, which must be thoroughly

doi:10.4304/jsw.9.1.111-115

investigated before modernizing any legacy system. Bennett et al. [8] established a two-phased decision model for assisting organizations in making informed decisions about their legacy systems. Their model is concerned with the business strategy and the technical aspects of the legacy system.

We observe that the above-described work focuses mainly on the business aspects of legacy systems in order to support CEOs in making informed decisions on whether to replace the entire system with a brand new one or to keep the legacy system functional and maintain it over time. However, none of the extant research describes an assessment for the purpose of re-architecting an organization's legacy system, as described in our prior work [9], apart from the work by Grace et al. [6], who identified the requirements to migrate into an SOA-compatible environment. Thus, the aim of this work is to assess legacy systems from the perspective of modifying their architectural styles to comply with new ones that can easily accommodate newly emerging e-business needs. Our assessment is built on combining the previous work described above and considering the key factors of it as a baseline with some modifications to fit the context of our study.

III. Assessment Framework

Generally, there are four conceptual strategies that might be followed to identify the most appropriate solution for systems evolutions, including:

- Replacing the legacy system with a new enterprise solution;
- Maintaining the legacy system in order to proceed with the organization's business with limited evolution;
- Re-architecting the legacy system to comply with modern architectural styles, while keeping the functionality untouched; and
- Extending the legacy system by wrapping it as a black box and exposing its standard interfaces to interact with new systems.

Each one of these strategies incurs some limitations and possibly a number of benefits, if implemented carefully. However, the decision to proceed with one strategy or another is relatively challenging and requires thorough investigation of the business value and the quality of the legacy system at hand. We identify a number of dimensions for this assessment, as follows:

- **Support:** This dimension is concerned with the hardware and software support provided to the legacy system. In addition, this dimension examines the availability of source code and the team that supports it.
- **Business:** The business requirement is the key aspect by which an organization can decide whether a system should be kept functional, replaced with a new system that satisfies their needs, or simply shut down completely. Therefore, this dimension covers the requirements of an organization in addition to the modelling technique used and the documentation of the business in the legacy system.
- **Architecture:** The building blocks of the system are defined in this dimension through the style used in the legacy system and the integration pattern between the different entities of that system and with external systems. It also relates to the way in which the functionality can be consumed by clients.
- **Technology:** This dimension discusses the type of technology adopted by the legacy system and whether the technology is still appropriate or not compared to emerging business needs.

This framework is abstract in nature and therefore is not exhaustive. However, it can be utilized as the basis for analysing the underlying environment of an organization, as will be seen in section 5.

IV. Case Study

UQU is a typical Saudi organization in that it runs a legacy system and thus is in need of an urgent update. UQU was therefore selected as the case study for the proposed model with the purpose of creating a fully integrated environment that supports e-government business. The institution needs a fundamental solution to cope with the changing environment without interrupting the routine working activities. Funding is also a major consideration that influences any decision regarding major development plans.

From a historical perspective, UQU launched its information systems in early 2001 to serve around 3,600 employees and just over 40,000 students. The system runs an outdated code procedure based on Oracle 6i for forms and reports, which are built entirely on a client–server pattern [3]. The major in-house subsidiaries include Enterprise Resource Planning (ERP), Student Information System (SIS), Library Information System (LIS), and Healthcare Information System (HIS). Twelve years later, the system has started to struggle with the new environment because of an increase in the number of users and the pressure to support e-government models. Today, the system serves around 75,000 students and more than 7,000 employees: an almost two-fold increase compared to 2001, although there have been only minor changes to the original core functionality. Moreover, outmoded software systems lack many capabilities that are, these days, considered core requirements, including compatibility with different environments (e.g. mobile devices) and other services provided to students and faculty members in the university. Additionally, due to the emerging e-government movements in Saudi Arabia, organizations need to apply major changes to their core systems in order to accommodate new requirements. One such requirement is process automation, which solely requires the splitting of the functional aspects of an application from the business aspects.

V. Assessment of Legacy System in UQU

We utilized the framework described earlier to assess SIS at UQU in order to build a conceptual understanding of the current state of that system. The different dimensions, together with their corresponding factors and the status of SIS at UQU, are described in Table I.

It is apparent from table I that UQU does not have many problems with the current support provided to their SIS, as its servers are up to date and the source code is completely owned and managed by the UQU team in the IT deanship. With respect to business, it seems that SIS is currently used by the university and hence constitutes part of their active systems. This is why the system is highly necessary for the university, even though it may lack some functionality that seems to be available in a number of competitive solutions in the market. However, the availability of a dedicated IT team does help in terms of adding extra functionality as per the emerging functional requirements of the business owner, and this seems to be a great advantage to the university in a business sense. We can identify a slight concern with respect to the modelling and documentation of the SIS business logic, which seem to be lacking at the moment. When we investigated this further, we observed that the system is dependent mainly on personnel who are working in the environment, including the business owner and senior developers. This might represent a real threat to the university business, as it could suspend the operational continuity of the system in the case of unforeseen circumstances.

Regarding architecture, the system complies with a client–server architectural pattern that we believe is somewhat outdated. Thus, extending the university business to satisfy some of the emerging e-business requirements might be very minimal. Our deep analysis of the current environment has identified that SIS is split into a front end, which is available on the web, and a back end. The front end is programmed purely in Java Server Faces (JSF), which can be considered a fairly modern technology. However, the current building blocks of JSF applications built for UQU are based mainly on object, rather than web-service, interaction. This might limit any potential utilization by different types of environments (e.g. mobile phone applications), as all objects need to be exposed as services beforehand. The back-end system, on the other hand, seems to be very old as it is programmed using Oracle 6i for forms and reports. One common problem in the current back-end system that may hinder its potential extendibility is that business logics are embedded inside Oracle forms. Hence, no application-to-application interaction is possible at the moment without embedding glue code inside the corresponding forms. With respect to data integration, it seems that UQU owns a unified database for most of its applications. However, we observed minor cases where the same data were presented differently on different screens, which can indicate the unnecessary availability of redundant data sources.

Moreover, report generation is a very time-consuming task as it requires manual intervention for creating views and queries. We observed that a considerable amount of IT time is consumed in responding to daily requests for reports due to the lack of a sophisticated tool that end users can utilize for report generation.

TABLE I.
Assessment dimensions of SIS legacy system

Dimension	Factors	Status at UQU
Support	Hardware	Virtual servers supported by CISCO
	Application server	Web-logic currently supported by Oracle
	Source code	Source code fully owned by UQU IT development team
	Database	Currently fully supported by Oracle
Business	Validity	SIS currently represents the core business of UQU
	Modeling	No business modeling technique used at the moment
	Documentation	No documentation of the business – just high-level descriptions of some aspects.
Architecture	Application integration	Ad-hoc interaction between applications using mainly glue-code
	Consumption	- Web application for users (e.g. students, faculties). - Desktop application on 6i forms for business owner
	Extensibility	The system cannot be extended by adding plug-ins to it. Extension must be done in the core functional classes.
	Interoperability	Conducted at the DB level through procures calls and triggers
	Data integration	Currently no data-centralized warehouse, and reports are generated manually by writing queries
	Style	Client-Server
Technology	Vendor	Oracle
	Version	Varies according to layers: - Database: Oracle 11g - Backend: Oracle 6i - Frontend: JSF 2.0
	License	Yearly Subscription for support only
	Data center	Good support for virtualization

From a technology point of view, UQU seems to be in good shape as it currently has many modern environments, such as Oracle 11g for databases and JSF 2.0. However, its back-end systems technology is almost obsolete and may shortly lose support from Oracle. Licences do not seem to be an issue as the IT department only pays yearly subscription fees for support during high-traffic seasons such as registration and admission. Apart from this, no other licences are paid as SIS is completely owned by the university. All the applications in the university are hosted in a centralized data centre that fully supports virtualization.

VI. Discussion

Based on the analysis described in the previous section, we have identified some strong points and weaknesses that the CEO must be aware of in order to make a decision regarding the system. The system's strong points can be summarized as follows:

- The current SIS satisfies most of the functional requirements of the UQU business owner, and the system is used frequently and effectively during the academic year.
- UQU currently has full control over the system. It can add new features or even disable unnecessary ones without the need to report back to any vendor.
- The UQU team fully understands the business logic of the system and can deal with any business-related modifications required by the business owner. Moreover, the team is skilled enough to modify and build new features smoothly.
- UQU owns a state-of-the-art environment in which to host different applications. Moreover, the current SIS complies with the new application of the server's technologies, as the university is using a WebLogic application server at the moment.
- The database technology is up to date and fully supported by Oracle.
- No costly licences need to be paid by UQU, as the system is fully owned by the university.

On the other hand, weaknesses in the current SIS environment are derived mainly from shortcomings in the overall environment with respect to emerging e-business needs, as described in [9]. We observed that these characteristics might significantly influence the CEO's decisions. The weaknesses can be summarized as follows:

- There is a lack of web-service capabilities for the back-end systems.
- The look and feel of the system is somewhat basic, as Oracle 6i forms do not support user-friendly interfaces.
- Report generation is difficult and time consuming as it involves specifically requesting that the IT department generates a report, due to the lack of tools and environments to support report generation. Consequently, some of the university's business processes might be negatively affected by this delay.
- The functional screens are not integrated properly into the workflow of the business process.
- The architectural style that is used by the university is somewhat out of date, and this type of client–server style is only normally used nowadays in small organizations. Currently, most of the enterprise solutions on the market have moved towards service-based architecture such as SOA [10] in order to ensure that their environments are extensible to accommodate future development; thus, UQU seems to be lagging behind in this dimension.
- Business logic is embedded inside Oracle forms. This can hinder flexible integration patterns with other applications or environments. Moreover, extending functionality might be an extremely time-consuming task, as the entire application must be put offline for full recompilation.

We used a simplified version of the weighted decision-making grid (WDMG) to help derive a more accurate decision in light of the strong and weak points identified. The weights given for each dimension were generated based on the importance of that dimension to stakeholders, including the business owner (with a 40% overall score weight), the IT team (with 35%), the university administration team (with 15%), and key users (with 10%). Table II lists the different dimensions and their assigned weights, out of 5, for each aspect.

TABLE II.
Weighted Decision-Making Grid

Pros	Score	Cons	Score
System functionality	5	Lack of web-services	3
Modification delivery time	5	Usability problems	3
Team support	4	Report generation	3
Technical Requirements	2	Architectural Style	2
DB technology	3	Oracle 6i problems	3
License	3	Business process problem	5
Overall	**22**		**19**

The table shows that the advantages of the current system outweigh its potential disadvantages by about 3. There is an interesting trade-off between "system functionality" and "business process problem", as both recorded a score of 5. The former is concerned with the basic functionality that the system can provide in terms of screens, while the latter relates to placing a functional screen into context via a pre-defined workflow. Both dimensions are significant and complement each other. However, we believe that the implementation of functionality is a prerequisite for implementing workflows. Thus, satisfying functional requirements is more significant at this stage than integrating applications with workflows, as the integration is currently done at the

database level and seems sufficient to fulfil UQU requirements during high seasons.

In general, although the difference in the overall scores seems tiny, the advantages have more weight. This might give a good indication that the current system should be kept in business and that the CEO needs to start a number of projects to address the disadvantages of the system. In doing this, UQU would be able to obtain not only a fully functional system but also an enterprise environment that can accommodate emerging business needs.

VII. Conclusion and Future Work

This paper has described our research work and experimentation for evaluating the legacy system at UQU. The key outcomes of this study should be useful to help the CEO of the university to make an informed decision about the ability of the current SIS to serve its mission and subsequent objectives. The provisional evaluation of SIS at UQU was in favour of re-architecting the system rather than replacing it with a brand new one. The next step in this work is to investigate a possible model for modifying legacy systems in order to comply with emerging architectural standards. As such, a study could be utilized to build a more solid plan for the actions to be taken in the development of SIS at the university.

Acknowledgment

The author wishes to thank the IT deanship at Umm Al-Qura University (UQU) for supporting part of this research and helping to provide necessary information to conduct the field study.

References

[1] Umm Al-Qura University, http://www.uqu.edu.sa [Accessed 5 Oct 2012].
[2] J. McGee, "Legacy Systems: Why History Matters", *Enterprise Systems Journal*, Dec 2005.
[3] L. Bass, P. Clements, and R. Kazma, *Software Architecture in Practice*, 3rd Edition, SEI Series in Software Engineering, 2012.
[4] I. Summerville, *Software Engineering*, 2010.
[5] J. Ransom, I. Sommerville, and I. Warren, "A Method for Assessing Legacy Systems for Evolution", *IEEE Proceedings of the Second Euromicro Conference on Software Maintenance and Reengineering*. March 8–11, 1998.
[6] L. Grace, M. Edwin, S. Dennis, and S. Soumya, *SMART: Analyzing the Reuse Potential of Legacy Components in a Service-Oriented Architecture Environment (CMU/SEI-2008-TN-008).* Software Engineering Institute, Carnegie Mellon University, 2008.
[7] R.C. Seacord, D. Plakosh, and G.A. Lewis, *Modernizing Legacy Systems.* Boston, MA. Addison-Wesley, 2003.
[8] K. H. Bennett, M. Ramage, and M. Munro, "Decision model for legacy systems", *IEE Proceedings – Software* 146(3): 153–159, 1999.
[9] B. Alkazemi, A. Baz, and G. Grami. "Toward an Architectural Model to Facilitate Adopting E-Government Business Model", *Proceedings of the 3rd International Conference on e-business*, Hong Kong, 2012.
[10] T. Erl. *Service-Oriented Architecture: Concepts, Technology, and Design*. Prentice Hall, 2005.

Dr **Basem Y. Alkezemi** is the currently holding the position of vice-dean of Umm Al-Qura University's IT Deanship for E-Government. He received his Bachelor degree in Electric and Computer Engineering in 1999. He then went to study his MSc and PhD in Software Engineering at Newcastle University in the UK which he received in 2004 and 2009 respectively. Dr. Alkazemi has published a number of articles in regional and international journals and participated in many specialized conferences around the world. His main research interests are in software engineering, wireless sensor networks, computer supported education, and e-government.

Research on the Open Source GIS Development Oriented to Marine Oil Spill Application

Ruifu Wang
Geomatics College, ShanDong University of Science and Technology, Qingdao 266510, China
Key Laboratory of Surveying and Mapping Technology on Island and Reef, SBSM, China;
Email: wangruifu@263.net

Nannan Liu, Maojing Xu and Xiangchao Kong
Geomatics College, ShanDong University of Science and Technology, Qingdao, China
Email: {liunannan_89@126.com, xumaojing0417@163.com, kongxiangchao9913@163.com}

***Abstract*—With the frequent occurrence of marine oil spill and the serious environmental pollution as well as enormous economic losses it causes, there is a growing demand for oil spill emergency response. It becomes a trend to research on spatial information analysis and publishing based on GIS. Compared with the expensive and system-huge commercial software, open source platform which is free and small-scale is becoming a new choice. This article develops the marine oil spill monitoring information analysis & publishing system based on DotSpatial, the upgrade version of the open-source .NET development of component library. In this system, the monitoring information of oil spill is visualized, rendered, analyzed and finally published on the web. However open source GIS is functionally limited and instable. DotSpatial can not read the spatial information of RS images well and the mapping module is unstable. This article solves some technical problems. For example, the spatial data is processed such as re-projected via GDAL to match the images layers with the vector layers. Vector oil spots data is generated and rendered, and the major axis and minor axis are drawn. Moreover the map extent to output can be determined by dragging a rectangle using GDI+, and the decorating of the map to putout is also improved. By adopting several developing methods comprehensively, this paper researches on the marine oil spill application oriented system development based on open source GIS. It provides references for other similar system researches and developments of spatial information expression and analysis.**

***Index Terms*—open source, GIS, oil spill, DotSpatial, monitoring information**

I. INTRODUCTION

A. Background

Marine oil spill occurs frequently in recent years, and it leads to serious pollution and enormous economic losses. After the outbreak of the disaster, the managers and the public should be informed of the degree and the extent of the disaster, so it's very important to publish the monitoring information and the spatial statistical result regularly and timely[1][2][3][4]. GIS is powerful in spatial analysis, it's often applied to the statistics of disaster distribution, area and some other spatial information.

GIS was being applied widely to various fields since it came into being in the 1960s. The commercial software which meets the demand of every industry is comprehensive in function and high in price. So it's not suitable for those functional single GIS applications.

It's just a little part of GIS to analyze and publish the oil spill monitoring information, and the commercial software cost much additionally. It's a new trend to develop systems based on the platform of open source GIS. Open source GIS means that the developers can release the source codes of the software according to some protocol, and also allow others to download, modify, apply, and release the codes on the premise of following the protocol [5]. It's best characterized as being free, but not so powerful in functions.

We use the platform of MapWinGIS/DotSpatial, the open source development component library, to develop our marine oil spill monitoring system.

This paper explores the oil information analysis and publishing system based on open source GIS, gives the corresponding solutions to some problems of open source GIS software.

B. Previous Related Work

With the development of GIS, more and more scholars and related researchers around the world choose GIS as the platform for marine environmental monitoring and emergency response. GIS does well in spatial visualization, spatial analysis and statistical mapping. It provides real-time information for decision-aid in marine accident response.

Yancheng Liu from Dalian Maritime University in China established the mathematical models of marine spilled-oil's transportation, spreading, evaporating and

Corresponding author: Nannan Liu.
This work was supported by the Public Science and Technology Research Funds Project of Ocean (No. 201205010-4).
An earlier version of this paper was presented at the 21st International Conference on Geoinformatics.

doi:10.4304/jsw.9.1.116-120

emulsification processes aimed at problems of marine oil spill crisis response. It can be the scientific bases of oil spill response decision making [6]. Long Ye from Shanghai Maritime University in China developed the system of contingency resource allocation and transport for dealing with the oil spilling accidents at sea, to research on the integration of the contingency plan and the resource allocation and transport [7].

In addition, a great number of researchers around the world reply RS technology together with GIS to the marine oil spill accidents, for example, to monitor, analyze and map the oil spill extent and its moving trend.

Our maritime workers have begun to utilize RS technology to monitor oil spill. Professor Ying Li monitored the oil spill occurred in Mexico based on a series remote sensing images and GIS technology. It's very helpful in cleaning and controlling the oil slicks [8]. Lei Bing, the engineer from Yantai oil spill response technical center of China maritime safety administration, developed a satellite remote sensing system for maritime application based on the integration of RS and GIS [9]. In Canada, H. Assilzadeh & Y. Gao from Department of Geomatics Engineering Schulich School of Engineering, the University of Calgary presented a method using SAR image and GIS technology applications for oil spill management in coastal area in their paper, mainly including extracting coastal oil-spilling information, predicting the movement and creating map products from various analysis aspects [10]. Mira MOROVIC from Croatia and Andrei IVANOV from Russian said that SAR together with GIS can significantly improve identification and classification of oil spills. Their method is used to product oil spill distribution maps [11].

Being aware of the advantages of open source platform, more and more people began to research on marine GIS based on it. Xiantao Li from Zhejiang University in China put forward a network three-dimensional visualization system of marine information under the open source stack [12]. Ei Fujioka et al. work on advancing global marine biogeography research with open-source GIS software and cloud computing [13]. However, it's hard to find researches on marine oil spill with open source GIS.

II. Application Analysis

This article aims at researching on the visualization, statistics and publishing of the oil spilling monitoring information based on open source GIS. MapWinGIS/DotSpatial is adopted as the development platform, with GDAL as a complement.

A. Development Mode

MapWinGIS is an open source component which is suitable for small and medium GIS applications. The core is an ActiveX control named MapWinGIS, based on which the developers can add GIS features into their own systems [14]. As the upgrade version of MapWinGIS, DotSpatial is more powerful. It can support more development environment.

GDAL (Geospatial Data Abstraction Library) is an open source library for reading, transforming, and editing the raster spatial data [17]. Many open source software and even commercial software are based on it. It has its own data models and APIs, and provides a series of command lines to process data.

B. Research Contents

The function of our system includes map viewing, data displaying, rendering, statistic, mapping, bulletins release and some other modules. The core is data display, rendering and mapping.

DotSpatial supports raster data differently from vector data when they are added into the map. Reprojection and some other data processes should be done in order to display them and match them well with each other. In our system, vector oil spots data is transformed from the raster monitoring data, then it's rendered, numbered, and major axis and minor axis of every spot are drawn. These can help show the disaster and its development trend clearly. For mapping the oil's spilling extent with other related information, users drag a rectangle to define the extent. Then the result bulletin is published as a web page. Figure 1 shows the scheme of the system.

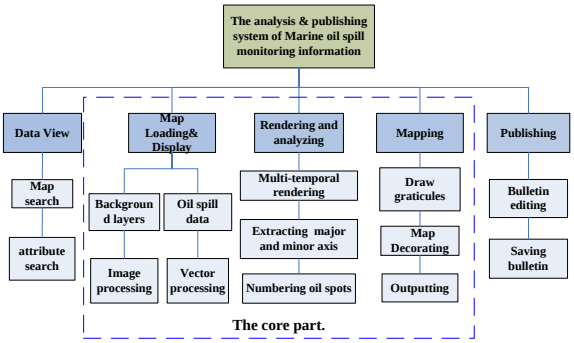


Figure 1. The system scheme.

III. Key Problems and Technologies

While developing the analysis & publishing system of marine oil spill monitoring information, there exist several problems in spatial data matching, data transforming, vector data rendering, mapping and outputting and webpage designing and making etc. This article gives the corresponding solutions to some of them.

A. Data Display and Manipulation

DotSpatial does well in manipulating vector data, but weak in manipulating raster data. For example, the data size should be limited below 40M, as larger images can not be added into the map. DotSpatial can not read the coordinate system information of raster data well, because it can only read the coordinate system of proj4, and it's always different from that of the vector data.

Moreover, DotSpatial can not stretch the image added

into the map automatically, thus the image can not reflect the differences between grids if the spatial distribution of the grid values is irregular.

The data used in this paper is an ENVISAT SAR image, and its size is always over 100M. So we use GDAL to resample, reproject, and stretch it before adding it into the system. The file size is reduced to less than 40M by resampling. To match the SAR image with the vector map layers, the projection is implemented by GDALWARP, an API of GDAL for image transformation. Pixel value is stretched to statistic the value distribution. To enhance the visual effect, the pixel value is converted to a grey range of 0~255 in this system.

B. Vector Information Extraction and Rendering

For the oil spill analysis, some responding algorithms are designed to extract the spatial structure of the oil spots, compute the attributes and render the multi-temporal data.

IV Extraction of Oil Spots Spatial Structure

The spreading trend of oil spots can be found in its shape. But the shape of every spot is always irregular. In order to show the movement and the change of every oil spot in long time series, the area, center point coordinate, major axis and minor axis and their breakpoint coordinates .etc should be calculated to represent the spatial structure.

The oil data transformed from RS image is raster data, which is unfit for spatial structure information statistic. So we transform it into vector data that is good at representing the spatial structure of every spot. DotSpatial does not have this function, so we use GDAL to transform the oil-spilling extents in the SAR image into polygon features.

The major axis of an oil spot is the line segment between two nodes which is the most distant from each other in the polygon boundary. The minor axis is the line segment perpendicular to the major axis and clipped by the polygon boundary. The mutually perpendicular major axis and minor axis together build the basic skeleton of an oil spot (Fig 2, Fig 3)

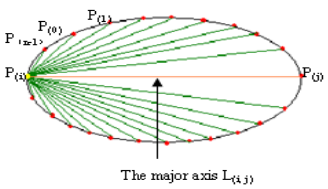


Figure 2. The major axis.

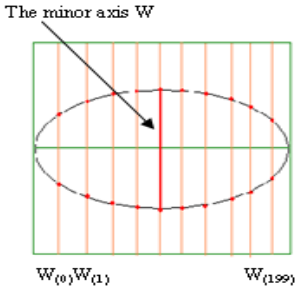


Figure 3. The minor axis.

Suppose the number of the nods of an oil spot is *n* ($P_{(0)}$, $P_{(1)}$,⋯,$P_{(n-1)}$). Link every nod with every other nod, we can get the line segments as follows:

$$L_{(0,1)} \quad L_{(0,2)} \quad L_{(0,3)} \quad L_{(0,4)} \quad \cdots \quad L_{(0,n-1)}$$
$$L_{(1,2)} \quad L_{(1,3)} \quad L_{(1,4)} \quad \cdots \quad L_{(1,n-1)}$$
$$\cdots$$
$$L_{(n-2,n-1)}$$

Suppose the longest one is the line between P (i) and P (j), then L (i, j) is the major axis (L) of the spot. Divide the major axis line into 200 equal parts, and draw the line segments perpendicular to the major axis at every dividing point and clipped by the polygon boundary. There may be more than two intersection points of every line segment and the polygon boundary due to the irregular shape of the polygon. In this case we draw the line between the farthest two points. At last, we choose the longest one from the 200 line segments as the minor axis of the oil spot (W).

V Multi-temporal Rendering

Multi-temporal data reflects the characteristic of the data in time series. The oil spots in the sea are always moving and changing influenced by wave, wind and some other factors. It's important for disaster managers to grasp the moving and changing trend of them. For this reason the oil spots need to be multi-temporal rendered. As the spots interpreted and transformed from RS images have differences in confidence due to several reasons, we should express the differences at the same time.

DotSpatial does not have the function of multi-temporal rendering. A rendering scheme is given in this paper which combines color filling and pattern filling to render the spots. Oil spots at different dates are filled with different colors and different patterns to distinguish each level of confidence. There are four levels of confidence including high, medium, low and non-confidence in this paper. We mark them respectively with vertical, backward-diagonal, horizontal, and point styles(Fig. 4).

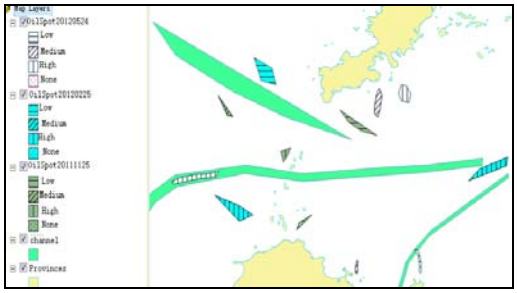


Figure 4. The result of multi-temporal rendering.

VI. THEMATIC MAPPING

The mapping module of DotSpatial provides a series of controls and APIs, such as LayoutInsertToolStrip, LayoutDocToolStrip and LayoutMapToolStrip etc. But it's still insufficient due to its instability and the spatial needs in this paper. For example, it can not draw the graticules, the scale bar and the legend controls do not work some times, and it does not allow user to specify a range by dragging the mouse etc.

Following the basic rules of mapping and decorating [18], mapping the monitoring information of oil spill is improved based on DotSpatial and Windows GDI+. Through Windows GDI+, the users can use the mouse to drag a rectangle as the output extent. The system draws the graticules by calculating the coordinate values and then drawing line elements together with text elements as labels. While decorating the map after determining the output extent, the scale bar and the legend controls of DotSpatial do not work due to the instability of open source platform. Therefore we group different elements to fabricate the scale bar and legend for our own needs. This program not only compensates for the controls of DotSpatial, but also makes the map rich and varied.

VII. CONCLUSION

This article explores the marine oil spill application oriented system development based on open source GIS. The system realizes data matching and displaying, information abstraction, rendering and attributes calculation, the information mapping and result publishing etc. Because of the imperfection of the open source platform, there exist several problems and difficulties during the development. So we make changes and innovations in the development idea, which combine multiple development platforms and technologies such as GDAL and GDI+, to compensate the imperfect open source GIS. This research may be useful to other similar researches and developments based on open source GIS.

With the increasing popularization of the open source technology characterized by being free, it is becoming a favorable way to analyze and distribute the spatial information. However the open source GIS software is still incomplete in function. If it can get more supervision and controls while distributed to the market, it will be a convenient and economical choice in the development of spatial information system.

ACKNOWLEDGMENT

The authors would like to express appreciations to colleagues in our laboratory for their valuable comments and other helps.

REFERENCES

[1] Y. Li, G. Lan, B. Liu and D. Chen, "Dynamic analysis on oil spill in Mexico Bay based on remote sensing and GIS," *Marine environmental science*, vol. 31(1), 2012, pp. 80-82.

[2] Y. Jin, D. Xiong and S. Yan, "Research on Marine Oil Spill Tracing and Monitoring System Based on GPS/ GSM/ GIS," *Traffic environmental protection*, vol. 24(6), 2003, pp. 6-8.

[3] B. Peng and F. Shao, "Study of a new method about marine spilled oil detection," China Sciencepaper, < http://www.paper.edu.cn/releasepaper/content/200703-247 >.

[4] J. Jiao, "Research on the prediction of oil spill based on GIS In Bohai Bay," *Marine environmental science*, vol. 30(5), 2011, pp.735-738.

[5] C. Yang, "Open GIS(WebGIS)," *Institute of remote sensing applications Chinese academy of sciences*, <http://wenku.baidu.com/view/c2c4245d804d2b160b4ec0ea.html>,

[6] Y. Liu, P. Yin, J. Lin and J. Zhang, "Prediction of Oil spreading and transport over the sea," *Journal of Dalian Maritime University*, Vol. 28(3), 2002, pp. 41-44.

[7] L. Ye, "System of Contingency Resource Allocation and Transport for dealing with the Oil Spilling Accidents at Sea," Unpublished Master dissertation, Shanghai Maritime University, China, 2006.

[8] Y. Li, G. Lan, B. Liu and D. Chen, "Dynamic analysis on oil spill in Mexico Bay based on remote sensing and GIS," *Marine Environmental Science*, Vol. 31(1),2012, pp. 79-82.

[9] L. Bing, F. Sun, C. Shu and G. Dong, "a satellite remote sensing system for maritime application based on the integration of RS and GIS," *Remote Sensing Information*, Vol. 27(5), 2012, pp. 97-101.

[10] H. Assilzadeh and Y. Gao, "Oil Spill emergency response mapping for coastal area using SAR imagery and GIS," OCEANS 2008.

[11] M. MOROVIC and A. IVANOV, "Oil Spill Monitoring in the Croatian Adriatic Waters: needs and possibilities," *ACTAADRIAT.*, Vol. 52(1), 2011, pp. 45-56.

[12] X. Li, "Study of Service-oriented Web 3D Visualization Based on Open source GIS," Unpublished Master dissertation, Zhejiang University, China, 2011.

[13] E. Fujioka, E.V. Berghe, B. Donnelly , J. Castillo; J. Cleary, C. Holmes, S. McKnight and P. Halpin, "Advancing Global Marine Biogeography Research with Open-source GIS Software and Cloud Computing," *Transactions in GIS*, Volume 16, Number 2, 1 April 2012 , pp. 143-160(18).

[14] J. Sun, "Open source exhibits the charm of spatial information," *Software World*, vol. 11(20), 2007, pp: 84-87.

[15] C. Liu and L. Chen, "GDAL Multi-source Spatial data Access Middleware," *geo-spatial information*, vol. 9(5), 2011, pp: 58-62.

[16] A. Dang, "Some topics on the standardization of the thematic maps," *Developments in surveying and mapping*, 1987, (6): 23-27.
[17] W. Li, X. Liang and J. Lin, "Mathematical Model and Computer Simulation for Oil Spill in Ice Waters Around Island Based on FLUENT," *Journal of Computers*, vol. 8, NO. 4, 2013, pp: 1027-1034.
[18] L. Qin and J. Zhang, "Development of Dangerous Source's Monitoring, Management and Emergency Rescue Decision-Making Support Information System," *Journal of Computers, Journal of Computers*, vol. 6, NO. 4, 2011, pp: 732-739.
[19] A. Muhammad and N. Tripathi, "Evaluation of OpenID-Based Double-Factor Authentication for Preventing Session Hijacking in Web Applications," *Journal of Computers*, VOL. 7, NO. 11, 2012, pp: 2623-2628.

Research on UAV Flight Dynamic Simulation Model Based on Multi-Agent

Chao Yun, Xiaomin Li
Department of UAV Engineering, Ordnance Engineering College, Shijiazhuang, 050000, China
Email: oec_ljw2009@163.com

***Abstract*—Simulation technology has been more and more important in the military weapon system. Simulation system has important research and application value. Flying simulation technology plays an important role in design and training period in the UAV (unmanned aerial vehicle) system. The multi-agent and object-oriented technology is adopted in the designing of the UAV flying simulator. The flying simulation system is established through three-layer framework which is based on delamination and modularization method. The delamination and modularization method can provide us a new idea in designing of the high efficiency simulator.**

***Index Terms*— Flight simulation; Multi-agent; Simulation system; Modularization**

I. INTRODUCTION

Flight simulation is concerned on the kinetic state of the aircraft, so we should propose the mathematical model based on flight mechanics, aerodynamic elements and flight control theory, and then conduct simulation experiments and perform the analysis of experiment results. Flight simulation is an integrate process based on simulation model, the character and moment law of aircraft [1]. Multi-agent technology is often adopted in system with complex aerodynamic characters, e.g., the formation of the aircraft flight. We can apply the multi-agent as reference in the designing work of the UAV flight simulation system, as UAV system is the complex system and it can be looked as the action platform, it also can be a reconnaissance or attack cell in the air. UAV system includes many sub-systems, each sub-system involves many modules. So the researching work of the flight simulation technology and applying other field technology have important values, as known that the multi-agent technology and combination module design could offer us the new idea in the design of UAV flight simulation system.

II. MUTLI-AGENT SIMULATION TECHNOLOGY

Now the object-oriented simulation technology is the mainstream technology in simulation field, object-oriented simulation adopts object-oriented modeling method, it consider the external world is consisted of different objects, this method can not only accord with the human thinking mode, but also it has characteristics of abstract, encapsulation, initiate and multi-state, so the object-oriented technology has advantages of modularize, repeat utilize, maintenance and flexible [2]. In practical application, one system could have many agents which have complicated dynamic characters; one agent can have manifold coupling relationships with each other. The flight simulation system may have many agent modules, but the object-oriented simulation technology could not solve the problem of self-check and preview with each subsystem, compared with tradition simulation technology, the agent-oriented simulation technology have many advantages in modeling, e.g., easily, flexible, inherit and hierarchical.

So we could apply the multi-agent technology in UAV flight simulation field, the flight simulation system is composed of many complicated sub-systems, each sub-system involves many modules, one module could be considered as one agent, one agent has complicated coupling relationships with the other agents under definite restrict condition, one agent will be transformed when other agents are changed, there exists some conflicts between each agent, so the related research will do the benefit to the researching work of multi-agent technology in heighten its effectively.

III. DESIGN OF UAV FLIGHT DYNAMIC COMBINATION SIMULATION MODEL

Modern simulation technology can be divided into three parts, system modeling, simulation modeling and simulation experiments. In the model aspect, the object-oriented modeling method can describe the abstract mathematics model in naturally style, it also can carry out that model's action through assembling and utilizing class libraries; in the modeling aspect, it adopts apart method in model and experiment, namely the data drive model; in the aspect of experiment, it adopts apart method in simulation operation control and experiment framework, it separates the output model definition and simulation model [3]. Agent is a new designing method in software system [4]. Despite now the agent is used in different fields such as computer science and artificial intelligence field, but the basic function of agent exchanges information from environments and receives outside useful information. As the specifically technique adopted in the information, one agent can be considered as a black box, multi-agent is an independent entity, which

doi:10.4304/jsw.9.1.121-128

apperceives the outside environment according to their own knowledge, ability and faith by themselves, and judgment of its target will affect other agent, one agent can accomplish the complicated task or acquire knowledge from outside environment through working together with others. Agent has the characteristics of independent, reactive, study, initiative, sociality, etc.

It is known that agent has the ability of encapsulation thinking and decision-making ability; therefore it can incarnate the independent of system. The framework of agent is to describe the process from abstract rule to idiographic realization, it is a different describing framework of arrangement for function system, and they are corresponding to different framework of implement arrangement. The work of these aspects includes how to make the system satisfy with each identity which is put forward by experts, the structure of software and hardware framework are perfect, and we should compartmentalize target of the agent according to the structure, agent generally includes cognitive agent, response agent and composite agent[5].

The cognitive agent can realize agent's represent and ratiocination through artificial intelligence (AI) method and expression by applying knowledge. Agent have the ability of cooperation, intelligence and consciousness, it can express inner word model and have definite immaterial state by symbol ratiocination and modify, this mode agent is composed of world model and layout equipment. One basic suppose is to module the cognitive module and research cognitive function in partial, and then combine them to make up of cognitive agent.

The response agent depends upon symbol express but export action is based on input, response agent is simply and it responses by inspirit from outside, which does not have model expression by symbol and complicated symbol ratiocination. Agent can analyze as human being, the behavior of agent can only be incarnated from communication with real world and the outside environment. The brainpower is depend on apperceive and action. Response agent could solve problem with high efficiency but its structure is very simple.

Composite agent has the advantages of the cognitive agent and response agent, which has strongly flexible and quickly response, composite system usually design two or more than two layers framework, the high layer is a cognitive layer which includes symbol world model, it performs the design of layout and decision-making by applying traditional method with symbol style, the low layer is an response layer which could quickly response and deal with paroxysmal matter, this layer does not adopt symbol expression and reasoning system. Response layer often has high preference, when it adopts delamination structure, and the problems should be solved are the control framework and the communicate mechanism of each layer.

VI. Design of UAV Dynamic Simulation Modeling

A. Analysis of Simulation Object

UAV flight simulation system adopts the design of flight control law and it is one part of the training system. The fidelity of the training system and the control law design are determined by the fidelity of simulation system. So the fidelity of simulation system is very important, the analysis of structure and function of UAV system are necessary. The flight simulation system is based on accurate model, which should reflect the essence of system.

UAV system can be divided into three parts in general, ground system, airplane system and task system. The structure of the system is shown as Fig.1, ground system involves ground assistant system, ground control system, flight and land system in ground station, telecontrol and distance sensing system in ground station; airplane system involves aerocraft platform, propulsion system, flight control system, navigation system, take off/landing system of aerocraft, telecontrol and distance sensing system of aerocraft; task load is the task equipment in the aerocraft, which can accomplish specifically assignment, e.g. recon task or attack.

The flight simulation system design in the paper is mainly used for self-contained training system. So we can take the task equipment in aerocraft as one module. This module is to accomplish the simulation function of the task equipment in aerocraft, namely to achieve the simulation function of recon equipment or attack equipment in the aerocraft.

Aircraft system and ground control station communicates through the UAV data-link, which is consisted of telecontrol and remote sensing system in aerocraft and ground station. UAV data-link takes charge of communication for instruction, in addition the maintenance personnel is one part of the UAV system which is not lacked, so it should consider the human factor in the design, research and employ process of the UAV system, the aerocraft system of UAV can be divided into some independence objects, and the each object should be modeled.

B. Design Project of the UAV Simulation System

- **Ideology of the system design**

In the object-oriented simulation technology, the external world can be taken as be composed by different objects which affects each other, the describing of the problem is according to the solving method of the problem, which can be easily understood, it is better to solve the reliability, accuracy and flexible for the model, the connection of UAV each subsystem is according to the designing demand and based on software develop theory, then adopt with multi-agent system and module idea by object-oriented technique to put forward a module and hiberarchy framework, take the multi-agent technology into the UAV flight simulation system's design process, so it could accomplish adaptability, fidelity and intelligence, the flow chart of designing idea is shown as Fig.2.

Step1: Make research on the function of the system, analyzes structure and framework of the system, then

make out the noumenon structure and function module by reasonable based on the demand of simulation system, and then set up the framework.

Step2:Choose whole saved or predigest management for the system, make the appropriate management according to the function or task requirement, some unimportant modules should be neglected or predigested and then make the research of important module.

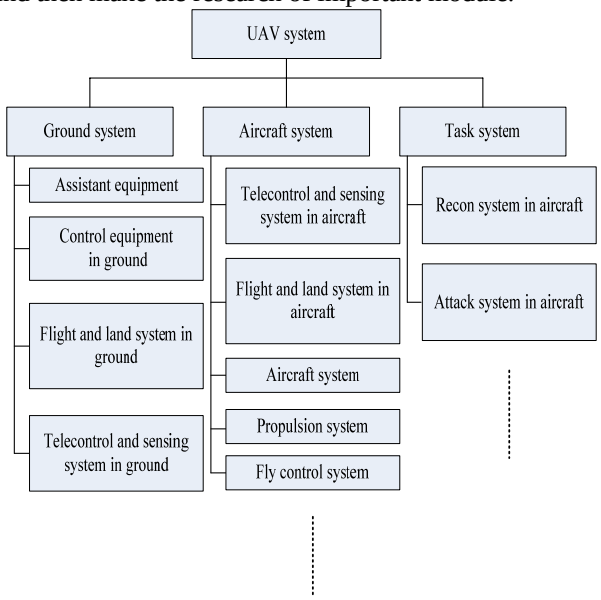


Fig.1 Structure of UAV system

Step3: Mark off the design of subsystem and module model arithmetic, this step is the core of the system design, in order to get the module's framework and operation mechanism of each subsystem, the implement method of every idiographic module. Design corresponding algorithm of the each module, and make them satisfy with the demand of system performance and function.

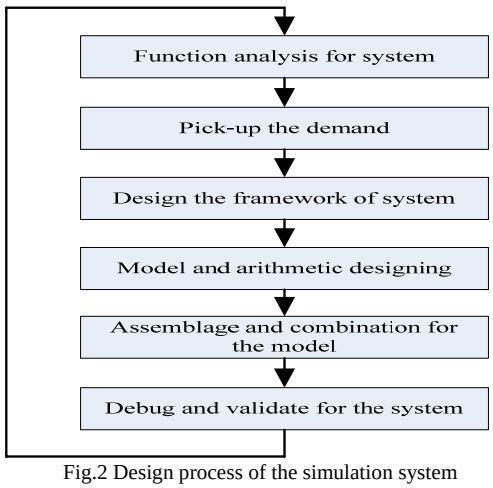


Fig.2 Design process of the simulation system

Step4: Assemble each module and debug the whole system, apply the every function module in the combination of subsystem, and actualize the whole function for the UAV simulation system, which is based on structure of framework, lastly make the analysis of the simulation results and demand design of the system, through the related simulation system, we optimize framework and model algorithm, finally achieve the optimized function of the whole system. As to some tune UAV system implement part, it is the integrative cooperation model for multi-agent, which has accurately control, because the control of UAV involves aerocraft attitude control, flight path control and task equipment control. There exists a coupling relationship between them.

Flight dynamic simulation model subsystem, it can be considered as operation part of the simulation system, some aerocraft body part includes the aerocraft physical body or function module, its intelligence is between flight computer model subsystem and task control system, it can drive each model module based on real data flow and then make each agent operate.

- **Subsystem Agent design**

UAV flight simulation system could be divided into three subsystems; each subsystem is composed of some different agents, according to function partition and cooperation of each agent, and performs the subsystem function.

Flight control computer subsystem, it mainly involves four agents, telecontrol order receive agent, distance sensing agent, task programming agent and flight management agent. Flight control computer subsystem has self-control ability, the structure of this subsystem adopts cognitive agent or composite agent, and then combine correlative algorithm. The framework of flight control computer subsystem is shown as Fig.4.

1.Receive agent of telecontrol order

Through decode ground telecontrol order (e.g.,flight control order or task equipment control order) and translate the received order to switch order signal or continuous order signal, then put this signal into the UAV automatic device or task implement equipment, according to control the flight attitude or task equipment.

2.Send agent of distance sensing information

It adopts various sensor or convertor, in decoding multi-signal (includes UAV dynamic state information or task equipment state information) based on distance sensing decode format through the data link. Ground station can display the flight state parameters and recon the information.

3Assignment agent of task programming and resource

Task programming needs entireness task order, and the analysis of implement target task, and it need ensure each target location, program of each task, create task queue, and then according to the results of flight path programming and the information synergetic result, it picks up information from task queue and make the whole flight programming combine with flight programming, after the flying of the UAV, it can collect the environment, state information and request by other agent in real time. When program the flight path, it should modify in real time; the resource assignment manages the whole resource for the system, the whole agents are in a dynamic environment, they collaborate with each other. This part could organize system's task and distribute resource for each resource, which could

assign resource by maximum, and then avoid conflict of software and hardware resource.

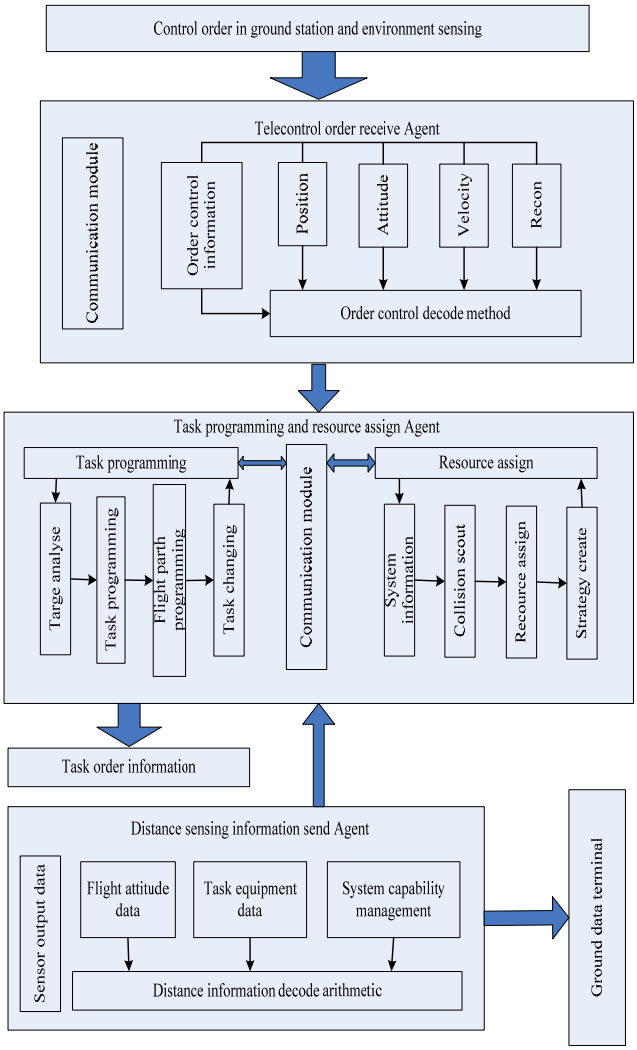


Fig.4 Flight control subsystem

4. Agent of flight management

Flight manage agent is a complicated agent, it mainly takes charge of tactical task, flight data management could manage expert knowledge in flight control field, which could improve navigation capability by itself.

- **Control and implement subsystem**

It mainly includes three agents, i.e., flight path track agent, flight attitude control agent and independence navigation agent, its structure is shown as Fig.5, they are group response agents, it control the flight attitude through drive aerocraft rudder, the subsystems have generally characteristics such as cooperation, work together and achieve flight control under task decision-making.

Flight path track agent is a response agent who is based on control device, it integrate flight path track algorithm inside and could transform the control order to flight order or propulsion force, control flight attitude agent, and then control UAV to fly in the set path.

Flight attitude control agent is a response agent who based on control agent. It integrates flight attitude control arithmetic inside and export real time rudder running order, then control the flight attitude of UAV.

Independence navigation agent is a response agent which is based on control device, it can receive the UAV current position by GPS or inertia navigation information, and measure the error of current flight path, compute flight path, and it can cooperate with flight path track agent and flight attitude control agent make the UAV flight in the set flight path.

1. Flight dynamic combination simulation model

It mainly includes four agents, flight mode switch agent, environment apperceive agent, aircraft task mode agent, aircraft mobile decision-marking mode. The intelligence of this model is in middle of system, it mainly achieved each agent harmonious operation, and the structure of flight dynamic combined simulation model is shown as Fig.6.

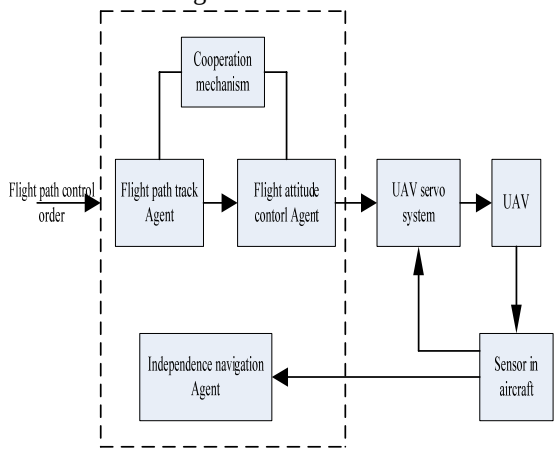


Fig.5 Nontrol implement subsystem

2. Agent of flight mode switch

Firstly, it receive the control mode signal from the flight operator, there are three flight operate modes, telecontrol mode, program control mode and independent control mode. When it selects the independent control mode, if the current state of UAV is out of control from the ground operator, it will be turned into independence executive task state, i.e., the state of take off, callback, landing, motion and mode of instancy flight operation, etc.

3. Module agent of environment apperceive

Environment apperceive agent module is mainly to scout enemy region information based on the sensor in aerocraft and its recon or communication system, includes radar, data link, GPS navigation information, vision sensor information and so on. It can pick-up the useful information from abundant uncertain information, then distribute useful information to other agent.

4. Module agent of aerocraft task Aerocraft task

Mode agent mainly involves aerocraft aerodynamic kinematics equation module and task in aerocraft module. Aerocraft aerodynamic kinematics equation module is the core of system. After calculate out the flight path parameters, It offer the flight attitude parameters to the system, in this module, it integrates every force and moment, compute velocity and angle speed in aircraft coordinate, using integral operation to compute

synthetical velocity. Task of aerocraft module is mainly to achieve the task equipment in aerocraft fidelity simulate working. Control work of flight attitude control and task equipment control are not isolated and there exists coupling relationships between them.

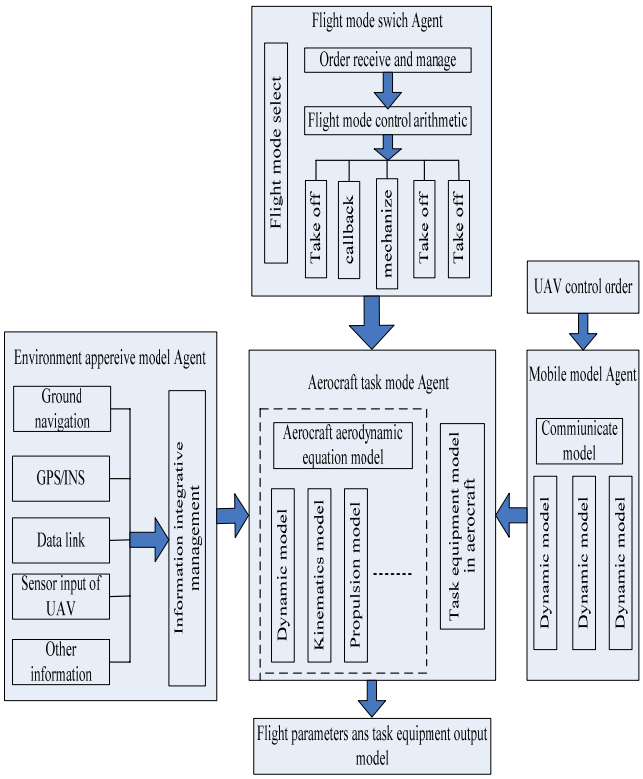


Fig.6 Subsystem of dynamic simulation model

5. Module agent of Aircraft movement decision-making

If we take the UAV formation in the future into account, the system should also be added in the decision-making module, when UAV is flying to the target, it can analyze the received data in time, then obtain the information of enemy firepower threaten, position threaten, landform threaten and so on. It can choose the relevant movement from movement database which can avoid threaten or transmit radar information and visual sensor information to aircraft's sensor, after veracious recognize enemy or ourselves, it can rapid locked the object and independent accomplish the recon task or attack task with high efficiency.

C. Communication and Coorperation Mechanism between Subsystem

Multi-agent communication mechanism plays an important role in multi-agent system. Each agent transmits complicated semantic information in time and ensure the system works effectively, when multi-agent system works in distributing mode, how to realize the multi-agent communicate and collaboration are very important in the whole system, it adopts transfer information mode in distributing multi-agent system and adopts synchrony time mode to realize control event synchronization. The semantic message is the core in the solving distributed problem. In the information mode, one agent could inform other agent when the event will happen or inquire agent information from other agent. Multi-agent communication mechanism not only has sociality characteristic as the person but also it can distinguish the traditional intelligent system and multi-agent system. Rational and finish intercommunion mechanism are the base of multi-agent system collaboration and arrangement, so the communication is the basic problem in multi-agent system.

- **Multi-agent communication mode**

Multi-Agent system communication mode always includes two kinds, blackboard mode and message mode [6]. Blackboard mode always make use of sharing data region or database who named blackboard with shareware memorizer, it exchanges message and data between different agents, which has characteristics of speediness and high efficiency, but it make against distributing control mode. Message mode is the direct communication mode for each agent who utilizes protocol; establish communication and cooperation mechanism based on message exchange between different agents. It can realize flexible and complicated strategy. In the message mode, agent communication language is used for message and knowledge exchanging. Agent communication language (ACL) usually generally includes three parts, external language, inner language and noumenon. External language define the meaning of message, inner language is used to express faith, desire and purpose, noumenon and it offer the related vocabulary[7].

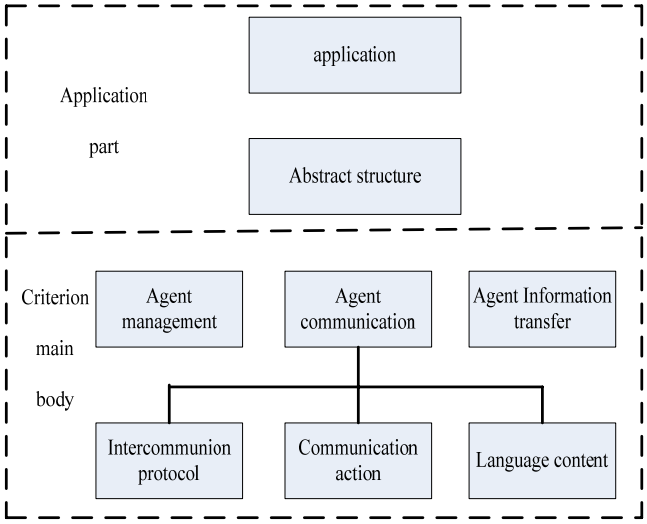


Fig.7 Frame structure of criterion gather for system FEPA

There are two kinds agent communication language, KQML and FIPA-ACL. In FIPA standard, the basic cell for the agent communication is FIPA-ACL message, generally one FIPA-ACL message include five elements, communication behavior type, communication actor, content of message, description of content and dialog control. As to these elements the communication behavior type is prerequisite element, the message sender, the message accepter and the content of message are the main contents. FIPA communicate actor is based on theory of language and action, which can carry out physical action. The corresponding actor involves

message sender, message accepter and revert object of message, there exists relationships between the current environment state and message accepter, it not only can accept request action, but also can refuse it, the message sender only can ensure send the message correctly.

Message content express refer content language, code and ontology. Content language is to show the message content which using formalize semantic description. FIPA offers optional semantic language, if both side of communication system know the current content language; the item can be passed over. Semanteme is expressed by semantic language and allow show the faith, desire and intent for one agent. Agent communication implies notion is one part the communication. The same notion may be described by using different language, communication needs ontology, the function of ontology is like vocabulary, which takes charge to explain the ontology, namely that correspond this ontology to popular meaning. Ontology makes up of expert knowledge database in flight control field, and it could make the agent comprehend by another in the communicate process.

- **Multi-agent cooperation mechanism**

Agent communication can promote multi-agent harmony and collaboration, it is an important characteristic of multi-agent and it is one another operation. The process of the intercommunion, this intercourse is called positive intercommunion, which is as in the person of agent synergic course; there exists influencing intercourse which is called conflict, the concerted process of multi-agent can be regarded as conflict avoid process, because every conflict reason is different, so the method to solve this problem is different, in the environment of multi-agent system, conflict could be considered as the contradiction of target, faith, purpose between different agent, there are much associated method to distinguish conflict, which can be separated into several types[7]:

Cognitive conflicts because of agent have different skill or knowledge background; there have existing different faith, knowledge, attitude, which can be considered as the cognitive conflict. Behavior conflict one member's behavior could result in others member could not run. In the result conflict, when the colony member is working, contrapose one problem each subsystem maybe obtain the different conclusion. In the target conflict, one member achieved the target result in the other could not achieved that target. In the resource conflict, when colony member use same resource at one time, the system could not satisfy the demand at this time, so it will bring on this member scramble for the same resource.

Though the conflict representation is different, but we could manage the conflict action and make the multi-agent behavior toward the same target, because of each agent in multi-agent system have independence, which appear conflict according to their purpose and ability in calculation process, so it should be correspond, concerted problem which are to manage inner depend on relationships between different agents, if there exists mutual action agent action, the concerted mechanism is needed.

Multi-agent system concerted method can be separated into showing concerted method and concealed method. Showing concerted is that the agent is designed to ratiocination for intercommunion and could consult with other agents if necessary, this method has clear and direct mechanism, when agent action is not consistent, it could adopt it to solve the problem. However this concerted method needs enough time for sustain, it is not applicable in some dynamic and real time environment; concealed method is the agent which is designed to follow some action rule in part.

- **Cooperation mechanism of subsystem Agent**

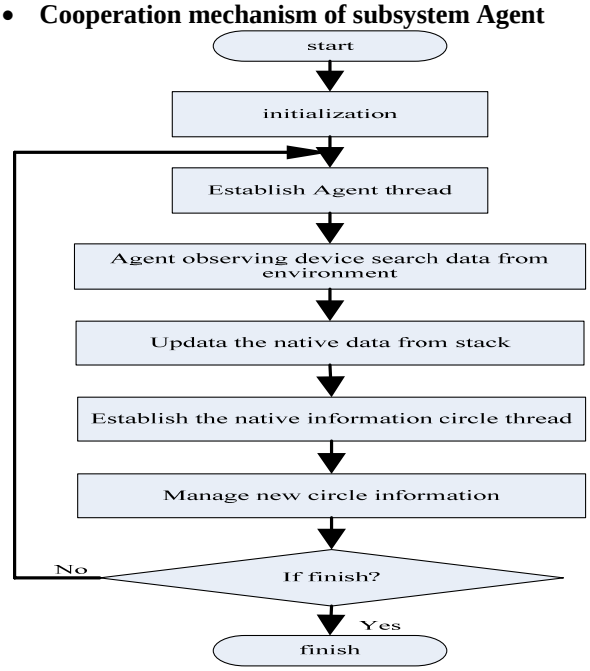


Fig. 8 Data active flow chart of each subsystem Agent

In the paper, it mainly studies on flight simulation system. The simulation system is face to signal personal computer, so it adopts windows operating system to establish the simulation software. Therefore, subject design of multi-agent system mostly complete the data in real time and it is based on windows operating system. The communication between process and inside process, in the communication process it adopts share memory pool mode, the inside communication process adopts thread synchronous mode. They can accomplish real time communication of inside process by share memory pool and thread synchronization [7]. The working step of each subsystem is as follows: 1)Initialize construct function, accomplish agent register, make message distributing; 2)Start message working process; 3)Observed register message, take out data from environment, then activate the message thread, at that time message thread pop-up message and transfer call-back function, it's working flow chart is showing as Fig.8.

The member of each UAV subsystem of agent template class includes the environment name, the environment crunode name and agent name. The member function mainly includes, initialization, bespeak, simple

call-back function and complicated call-back function. Observe and message manage thread implement by operation environment. When we empolder subsystem agent, only need to achieve member function in template.

UAV subsystem agent sort and layer are different, the concerted action between them need to be analyzed based on different layer and grade, as to different grade agent, when superior agent concerted with inferior agent, it adopts command, the inferior agent must perform the order by superior agent, then return the executive result to the superior agent; it adopts advice between the same level agent, the other side can evaluate this advice, then it can accept or refuse this advice based on actual status[8].

UAV flight simulation system based on multi-agent which can be divided into some autonomic agent, each subsystem have relative independence, when it perform local simulations, it may bring the confliction, so it should correspond with the decision-making of each agent and avoid conflicts, and make each unattached agent toward the same direction, then it will accomplish the holistic function of flight simulation system [9-15].

V. CONCLUSION

Multi-agent technology is a new researching direction of computer science and artifical intelligence(AI), which have a wide foreground, construct logical agent can fall down the complicated system, and improve the efficiency of system, the flight simulation system based on multi-agent and modularize idea can not only satisfy the independence, real time and information distributing of the simulation system, but also can expand the system function by maximum, fall down complexity of the system and heighten the efficiency of system. Contrast with tradition flight simulation system, the flight simulation system based on multi-agent could achieve self-control and intelligence to certain extent, which have large potential in opening and modularization aspect, and it is the develop direction of the flight simulation system.

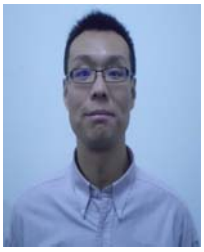
ACKNOWLEDGEMENTS

The Authors would like to thank Professor Lawson Richard for critically evaluating the manuscript and the control group members of UAV staff room for their kind help at various stages of the research.

This project is supported by key basic research program of China.

REFERENCE

[1] Xingren Wang, real time flight simulation system and technology. *Beijing University of Aeronautics and Astronautics Press*.1998.
[2] Lei Zhang, Flight simulation modeling and software development for flight simulator [D]. *Harbin, Harbin Institute of Technology*.2007.
[3] Fengju Kang, Application and Intelligence simulation in Military UUV equipment system research[J]. *TORPEDO TECHNOLOGY*. 2011.
[4] Lei Zhang, Agent-based motion control system architecture of autonomous underwater vehicle. *Harbin Engineering University [D]*, 2010,12.
[5] Kaihua Xu, Researching and application of communication mechanism for multi-Agent system[J]. *CD technology*.2009.
[6] Feng Wang, Research on autonomous flight control system for UAV based on multi-Agent system[D].*NanJing University of Aeronautics and astronautics*, 2009.
[7] BAJODAH A H. Generalized dynamic inversion spacecraft control design method [J]. *IET Control Theory App*, 3(2),2009,pp.76-84.
[8] POSADAS J L, POZA J L, eta.l Agent- based distributed architecture for mobile robot control[J]. *Engineering Applications of Artificial Intelligence*, 21(6),2008 ,pp.34-41.
[9] WOOLDRIDGE M. An introduction to Multi-Agent Systems[M]. *John Wiley & Sons, Inc* , 2002 .
[10] Ferrante Eliseo. A Control Architecture for a Heterogeneous Swarm of Robots: The Design of a Modular Behavior-Based Architecture. *Tech Rep IR/ IRIDIA/2009- 010, IRIDIA*, Universié Libre de Bruxelles, Brussels, Belgium, 2009.
[11] WANG Jian, KANG Long- yun. Study of Energy Complementary Control of Distributed Power Generation System Based on Renewable Energy[J]. *Journal of System Simulation*, 17(6),2005, pp.1438- 1440.
[12] Reichard K M, Banks J, Eddie C C, et al. Intelligent self-situational awareness for increased autonomy, *reduced operational risk, and improved capability*, AIAA, 2005, pp.1~8.
[13] Yajuan Yang, Wenxue Niu. Multi-Agents Model and Simulation for the Evolution of Industrial Clusters, *Journal of computers*,Vol.8, No.2, February,2013, pp:326-33.
[14] Weizi Li, Kecheng Liu, Shuzhang Li, Hongqiao Yang, A Semiotic Multi-Agent Modeling Approach for Clinical Pathway Management, *Journal of computers*, Vol.5, No.2, February,2010, pp:266-273.
[15] Weidong Zhao, Haifeng Wu, Weihui Dai, Xuan Li . Multi-agent Middleware for the Integration of Mobile Supply Chain, *journal of computers*, Vol.6, NO,7, July,2011. pp:1469-1476.



Chao Yun was born in baoji, shaanxi PR. China, Dec.1983. He received the B.S. degree in electrical engineering from the Xi'dian University, Xi'an, China, in 2007 and the M.S. degree in navigation, guidance and control from Mechanical Engineering College, Shijiazhuang, China, in 2009, where he is currently working toward the Ph.D. degree in the control science and engineering since the spring of 2010.His research field is unmanned aerial vehicle (UAV) flight simulation and simulation technology.

Xiaomin Li was born in Baoding c, Hebei, PR. China. He received the B.S. degree in electrical engineering from Mechanical Engineering College, Shijiazhuang, China, in 1990, and the M.S.and Ph.D.degree in communication and information system from Beijing University of Aeronautics and Astronautics, Beijing, PR. China, in 1996 and 1999. From 2000 to 2002, He was with the Mobile Station for Postdoctoral Research Program, Institute of Acoustics;

Chinese Academy of Sciences Beijing. He is currently a Professor and Supervisor of doctoral candidates and also the Director of the Research Institute of Navigation, Guidance and Control.

His research interests include application of navigation and guidance technology, analog simulation and high-speed data link control.

Availability Modeling and Analysis of a Single-Server Virtualized System with Rejuvenation

Jian Xu, Xuefeng Li, Yi Zhong and Hong Zhang
Institute of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing, 210094,China
dolphin.xu@njust.edu.cn

***Abstract*—Availability of business-critical application servers is an issue of paramount importance that has received special attention from the industry and academia in the last decade. This paper presents two stochastic reward net based availability models for a single-server virtualized system. The similarity in both models is that software rejuvenation is applied at not only virtual machine monitor (VMM) level using a time-base policy but also at virtual machines (VMs) using a prediction-based policy. The key difference is that the passive software replication and the active software replication are respectively adopted at the VM level of both models. We compare these models in terms of steady-state system availability by numerical analysis. Results show steady-state system availability with the active replication style gets a bit better than that of the passive one. Further, we study the impact of two critical parameters, the VMM rejuvenation interval and the VM aging detection probability, on downtime and on the number of transaction lost by sensitivity analysis.**

***Index Terms*—Analytic model, virtualization, availability, stochastic reward net, software rejuvenation**

I. INTRODUCTION

Software aging is the phenomenon of progressive degradation of running software image which might lead to performance reduction, hang ups or even crashes [1]. The primary causes are exhaustion of systems resources, like memory-leaks, unreleased locks, non-terminated threads, shared-memory pool latching, storage fragmentation, or data corruption. This undesirable phenomenon has been observed in enterprise clusters [2,3], telecommunications systems [4,5], web servers [6] as well as other software. It is most likely to manifest itself in long-running or always-on applications such as web and applications servers, components of web services, and complex enterprise systems.

The primary method to fight aging is software rejuvenation proposed by Huang et al. [1]. The main idea behind software rejuvenation is to gracefully terminate an application and periodically or adaptively restart it at a clean internal state. Garbage collection, flushing operating system kernel tables, reinitializing internal data structures are some examples of what cleaning the internal state of a software might involve. An extreme, but well known example of rejuvenation is a hardware reboot. Rejuvenation has been implemented in various types of real life systems – telecommunication systems [4,5], transaction processing systems [7], web servers [6] and cluster servers [2, 3]. In this paper, we focus on the virtualized system, which is becoming more and more important as the emergence of cloud computing.

Virtualization technology is the key element in cloud computing[18,19], which is used for software infrastructure of cloud computing services to provide computing resources over the Internet. A virtual machine monitor (VMM) or hypervisor is a thin software layer that virtualizes machine resources to allow multiple virtual machines (VMs) to be multiplexed on a single physical machine and ensures VMs functionally isolated from one another. The use of virtualization to consolidate servers for enterprise applications is currently used widely as a solution to improve system availability [8-10,17]. However, both VMM and VMs in a virtualized system are subject to software failures during their continuous execution due to residual aging bugs. Especially for the VMM, it plays a critical role of a single-server virtualized system and often becomes the single point of failure. Thus, there is an urgent need to apply software rejuvenation to such systems to further improve system availability.

The main contribution of this paper is to propose new availability models for a single-server virtualized system and to discover novel results of comparing existing models. For a single-server virtualized system hosting two VMs in a passive or active replication mode, stochastic reward net (SRN) models of the virtualized system are developed by applying a combinatory rejuvenation technique that uses a time-based policy for a VMM and a prediction-based policy for VMs, which capture aging states of VMs and the VMM as well as their failures caused by software aging. And then we demonstrate that the availability of the virtualized system with an active replication mode is higher than the one with a passive replication mode, and analyze the combined effect of the rejuvenation interval (defined as the time between successive rejuvenations) in the time-based policy and the detection probability in the prediction-based policy on the steady state expected availability, downtime and transaction lost by numerical

doi:10.4304/jsw.9.1.129-139

solutions. Further, comparing with the existing models for a single-server virtualized system, we discover some novel results.

The rest of paper is organized as follows. Section 2 presents some related work. Section 3 focuses on some motivations for this work. Section 4 presents a considered architecture for a single-server virtualized system with virtualization and software rejuvenation and provides availability models with different rejuvenation policies using SRN. To validate the technique, the analysis results are presented in Section 5. Finally Section 6 concludes the paper.

II. Related Work

There are too many works to improve system availability in the literature of software rejuvenation, which aim at determining an appropriate rejuvenation technique and rejuvenation schedules to minimize system downtime or maximize system availability. These works can be approximately divided into two categories: periodical rejuvenation based on time or work performed, and adaptive or proactive rejuvenation where the time to resource depletion or performance degradation is estimated. Countless studies have shown that the latter approach is more efficient, resulting in higher availability and lower cost. Our work also falls into the latter approach.

Among the methods to apply proactive software rejuvenation two are dominant: time-based approach [1-5,7], and the prediction-based (or measurement-based) approach [6,11]. The first method attempts to obtain an analytic model of a system taking into consideration various system parameters such as workload, MTTR and also distributions of failure. On this basis, an optimized rejuvenation schedule is obtained. The tools used here include CTMC models [1], MRGP models [3], SRN [2,4,5] and others [7,20,21]. In the prediction-based approach, the behavior of running software is monitored and the rejuvenation process is only triggered upon detection of any anomalies in the behavior of software. In our work, we integrate the analytic-based approach with the prediction-based approach in a model.

As the emergence of cloud computing, there are a few works focusing on software rejuvenation in a virtualized system. Combining virtualization and rejuvenation to achieve high availability is used by Machida et al.[8], Thein et al.[9,13] and Kourai et al.[10,14,15]. These works benefit from consolidation property of system-level virtualization.

Thein et al. [13] present a continuous-time Markov chain based analytical model to capture the behavior of the virtualized clustering system with software rejuvenation. They analyze system availability with the time-based rejuvenation policy under different cluster configurations, 2 VMs hosted on a single physical server and 2 VMs per a physical server in dual physical servers. Analysis results show that it is possible to benefit from increased availability by integrating virtualization, clustering and software rejuvenation. Based on the previous work [15], Thein et al. [9] further present a virtual machine based software rejuvenation framework named VMSR to offer high availability for application server systems. They again use a continuous-time Markov chain to model a single physical server hosting multiple virtual machines in the scheme of hot standby with the VMSR framework. Both works [9,13] only use the time-based rejuvenation policy for the VM failure without considering the VMM failure and its rejuvenation issues. However, VMM as the single point of failure of a consolidated system plays a critical role in improving system availability. Hence we propose a combinatory rejuvenation technique here for a single server virtualized systems considering the failures and rejuvenation of both VMs and the VMM.

Due to the critical role of VMM, a fast software rejuvenation technique for VMM named Warm-VM reboot was presented by Kourai et al. [14,15]. Compared with Cold-VM reboot that stops all the hosted VMs at the VMM rejuvenation, Warm-VM reboot improves the availability of the application hosted on VMs by introducing the on-memory suspend technique and the quick reload mechanism. However, their work only focuses on rejuvenating a parent component when the parent component is a VMM and the subcomponents are VMs. In this paper, we not only take the failures and rejuvenation of both VMs and the VMM into account but also adopt a different rejuvenation policy for them.

A comprehensive availability model for a server virtualized system with time-based rejuvenations for VM and VMM was presented by Machida et al.[8]. Their model focuses on the evaluation of the rejuvenation techniques for VMM including Warm-VM rejuvenation, Cold-VM rejuvenation and Migrate-VM rejuvenation. Further, they leverage existed availability models for time-based rejuvenation and apply them to a server virtualized system to determine the optimum rejuvenation schedules in terms of downtime. It is important to note that our approach is different from their works in terms of rejuvenation policy. They use the time-based rejuvenation policy for both VMs and VMM while we are proposing a new combinatory rejuvenation technique that uses a time-based policy for the VMM and a prediction-based policy for VMs. Moreover, our work discusses the impact of the configuration of VMs on rejuvenation process. For the VM level of a single-server virtualized system, both VMs can work in an active or passive software replication mode and provide similar services. Thus, we develop two SRN models for the cases of using the active and passive replication at the VM level respectively to analyze system performance from the aspects of transaction lost as well as availability and downtime. Moreover, we discover some novel results through comparing the existing models.

III. Motivation

In the following text, we focus on the motivation of using a combinatory policy and applying SRN to model system behaviors respectively.

In a single-server virtualized system, there are two critical components, the VMM and the VM hosted on the

VMM. Both of them may be failure because of aging-related bugs. Because of the VM hosting on the VMM, the VM can also be rejuvenated by the rejuvenation of its underlying VMM. But downtime cost due to the VMM rejuvenation is much more than downtime cost due to the VM rejuvenation. This motivates us to handle the VM rejuvenation as well as the VMM rejuvenation. Further, to rejuvenate any one of the VMM and the VM in a proactive way, we have two choices for rejuvenation policy, namely the time-based policy and the prediction-based one. For the former, we need only build an analytical model using assumptions about its operational profiles or failure distribution, to make the model as close as possible to a real life system taking no consideration of its real operation process. So in whatever situation, the time-based approach is easy to be used. But the approach is not precise to some extent. For the latter, we need monitor the behavior of running software, collect some resource-related or time-related data, validate the existence of aging, analyze system performance level and trigger the rejuvenation. The above actions can not be taken if absence of the detailed configuration of a running system and some embedded functionalities in the system. So the prediction-based approach is the sole way to apply the optimal rejuvenation schedule produced from the time-based approach to a real life system, which makes rejuvenation come true. Of course, comparing with the time-based approach, the prediction-based approach is relatively complex, but more precise. In our work, we have designed a component named Software Rejuvenation Agent (SRA) inside each VM to monitor consumable resources and states and carry out rejuvenation operations. The existence of SRA makes the adoption of a prediction-based policy to the VM possible. This motivates us to use a combinatory rejuvenation policy, namely the prediction-based policy at the VM level and the time-based policy at the VMM level respectively.

And then we focus on the motivation of adopting SRN to model system behaviors dynamics. Models are system abstractions in one or more specific aspects, and provide the basis for the analysis of system behavior. There are several model types that have been used for modeling the performability of complex systems. However, the most common used model is the state-space based model, which can capture the complicated system dependencies. This kind of model demands the collection of system variables, the values of which define the system state at a given point. The state-space based model can further be divided into two sub-types: the low-level model and the high-level one.

The low-level model usually uses a stochastic process to characterize system behavior dynamics since there are significant uncertainties and unpredictable variations either inherent in the system or in its inputs. Such uncertainties can be taken into consideration via stochastic modeling and solution techniques. Several stochastic models, such as CTMC (Continuous time Markov chain)[1], SMP (Semi-Markov process)[20], MRGP (Markov Regenerative Process)[3] and MRM (Markov reward model)[21] and so on, has been widely used in the field of software rejuvenation modeling. To achieve the solutions of these models to analyze system performance, we usually make the resulting process a homogeneous CTMC by some converting techniques regardless of the original type of processes. For example, in order to solve the MRGP, we choose to approximate the deterministic transitions in MRGP using an r-stage Erlang distribution, so the resulting process becomes a homogeneous CTMC and the solution techniques for Markov chains can be applied. But, this approach has a significant shortcoming that the state space of the CTMC increases by r due to the approximation. And if we wish to model a single-server virtualized system with n standby VMs where each VMs has less than six states (more details in section 4.1), the overall state space will become unmanageable if we were to build the CTMC by hand. Thus, in order to avoid the manual construction of a high fidelity model we may resort to the following higher level model.

The high-level model usually has not only a rigorous mathematical basis, but also a powerful graphical representation. With a rigorous mathematical basis, they can be automatically transformed into a certain stochastic process, and then use the same way as the low-level model to analyze system performance. With the powerful graphical representation, they allow the designer to focus more on the system characteristics being modeled rather than on the error-prone specification of system state space. From this perspective, the modeling power of the high-level model is remarkably greater than the low-level one. Due to the graphic nature of the high-level model, the changes to models are done easily, while minor changes in a Markov chain require redefining all the states in the model. This motivates us to use the high-level model in our work.

The widely used high-level models in the field of software rejuvenation modeling include SPN(Stochastic Petri Net), GSPN(General Stochastic Petri Net)[22,23], DSPN(Deterministic and Stochastic Petri Net)[3,7] and SRN(Stochastic Reward Net)[2,4,5,8,16], etc. SPN only allows exponentially distributed firing times for transitions. GSPN extend the SPN by allowing zero firing time for some transitions, in which transitions with exponentially distributed firing times are called timed transitions while the transitions with zero firing times are called immediate transitions. For SPN and GSPN, they contain only immediate transitions and/or timed transitions with exponentially distributed firing time, so the underlying stochastic process is a homogeneous CTMC. However, we design a transition with deterministic distributed firing time for VMM rejuvenation clock in our models. Obviously, SPN and GSPN can be applicable no longer. As for DSPN, it requires all transitions are deterministic. However, our models contain not only deterministic transitions, but also exponentially distributed firing time transitions. Obviously, DSPN can also be inapplicable. As our choice in this paper, SRN is a variant of GSPN with a more powerful modeling power by several extensions. The first

extension is its ability to allow extensive marking dependency, which can specify parameters, such as the firing rate of the timed transitions, the multiplicities of input/output arcs and the reward rate in a marking, as functions of the number of tokens in any place in the SRN. In our models, the output measures are expressed in terms of the expected values of the reward rate functions. Another important extension is the ability to express complex enabling/disabling conditions through guard functions. This can greatly simplify the graphical representations of complex systems. In our models, almost each immediate transition is assigned with a guard function. Moreover, as same as the other high level models, an SRN can be automatically transformed into a Markov reward model (MRM), steady-state and/or transient analysis of the MRM by the tool SPNP [24] solves the SRN models. This motivates us apply the tool SRN to model the process of software aging and software rejuvenation in this paper.

IV. Availability Models

The benefits of software replicas created by virtualization technology are to reduce service interruption and optimize the rejuvenation process without any additional physical nodes. The proactive software rejuvenation with virtualization is just based on this principle. In order to study the effects of virtualization and software rejuvenation on availability for a single-server virtualized system, we provide two high level availability models using SRN to depict the process of software aging and software rejuvenation. Further, we analyze these models in terms of system availability, downtime and the number of transaction lost by sensitivity analysis.

A. System Architecture

The system architecture of a single-server virtualized system is shown in Fig.1. The single-server virtualized system consists of a hosting server installing a VMM and three VMs running in a dispatcher-worker mode on top of this VMM.

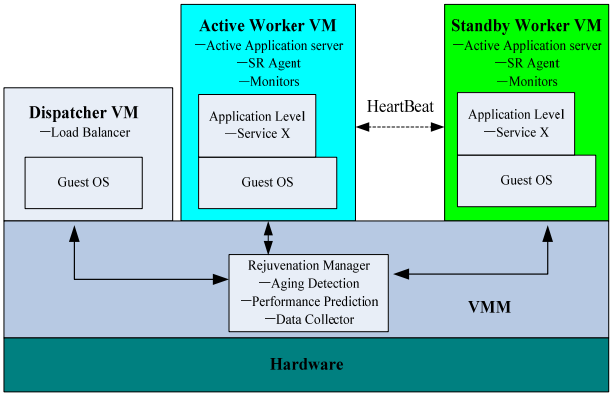


Figure 1. The considered architecture for a single-server virtualized system.

Dispatcher VM will be used for providing fail-over capabilities and a myriad of load balancing policies. The remaining VMs are in operation and deploy the same services, named Worker VM. Our idea is to hold multiple replicas of an application in a single physical server by virtualization technology, in which one replica is designated as primary and all others are designated as standbys (or backups). If the primary fails, one of the backups takes over as the new primary. This approach uses VMs as containers for the replica in order to avoid the need for additional hardware and it can provide continuous services during rejuvenation. In this paper, we create two Worker VMs. The primary application server and the standby one will be running on the active Worker VM and the standby Worker VM respectively. The VMs inform each other about their health using a heartbeat mechanism. We also designs a component named Software Rejuvenation Agent (SRA) inside each VM to monitor consumable resources and states, and another component named Rejuvenation Manager (RM) inside the VMM to analyze VMs' behavior, detect their anomalies and trigger the rejuvenation of a VM when it detects anomalies in the behavior of that VM. The existence of SRA and RM makes a prediction-based policy for VM possible. Similarly, due to absence of the above components, the time-based rejuvenation policy is the only one applicable for the VMM.

B. SRN Models

For a VMM rejuvenation, we use the simplest rejuvenation approach that shuts down all the hosted VMs prior to the rejuvenation regardless of the execution states of the VMs. The greatest strength of this approach is to clear all of aging states in VMs and VMM by a VMM rejuvenation. Of course, this weaknesses of this approach are also obvious. Because of the dependency between VMs and VMM, the execution of VMs running on the VMM may also be interrupted, which results in transactions lost and unnecessary downtime of the VMs.

For a VM rejuvenation, because of the replication mode used at the VM level in our considered architecture, there are also two different styles, a passive replication style and an active one. The former has no backup replicas in memory. Upon primary replica failure, a backup replica is loaded into memory and assumes the role of the new primary replica. The new primary replica's state is initialized from the last checkpoint to ensure its state is identical to the state of the old primary replica before its failure. The latter, in contrast, has all backup replicas created, initialized, and loaded in memory. The primary replica state is transferred to all backup replicas at the end of every operation on the primary replica. When the primary replica fails, a new primary replica is chosen from the backup replicas. Intuitively, application of the passive replication style will result in lower VM availability, longer downtime and higher the number of transaction lost. Two rejuvenation models using these two policies respectively will be built in this section, and this assumption will be verified through experiments in section 4.

In our proposed models, a Petri Net (PN) is a bipartite directed graph whose nodes are divided into two disjoint

sets - places and transitions. Input arcs are directed arcs which connect places to transitions and output arcs are directed arcs which connect transitions to places. A cardinality may be associated with these arcs. An arc with multiplicity *m* is represented by an '/m' on the arc. The distribution of tokens on the places of the PN is called a marking of the PN. When representing a PN graphically, places are represented by circles and immediate transitions, timed transitions and deterministic transitions are shown by narrow bars, hollow rectangles and filled rectangles, respectively. The number of tokens *n* in place *P* is represented graphically as the number *n* inside the circle for place *P*. Variable cardinality of an arc is represented by adding a *Z* on the arc. Each transition can also be associated with a guard function, which is usually a function of a marking. The transition is enabled only when the guard function is evaluated to TRUE and all other conditions relating to priorities and input arc conditions are met. The reader is referred to [25] for a detailed description of SRNs.

The SRN model with a combinatory rejuvenation policy is shown in Fig. 2. The model is represented by four SRNs, where Fig.2(a) is the SRN using the prediction-based policy at the VM level and the time-based policy at the VMM level, and Fig. 2(b) is the SRN for the VMM clock model, which is used for triggering time-based rejuvenation of VMM. Two different replication styles for the standby VMs are modeled by the Fig. 2(c) and Fig. 2(d) respectively.

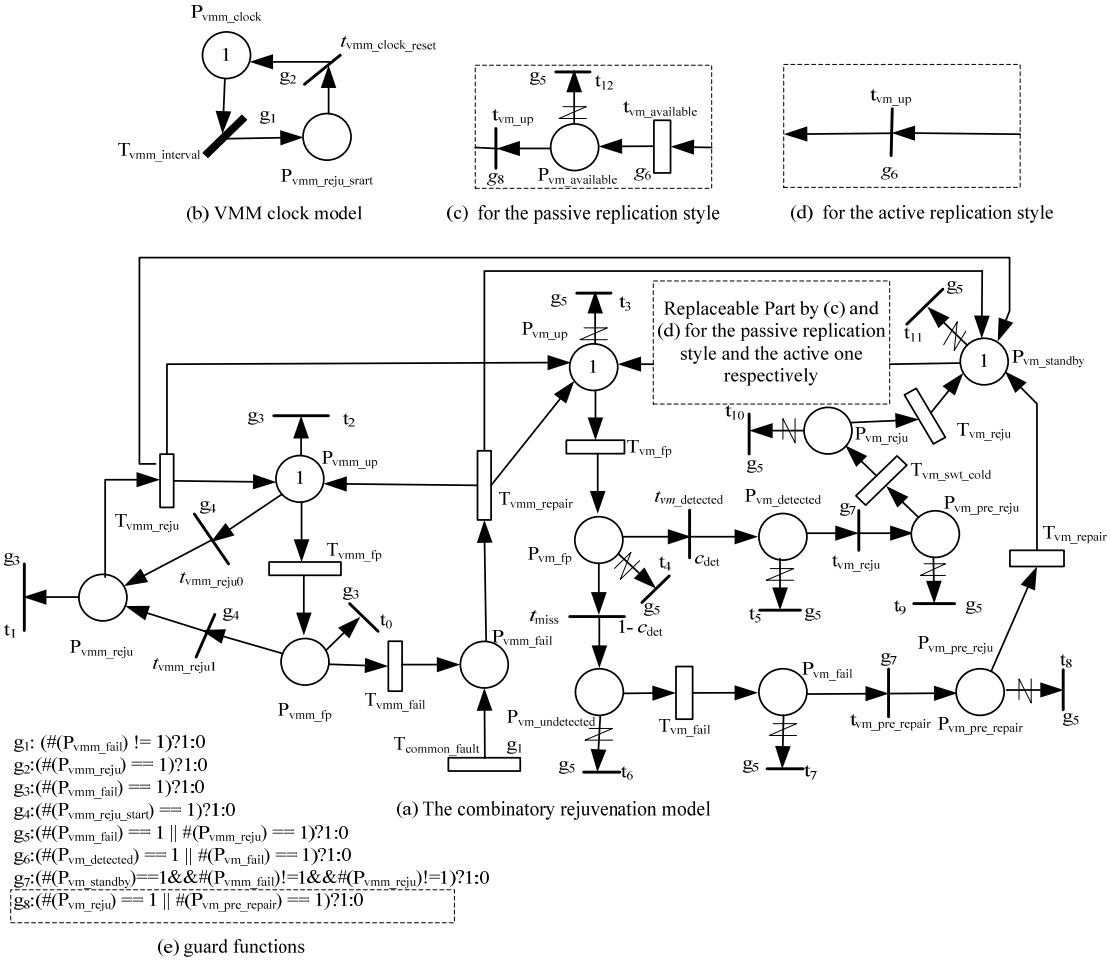


Figure 2. SRN models with different replication styles at the VM level

Combining part (a), part (b) and part (c) of Fig. 2, the integrated SRN model represents the failure process, recovery process, and combinatory rejuvenation of VMM and VMs with the passive replication style. Initially there is one token in the P_{vm_up}, $P_{vm\_standby}$ and P_{vmm_up} respectively, which demonstrates fully stable states of VMs and VMM. As time passes, each active VM eventually transits to an unstable state (place P_{vm_fp}) through the transition T_{vm_fp} representing the software aging of the VM. The active VM still works in this state but its failure chances increase. It is assumed that the RM can detect the aging with probability c_{det}. The P_{vm_fp} place has two immediate transitions with the appropriate probability for detecting aging or failures during detection process. If the aging is detected, a token is fired through $t_{vm\_detected}$ and will be deposited in $P_{vm\_detected}$. If the detection process fails, a token is put in $P_{vm\_undetected}$. As time progresses, the active VM eventually transits to a failure state (place P_{vm_fail}) through the transition T_{vm_fail}. Whenever a token is deposited in $P_{vm\_detected}$ or P_{vm_fail}, the active VM suspends all user requests and provides no longer services.

The recovery process consists of the standby VM loaded in memory, the standby VM's internal state catch up and the switching of the current active VM with the standby VM. The transition $P_{vm\_standby} \rightarrow T_{vm\_available} \rightarrow P_{vm\_available}$ in the SRN model represents the standby start time required to perform the first step. On a token in place $P_{vm\_available}$, the standby VM is available. The latter two steps of this rejuvenation process are performed by using the timed transitions $T_{vm\_swt\_cold}$. The rejuvenation and repair of the active VM can begin when the standby VM is in an available state (place $P_{vm\_available)}$ and the underlying VMM is neither in the failure state nor in the rejuvenation state. The guard function g_7 ensures this condition. In passive replication mode, the standby VM's internal state is initialized from the last checkpoint to ensure its state is identical to the state of the active VM before the failure. Hence, the time for the final catch up step mainly includes the time to transfer all pending requests and current sessions from the active VM to the standby one. After the switch is completed, a token is deposited in place P_{vm_reju} to mark the completion of rejuvenation. When the active VM is completely rejuvenated, it is placed back in service as the new standby VM. The process can repeat continuously. Because of the dependency of VMs and VMM, all tokens representing VMs' operational nodes (i.e. tokens in places P_{vm_up}, P_{vm_fp}, P_{vm_fail}, $P_{vm\_pre\_repair}$, P_{vm_reju}, $P_{vm\_pre\_reju}$, P_{vm_detect}, $P_{vm\_undetected}$) are removed when the system is considered failed (i.e. token in place P_{vmm_fail} or P_{vmm_reju}). This is accomplished by the guard g_5, which enables the immediate transitions t_3, t_4, t_5, t_6, t_7, t_8, t_9, t_{10}, t_{13}, t_{12}, when it detects a token in place P_{vmm_fail} or P_{vmm_reju}. In this case, it is inevitable to involve unnecessary downtime and lose transactions.

Similarly, when the transition T_{vmm_fp} fires, a token is deposited in P_{vmm_fp}. If the transition T_{vmm_fail} fires, a token is deposited in P_{vmm_fail} which represents the VMM failure due to the software aging. The effects of common mode faults are applied using T_{common_fault}. When this transition is fired, VMM failure also occurs. When the VMM is recovered from the failure state, the token in P_{vmm_fail} is removed and a token is deposited in P_{vmm_up}, P_{vm_up} and $P_{vm\_standby}$ respectively by T_{vmm_repair} transition. The time-based periodic rejuvenation is driven by a deterministic clock shown in Fig.2(b). When the deterministic transition $T_{vmm\_interval}$ fires and deposits a token in place $P_{vmm\_reju\_start}$ each d time units, the VMM rejuvenation is triggered and the immediate transitions t_{vmm_reju0} and t_{vmm_reju1} are enabled by guarding function g_4 and a token is deposited in P_{vmm_reju}. Similarly, when the VMM rejuvenation cleans up the aging states, the token in P_{vmm_reju} is removed and a token is deposited in P_{vmm_up}, P_{vm_up} and $P_{vm\_standby}$ respectively by T_{vmm_reju} transition. Whenever in case of VMM rejuvenation or VMM repair, both leads to rejuvenation of the whole system and those VM related places flushed out because of VMs running on the VMM.

Combining part (a), part (b) and part (d) of Fig. 2, the new integrated SRN model represents the failure process, recovery process, and combinatory rejuvenation of VMM and VMs with the active replication style. The most noteworthy difference is that there is no need to take some time to make the standby VM activated. Hence we use the immediate transition t_{vm_up} to represent this step instead of the timed transition $T_{vm\_available}$ in Fig. 2(c). The rejuvenation process in practice only consists of standby replica's internal state catch up and the switching of the current active replica with the standby replica, which can be represented by timed transition $T_{vm\_swt\_hot}$. Moreover, the standby VM's internal state is continuously updated with the active VM internal state changes. Hence, the total time including the time for the final catch up step and the replica switch time in active replication style is shorter than the total one in passive replication style. After the switch is completed, a token is deposited in place P_{vm_reju} to mark the completion of rejuvenation.

The guard functions used by these two models are summarized in Fig. 2(e), where the guard function g_8 is only suitable for the model with the passive replication style.

V. Analysis and Results

We used the stochastic Petri net package (SPNP) tool [24] to have an evaluation of two rejuvenation models applied to the target system. We assumed that all transition times of timed transitions in the models are exponentially distributed except for $T_{vmm\_interval}$ which is deterministic because it represents the fixed rejuvenation trigger intervals of VMM. There are many previous studies [3-5,8-9,13,16] supporting the use of exponential distributions. For examples, in a CTMS (Cable Modem Termination System) cluster system, Yun Liu. [4,5] have assumed that the distribution of time between hardware failures and software failures caused by Heisenbugs are exponential, the distribution of time between software failures caused by aging-related faults is hypo-exponential, and the distribution of failure detection time and node switchover/reboot/rejuvenation/giveback time are exponential. Of course, the assumption of the exponential distribution is not always well-suited for all real-world applications. For examples, in Salfner [7], it has been concluded from data of a commercial telecommunication platform that the distribution of time-to-failure can be approximated best by a lognormal distribution. In our experiments, the assumption of the exponential distribution makes the modeling and computation easier. However, our models are not restricted to exponential distributions; other well-known distributions such as lognormal and Weibull could be used as well. The model parameters need be varied with different distributions, while the model solutions can be left to the tool SPNP.

Because of the existence of the deterministic transition, we used 10-stage Erlang distribution for approximating it. The model parameter values used were based on prior investigations [8,16] of software aging related failures and the application of the software rejuvenation as the solution, as shown in Table 1. For an example of λ_{vm_fp}, the calculation of the default value is as follows. We

assume that the mean duration time observed from the robust state to the unstable state is one week, namely 7×24 hours. Thus, the VM aging rate is $1/(7 \times 24)=0.005952381$, which means the number of aging appearance is 005952381 per hour.

TABLE I.
PARAMETERS USED IN ALL MODELS

Parameter		values	
Symbol	Description	Default Value	Mean Time
λ_{vm_fp}	VM aging rate	0.005952381	1 week
λ_{vm_fail}	VM failure rate after aging	0.013888889	3 days
$\lambda_{vm\_recovery}$	VM failure recovery rate	2	30 mins
λ_{vm_reju}	VM rejuvenation rate	60	1 min
$\lambda_{vm\_available}$	Standby VM activation rate in cold-standby	60	1 min
$\lambda_{vm\_swt\_cold}$	VM state transition rate in cold-standby	120	30 secs
$\lambda_{vm\_swt\_hot}$	VM state transition rate in hot-standby	1200	3 secs
λ_{vmm_fp}	VMM aging rate	0.001388889	1 month
λ_{vmm_fail}	VMM failure rate after aging	0.005952381	1 week
$\lambda_{vmm\_recovery}$	VMM failure recovery rate	1	1 hour
λ_{vmm_reju}	VMM rejuvenation rate	30	2 mins
$\lambda_{vmm\_reju\_inter}$	VMM rejuvenation trigger rate	--	--
c_{det}	VM aging detection probability	--	--

For the simplicity of description, we call the model using the combinatory rejuvenation policy with the passive replication style “Model A”. Similarly, we call the model using the active replication style “Model B”.

A. Model A VS. Model B

In this section, we compare these two models only from the aspect of system steady-state availability regardless of downtime and transaction lost. The main causes are as follows. For downtime, the expected total downtime over time interval T is calculated as $T*\left(1-P_{\text{avail}}\right)$, where P_{avail} is system steady-state availability probability. Thus, it is easy to find that the variation tendency of the expected total downtime is opposite to that of steady-state availability. For transaction lost, when the active VM is rejuvenated or repaired, there are no transactions lost because of the current transactions transferred to the standby VM and the subsequent user requests queued by the Dispatcher VM. Thus, the replication style using by both models should be no impact on whether transactions lose or not.

Availability models capture the failure, repair and rejuvenation behavior of systems and their components. In the above two models, the impact of critical parameters, such as the rejuvenation trigger intervals of VMM and aging detection probabilities of VM, on steady-state availability was studied. Service is available when VMM is in the robust state or the failure probable state and the active VM pertains to one of states: the robust state, the failure probable state and the failure detection missing state. Fig.3 shows the results of steady-state availability by varying the VMM rejuvenation trigger interval and the VM aging detection probabilities independently.

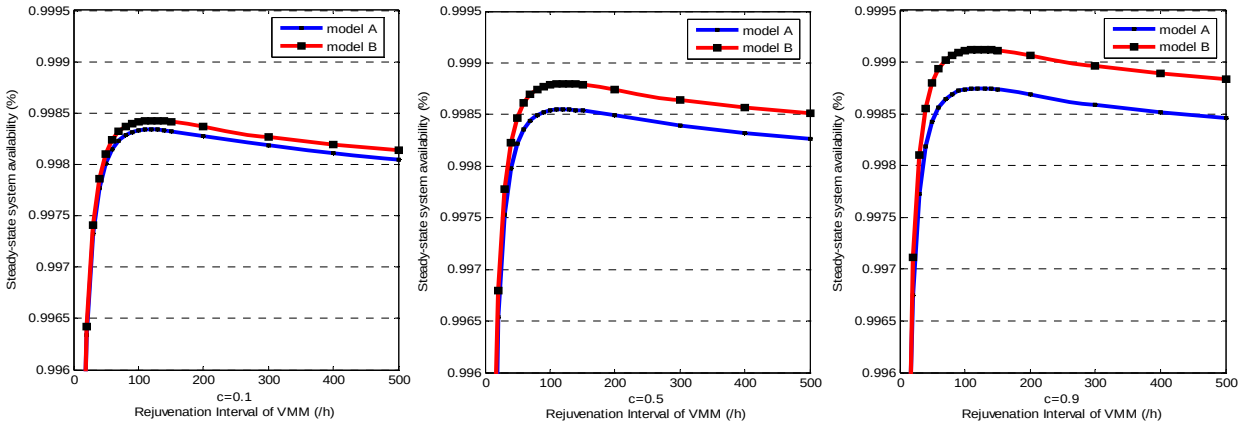


Figure 3. Steady-state availability for both models by varying the rejuvenation interval of VMM and aging detection probability of VM

In the first case, the VM aging detection probability is fixed at 0.1, 0.5 and 0.9 respectively. For an example of the aging detection probability c=0.5, when varying the VMM rejuvenation interval from 5 hours to about 100 hours, we can find that the larger rejuvenation interval lead to the higher system steady-state availability. At a certain rejuvenation interval, in this case $\lambda_{vmm\_reju\_inter} \approx 100$, system steady-state availability is maximized. System availability appears to drop very slowly with the rejuvenation interval greater than 100 hours. We may directly see that there is such a variation tendency for both models. This is caused by the fact that more frequent rejuvenation increases the availability due to the rejuvenation and less frequent rejuvenation also increases the availability caused by software failure. Further, we see that system steady-state availability of model B is almost better than that of model A if the rejuvenation interval increases over 20 hours. This result is caused by

the fact that the time to rejuvenation for the passive replication style is longer than that of the active one because of no time needed for the standby VM loaded in memory with the active replication style.

In the second case, when the VMM rejuvenation interval is fixed, we can find that the higher aging detection probability is better than the lower one in terms of system steady-state availability. This result shows that it is very important to make the aging detection probability more close to 1 in the prediction-based rejuvenation policy. In fact, it is also very difficult and impossible to do this. So in the following discussions, we assume that the highest detection probability is 0.9.

From the above discussions, we can draw a conclusion that model B using the active replication style is better than model A using the passive one in terms of steady-state system availability.

B. Sensitivity Analysis

For an example of Model B, we focus on investigating the impact of two critical parameters, aging detection probability and the VMM rejuvenation interval, on the downtime in this section. The expected total downtime consists of the downtime due to software rejuvenation and the downtime due to system failure. Hence, we also analyze the two downtime components that contribute to the expected total downtime here. In case of software rejuvenation or software failure, the expected downtime over time interval T is calculated as $T * P_{unavail}$, where $P_{unavail}$ is system steady-state unavailability probability due to software rejuvenation or software failure, T is time interval and its value is set to 1,440 minutes.

In the first case of the VMM rejuvenation interval is set to 120 hours, execution results of model B by varying values of the aging detection probability c_{det} are shown in Fig. 4. As the probability c_{det} increases, the expected downtime due to software rejuvenation only slightly increases, however the expected downtime due to software failure and the expected total downtime markedly decrease. Further, we find that the expected downtime of software failure is always greater than that of software rejuvenation regardless of values of c_{det}. Hence, we can draw a conclusion that at a given rejuvenation interval, the recovery process is the main contributor to the expected downtime and the higher the aging detection probability leads to the lower the expected total downtime.

In the second case of the aging detection probability c_{det} is set to 0.9, execution results of model B by varying the VMM rejuvenation interval are shown in Fig. 5. As the rejuvenation interval increases, the downtime due to software rejuvenation firstly rapidly drops and then slightly increases, meanwhile the downtime due to software failure firstly slightly increases and then slightly drops. The variation tendency of the expected total downtime is almost the same as that of the downtime due to rejuvenation. When the rejuvenation interval is 80 hours or less, the rejuvenation process is the main contributor to the expected total downtime with 51.1% to 99.9% of the expected total downtime. Especially when the rejuvenation interval are less than 30 hours, the rejuvenation process contributes to the expected total downtime with 91.7% to 99.9% of the expected downtime. On the other hand, when the rejuvenation interval is more than 80 hours, the failed system with 52.9% to 80.7% of the expected downtime is the greater contributor. This finding is inline with the premise that the use of proactive rejuvenation reduces the chance of system failures caused by software aging. The above results are caused by the fact that more frequent rejuvenation increases the downtime due to the rejuvenation and less frequent rejuvenation also increases the downtime caused by software failure. By finding the point which minimizes the expected downtime, we can solve the optimal rejuvenation interval.

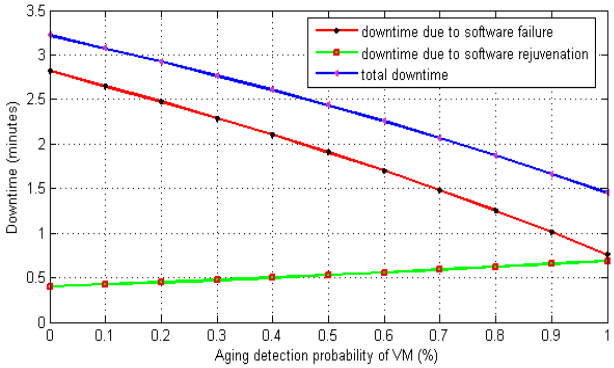


Figure 4. The expected downtime due to software rejuvenation and failure with different aging detection probabilities of VM

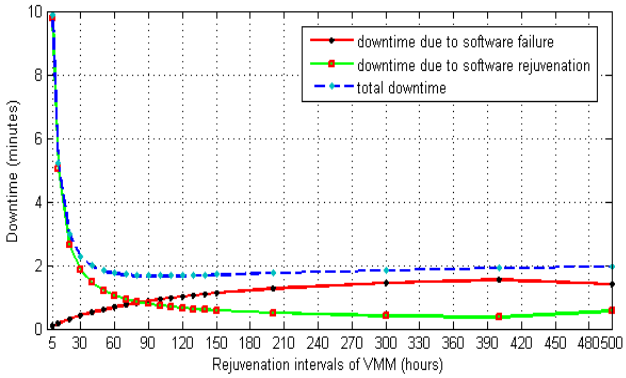


Figure 5. The expected downtime due to software rejuvenation and failure with different rejuvenation intervals of VMM

As analyzed before, the aging detection probability should be no impact on whether transactions lose or not. Hence, we focus on the impact of the VMM rejuvenation interval on the number of transactions lost. When VMM is rejuvenated or repaired, transactions lose because of VMM shutting down all the hosted VMs prior to the rejuvenation or repair regardless of the execution states of the VMs. The expected number of transactions lost due to VMM rejuvenation and VMM repair can be computed from the throughputs of the transitions T_{vmm_reju} and T_{vmm_repair} for each SRN model. We will execute model B again to analyze the expected number of transactions lost with different VMM rejuvenation intervals. Results with

varying rejuvenation intervals and the fixed value of 0.9 for detection probability c_{det} are shown in Fig. 6.

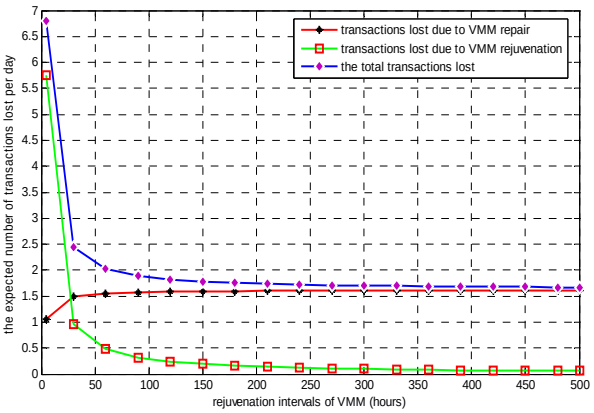


Figure 6. The expected number of transactions lost with different rejuvenation intervals

As seen from Fig.6, the expected number of transactions lost due to VMM rejuvenation is monotone decreasing with the increasing rejuvenation interval. The higher rejuvenation rate (i.e. the rejuvenation interval is less than 30 hours) has a significant impact on the expected number of transactions lost. However, when the rejuvenation interval increases to more than 30 hours, VMM repair instead of VMM rejuvenation is the new greater contributor to the expected number of transactions lost. Further, when the rejuvenation interval increases from 80 to 500, the expected number of transactions lost due to rejuvenation gradually levels off at about 0.159. When the rejuvenation interval increases to infinity, this means that VMM has no rejuvenation operation. The expected number of transactions lost will be equal to the number of transactions lost associated with VMM repair. Form the above analysis, we can find that the rejuvenation interval has almost no impact on the expected number of transactions lost only if it is greater than a proper value got from the solution of SRN model.

C. *Model B VS. Other Models*

To further validate the effect of our models and rejuvenation policies, we consider the existing models with different policies including no rejuvenation, just the VMs rejuvenation using the prediction-based rejuvenation policy, just the VMM rejuvenation using the time-based rejuvenation policy, and both the VMM and the VMs rejuvenation with the time-based policy. Further, we compare the effect of these policies with model B, and the results are shown in Fig. 7, where the aging detection probability of the VMs used in the prediction-based policy is fixed at 0.9 and the VM interval used in the time-based policy is 120 hours.

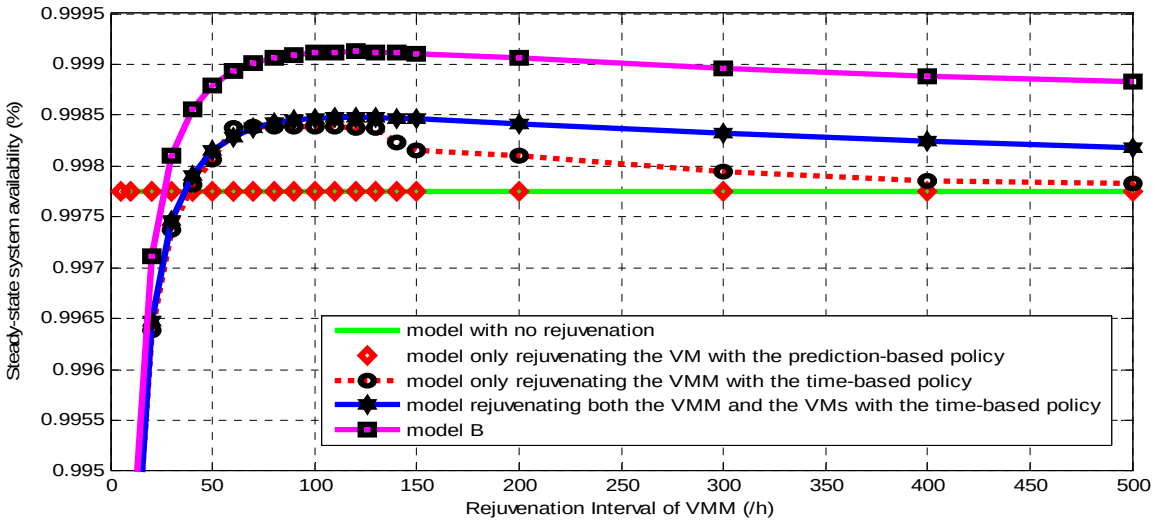


Figure 7. Comparison of rejuvenation effects using different rejuvenation policies

From Fig. 7, the findings we got are as followings:

- There is no system availability improvement in case of just rejuvenating the VMs by comparison to the case of no rejuvenation. However, there is an obvious system availability improvement in case of just rejuvenating the VMM by comparison to the case of no rejuvenation. The result shows that due to the availability of the upper-level VMs depending on the availability of the lower-level VMM, the extreme limit of system availability depends on the maximum VMM availability. Thus, rejuvenating the VMM is the most efficient way of improving system availability.
- There is an obvious system availability improvement in case of rejuvenating both the VMM and the VMs regardless of rejuvenation policies used by comparison to the case of just rejuvenating the VMM. The results show that the further system availability improvement depends on simultaneously improving the availability of both of the VMM and the VMs. Further, comparing our policy with the time-based policy applied to both the VMM and the VMs, we find that our policy is much better than the competitor.

VI. CONCLUSIONS

We have presented and analyzed comprehensive availability models for a class of system with deployment of virtualization technology and software rejuvenation. Results of the first experiment showed two models were with the same variation tendency and the model with the active replication style is obviously better than that of the model with the passive one in terms of system steady-state availability. Further, for an example of model B, we finished two other experiments in order to analyze system rejuvenation and repair process by varying two critical parameters, the VM aging detection probability and the VMM rejuvenation interval. Experimental results showed that the aging detection probability had a very important impact on the expected downtime and the higher the aging detection probability led to the lower the expected total downtime. However, we also showed the aging detection probability had no impact on whether transactions lost or not. Under a given parameter value for the aging detection probability, we observed that more frequent rejuvenation increases the downtime due to the rejuvenation and less frequent rejuvenation also increases the downtime caused by software failure. By finding the point which minimizes the expected downtime, we could solve the optimal rejuvenation interval. Moreover, we also observed that a proper VMM rejuvenation interval has almost no impact on the number of transactions lost and the repair process is the main contributor to the expected number of transactions lost.

In the future work, we will discuss some methods to carefully determine the optimal combinatory of the VMM rejuvenation interval and the VM aging detection probability so as to achieve higher steady-state availability and lower downtime.

ACKNOWLEDGEMENT

This work is funded by a grant from the Natural Science Foundation of Jiangsu Province, China under grant No. BK2011023.

REFERENCE

[1] Y. Huang, C. Kintala, N. Kolettis, and N.Fulton, "Software Rejuvenation: Analysis, Module and Applications," *Proc. Int'l Symp. Fault-Tolerant Computing*, pp. 381-391,1995.

[2] K. Vaidyanathan, R.E. Harper, S.W. Hunter, K.S. Trivedi, "Analysis and implementation of software rejuvenation in cluster systems," *ACM SIGMETRICS Performance Evaluation Review, Joint International Conference on Measurement and Modeling of Computing Systems*, pp. 62-71, 2001.

[3] Wang,D.Z., Xie, W, Trivedi, K.S., "Performability analysis of clustered systems with rejuvenation under varying workload," *Performance Evaluation*, vol. 64, pp.247-265,2007.

[4] Y. Liu, K. Trivedi, Y. Ma, J. Han, and H. Levendel, "Modeling and analysis of software rejuvenation in cable modem termination systems," *The 13th International Symposium on Software Reliability Engeineering (ISSRE)*, pp.159-172, 2002.

[5] Y. Liu, K. Trivedi, Y. Ma, J. Han, and H. Levendel, "A proactive approach towards always-on availability in broadband cable networks," *Computer Communications*, vol. 28, pp.51-64,2005.

[6] L. Li, K.Vaidyanathan, and K.S. Trivedi, "An Approach to Estimation of Software Aging in a Web Server," *Proc. Int'l Symp. Empirical Software Eng. (ISESE 2002)*, pp.45-52, 2002.

[7] F. Salfner, K. Wolter, "Analysis of service availability for time-triggered rejuvenation policies," *Journal of Systems and Software*, vol. 83, pp.1579-1590, 2010.

[8] F. Machida, D. Kim, and K. Trivedi, "Modeling and Analysis of Software Rejuvenation in a Server Virtualized System," *Proc. of 2nd Workshop on Software Aging and Rejuvenation (WoSAR2010)*, pp.1-6, 2010.

[9] Thein T, Park J S, "Availability Analysis of Application Servers Using Software Rejuvenation and Virtualization," *Journal of Computer Science and Technology*, vol. 24, no.2, pp. 339-346, 2009.

[10] K. Kourai, "Fast and Correct Performance Recovery of Operating Systems Using a Virtual Machine Monitor," *Proc. of the 7th ACM SIGPLAN/SIGOPS international conference on Virtual execution environments*, vol.46, no.7, pp. 99-110,2011.

[11] Y. Bao, X. Sun, and K. S. Trivedi, "A Workload-Based Analysis of Software Aging, and Rejuvenation," *IEEE Transactions on Reliability*, vol.54, no. 3, pp. 541-548, 2005.

[12] K. Trivedi, K. Vaidyanathan, K. Goseva-Popstojanova, "Modeling and Analysis of Software Aging and Rejuvenation," *Proc. of 33rd Annual Simulation Symposium*, IEEE Computer Society, pp. 9-24,2000.

[13] T. Thein, S. Chi and J. Park, "Availability Modeling and Analysis on Virtualized Clustering with Rejuvenation," *Int'l Journal of Computer Science and Network Security*, vol.8, no. 9, pp.72-80, 2008.

[14] K. Kourai and S. Chiba, "A fast rejuvenation technique for server consolidation with virtual machines," *Proc. Int'l Conf. on Dependable Systems and Networks (DSN 2007)*, pp. 245-255, 2007.

[15] K. Kourai and S. Chiba, "Fast software rejuvenation of virtual machine monitor," *IEEE Trans. on Dependable and Secure Computing*, vol.8,no.6,pp.839-851,2011.

[16] A. Rezaei and M. Sharifi, "Rejuvenation high available virtualized systems," *Proc. of 5th International Conference on Availability, Reliability and Security (ARES2010)*, pp. 289-294, 2010.

[17] Yi Yang, Lichao Wang, Rui Kang, "Discretization model of instantaneous availability for continuous-time systems", *Journal of Computers*, vol.7, no.4,pp.977-981,2012.

[18] Yanyan Hu, Xiang Long, Jiong Zhang, "I/O Behavior Characterizing and Predicting of Virtualization Workloads", *Journal of Computers*, vol.7, no.7, pp. 1712-1725,2012.

[19] Yunpeng Xiao, Guangxia Xu, Yanbing Liu, Bai Wang, "A Metadata-driven Cloud Computing Application Virtualization Model," *Journal of Computers*, vol.8, no.6, pp. 1571-1579,2013.

[20] Okamura,H., Dohi, T., "Comprehensive evaluation of aperiodic checkpointing and rejuvenation schemes in operational software system," *Journal of Systems and Software*, vol. 83, pp. 1591-1604,2010.

[21] K. Vaidyanathan, K. S. Trivedi, "A Comprehensive model for software Rejuvenation," *IEEE Transaction on Dependable and Secure Computing*, vol.2, no.2, pp. 124-137, 2005.

[22] M.M. Hosseini, R.M. Kerr and R.B. Randall, "An

Inspection Model with Minimal and Major Maintenance for a system with Deterioration and Poisson Failures," *IEEE Trans. Reliability*, vol. 49, no.1, pp.88-98, March 2000.

[23] Letian Jiang, Guozhi Xu, "Modeling and analysis of software aging and software failure," *Journal of Systems and Software*, vol.80,no.4, pp. 590-595, 2007.

[24] C. Hirel, B. Tuffin, K. Trivedi, "SPNP: Stochastic Petri Nets. Version 6.0," *Proc. of the 11th International Conference on Computer Performance Evaluation: Modeling Techniques and Tools*, pp. 354-357, 2000.

[25] J. K. Muppala, G. Ciardo and K. S. Trivedi, "Stochastic Reward Nets for Reliability Prediction," *Communications in Reliability, Maintenability and Serviceability*, pp. 9-20, July 1994.

Jian Xu received a Ph.D. in Computer Science in 2007 from Nanjing University of Science and Technology, Nanjing, China. Now he holds the position of an associate professor at Nanjing University of Science and Technology. His research interests are software engineering, particularly monitoring and rejuvenation of smoothly degrading systems, and he has published about 20 papers in journals and refereed conference proceedings in those areas. He is a member of ACM and IEEE.

Xuefeng Li is currently a master candidate of Nanjing University of Science and Technology, Nanjing, China. His major research interests are software rejuvenation and virtualization.

Yi Zhong is currently a Ph.D. candidate of Nanjing University of Science and Technology, Nanjing, China. Her major research interests are software rejuvenation and virtualization.

Hong Zhang is a professor at Nanjing University of Science and Technology, China. His research interests are information security, specially in wireless sensor network security and cloud security, and he has published more than 100 papers in journals and refereed conference proceedings in those areas.

Study on Passenger Flow Simulation in Urban Subway Station Based on Anylogic

Yedi Yang
School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou, China
Email: 780127184@qq.com

*Jin Li
School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou, China;
Contemporary Business and Trade Research Center of Zhejiang Gongshang University, Hangzhou, China
*Corresponding author: jinli@mail.zjgsu.edu.cn

Qunxin Zhao
College of Foreign Languages, Zhejiang Gongshang University, Hangzhou, China
Email:1113197351@qq.com

***Abstract*—In this paper, taking Hangzhou Metro Line 1 Wulin Square Station for example, we dynamically optimize the opening number of the entrance ticket windows at the station based on Anylogic pedestrian library, and study the impact of some parameters e.g. the pedestrian arrival rate and the opening number of the ticket windows in peak and off-peak periods, etc., on the average queuing number and utilization rate of the ticket windows. The aim is to provide a favorable reference and decision support tools for planners, designers, and operators. The simulation results show that for the off-peak period, that is, when the pedestrian velocity reaches to 1500/hour, opening two ticket windows can achieve the best average queuing number and the utilization rate of the ticket windows, and at the peak period, i.e. the pedestrian velocity is about 2500/hour, opening four ticket windows is the best strategy.**

***Index Terms*—urban subway, pedestrian simulation, dynamic optimization, AnyLogic, queuing**

I. INTRODUCTION

In recent years, China's urban rail transit is developing in an unprecedented speed. According to the relevant statistics, in Mainland China, there have been 33 cities planning to construct rail transit, in which 28 cities have been approved. Hangzhou Metro Line 1 was opened on Nov.24, 2012, which is Hangzhou, even Zhejiang's first subway line; Beijing opened four new Metro Lines on Dec.30, 2012, which were: Line6, Line8, the northern section of Line 9 and Line 10.

Undoubtedly, the subway relieves the traffic pressure to some extend, facilitates the movement of residents. We learned it from Hangzhou Hong Kong Metro Corporation Limited that on the first month of trial operation, the train ran totally 11,385 times. Averagely, it ran 379.5 per day, including 392 extra trains in weekdays' peaks. The total number of passengers was up to 4,378,667, and the daily amount was 14.5956 million. The maximum which appeared on December 9, 1999 (Sunday) was reaching 219,000. There are 30 sites and more than 200 ticket vending machines on Metro Line1, and a total of 1,653,696 one-way tickets were sold. The 3 stations with highest passenger flow are in turns as follows: Wulin Square, Hangzhou Railway Station, Lung Bridge.

However, with the growing of the passenger flows, the problem of people's queuing for tickets becomes more and more severe. The time they spend on ticket queuing, and the number of queuing have the direct impact on passengers' experience of rail transit. The ticket sellers in the ticket window system contact with passengers directly, so the quality of their service has a great influence on the evaluation given by passengers. Therefore, in order to reduce the passengers' queuing time, the prominent concern is to optimize the queuing system by opening ticket windows dynamically and reasonably in the process of operation which of course should at a reasonable cost. It can not only improve the competitiveness but also improve the quality of the service.

At present, many scholars have started carrying out researches concerning rail transit science and they have already been doing a lot of work. The former research can be divided into three categories according to the usage of the different methods. The first category is to establish a mathematical model to do the research of the railway ticket window system based on queuing system and routing optimization problem[1-10]. For example, Jitao Li and JunFeng Yang [1] from Dalian Jiaotong University who used the theory of queuing model to analyze the characteristics of the railway station ticket window queuing system, established a ticket windows optimization model based on the acceptable time of waiting, and gave a model of algorithm and processes.

doi:10.4304/jsw.9.1.140-146

Based on how to optimize the facilities, Qiwen Jiang [2] from Beijing Jiaotong University introduced the queuing theory, and correspondingly, the mathematical model. His study focused on the station automatic ticket machines, the station stairs and the station channel so as to optimize the configuration of the facility. In order to attract more passengers and improve operational efficiency, they provide their best service. The second category is to acquire the results by using simulation software such as Anylogic, simwalk, based on the theories such as Agent, queuing system [11-21]. For example, Lu Yu and Xi Zhang [11] from Beijing Jiaotong University used Anylogic simulation software systematically to analyze the layout of Beijing Xizhimen subway station rail transportation hub, passengers organizations streamline, and found the bottleneck of a guest stint distribution and also proposed some suggestions. Zhao Yafang [12] established a evaluation model of the layout of ticketing equipment and the configurable number by applying the method of queuing theory, which can analyze the arrangement form of the automatic ticketing equipment at the station and then raise up the proper form according to the place of the station. Based on the simulation software, Anylogic, the evaluation model can be verified. The third category is to do the simulation study by establishing physics models. For example, Guangzhou Transport Planning Institute's Yunbin He [21], through constructing a pedestrian simulation platform which based on the physical model of the hub, analyzed the relationship between the window average queuing number and ticket demand, and thus to know how many ticket windows are needed according to different queuing time. This article we dynamically optimize the number of the station pit mouth open ticket windows , based on Anylogic pedestrian library , taking Hangzhou Metro Line 1 Wulin Square Station as the background, and research the impact of parameters on the number of queuing and utilization of the window according to the pedestrian arrival rate and the number of the ticket windows open in peak and off-peak periods, providing a favorable reference for planners, designers, operators and decision support tools. At last, we come up with an improvement program which aims at the unreasonable facts after evaluating the rationality of the automatic ticketing equipment and the configurable number. And then the improvement program is verified.

This paper is organized as follows. The introduction to the Anylogic simulation principle, the scene of simulation and modeling process is described in Section 2. In Section 3, the specific analysis to the results of simulation is given. Finally, the concluding remarks are concluded in Section 4.

II. PRINCIPLES AND METHODS

A. Simulation Software

AnyLogic simulation software is used to create a professional virtual prototyping environment, and it is also designed for discrete, continuous and mixed behavior of complex systems. The AnyLogic can quickly build design system simulation model (virtual prototyping) and the external environment, including the physical equipment and operating personnel. Its applications include: control systems, traffic, dynamic systems, manufacturing, supply lines, logistics departments, telecommunications, networks, computer systems, machinery, chemicals, sewage treatment, military, education etc. The AnyLogic is powerful and flexible, and can offer a variety of modeling methods: object-oriented modeling method based on UML language, flowchart modeling method based on the square of Statecharts (state machine), which can be divided into ordinary and mixed, differential and algebraic equations, Java modeling.

Anylogic also includes the following standard databases which can be used to build the models rapidly. The Enterprise Library is mainly used to simulate discrete events which are related to manufacturing industry, supply chain, logistics resources, medical treatment etc. Solid models (trades, customers, products, components, vehicle etc.), technological processes (the typical working process, including wait, delay, resource utilization) can be built with the help of Enterprise Library. The Pedestrian Library concentrates on simulating a physical environment. It can be used to build a structure (Railway station, safety check etc) or a street which is full of people. The models can not only collect data such as density of pedestrians in different regions, but also calculate the efficiency of the load in service point. The simulation of interaction of pedestrians is complex behaviors' agent. However, The Pedestrian Library provides an advanced use interface which can build flow-process diagram of pedestrian quickly. The Rail Yard Library can help to build various railway shunting models and make it visually. Railway shunting model can combine discrete events and agents in order to simulate loading and unloading, allocating resources, maintaining business processes and other transport activities. Except those standard resources, users can build their own databases according to their own needs.

B. Simulation Scenarios

In this paper, we establish a subway entrance pedestrian distribution model, taking the Wulin Square Station in Hangzhou Metro Line 1 as the background, by designing different simulation environments and simulating passengers at the station distribution, to study the utilization of the facilities in the subway station and then to analyze. So we can provide support for the optimization of the rail transport. Figure 1 is a diagram of Hangzhou Metro Line 1 Wulin Square station. This station is an island platform with three layers. It looks like a rectangular solid with a length of 161.75 meters, a width of 36.6 meters and a depth of 27 meters.

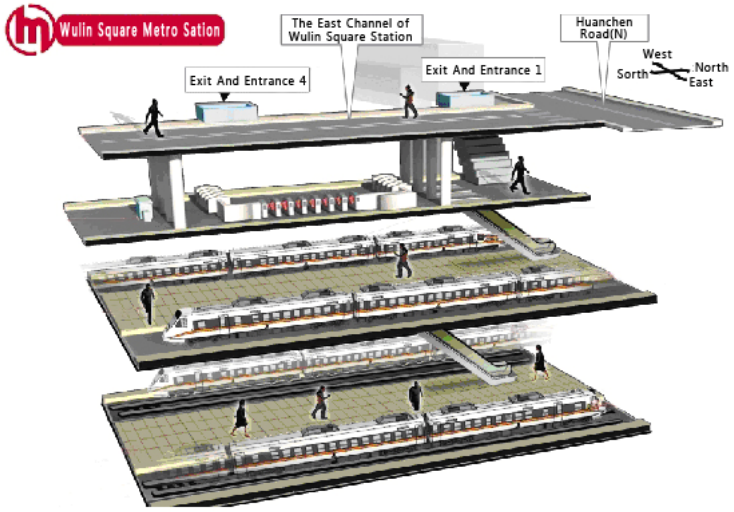


Figure 1. Space diagram of Hangzhou Metro Line 1 Wulin Square station in China.

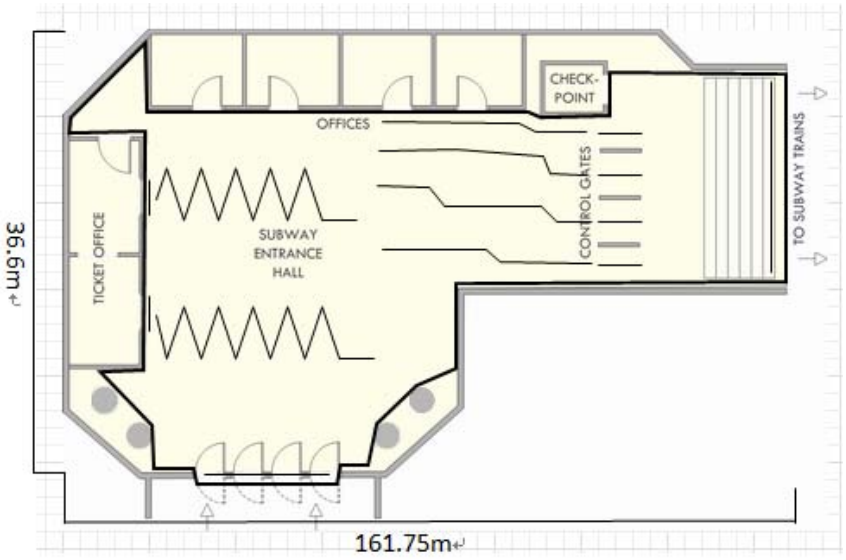


Figure 2. Subway entrance layout in the Anylogic simulation environment.

The top layer is the station hall; the middle layer is the device layer, and the following is the platform layer. This article will chose the top-level concourse level entrances as the simulation scene to simulation study, in Figure 2 is the site No. 4 in the Anylogic simulation environment at the entrance layout.

C. *Research Principle*

This article aims at evaluating comprehensively parameters such as pedestrian arrival rate and the number of the ticket windows opens which impact on queue length and utilization of the window, given the number of different scenarios, the best ticket booth. Wherein the average queue length is calculated as follows:

$$L_q = \sum L_{q,i} / N_i \tag{1}$$

Where L_q Indicates the queue's length, $L_{q,\mathrm{i}}$ is queue's length at the point of i, N_{i} indicates the total number of time points at the simulation. The window utilization calculation formula is as follows;

$$\partial = T_{\mathrm{m}} / T \tag{2}$$

Where ∂ indicates windows utilization, T_{m} is the working time for the window at simulation, T represents the total time at simulation.

D. *Simulation Process*

Wulin square, the subway no. 4 has four brake machine gates, the six automatic ticket offices (basically only four open) on the presence of the rush hour, the simulation environment is divided into peak and off-peak

periods into two categories; the difference is the pedestrian arrival rate parameter settings. Combined with the actual passenger traffic, pedestrians to reach the peak of the rate is set to 2500/hour, and the peak of the pedestrian arrival rate is set to 1500/hour. The number of the port gates fixed to 4, the number of the ticket windows at different times from 1 to 6, setting the rate of pedestrians from 500-2500/hour, 500 rate interval, research in different pedestrian arrive rate, opening how many the ticket windows to ensure appropriate average queue length, and to get the maximum utilization of facilities.

When Passengers arrive at the station, someone who has public transportation card can enter into the station directly, but others should queue up for the ticket first. According to the site statistics, about 85% of the passengers do not need to queue up for the ticket, while 15% passengers have to wait in line. As shown in Figure 3 it is the inbound module map; queuing time for which the ticket windows obey the triangular distribution Triangular (15 * second (), 25* second (), 35*second ()), the service time of the wicket obey uniform (2.0 * second (), 3.0 * second ()) distribution.

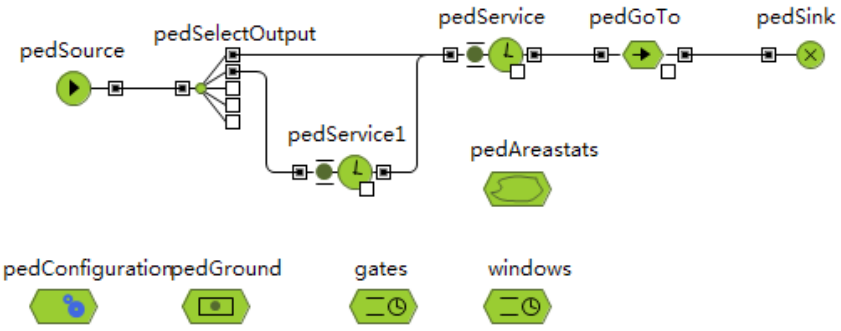


Figure 3. The subway entrance stint block diagram

TABLE I.
QUEUE LENGTH AND WINDOW UTILIZATION RATE IN THE 500 - 2500/HOUR WITH DIFFERENT WINDOW NUMBER

Rate（/hour） / Window's number	500	1000	1500	2000	2500
1	1 60%	15 93.3%	53 98.3%	75 100%	80 100%
2	0 10%	0 18%	2 65%	17 96.7%	47 100%
3	0 7.4%	0 14.3%	0 22.4%	1 28.3%	27 93.3%
4	0 4.3%	0 8.4%	0 15.3%	0 20.4%	20 86.7%
5	0 1.2%	0 4.3%	0 5.2%	0 7.1%	0 9.8%

III. SIMULATION AND DISCUSSION

A. *Analysis of the Simulation Results at Different Pedestrian Arrival Rate*

We simulated the queuing situation and the utilization rate of window under the following circumstances. The figure in the upper part of the sheet represents the average length of the queue at a certain window and a certain rate, and the figure in the lower part of the sheet represents the utilization rate of windows under corresponding circumstance.

As you can see from the sheet, different numbers of windows at different pedestrian arrival rate have an

influence on the length of queue and the utilization rate of window. Obviously, on one hand, the more the ticket windows open, the shorter the length of queue will be and the lower the utilization rate of window will be. On the other hand, at a certain number of the ticket windows, the higher of pedestrian arrival rate, the longer the length of queue will be, accordingly, the utilization rate of window will be higher.

If analyzed the dates in the sheet separately, we found that the length of the queue and the utilization rate of window have positive correlation. But we hoped it could be passive correlation, that is, when the length of queue is shorter, the utilization rate of window will be higher. As far as we can see, it is not a fact. So, we are considering choosing the number of ticket windows that has the highest utilization rate within an acceptable length of queue. Then, we will analyze situations concretely, that is, in peak hours (the pedestrian arrival rate is 2500/hour) and in off-peak hours (the pedestrian arrival rate is 1500/hours).

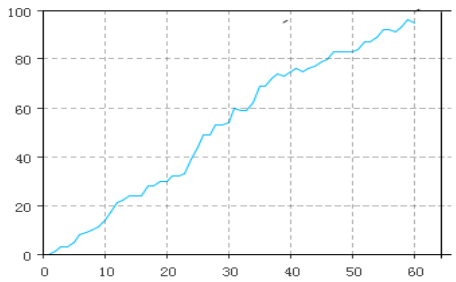
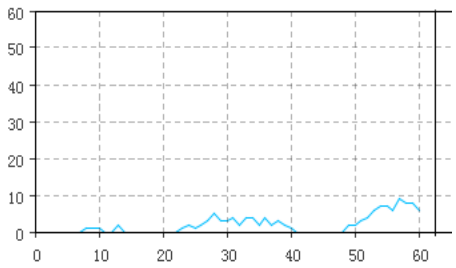
B. Analysis of the Simulation Results in Peak and Off-peak Hours

In off-peak hours, the pedestrian arrival rate is 1500/hour, the simulation results are shown as follows:

In off-peak hours, compared the utilization rate and the average passengers waiting in line, we realized that when there is one ticket window, the utilization rate is 98.33%, while there are two ticket windows, the utilization rate is 65%. Compared the utilization only, we could find out easily that the former is much larger than the letter. However, if we combine the number of passengers with it, we could find that the average passengers in situation 1 are 52.05 and the letter are only 2.02. When there are 3 ticket windows, according to the result of simulation, it can hardly form a line. Therefore, taking the utilization rate and the average passengers both into consideration, it is best to open two ticket windows in off-peak hours.

Figure 4 shows the simulation diagram when the ticket window number is 2. At its peak, the pedestrian arrival rate of 2500/hour number of different ticket booth under the simulation results shown in Table 3.

TABLE Ⅱ.
QUEUING AND UTILIZATION OF THE WINDOW WHEN THE TICKET WINDOW NUMBER IS IN THE OFF-PEAK PERIODS (1500/HOUR)

The Number of Ticket Windows	The Average Number of Queuing Passenger	The Utilization Rate of Ticket Windows	Line Chat of Queue Number
1	52	98.3%	
2	2	65%	
3	0	22.4%	—

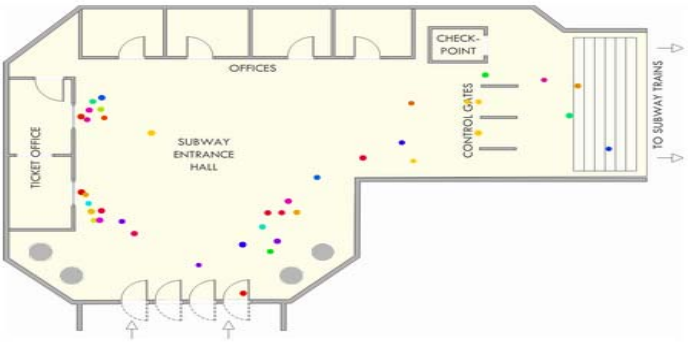
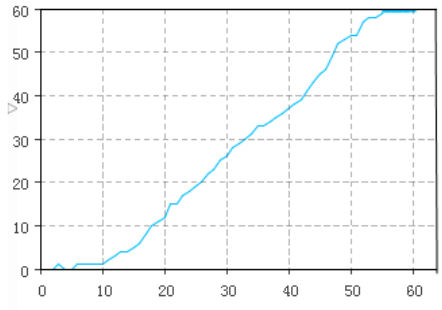
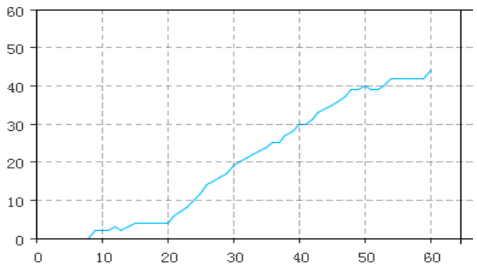


Figure 4. Off-peak hours queuing

TABLE III.
THE PEAK OF THE TICKET BOOTH NUMBER IS NOT THE SAME QUEUE AND WINDOW UTILIZATION

The Number of Ticket Windows	The Average Number of Queuing Passenger	The Utilization Rate of Ticket Windows	Line Chat of Queue Number
3	27.72	93.30%	
4	19.58	86.70%	
5	0	9.8%	—

When compared with the number of ticket windows in scenarios 3 and 4. Although there are more people queuing, it is a normal phenomenon considering the fact which will appear in the peak period. Utilization, the ticket window number 3 is slightly higher than the 4, and from the number of queuing point of view, the ticket window number 4 is better than 3. When the ticket window number is 5, we find that it hardly forms a queue in front of the ticket windows, but the window utilization is quite low. Therefore, the paper considers that open the four ticket window better during peak periods.

IV. CONCLUSION

We used the Anylogic to study the passenger flow at the entrance of Wulin Station, and after contrasting the different numbers of ticket windows according to different pedestrian arrival rate, we can draw a conclusion: During peak hours (the pedestrian arrival rate is 2500/hour), it is better to open 4 ticket windows. During off-peak hours (the pedestrian arrival rate is 1500/hour), it is better to open 2 ticket windows. As time is limited and the other subway lines in Hangzhou

haven't been opened, the statistics of pedestrian arrival rate in peak and off-peak hours haven't been exactly determined in this article. The simulation model we used in this article can also be used in other subways' entrances, which can easily change the pedestrian arrival rate. Therefore, a more extensive study can be carried out on the distance between the ticket window and the ticket entrance. There is specific introduction about the application of the software in the second section.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their valuable comments. This work was supported in part by the Contemporary Business and Trade Research Center of Zhejiang Gongshang University which is the Key Research Institute of Social Sciences and Humanities Ministry of Education (Grant No.12JDSM16YB), Humanities and Social Sciences Foundation of Ministry of Education of China (Grant No. 12YJC630091), Zhejiang Provincial Natural Science Foundation of China (Grant No. LQ12G02007), the National Natural Science Foundation of China (Grant No.71171178), and Zhejiang Provincial Commonweal Technology Applied Research Projects of China (Grant No. 2013C33030), National Training Programs of Innovation and Entrepreneurship for Undergraduates (No.3080JQ43130 17).

REFERENCES

[1] Jitao Li, JunFeng Yang, Jia Fu, "Simulation Optimization of the Queuing System in front of Railway Station Ticketing Office," *Railway Transport and Economy*, pp.67-70, December 2007.

[2] Qiwen Jiang, "Research on Allocation Optimization for Entering and Leaving Facility in Urban Railway Transit Station," In: *Beijing Jiaotong University*, 2009.

[3] Yehui Sun, "Subway window to buy a ticket of the queuing system simulation," *China Water Transport (second half)*, pp.195-197, February 2008.

[4] Zhongkai Wu, "HarBin's station ticket window allocation simulation," *Railway Transport and Economy*, pp.50-53, May 2012.

[5] Kangzhou Wang, Na Li, Zhibin Jiang, "Queuing system with impatient customers: A review," Service: pp.82 – 87, 2010.

[6] Susan H. Xu, Long Gao, Jihong Ou, "Service Performance Analysis and Improvement for a Ticket Queue with Balking Customers," *Management Science*, vol. 53, no. 6 , pp.971-990, June 2007.

[7] Jin Li, "Vehicle routing problem with time windows for reducing fuel consumption," *Journal of Computers*, vol.7, no.12, pp.3020-3027,2012.

[8] Jin Li, Peihua Fu, "A label correcting algorithm for dynamic tourist trip planning," *Journal of Software*, vol.7, no.12, pp.2899-2905, 2012.

[9] Jingwen Huang, Hongguang Li," Process Goose Queue Methodologies with Applications in Plant-wide Process Optimization," *Journal of Computers*, vol.7, no.10, pp.2462-2470, 2012.

[10] Hui Zeng, "Efficient Graduate Employment Serving System based on Queuing Theory," *Journal of Computers*, vol.7, no.9, pp.2176-2183, 2012.

[11] Lu Yu, Xi Zhang, "Assisted Decision-making for Incoming Passenger Flow Management at Urban Rail Transit Hub Stations," *Logistics Technology*, pp.135-138, September 2011.

[12] Yafang Zhao, "Research on Simulation Evaluation of Ticket Vending Equipment's Layout and Configuration in Railway Passenger Station," In: *Beijing Jiaotong University*, 2010.

[13] Hongxu Li, Haiying Li, Xiao Fan, Xinyue Xu, "Anylogic-based simulation analysis and evaluation of subway stations assemble capacity," *Railway Computer Application*, vol.21, pp.48 -50, 2012.

[14] Hong Cao, JiuZhou Wang, JianXin Li, "Application case of traffic simulation in metro engineering design," *China Investigation & Design*, pp.66-69, 2011.

[15] Yanqing Xue, Xi Zhang, "Analysis on optimizations of passenger flow organizations in Beijing South Station based on Anylogic simulation," *Railway Computer Applications*, pp.5-8, February 2012.

[16] Felisa J. Vázquez-Abad, Lourdes Zubieta, "Ghost Simulation Model for the Optimization of an Urban Subway System," *Discrete Event Dynamic Systems*, vol 15, no 3, pp.207–235, September 2005.

[17] Hao Jiang , Wenbin Xu, Tianlu Mao, Chunpeng Li, Shihong Xia, Zhaoqi Wang, "A semantic environment model for crowd simulation in multilayered complex environment," In: *Proceedings of the 16th ACM Symposium on Virtual Reality Software and Technology*, pp:191-198, 2009.

[18] Bernd Heidergott, Felisa J. Vázquez-Abad, "Gradient estimation for a class of systems with bulk services: A problem in public transportation," *ACM Transactions on Modeling and Computer Simulation*, vol 19, no 3, June 2009.

[19] Glenn I. Hawe, Graham Coates, Duncan T. Wilson, Roger S. Crouch, "Agent-based simulation for large-scale emergency response: A survey of usage and implementation," *ACM Computing Surveys*, vol 45, no 1, November 2012.

[20] Bikramjit Banerjee, Landon Kraemer, "Evaluation and comparison of multi-agent based crowd simulation systems," In: *Agents for games and simulations II*, pp: 53-66, 2011.

[21] Yunbin He, Hai Ji "Study on plan Method of Fine profit Ticket window in Passenger Transport Hub," *Traffic & Transportation (Academic Edition)*, pp.63-65, January 2012.

Object Tracking Based on Camshift with Multi-feature Fusion

Zhiyu Zhou
College of Information, Zhejiang Sci-Tech University, Hangzhou, China
Email: zhouzhiyu1993@163.com

Dichong Wu
Business Administration College, Zhejiang University of Finance & Economics, Hangzhou, China
Email: 1601441815@qq.com

Xiaolong Peng
College of Information, Zhejiang Sci-Tech University, Hangzhou, China
Email: wheelo@163.com

Zefei Zhu
College of Mechanical Engineering and Automation, Zhejiang Sci-Tech University, Hangzhou, China
Email: zzf.3691@163.com

Kaikai Luo
College of Information, Zhejiang Sci-Tech University, Hangzhou, China
Email: anhuiluokai@foxmail.com

***Abstract*—It is very hard for traditional Camshift to survive of drastic interferences and occlusions of similar objects. This paper puts forward an innovative tracking method using Camshift with multi-feature fusion. Firstly, SIFT features and edge features of the Camshift in RGB space are counted to reduce the probability of disruption by occlusion and clutter. Then, the texture features are collected to resolve the problems of analogue interference, the texture similarity between current frame and previous frames are calculated to determine the object area. The paper also describes the GM(1,1) prediction model, which could solve the occlusion problems in a novel way. Finally, through the motion trajectory, it can anticipate the exact position of the object. The results of several tracking tasks prove that our method has solved problems of occlusions, interferences and shadows. And it performs well in both tracking robustness and computational efficiency.**

***Index Terms*—Camshift, GM(1,1), SIFT features, Object tracking**

I. INTRODUCTION

Mean Shift [1-2] has been widely used in the field of object tracking, yet lacking of the necessary model updates, in addition of the fixed window width of kernel function, both of them will have evil impacts upon the accuracy of tracking. Camshift [3] appears as an improved algorithm which could automatically adjust the window size to fit the object, thus solving the troubles of scale variations. However, the traditional Camshift exists the following disadvantages:

- The tracking results could be very easily disrupted by similar objects.
- The lack of motion behavior prediction, which might lead to a failure of object tracking, especially when the objects move too fast, running beyond the searching scale of the previous frames, or being interfered by other objects.
- The searching window would shrink to a tiny point when the tracking objects get lost.
- Tracking results are susceptible to the illumination changes.

Dozens of scholars have shown interests on the solutions of these problems. In order to overcome the impacts of scale variations and partial occlusions, Shen Xuanjing [4] introduced a kernel density estimation through a model of color distribution, tracking the moving objects with the image moments by Camshift. Li Chao [5] overcame occlusions and information losses of image likewise, but more elegantly, he proposed a face tracking method based on Haar features detection, improving Camshift algorithm with a weighted histogram probability model. In order to conquer the influence of analogue interferences and scene illumination changes, Sun Hongguang [6] combined the color and motion information together into the Camshift, tracking objects adaptively with an optimized particle filter. Wang Zhaowen [7] put forward a Camshift guided particle filter for object tracking, and he incorporated the particles into the probabilistic framework for proposal distribution. In

Manuscript received April 29, 2013.
Corresponding author: Zhiyu Zhou

doi:10.4304/jsw.9.1.147-153

order to handle the issues of fast movement and strong background disturbances about objects, Wang Xin[8] embedded the improved Camshift algorithm into particle filter, he redistributed the random particle samples, whereby the objects could move toward their maximal posterior probability density. However, particle filter needs collecting considerable amount of particles to approximate complex filtering distribution throughout the entire sampling process, which might give rise to a tremendous computation complexity. Li Jianhong [9] got rid of similar color interference of objects with robustness, who put forth an improved algorithm with SURF. And Exner David [10] presented a multi-histogram accumulation to accomodate complex object changes, handling ambiguous cases of partial or full occlusions. Chu Hongxia [11] combined Camshift with frame difference, can track motion object instantly and accurately. Liang Juan [12] has improved the Camshift effect by a large scale with the Kalman filter, which was used to estimate initial parameters of moving object and adjust iteratively to approach location of each objects. Based on an improved Camshift and Kalman filter, Peng Juanchun [13] proposed a real-time hand tracking system for humanoid robot with a stereo vision method.

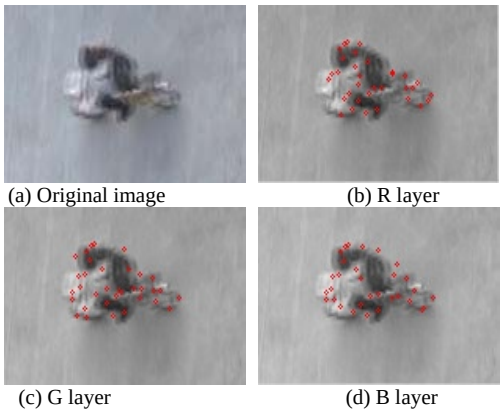
Kalman filter presumes smoothness in relevant motion, which makes possible the process of the modeling in a minor state space, as well as the search in a minor region, maintaining a reliable robustness under the liner time-invariant conditions. Yet in practice, nonlinear situations occur now and then, the deficiency of Kalman filter would expose little by little. However, in the grey system, the internal structures, features and parameters are supposed as unknown. Through a grey generation by limited external behavior of clutter data, the randomness of data would be alleviated. In this paper, we will use grey differential equation to reflect the difference information and harvest the GM(1,1) model [14]. In the actual environment of object tracking, we might meet with the situation of impoverishment and uncertainty in the data information, so as to propagate robust results, it comes necessary to merge grey system theory into the Camshift.

In this paper, edges, textures and SIFT features are fused into the CamShift algorithm. Firstly, we apply Canny operators for the edges detection and extract parameters from the co-occurrence matrix as the texture features in the quantifying process. And then we extract three-layer SIFT features in RGB and track the objects with the fusion of CamShift and GM(1,1) model prediction. The experiment has a satisfactory result that, we can solve the disturbance and the occlusion of similar objects in a robust way.

II. SIFT Features Extraction

SIFT appears as a superior algorithm standing loftily at the pinnacle of computer vision [15]. Traditional SIFT draws out interest points in the scale space of binary image first. At each candidate points, it will determine location and scale of the fancy key points through stability. And then orientations will coin into each key point as well, based on local image gradient directions. In the end, descriptors will be selected around the whole key points, which allows for robust levels of environment changes.

Different from the traditional SIFT, in this paper we will extract the features separately on three channels of RGB space, in such a way that we will get more plentiful features of avail, thus increasing reliability of probability distribution. Figure 1 describes the SIFT features in three-layer space of RGB.



(a) Original image (b) R layer

(c) G layer (d) B layer

Figure1 SIFT features in RGB three-layer space

(a) Original image (b) Matching of target and candidate target

Figure 2 Matching of SIFT features between target and the candidate target

When the features in RGB space generate, we can use Euclidean distance of descriptors as the image similarity criterion. We extract one key point in the first image, finding two closest key points in another image. By comparing the distance of the closest neighbor to that of the second-closest neighbor, we can get a ratio which will thus denote the exact matching points. Figure 2 shows the matches between the tracking object and the candidate object, for the rigid objects in the vehicle, they are saturated with SIFT features.

III. GM(1,1) Model

The grey system is a new discipline founded by Prof. Deng Julong, it stands out recently owing to its excellent predicting performance, even under the condition of barren information. The GM(1,1) model is defined as followings[14]:

Suppose a non-negative sequence:

$X(0)=\{x^{(0)}(1), x^{(0)}(2),\ldots,x^{(0)}(n)\}$,

Let $x^{(1)}(t)=\sum_{i=1}^{t} x^{(0)}(i), t=1,2,\cdots,n$. Such that we get accumulative sequence:

$X^{(1)}=\{x^{(1)}(1), x^{(1)}(2),\ldots, x^{(1)}(n)\}$. Then let

$$z^{(1)}(k)=\frac{1}{2}[x^{(1)}(k)+x^{(1)}(k-1)],\ \mathrm{k}=2,3,\ldots,\mathrm{n} \quad (1)$$

where $Z^{(1)}$ is the $X^{(1)}$ adjacent mean generating sequence, $Z^{(1)}=(z^{(1)}(1),z^{(1)}(2),\cdots,z^{(1)}(n))$, we name:

$$x^{(0)}(k)+az^{(1)}(k)=b \quad (2)$$

as the grey differential equation, also known as GM(1,1) model. A simple form of the differential equations is:

$$\frac{dx^{(1)}}{dt}+ax^{(1)}(k)=b \quad (3)$$

where a and b are the undetermined parameters in the modeling process. Suppose $\hat{a}=[a,b]^T$ are the parameters, and

$$Y=\begin{bmatrix}x^{(0)}(2)\\x^{(0)}(3)\\\vdots\\x^{(0)}(n)\end{bmatrix},\quad B=\begin{bmatrix}-z^{(1)}(2) & 1\\-z^{(1)}(3) & 1\\\vdots & \vdots\\-z^{(1)}(n) & 1\end{bmatrix} \quad (4)$$

then parameter estimation of the least square in the GM(1,1) model: $x^{(0)}(k)+az^{(1)}(k)=b$ will satisfy:

$$\hat{a}=(B^TB)^{-1}B^TY \quad (5)$$

Once we get the parameter $\hat{a}$, we are capable to predict the data, the prediction formula is:

$$x^{(0)}(k)=(\beta-\alpha x^{(0)}(1))e^{-a(k-2)} \quad (6)$$

where $\beta=\frac{\mathrm{b}}{1+0.5\mathrm{a}},\alpha=\frac{a}{1+0.5a}$.

We utilize the overall centroids of previous four frames in objects, anticipating their possible position in the following fifth frame. The parameters in GM(1,1) model iterate gradually, such that we guarantee the accuracy of the GM(1,1) model. For the sake of boosting real-time performance of the system, we might as well reduce the computational complexity. To take the x, y coordinates into account respectively, we track objects in either X or Y direction using concurrent GM(1,1) model, descending tracking dimension into one, in such a way that we ameliorate computational complexity of the system.

IV. Camshift Algorithm

For the traditional Mean Shift, the lack of model updates, as well as the fixed window width of kernel function often has negative effects on the tracking accuracy. As an upgraded version of Mean Shift, Camshift could adjust the window automatically to fit the size of the object, particularly competent for tracking objects with great variations in scale. The major steps of traditional Camshift tracking are as follows：First, it converts the tracking image into HSV space. Through the back projection of color histogram, it can get the probability distributions of colors. At last, by calculating the zero-order moment and first-order moment of image, it will obtain centroid position and the object window size.

The zero-order moment of Camshift is defined as:

$$M_{00}=\sum_x\sum_y I(x,y) \quad (7)$$

The two first-order moments are:

$$M_{10}=\sum_x\sum_y xI(x,y) \quad (8)$$

$$M_{01}=\sum_x\sum_y yI(x,y) \quad (9)$$

The centroid position of searching window defined as:

$$x_c=\frac{M_{10}}{M_{00}},\quad y_c=\frac{M_{01}}{M_{00}} \quad (10)$$

And the size of search window is:

$$s=2\times\sqrt{\frac{M_{00}}{256}} \quad (11)$$

Aiming at the disadvantages of traditional Camshift, in this paper, we will propose an improved Camshift with multiple features fusion. The innovations of our research are as follows:

(1) Instead of utilizing the single H channel in HSV space as the color probability, we will extract the objects information in the channels of RGB.

(2) We will use the SIFT features as the complement of color distribution. As most of features fall upon the objects, we can obtain color probability better via their statistic pixel values.

(3) In either case of existing barren features or existing vast mismatching features, the accuracy of image probability statistics would decrease drastically. Thereby we combine the edge and SIFT features together and extract the color probability distribution from the fusing results to solve these troubles.

(4) Through a fusion of the Camshift and the texture features, we overcome the interference problems of similar objects.

(5) Rather than adopting the true values, we will employ a GM(1,1) model prediction to enhance the anti-occlusion ability when the objects get occluded.

V. Objects Tracking based on GM(1,1) and Camshift with Mult-feature Fusion

Following are the major stages of our computation used to track objects:

(1)To preprocess the image first, and then we are to acquire the edges of objects with the Canny operators.

(2)To extract the SIFT features in three channels of RGB space. Through the statistical feature descriptors we will acquire the accurate size and location of the current objects.

(3) We analyze the pixels of all features, and through the probability histogram of features we could update the objects and recover the original image by the back projection technique.

(4) We utilize the Camshift to track the objects in image sequences continuously. And then we could figure out the exact positions of objects through a comparison of the

texture features between current frames and the previous, judging whether there exist similar objects in color around the objects or not.

(5)If the objects shrink or lose focus suddenly, yet within the range of a frame, we'll predicate them as being occluded. With the attachment of GM(1,1) model, we could predict their exact position in the next frame. At last, we are going to seek the objects in a searching window, whose position lies at center point of prediction and whose size is about 1.5 times of objects in current frame.

VI. Experimental Results and Analysis

A. *Tracking of maneuvering Object*

In this paper, we first get the difference image by the interframe difference and extract the contours by the thresholding binary image, then we draw out the SIFT features from the R, G and B space respectively within the region of contours. The statistical pixel values of SIFT features around the real objects are exploited to calculate the color histogram, and we recover the color probability distribution of original image with the back projection. And then we would acquire center point position and size of the objects in the color probability distribution by the Camshift. After that, we utilize GM(1,1) model to predict the position of the objects in the next frame with the trajectory history, the results manifest that the searching time has been shortened, whereby the real-time performance of the system has increased accordingly. The tracking results of the multiple people are shown in figure 3, and the results of vehicles at crossroads are as shown in figure 4. Despite of a cluster of dynamic changes in vehicles, i.e. the turning or the brake condition, etc., we can still get a stable tracking result with the Camshift. The real-time contrast diagram of the traditional Camshift and our algorithm (figure 4) is shown in figure 5. The experiment results have registered an enhancement in real-time performance of the system.

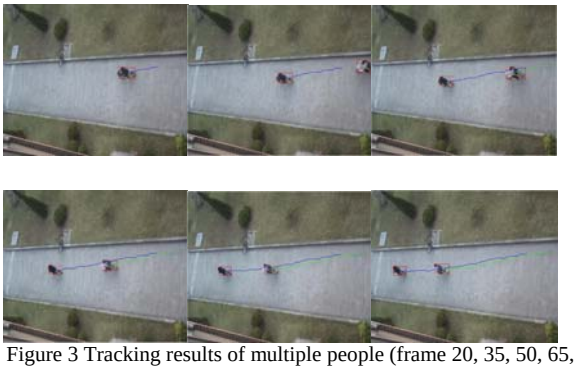


Figure 3 Tracking results of multiple people (frame 20, 35, 50, 65, 80, 95)

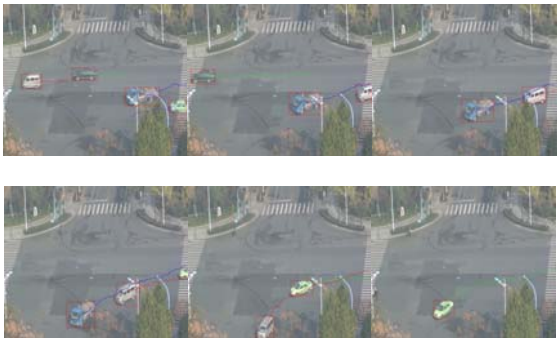


Figure 4 Tracking results of multiple vehicles (frame 50, 65, 80, 95, 125, 140)

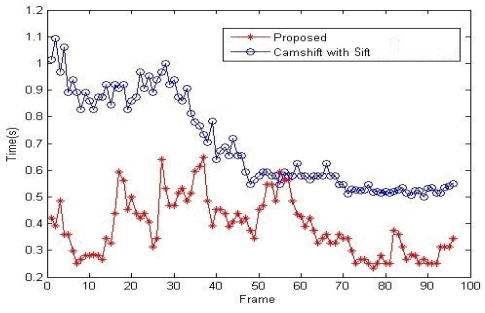


Figure 5 Contrast diagram of traditional Camshift and our algorithm

B. *Object tracking with Occlusions*

When we track the objects, a frequent situation we will encounter is the occlusions. In this case, the object area will shrink suddenly or even disappear. When we get the original image by back projection, the areas ratio of probability histogram of current frame to the previous frames will decrease. Similar to this situation, when the Camshift's applied, the center position and the size of the object probability distribution will both grow smaller, once the objects get occluded completely, the Camshift would become invalid at all, which doomed to bring out a tracking failure. Figure 6 shows the tracking results of traditional Camshift algorithm with the SIFT.

As it can be seen from figure 6, without the occlusions, we could track the objects precisely by the traditional Camshift, but as soon as the object's occluded, the true object would easily get tangled with what is not. In this paper, we will assess the occlusions based on measures of whether the objects shrink and disappear. And then we introduce a RGB color probability distribution, owing to the variations of RGB color, the distributions of differed objects might be discrepant as well, thus the tracking objects are non-interfering. When processing the frame, the size and shape of image will be measured, we determine the occlusions by judging whether the ratio of the mean value of them in current frames and previous frames is less than one threshold, in specific, when the ratio of two consecutive frames and the previous frames is consistently less than a threshold, we will discriminate objects as the occlusions. In this sense, we will take advantage of the single GM(1,1) model prediction other than Camshift, and will never modify the size of the object until we track one afterwards. Figure 7 shows the results of our algorithm and marks the trajectory of moving objects in addition.

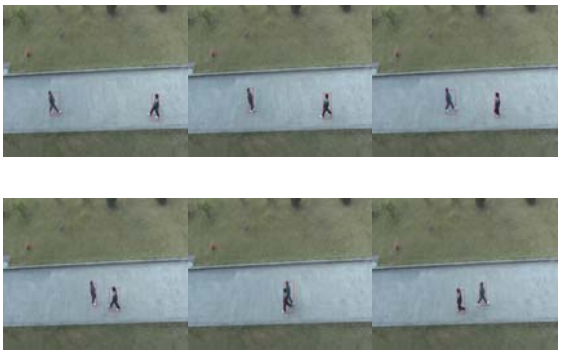


Figure 6 Tracking results of multi-people by the traditional Camshift with occlusions (frame 72, 103, 134, 165, 196, 227)

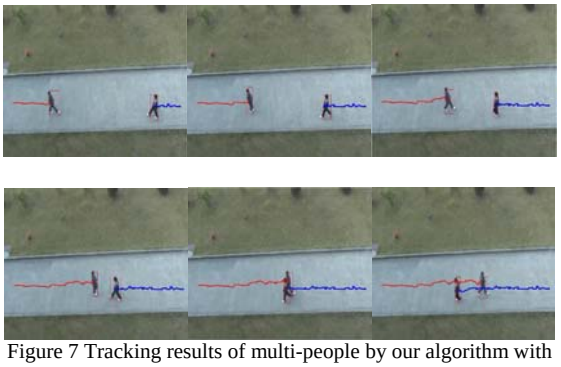


Figure 7 Tracking results of multi-people by our algorithm with occlusions (frame 72, 103, 134, 165, 196, 227)

Figure 8 Tracking results of multi-vehicles by the traditional Camshift with occlusions (frame 65, 76, 87, 98, 109, 120)

Figure 9 Tracking results of multi-vehicles by our algorithm with occlusions (frame 65, 76, 87, 98, 109, 120)

In the process of monitoring the vehicles, similarly, the occlusions occur now and then, i.e. there is a guideboard or other obstacles standing in front. Figure 8 shows the tracking results of traditional Camshift when existing occlusions. And figure 9 shows the tracking results of our algorithm with the occlusions. Figure 10 is the error contrast diagram of vehicle sequences between traditional Camshift with SIFT and our algorithm, the results have proved our algorithm with a higher accuracy.

C. Objects tracking with the Interference of Similar Objects

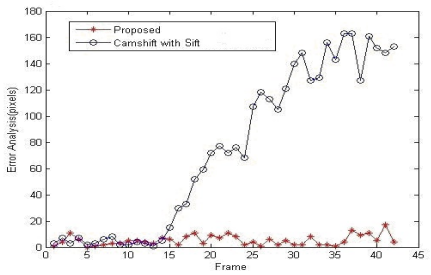


Figure 10 Error contrast diagram of figure 8 and figure 9

When monitoring the track of multiple vehicles in the intersection, some similar vehicles often emerge as the outside interference to spoil the whole color space. While two vehicles of similar colors meet each other halfway, the traditional Camshift algorithm will identify different cars as the one, figure 11 shows the tracking results of traditional Camshift with the interferences. Once some distractions interfere around the tracking objects, the precision of color probability distribution will decrease in response. Thus the features of textures are merged into the algorithm and we can distinguish different objects by textures similarity. After that, the GM(1,1) model is also complemented to solve the occlusion problems. Figure 12 shows the tracking results of vehicles with the occlusions.

D. Object tracking with Shadows

In a natural environment (i.e., the shaded outdoor), the context of shade would be severely troublesome for object tracking. As a practical example, we take portions of human body in shade using the traditional Camshift. As is shown in figure 13, the sunshine reflection would blur tracking window, causing numerous mismatches in the process of tracking. A contrast experiment with our algorithm is shown in figure 14. It turns out that the improved algorithm bears an extraordinary robustness, which could survive of strong shadow interferences.

The benefits of improved Camshift algorithm are summarized as follows:

1) Instead of employing color probability of single H component in HSV space, a three-layer RGB space would be utilized otherwise. As the abundance of RGB space, available features in specific class of objects will be saturated.

2) As background information appears to be simple and invariable. SIFT algorithm will also imposed in the calculation of color probability. When SIFT draws out features in image sequences, the majority of features will fall on the real target, color probability would be acquired by the statistic features pixel.

3) The accuracy of probability histogram would be decreased when the features of target are barren and the mismatches occur now and then. In this sense, edge features and the features in the scale of SIFT will be fused as a whole. Through the color histogram of the joint

features, the mismatches have decreased by a large margin.

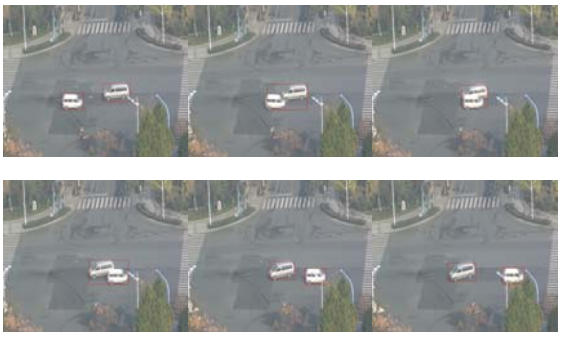


Figure 11 Tracking results of multi-vehicles by the traditional Camshift with interferences (frame 15, 20, 25, 30, 35, 40)

Figure 12 Tracking results of multi-vehicles by our algorithm with interferences (frame 15, 20, 25, 30, 35, 40)

Figure 13 Tracking results of human by the traditional Camshift with shadows (frame 10, 20, 30, 40, 50, 60)

Figure 14 Tracking results of human by our algorithm with shadows (frame 10, 20, 30, 40, 50, 60)

4) Once the interferences of color analogue occur around the target, texture features are attached to recognize the target. Through a combination of Camshift and textures, the analogue interferences have been alleviated to certain degree.

5) When moving objects get occluded, the size of image stays invariable. GM(1,1) model will be kept utilizing to predict the motion position of next frame until the target emerges. Searching in the position of filter prediction, searching time has been saved largely.

VII. Conclusion

In this paper, we first improve the traditional Camshift, instead of extracting the features in single H channel, we extract the features in all RGB channels with the SIFT, the statistical pixel values are calculated to get the probability distribution, and together with the edges features of object, we improve the precision of the probability distribution by a large margin. When the tracking process is interfered by similar objects, the texture features of the historical frames and the current frames will be compared to determine the exact tracking position. And then on a basis of the continuity of moving objects, we utilize the GM(1,1) model to anticipate the objects' best position in the next frame, narrowing the searching scale sharply. The GM(1,1) model will keep the continuity of the tracking, behaving rather serviceable when existing the occlusions. The experiment results demonstrate our algorithm with a splendid performance of robustness and instantaneity.

Acknowledgment

This work is supported by Zhejiang Provincial Natural Science Foundation of China (No.LY13F030013), and Teacher's development projects of visiting scholar with higher education in Zhejiang Education Department (No.FX2012012).

References

[1] Comaniciu Dorin, Ramesh Visvanathan, and Meer Peter, "Real-time tracking of non-rigid objects using Mean Shift," *Proc of the IEEE Conf on Computer Vision and Pattern Recognition*, pp.142-149, 2000.

[2] Comaniciu Dorin, Ramesh Visvanathan, and Meer Peter, "Kernel-based object tracking," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, v25, n5, pp.564-577, 2003.

[3] Bradski Gray R, "Computer Vision Face Tracking For Use in a Perceptual User Interface," *Intel Technology Journal*, v 2, n2, pp.1-15,1998.

[4] Shen Xuanjing, and Zhang Bo, "CamShift tracker based on image moments," *Journal of Beijing University of Technology*, v 38, n 1, p 105-109, 2012.

[5] Li Chao, Liu Tiegen, Liu Hongli, et al., "Face tracking based on Haar detection and improved Camshift algorithm," *Journal of Optoelectronics Laser*, v 22, n 12, p 1852-1856, 2011.

[6] Sun Hongguang,Zhang Jin,Liu Yantao,et al., "Optimized Particle Filter Tracking by CamShift Based on Multi-feature," *Opto-Electronic Engineering*, v37, n2, pp 1-6,31,2010.

[7] Wang Zhaowen, Yang Xiaokang, Xu Yi, et al., "CamShift guided particle filter for visual tracking," *Pattern Recognition Letters*, v 30, n 4, pp.407-413, 2009.

[8] Wang Xin, and Tang Zhenmin, "An improved camshift-based particle filter algorithm for real-time target tracking," *Journal of Image and Graphics*, v15, n10, pp.1507-1515, 2010.
[9] Li Jianhong, Zhang Ji, Zhou Zhenhuan, et al., "Object tracking using improved Camshift with SURF method," *2011 IEEE International Workshop on Open-Source Software for Scientific Computation*, pp.136-141, 2011.
[10] Exner David, Bruns Erich, Kurz Danielet, et al., "Fast and robust CAMShift tracking," *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp.9-16, 2010.
[11] Chu Hongxia, Ye Shujiang, Guo Qingchang, et al., "Object tracking algorithm based on camshift algorithm combinating with difference in frame," *Proceedings of the IEEE International Conference on Automation and Logistics*, ICAL 2007, pp.51-55, 2007.
[12] Liang Juan, Hou Jianhua, Xiang Jun, et al., "An effective automatic tracking algorithm based on Camshift and Kalman filter," *Proceedings of SPIE*, v8003, 2011.
[13] Peng Juanchun, Gu Lizhong, and Su Jianbo, "Hand tracking for humanoid robot using Camshift algorithm and Kalman filter," *Journal of Shanghai Jiaotong University*, v 40, n 7, pp.1161-1165, 2006
[14] Liu Sifeng, Dang Yaoguo, and Fang Zhigeng, "Grey theory and applications," *Third Edition. Beijing: Science Press*, 2004.
[15] Lowe David G, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, v60, n2, pp.91-110, 2004

Zhiyu Zhou received B.S. and M.S. degree from Zhejiang Sci-Tech University in 1997 and 2004, respectively. He is now an associated professor at Zhejiang Sci-Tech University and mainly engaged in computer vision, grey systems and robotic tracking. He has published dozens of research papers, 13 papers among them have been included in EI with the first author. He enjoys a profession of guest reviewer in Chinese "Journal of image and graphics" and has been awarded the outstanding reviewer in 2010. He has just accomplished a Natural Science Fund Project of Zhejiang Province - "Target Vision Analysis based on Grey Model" (No.Y1090256), and now presided over another provincial Natural Science Fund Project - "Research on Key Technology of Robotic Autonomous Navigation based on Stereo Vision in Natural Environment" (No.LY13F030013).

A Secure Dynamic Identity based Single Sign-On Authentication Protocol

Qingqi Pei
State Key Laboratory of Integrated Service Network, Xidian University, Xi'an 710071, P.R. China
Email: qqpei@mail.xidian.edu.cn

Jie Yu
State Key Laboratory of Integrated Service Network, Xidian University, Xi'an 710071, P.R. China
Email: yujie8830@gmail.com

***Abstract*—In the current Internet world, most of the Internet services are based on the single server model and use the password identity authentication to provide application service for the users, this means that the user must enter the identity and password, before his/her wants to login in the application service server. It is extremely hard for user to remember the different ID and password, so the single sign-on (SSO) system has been proposed to solve this problem. There many Authentication protocol proposed for the SSO system. In this paper, we first introduced the SSO system and expounded the importance of the authentication protocol in the SSO system. Then we researched on some authentication protocols which can be used in the SSO system, but there are some serious secure problems in their schemes. So we propose a secure dynamic identify based Single Sign-On authentication protocol using smart card. Our protocol can resist several kinds of attacks, such as replay attack, impersonation attack, stolen smart card attack, leak-of-verifier attack and can provide user's anonymity. In our proposed protocol, it removes the aforementioned weaknesses of their protocols and only uses the one-way hash functions and XOR operations which make the protocol very effectively.**

***Index Terms*—Single sign-on, Authentication, Dynamic identity, Smart card, Password**

I. INTRODUCTION

With the development of the Internet and information technology, different kinds of service systems are provided via the Internet, such as online shopping, online games, electronic commerce, etc. Every system has its own security policy to authenticate the identity of remote users, the most familiar and sample authenticate mechanism is the password authentication which asking user to import his or her legal identity (ID) and password to access a service. Most of the existing password authentication protocols for these service systems are based on single-server model. With the increasing of the service systems, it is extremely hard for user to remember too many different IDs and passwords when he/she to login these remote application systems, the management of the servers is very complicated, and it is consumed huge network resource. So the single sign-on (SSO) system has been proposed to solve this problem.

The SSO technology is a secure network access technology for the multi-server architecture. The user only has one active authentication in the SSO system, and then he/she can have all the authorization of the services in the whole SSO system. The essence of the SSO system is that users access to the entrance of a group application programs via a related authentication protocol and only need to login to the system once. In the SSO system, all the application servers use the same one authentication protocol to improve the system security strategy. So a secure authentication protocol is very important for the SSO system is very important.

In this paper, we first researched on some authentication protocols which can be used in the SSO system in section II. Then we provide a review of the SSO authentication architecture with smart card which used in this paper, in section III. In section IV, the secure dynamic identify based single sign-on authentication protocol using smart card we proposed is introduced. We discuss the security analysis of the proposed protocol and the comparison of the cost and functionality of the proposed protocol with other related protocols in section V. Finally, here is a conclusion in section VI.

II. RELATED WORKS

Since Lamport first proposed password based authentication protocol [1] in 1981, there are many different kinds of password based authentication protocols. Most of the proposed authentication protocols are based on single server architecture. But because of the popularization of the single server applications, the users feel very inconvenient to remember different IDs and passwords, and it is very complicated for the management of the servers. The SSO system is appeared in this time.

In 2000, The Novell Company taked the lead in publishing two kinds of the SSO application -- Novell(r) Single Sign-on Bundle and NDS Authentication Services 3.0,which provide good supports in Windows NT and 2000, Linux, Solaris, OS/390, NetWare, HP-UX, AIX, Free BDS, Radius, Internet Information Server, etc. The e-commerce CA also published a SSO solution -- sTrust Single Sign-on (SSO) 6.5 for electronic commerce. Tivoli Global Sign-on which is provided by IBM, used a center

doi:10.4304/jsw.9.1.154-161

server to collect all the login information in the system, and returned an application authorization list for the users after they login to the system successfully. All these solutions of the SSO system is the multi-server architecture based authentication protocol.

In 2004, Juang [9] proposed a multi-server architecture authentication protocol using smart card. In this protocol, it used the symmetric encryption algorithm and did not maintain any identity authentication lists among the servers. In the same year, Chang and Lee [10] improved Juang's protocol and proposed a similar smart card based multi-server architecture authentication protocol. Chang and Lee's protocol is much more efficient than Juang's. In 2007, Hu et al.'s [11] proposed an effective password authentication key agreement protocol. This protocol is used in the multi-server architecture, and users can use a smart card and a weak password to access multi servers, the user shared a common secret session key among each server. This proposed protocol is much more efficient and user friendly than the protocol proposed by Chang and Lee (2004).

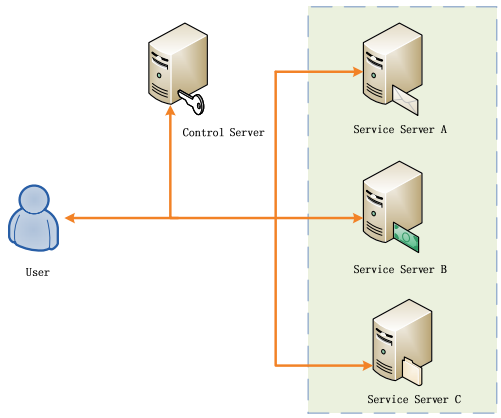
The most famous authentication in SSO system – the Kerberos [12] protocol also has some limits, like all the servers are exposed for users and two servers are both used to authenticate users. In 2006, Yang et al. [13] proposed an authentication and key exchange protocol which is similar to the Kerberos protocol. There are also two servers in the system used to authenticate users in the protocol, but only one front-end server is exposed to users directly and one control server dose not communicate with users. The methods of sharing keys and using two servers to authenticate users make attackers must to compromise two servers so that they can use the offline dictionary attack successfully. In the same year, Mackenzie et al [14] proposed a key exchange authentication protocol based on password, in which there are a group of servers and public keys used to authenticate. But the use of public key makes this protocol computation intensive. Tsai [15] proposed a smart card used authentication protocol based on multi-server architecture in 2008. Because this protocol used one-way hash function as its mathematics foundation, there is no need for servers and registration center to store any authentication form. In this protocol, there is no symmetric and asymmetric encryption algorithm, so it is much more efficient than any other protocol which is introduced above.

However, all the multi-server architecture based password authentication protocol introduced in our paper are based on static ID, it is means that there is a chance for attacker to pretend a legal user. In 2009, Liao and Wang [16] proposed a dynamic identity based remote user authentication protocol using smart card. This protocol only uses one-way hash function to implement a strong authentication and provides a secure method to update the user's password without the help of trusted third party. But in the same year Hsiang and Shih found that Liao and Wang's protocol cannot resist insider attack, masquerade attack, server spoofing attack, registration center spoofing attack and cannot give the mutual authentication. In Ref. [17] Hsiang and Shih proposed an enhance protocol based on Liao and Wang's protocol. In 2011, Sood et al. found that Hsiang and Shih's protocol still had some secure problem. They found that Hsiang and Shih's protocol cannot resist replay attack, impersonation attack and stolen smart card attack. Furthermore, the password change phase of their protocol is wrong. Then Sood et al. in Ref. [18] proposed an enhance protocol. But Sood et al. actually is susceptible to leak-of-verifier attack, stolen smart card attack and cannot finish the mutual authentication and session key agreement. In the same year, Li Xiong et al. proposed an efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards on the basis of Sood et al.'s protocol and claimed their protocol can tackle these problems. But In our analysis, Li Xiong et al.'s protocol still has some fatal secure problems, like replay attack, Impersonation attack and stolen smart card attack.

Based on all the authentication protocols above, we know that a secure and efficient remote user authentication protocol for multi-server environment should provide mutual authentication, key agreement, secure password update, low computation requirements and resistance to different feasible attacks. So we provide a multi-server architecture authentication protocol using smart card which can be used for SSO system to satisfy all the requests.

III. SSO Authentication Architecture with Smart Card

The protocol we proposed in this paper in based on SSO authentication architecture with smart card. This SSO authentication architecture is based on the Broker-Based SSO architecture. In the traditional Broker-Based SSO architecture in Fig. 1, there is a control server which is used to register and authenticate users and the service providing servers. The control server communicates with the users directly, so it can easily attack by the malicious users or attackers.



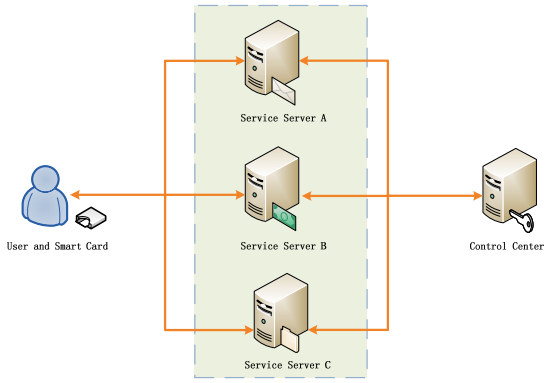
Figrue 1. Broker-Based SSO architecture

In allusion to solve the secure problem in Broker-Based SSO architecture, our SSO authentication

architecture with smart card puts the control server behind the service providing servers and not communicates with the users directly. In Fig.2, there are three parties in our authentication architecture, the user with smart card, the service providing server, and the control server *CS*.

A. The Control Server CS

The control server *CS* is equivalent to the registration center. It manages all the registrations with the service providing servers and the users, and stored their secret identity information for the authentication. The control server *CS* only communicates with all the service providing servers, and it is not directly accessible to the users and thus it is less likely to be attacked. When a user wants to get some services, the control server needs to verify not only the user, but also the service providing server which provides the services the user needs.



Figrue 2. SSO authentication architecture with smart card

B. The Service Providing Server

The service providing server is the bridge between the user and the control server *CS*, when the user wants to verity him/her. In the architecture, there are many service providing servers to provide different kinds of services only to all the users. When a service providing server wants to provide services to the user, it must register itself to the control server CS.

C. The User with Smart Card

Every user has his/her own smart card to login the service providing servers with the identity and the password. The smart card can store some secret information of the user in the authentication, and perform some cryptographic operations to verify the authenticity of the user.

IV. Single Sign-On Authentication Protocol Using Smart Card

In this section, we propose secure dynamic identify based single sign-on authentication protocol using smart card. In Table I, the notations used in this section are listed. This protocol consists of four phases, the registration phase, the login phase, the authentication phase, the session key agreement phase and the password change phase, which are summarized in Fig. 2, Fig.3 and Fig. 4. In our proposed protocol, we only use one-way hash function to provide a strong mutual authentication, and use various different random numbers to achieve dynamic identify. When our protocol used in SSO system, it only needs one login phase when user login to the system in first time.

TABLE I.

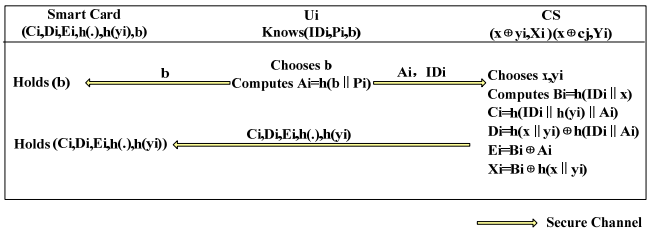
NOTATIONS USED IN THIS PAPER

Notation	*Descriptions*
U_i	The *i* th user
S_j	The *j* th service providing server
CS	The control server
ID_i	The identity of the user U_i
P_i	The password of the user U_i
SID_k	The identity of the server S_k
y_i	The random number chosen by *CS* for user U_i
x	The master secret key maintained by CS
b	A random number chosen by the user for registration
CIDi	The dynamic identity generated by the user U_i for authentication
SK	A session key shared among the user, the service providing server and the *CS*
N_{i1}	A random number generated by the user U_i's smart card
N_{i2}	A random number generated by the server S_k for the user U_i
N_{i3}	A random number generated by the *CS* for the user U_i
h(.)	A one-way hash function
⊕	Exclusive-OR operation
||	Message concatenation operation

A. Registration Phase

There are two parts in the registration phase, the one is the user registration, and the other is the server registration.

When the user U_i wants to access the services legally, the user must register himself/herself to the *CS* server with the identity and the password. The details of the user registration phase are as follow:



Figrue 2. User registration phase

- Step1: The user U_i chooses his/her own identity ID_i and password P_i, and chooses a random number *b*. Then U_i computes $A_i=h(b||P_i)$,and transforms ID_i and A_i to the control server *CS* via a secure channel, which guarantee the security of the user identity to avoid network attack like impersonation attack.
- Step2: When the control server *CS* receiving the massage (ID_i, A_i) from the user U_i, *CS* chooses a master secret key *x*, and a random secret key y_i

which is unique for user U_i. Then the control server *CS* calculates

$B_i=h(ID_i \| x)$,

$C_i=h(ID_i \| h(y_i) \| A_i)$,

$D_i=h(x \| y_i) \oplus h(ID_i \| A_i)$,

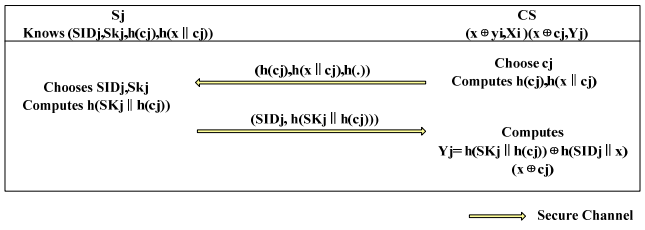
$E_i=B_i \oplus A_i$, $X_i=B_i \oplus h(x \| y_i)$.

At the same time, the *CS* stores $(x \oplus y_i, X_i)$ in its client database, and stores the security parameters $(C_i, D_i, E_i, h(y_i), h(.))$ in the smart card of the user U_i, then transforms the smart card to the U_i via a secure channel.

- Step3: After the receiving the smart card, the user U_i enters the random number b in his/her smart card. Finally, the smart card contains security parameters as $(C_i, D_i, E_i, h(y_i), h(.), b)$.

In the server registration phase, when a service providing server S_j wants to provide service in this system, it must to register itself to the control server *CS*, the details of the registration phase are as follow:

- Step1: After the receiving the registration request from the service providing server S_j, the control server *CS* chooses a unique secret key c_j for the S_j and computes $h(c_j)$, then sends the security para-meters$(h(c_j), h(x \| c_j), h(.))$ to the S_j through a secure channel.
- Step2: After the server S_j receiving the massage $(h(c_j),h(.))$, S_j chooses its identity SID_j and a secret random number SK_j, then computes $h(SK_j \| h(c_j))$, and sends the security parameters$(SID_j, h(SK_j \| h(c_j)))$ to the control server *CS* via the secure channel.

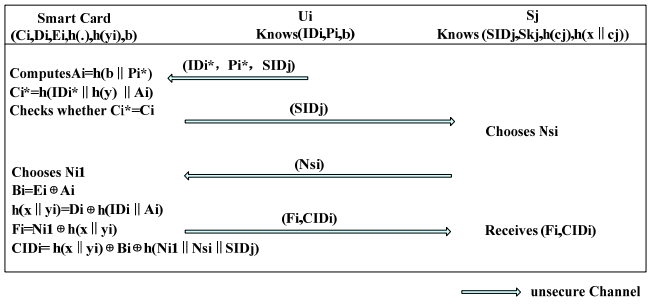


Figrue 3. Server registration phase

- Step3: When receiving the massage $(SID_j, h(SK_j \| h(c_j)))$, the control server *CS* computes $Y_j= h(SK_j \| h(c_j)) \oplus h(SID_j \| x)$. The *CS* stored the parameters $(x \oplus c_j, Yj)$ in its server database, and computes $h(x \| c_j)$. The security parameters $h(x \| c_j)$ is send to the service providing server S_j through the secure channel.

B. Login Phase

- Step1: When the user U_i wants to login to the service providing server S_j, the user U_i inserts his/her smart card into the card reader, and enters his/her identity ID_i , password P_i and the server identity SID_j. The smart card computes
$A_i=h(b \| P_i)$,
$C_i'=h(ID_i \| h(y_i) \| A_i)$,
and checks whether $C_i'=C_i$. If they are equal, that means the user U_i is a legal client, otherwise, the user U_i enters correct identity and password again.
- Step2: After verification, the smart card sends the authentication request message (SID_j) to the service providing server S_j through a public channel. After receiving the request message, the server S_j chooses a random number Ns_i, and sends it to the user U_i.



Figrue 4. Login phase

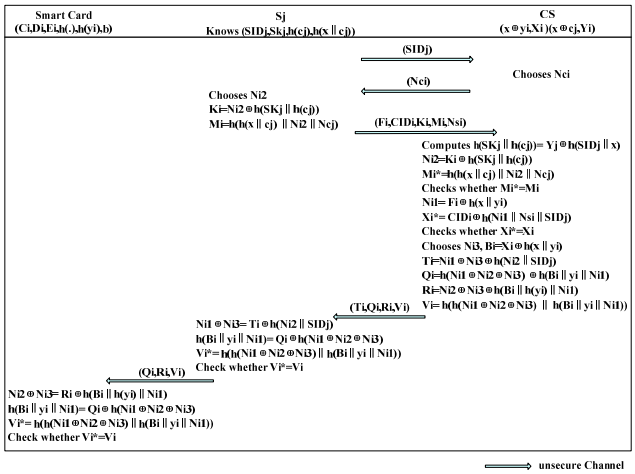
- Step3: Upon receiving the random number Ns_i from the S_j, The smart card generates a random number N_{i1} and computes:
$B_i=E_i \oplus A_i$,
$h(x \| y_i)=D_i \oplus h(ID_i \| A_i)$,
$F_i=N_{i1} \oplus h(x \| y_i)$,
$CID_i= h(x \| y_i) \oplus B_i \oplus h(N_{i1} \| Ns_i \| SID_j)$.
Then the smart card sends the login request message (F_i, CID_i) to the service providing server S_j through a public channel.

C. Authentication Phase

- Step1: When receiving the login request message from the user U_i, the service providing server S_j sends an authentication request massage (SID_j) to the control server *CS*.
- Step2: After the control server *CS* receiving the authentication request massage (SID_j), it returns a random number Nc_j.
- Step3: Upon receiving the return message Nc_j, the service providing server S_j chooses a random number N_{i2} and computes
$K_i=N_{i2} \oplus h(SK_j \| h(c_j))$,
$M_i=h(h(x \| c_j) \| N_{i2} \| Nc_j)$.
Then the login request massage $(F_i, CID_i, K_i, M_i, Ns_i)$ is send to the control server *CS* via a public channel.
- Step4: After receiving the login request massage$(F_i, CID_i, K_i, M_i, Ns_i)$, based on the identity of the service providing server S_j $-SID_j$, the control server *CS* finds the corresponding authentication massage $(x \oplus c_j, Y_i)$ in its server

database. The *CS* computes *cj* by $x \oplus c_j$, and
$h(SK_j \| h(c_j))=Y_j \oplus h(SID_j \| x)$,
$N_{i2} =K_i \oplus h(SK_j \| h(c_j))$,
$Mi'=h(h(x \| c_j) \| N_{i2} \| Nc_j)$,
and checks whether M_i' equal to the received M_i. If they are equal, that means the server S_j is a legal client, otherwise, the *CS* terminates the session.

- Step5: After verification, the control server *CS* computes
  $N_{i1}= F_i \oplus h(x \| y_i)$,
  $X_i'= CID_i \oplus h(N_{i1} \| Ns_i \| SID_j)$.
  Then finding the corresponding X_i to compare with X_i', If the value of X_i' does not match with any value of X_i in its client database, the *CS* rejects the login request and terminates this session, otherwise, the *CS* accepts the login request of the user U_i.
- Step6: After the control server *CS* accepts the login request of the user U_i, it generates a random number N_{i3},and computes:
  $B_i=X_i \oplus h(x \| y_i)$,
  $T_i=N_{i1} \oplus N_{i3} \oplus h(N_{i2} \| SID_j)$,
  $Q_i=h(N_{i1} \oplus N_{i2} \oplus N_{i3}) \oplus h(B_i \| y_i \| N_{i1})$,
  $R_i=N_{i2} \oplus N_{i3} \oplus h(B_i \| h(y_i) \| N_i1)$,
  $V_i= h(h(N_{i1} \oplus N_{i2} \oplus N_{i3}) \| h(B_i \| y_i \| N_{i1}))$.
  Then, the control server *CS* sends the mutual authentication message (T_i, Q_i, R_i, V_i) to the server S_j.



Figrue 5. Authentication phase

- Step7: When receiving the message (T_i, Q_i, R_i, V_i), the service providing server S_j computes:
  $N_{i1} \oplus N_{i3}= T_i \oplus h(N_{i2} \| SID_j)$,
  $h(B_i \| y_i \| N_{i1})= Q_i \oplus h(N_{i1} \oplus N_{i2} \oplus N_{i3})$,
  $V_i' = h(h(N_{i1} \oplus N_{i2} \oplus N_{i3}) \| h(B_i \| y_i \| N_{i1}))$.
  The S_j checks whether $V_i'= V_i$. If they are not equal, the S_j terminates the session. Otherwise, the server S_j sends the mutual authentication message (Q_i, R_i, V_i).
- Step8: When the user U_i receives the message (Q_i, R_i, V_i) from the server S_j, the smart card computes:
  $N_{i2} \oplus N_{i3}= R_i \oplus h(B_i \| h(y_i) \| N_{i1})$,
  $h(B_i \| y_i \| N_{i1})= Q_i \oplus h(N_{i1} \oplus N_{i2} \oplus N_{i3})$,
  $V_i' = h(h(N_{i1} \oplus N_{i2} \oplus N_{i3}) \| h(B_i \| y_i \| N_{i1}))$,
  and checks whether The S_j checks whether $V_i'= V_i$, If they are not equal, the S_j terminates the session. Otherwise, the user U_i is a legal client.

D. Session Key Agreement Phase

After the user U_i, the server S_j and the server *CS* finish the mutual authentication, all of them can calculate the session key from the massage (T_i, Q_i, R_i, V_i) send by the server *CS*. This session key is used for the encryption of the communication between the user U_i and server S_j.
In the session key agreement phase, the server *CS* bases on the computed authentication parameters $\{B_i, y_i, N_{i1}, N_{i2}, N_{i3}\}$ can calculate the session key *SK*, and the server S_j uses the massage (T_i, Q_i, R_i, V_i) to calculate the session key *SK*, and the user uses the massage (Q_i, R_i, V_i) to calculate the session key *SK*. Finally, the user U_i, the server S_j and *CS* agree on the common session key:

$$SK = h\left(h\left(B_i \| y_i \| N_{i1}\right) \| \left(N_{i1} \oplus N_{i2} \oplus N_{i3}\right)\right).$$

E. Password Change Phase

When the user U_i changes his/her password P_i to a new password P_i^{new}, there is no need for the control server to join in. The user U_i inserts his/her smart card and enters the identity ID_i and P_i, the smart card computes:
$A_i=h(b \| P_i)$,
$B_i=E_i \oplus A_i$,
$h(x \| y_i)=D_i \oplus h(ID_i \| A_i)$,
$C_i'=h(ID_i \| h(y_i) \| A_i)$,
and checks whether $C_i'=C_i$. If they are equal, the user U_i asks to submit a new password P_i^{new}. Then the smart card computes
$A_i^{new}=h(b \| P_i^{new})$,
$C_i^{new}=h(ID_i \| h(y) \| A_i^{new})$,
$D_i^{new}= h(x \| y_i) \oplus h(ID_i \| A_i^{new})$,
$E_i^{new} =Ai^{new} \oplus B_i$,
and stores the new parameters C_i^{new}, D_i^{new}, E_i^{new} into the smart card to replace C_i, D_i, E_i to finish the password change phase.

V. Protocol Analysis

In this section, we discuss the security analysis of the proposed protocol within replay attack, impersonation attack, stolen smart card attack, leak-of-verifier attack, and user's anonymity. And then we talk about the performance and functionality between the proposed protocol and other related multi-server architecture authentication protocols.

A. Security Analysis

1) Replay attack

In this type of attack, an attacker may try to pretend a legal user to login the server S_j with the message which is

send before by a legal user. In each phase of the proposed protocol, the user U_i, the service providing server S_j and the control server *CS* choose the different random numbers N_{i1}, N_{i2}, N_{i3} to compute and verify the identity authenticate message. When the user U_i verifying his/her own identity to the service providing server S_j, the S_j send a random number Ns_i to the U_i. When the service providing server S_j verifying his/her own identity to the control server *CS*, the *CS* send a random number Nc_j to the S_j. These random numbers N_{i1}, N_{i2}, N_{i3}, Ns_i and Nc_j guarantee that the authenticate messages transmitted in a public channel are different and legal only in every session of the protocol. The control server *CS* via random numbers Ns_i and Nc_j to ensure the login request messages of the user U_i and the server S_j are fresh, it is effective to prevent the replay attack.

2) Impersonation attack

An attacker or a malicious user using the previously eaves-dropped message or the information obtained from the lost smart card, to forge a legal login request message (F_i, CID_i) to pretend a valid user. However, in our proposed protocol, the attacker and malicious user U_k cannot compute the legal identity message A_i, B_i and CID_i from the previous login request message. If the malicious user U_k has his/her own smart card, he/she can calculate these information $h(y_i)$ and $h(x \| y_i)$ related to the control server *CS*, but every legal user has different y_i, so the malicious user U_k cannot compute the effective identity information to pretend a valid user since he/she cannot get A_i, B_i, E_i. Because the identity information of the valid users are stored in the client database of the control server *CS*, the malicious user U_k cannot guess A_i and B_i to forge a login request message to start an impersonation attack.

3) Stolen smart card attack

We assume that the user U_i's smart card has been lost or stolen, then the attacker can get the information stored in the smart card $(C_i, D_i, E_i, h(\bullet), h(y), b)$. Since the attacker cannot get the information x and y_i, he/she cannot guess the real identity ID_i and password P_i from the breached information, and cannot get or refresh the user U_i's password P_i. In addition, if the attacker gets both the U_i's smart card and the previous legal login request message, he/she also cannot compute A_i and B_i through the information above, since the attacker has no way to get $h(x \| y_i)$. So our protocol can prevent the stolen smart card attack.

4) Leak-of-verifier attack

For the user part, in our protocol, even though there some secret information related to the authentication is stored in the client database of the control server *CS*, but the attacker also cannot compute the user's identity information B_i and the secret parameter y_i from the leaked information of the control server *CS*'s database, since the *CS* has the master secret key x which is supposed to be safe. So our protocol can resist the Leak-of-verifier attack for the user.

For the service providing server part, if the database of the control server *CS* is leaked, the attacker also cannot get any effective information from S_j, because of the safety master secret key x. So our protocol can resist the Leak-of-verifier attack for the service providing server.

5) User's anonymity

A secure channel between the user and the control server *CS* protects the identity information not to be published in the registration phase. In this phase, the user sends a masked identity $CID_i = h(x \| y_i) \oplus B_i \oplus h(N_{i1} \| Ns_i \| SID_j)$ to the service proving server S_j and the control server as a substitute for the real identity ID_i for its authentication. The method proposed by authentication and session key agreement is based on computing the secret information B_i and y_i, but not the real identity ID_i. So when the user logging in the system, the dynamic authentication CID_i is different in every phase and the attacker cannot distinguish the differences among the different phases. So we can say our protocol can provide the user's anonymity.

B. Performance and Functionality Analysis

In this section, we discuss the performance and functionality of our proposed protocol and then make comparisons with some related multi-server authentication protocols. We analyze our protocol and some related protocol in two ways, the one is the computational complexity, and the other is security and functionality properties.

TABLE II.

COMPUTATIONAL COMPLEXITY COMPARISONS

Protocols	Login phase	Verification phase	Total
Proposed protocol	4 T_h	21 T_h	25 T_h
Li X et al (2011)	7T_h	21 T_h	28 T_h
Sood et al. (2011)	7 T_h	18 T_h	25 T_h
Hsiang and Shih (2009)	7 T_h	17 T_h	24 T_h
Liao and Wang (2009)	6 T_h	9 T_h	15 T_h

In the analysis of the computational complexity of the protocols, we define the notation T_h as the time complexity for the hashing function $h(\sim)$. Because XOR operation requires very few computations, it is usually negligible considering its computation cost. In Table II, it shows the computational complexity of our protocol and other related protocols, we first consider for two parts: login phase, and authentication and session key agreement phase, because in these two phases, there is a strict request for the running time. From Table II, we can see that our protocol does not have an obvious predominance in the computational complexity, but it is worth to achieve these security and functionality properties with several additional hash operations.

TABLE III.

FUNCTIONALITY COMPARISONS

Functionalities	Proposed protocol	Li X et al (2011)	Sood et al. (2011)	Hsiang and Shih (2009)	Liao and Wang (2009)
User's anonymity	Yes	Yes	Yes	Yes	Yes
Computation cost	Low	Low	Low	Low	Low
Single registration	Yes	Yes	Yes	Yes	Yes
No time synchronization	Yes	Yes	Yes	Yes	Yes
Resist replay attack	Yes	No	Yes	No	No
Resist imperson-ation attack	Yes	No	No	No	No
Resist leak-of-verifier attack	Yes	Yes	No	Yes	Yes
Resist stolen smart card attack	Yes	No	No	No	No

In the analysis of the security and functionality properties of the protocols, we consider about User's anonymity, Computation cost, Single registration, No time synchroni-zation, Resist replay attack, Resist impersonation attack, Resist leak-of-verifier attack, Resist stolen smart card attack, Correct password update, Correct mutual authentication, Correct session key agreement. In Table III, we can find that our proposed protocol has the advantage over the other related protocols.

VI. CONCLUSION

In this paper, we first described the application condition of SSO system in the network, and the importance of the authentication protocol in the SSO system. Then we introduced some authentication protocols which can be used in the SSO system. And we abstracted a SSO authentication architecture using smart card to solve the authentication problem in SSO system. In this architecture there are three actors: the control server *CS*, the service providing server S_j and the user U_i with smart card. Then secure dynamic identify based single sign-on authentication protocol using smart card based on the architecture talked above. Finally, we make a secure analysis of our proposed protocol, and some performance and functionality comparisons with our proposed protocol and some related multi-server authentication protocols. In conclusion, our proposed protocol keeps the efficiency and is more secure. So our proposed protocol is suitable for the SSO system applications.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grant No.61172068, 61003300; the Fundamental Research Funds for the Central Universities (Grant No.K50511010003), the Key Program of NSFC-Guangdong Union Foundation under Grant No. U0835004 and Program for New Century Excellent Talents in University(Grant No. NCET-11-0691).

REFERENCES

[1] Lamport L. Password authentication with insecure communication. Communications of the ACM 1981; 24(11):770–2.

[2] Ford W, Kaliski BS. Server-assisted generation of a strong secret froma password. In: Proceedings of IEEE 9th international workshop enabling technologies, June 2000, p. 176–80.

[3] Jablon DP. Password authentication using multiple servers. In: Proceedings of the RSA security conference, April 2001, p. 344–60.

[4] Lee WB, Chang CC. user identification and key distribution maintaining anonymity for distributed computer network. Computer System Science 2000; 15(4): 211–4.

[5] Li L-H, Lin L-C, Hwang M-S. A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neura Networks, vol. 12(6), pp.1498–504, 2001.

[6] Lin IC, Hwang MS, Li LH. A new remote user authentication scheme for multi-server architecture. Future Generation Computer System 2003; 19(1):13–22.

[7] Raimondo MD, Gennaro R. Provably secure threshold password-authenticated key exchange. In: Proceedings of the advances in cryptology (Eurocrypt' 03), p. 507–23, May 2003.

[8] Brainard J, Juels A, Kaliski B, SzydloM. A new two-server approach for authentication with short secrets. In: Proceedings of the USENIX security symposium, August 2003, p. 201–14.

[9] Juang W-S. Efficient multi-server password authenticated key agreement using smart cards. IEEE Transaction on Consumer Electronics, vol. 50(1), pp. 251–5, 2004.

[10] Chang C-C, Lee J-S. An efficient and secure multi-server password authentication scheme using smart cards. In: Proceedings of the third international conference on cyber worlds, pp417–22. November 2004.

[11] Hu L, Niu X, Yang Y. An efficient multi-server password authenticated key agreement scheme using smart cards. In: Proceedings of the international conference on multi media and ubiquitous engineering (MUE'07), April 2007, p. 903–07.

[12] J Steiner, C Nevman, JI Schillier. Kerberos: an Authentication Service for Open Network Systerms[c]. In: Proc of Winter Usenix Conference, Dallas, 2005.

[13] Yang Y, Deng RH, Bao F. A practical password-based two-server authentication and key exchange system. IEEE Transactions on Dependable and Secure Computing 2006; 3(2): 105–14.

[14] Mackenzie P, Shrimpton T, Jakobsson M. Threshold password-authenticated key exchange. Journal of Cryptology 2006;19(1):27–66.

[15] Tsai J-L. Efficient multi-server authentication scheme based on one-way hash function without verification table. Computers & Security, vol. 27(3-4), pp.115-21, 2008.

[16] Liao Y-P, Wang S-S. A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, vol. 31(1), pp.24-9, 2009.

[17] Hsiang H-C, Shih W-K. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, vol. 31(6), pp.1118-23, 2009.

[18] Sood S-K, Sarje A-K, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications, vol. 34(2), pp.609-18, 2011.

[19] Li X, et al. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. Journal of Network and Computer Applications 2011.

Qingqi Pei received his BEng, MEng and Ph.D. degrees in Computer Science and Cryptography from Xidian Univ, in 1998, 2005 and 2008, respectively. He is now an associate professor and member of the State Key Laboratory of Integrated Services Networks, also a Professional Member of ACM and Member of IEEE, Senior Member of Chinese Institute of Electronics and China Computer Federation. His research interests focus on digital contents protection and wireless networks and security.

Jie Yu is a Master in cryptography. Her research interests focus on networks and security.

Research and Implementation of an RFID Simulation System Supporting Trajectory Analysis

Tiancheng Zhang, Yifang Yin, Dejun Yue, Xirui Wang, Ge Yu
School of Information Science and Engineering, Northeastern University, China
Email: tczhang@mail.neu.edu.cn

Abstract—**Radio Frequency Identification (RFID) has been playing more and more important roles in domains such as supply chain management, commodity retail and health custody. RFID data can support functions such as object location, object tracking and trajectory analysis. However, at some point, to deploy many RFID devices into a real application scenario would be very difficult. In this paper, we present a RFID simulation system which could support effective data analysis and help users judge the effectiveness of deployment. This system implements part of ISO 18000-6C communication protocol and supports the path loss, backscatter, capture and tag mobility models. It provides a user-friendly visual platform for users to build their own virtual scenarios and deploy RFID devices into it. Further more, in order to improve the efficiency of operations in the application scenarios, we combine R-Tree with TSB-Tree to support the RFID object location and the trajectory analysis.**

Index Terms—**Radio Frequency Identification (RFID), Simulation, ISO 18000-6C, Trajectory analysis**

I. INTRODUCTION

As a developing automatic identification and data acquisition technology, Radio Frequency Identification (RFID) has the following features such as noncontact, high-speed, low-cost, long-life, pollution-against, hash environment-adaptive, et al. RFID is considered to be one of the most promising information technologies in the 21st century. It has been widely used in a variety of applications where it is necessary to automatically identify objects which are not proximate. Compared with traditional data, RFID data has the characters of real-time identification, rich semantics, uncertainty and magnanimity. By analyzing the data collected from readers, users can locate the position of a certain object or even track its movement by means of a proper algorithm. It will save a large quantity of labour force since this technology generates practical use.

As fully discussed in [1,2], an RFID system is superior to a conventional barcode system in many aspects. However, it also has some shortcomings such as signal interference and potential privacy invasion. In addition, contrasting with traditional RFID applications such as keyless entry badges where readers could be sparsely deployed, today's RFID applications, most of which are designed for the purpose of target location, are always required to deploy readers densely. but at some point, to deploy many RFID devices into a real application scenario would be very difficult. On one side, it is almost impossible to use real devices to perform the experiment in some certain application scenarios. On the other side, once some significant design weaknesses appear, the devices must be deployed all over again. Therefore, lots of situations must be taken into consideration before the facility deployment. In this paper, we present a novel RFID simulation platform to provide the entity models such as RFID readers and tags. This system is also designed to implement part of the ISO 18000-6C communication protocol. It provides a user-friendly visual platform for users to build their own virtual scenarios and deploy RFID devices into it. Users could print out the simulation results on the console or store them in the database as well. Further more, in order to support the RFID object location and the trajectory analysis, we combine R-Tree (the spatial object index mechanism) with TSB-Tree (Time-split B Tree, the temporal index method). Both the spatial state and the temporal interval of the label objects will be stored in the index entry. Then we can get a hierarchical RT-tree by grouping the close regions into the same cluster in different geographical scales.

II. RELATED WORK

Several RFID simulators have been developed in the past. RFIDSim [3] relies on a discrete event simulator and can be used to simulate large populations featuring thousands of RFID tags. It has also implemented the ISO 18000-6C RFID protocol and supports the path loss, fading, backscatter, capture and tag mobility models, so it can be used to facilitate the relative comparison of different medium access protocols, transmission control strategies, settings in ISO 18000-6C, and privacy and security enhancements. There is also a configurable simulation platform for RFID application deployment [4].

This paper is based on "A Simulation Platform For RFID Application Deployment Supporting Multiple Scenarios", by Tiancheng Zhang, Yifang Yin, et al, which appeared in Proceedings of the Eighth International Conference on Computataional Intelligence and Security, 17-18 Nov. 2012, Guangzhou, China.

This work was supported in part by the National Natural Science Foundation of China under Grant No.61272180, 61202086, 61272177, 61272179.

doi:10.4304/jsw.9.1.162-168

It provides users a visual developing platform but has not implemented any protocols. All the data related in modeling is sourced from an RFID test database. An RFID simulator called SERFID based on SystemC modeling is presented in [5]. This simulator is able to simulate a complete HF RFID system, from tags to the middleware. It can help to evaluate and optimize the robustness HF RFID systems. A configurable simulator is introduced in [6]. It is designed for RFID-aided supply chains that is capable to create consistent and realistic event data.

All the details of ISO 18000-6C protocol can be found in [8]. It defines the physical and logical requirements for a passive-backscatter, interrogator-talks-first, radio-frequency identification system operating in the 860 MHz–960 MHz frequency range. In this system, an interrogator transmits information to a tag by modulating an RF (Radio Frequency) signal in the 860 MHz–960 MHz frequency range. An interrogator receives information from a tag by transmitting a continuous-wave RF signal to the tag, the tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the interrogator. The RFIDSim presented in this paper is designed to feature some main reader commands, tag replies and states to support the simulation.

The path loss model is very important in a wireless simulation system. Hashemi [9] presents a path loss model with variable environmental factor which is extremely suitable for the case of RFID. And Leong et al. [10] improve the path loss model according to the measurement results from their lab. It suggests that walls have been shown to have a great impact on the environmental factor. Within a room, one fixed environmental factor can be used, but it must be increased when a wall is encountered as the distance increases.

During the past years, the trajectory analysis has been performed based on individual location history represented by GPS, RFID or Wireless Sensor trajectories. Using the GPS trajectories generated by multiple users, [11] mined interesting locations and classical travel sequences within a given region. A HITS (Hypertext Induced Topic Search)-based inference model has been proposed to infer a user's travel experience and the interest of a location.

While the RFIDSim discussed in [3] is focused on the physical performance of readers and tags, it can only provide users a simple simulation process of RFID facility deployment. On the other hand, though the RFID simulation platform discussed in [4] can help users to deploy RFID application systems and supply with a user-friendly visualized development platform, it has not implemented any protocols. Thus, we try to develop an improved deployment simulation platform for the RFID application which could implement part of the ISO 18000-6C communication protocol and supports the path loss, backscatter, capture and tag mobility models as well. Moreover, we abstract some common reader APIs (Application Program Interface) and also present a special language to control the behavior of the simulation process. All the data collected during the simulation process would be stored in the database for further processing such as target tracking.

III. OVERVIEW

The objective of RFIDSim is to provide users a visual developing platform for RFID applications. Common objects such as walls and tables are abstracted as elements to build a virtual RFID application scenario. After setting location and motion of RFID devices, a simulation process could be started up. The simulation engine is driven by a discrete event simulator. Since RFIDSim has implemented part of ISO 18000-6C protocol, it could be used to simulate the identification process, memory access etc. The simulation behavior differs due to different programmes that users write by using the special language we have mentioned above. At the end of the simulation process, all the data collected would be stored in the database for further processing and presented to users on the console. Considering a situation that an RFID system is designed for indoor target tracking, this RFIDSim could facilitate users to figure out the balance between the reader deployment and the location algorithm.

IV. SIMULATION MODELS

To support the RFID application deployment, we need to model entities such as readers, tags and walls to build an application scenario, and to model tag movements and reader APIs to initialize a simulation process. It is also necessary to model the reader commands, signal propagation, capture and backscatter to simulate the signal transmission and the reception process. All the models are discussed respectively in the following sections.

A. RFID Reader

At the logical layer, an RFID reader features the main commands and their parameters specified in ISO 18000-6C as shown in Table I. It can also generate proper command sequences according to users' different intentions. For instance, the typical inventory sequences look like a Query command is followed by Ack, QueryRep and QueryAdj commands until a tag population is successfully identified.

TABLE I
MAIN READER COMMANDS SPECIFIED IN ISO 18000-6C

Category	Command
Selection	Select
Inventory	Query, QueryRep, QueryAdj, ACK, NAK
Access	Read, Write, Lock, BlockWrite, BlockErase

At the physical layer, an RFID reader radio transmitter is characterized by the carrier frequency and the transmitting power which are required to compute the received signal strength at the RFID tags. Directive

reader antennas are adopted here. The radiation pattern of the antenna can be specified as part of the configuration which is shown in Fig. 1 [3]. So the orientation of the RFID reader antenna also needs to be specified.

The capture model for an RFID reader radio receiver chosen to be implemented is the most commonly used power model [5] as equation (1) shows.

$$P_{R_0} \geq c\sum_{i=1}^{k} P_{R_i} \tag{1}$$

Where P_{R_0} denotes the received signal strength of the strongest signal, P_{R_i} denotes the received signal strength of one of the k other tag signals and c is a factor denotes the capture ratio. The P_{R_0} s.t. equation (1) is ass umed to be captured successfully.

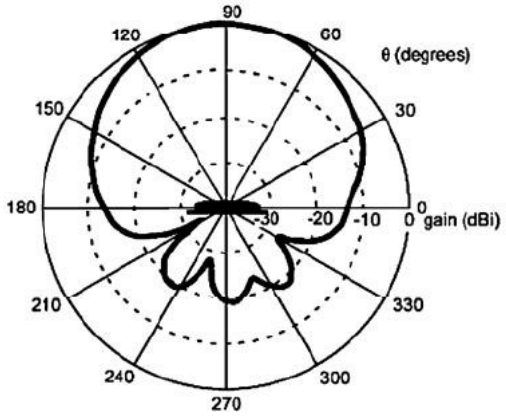


Figure 1. Sample radiation pattern of an RFID reader antenna

B. RFID Tag

An RFID tag model needs to generate the replies and change states according to the commands received from an RFID reader. According to ISO 18000-6C protocol, we implement the main states including ready, arbitrate, reply, acknowledged and secured. The details about ISO 18000-6C protocol can be found in [6].

At the physical layer, an RFID passive tag uses a backscatter model to calculate the backscattered power. The model we choose is a simple linear model [3] that relates the backscattered power P_B to the received power P_R.

$$P_B = \alpha P_R \tag{2}$$

Where α denotes a constant that specifies which proportion of the incident signal is reflected.

C. Signal Propagation

In free space, the path loss model for simulation is considered as a simple function of distance. However, a typical RFID deployment zone is like a warehouse filled with commercial products, so logically a more complex model is required. It is found that a path loss model with variable environmental factor, *n*, is most suitable for the case of RFID as shown in equation (3) [7]:

$$PL(dB) = PL(d_0) + 10n\log\left(\frac{d}{d_0}\right) \tag{3}$$

where d_0 is an arbitrary reference distance, n is the environment factor, d is the separation distance between two antennas and $PL(d_0)$ is the free space path loss for a distance d_0. Considering the fact that the n increases as the distance increases, equation (3) is modified as shown as equation (4) [8]:

$$PL(dB) = \begin{cases} PL(d_0) + 10n_1\log\left(\frac{d}{d_0}\right) & 0 \leq d < 8m \\ PL(d_0) + 10n_2\log\left(\frac{d}{d_0}\right) & d \geq 8m \end{cases} \tag{4}$$

where $n_2 > n_1$. As the experiment shows, a fixed n value can be used within a room. However, n must be increased when a wall is encountered as the distance increases. Thus, for every obstruction abstracted from an RFID application scenario, we set an attribute, *n*, to denote the environment factor discussed here. When a signal transmitted from a reader to a tag meets an obstruction, the attribute *n* of this obstruction will be used in the path loss model. Moreover, users can carry out on-site measurement to determine the best *n* for a certain area and configure it in simulations.

D. Simulation Data Management and Analysis

In this module, the simulation data is used to support a series of functions such as the target location, trajectory analysis, etc. We simulate the procedure where a reader identifies a label id. When a label enters into the sensing field of a reader, the original simulation data including the label id and the sensing time would be generated. After the simulation procedure, this module will process these raw simulation data by some frequently-used RFID processing algorithms such as the label location. Therefore, this system could support the upper lever functions such as the trajectory analysis by utilizing the common RFID data from the low level. Users could output the simulation data on the console or store them in the database alternatively.

RFIDSim is designed to support a range of functions for constructing the virtual RFID application scenario, recording the moving trajectory of the label, etc. In order to improve the efficiency of the insert, delete, update and search operations of the models, we need to adopt an appropriate spatial index to represent the location information of some modes such as the RFID equipments, the entities in the simulation environment, etc.

Since the environment entity will be accessed and queried frequently when the simulation signal is propagated as well as the label is moving, we adopt R-Tree as the index of the simulation environment entity in the virtual scenario. R-Tree is a completely dynamic spatial index structure supporting the insert, delete and search operations which can be executed simultaneously. Meanwhile, it requires no periodic index reorganization. In R-Tree, spatial objects are partitioned according to the region. And each node corresponds to a certain region and a disk page. The disk page of each non-leaf node stores all the area regions of all its child nodes, which means the regions of all its child node fall into its own scope. The disk page of each leaf node stores the

bounding rectangles of all the spatial objects within its scope. Each node has an upper bound and a lower bound for the number of child nodes. The lower bound ensures the effective utilization of the disk space, and the upper bound ensures that each node corresponds to a certain disk page. When the required space after inserting a new node exceeds a disk page, the original node will be divides into two nodes. An example of R-Tree is shown in Fig. 2.

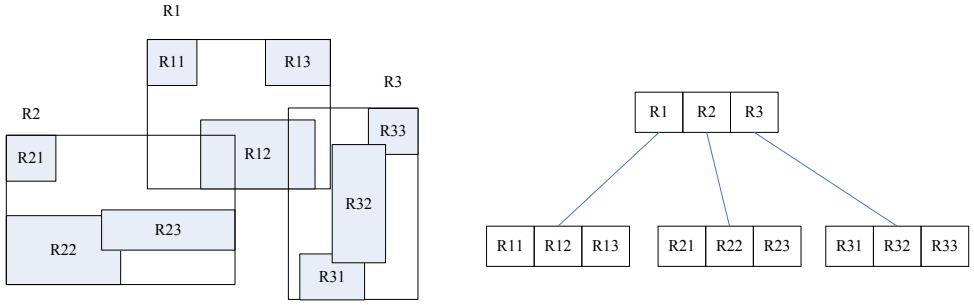


Figure 2. The Structure of R-Tree

Further, we combine R-Tree (the spatial object index mechanism) with TSB-Tree (Time-split B Tree, the temporal index method). Both the spatial state and the temporal interval of the label objects will be stored in the index entry. When the spatial state changes, a new generated data item will be inserted into the index. In order to support the trajectory query and the moving pattern discovery much more efficiently, we also optimize the structure of RT-Tree by the technology of the hierarchical tree. We utilize the density-based clustering algorithm and cluster the regions of the label objects. In this way, we could get a hierarchical RT-tree by grouping the close regions into the same cluster in different geographical scales. As shown in Fig. 3, the nodes in the tree represent different region clusters and different levels represent different geographical scales. A deeper level indicates a finer granularity and smaller space for the nodes.

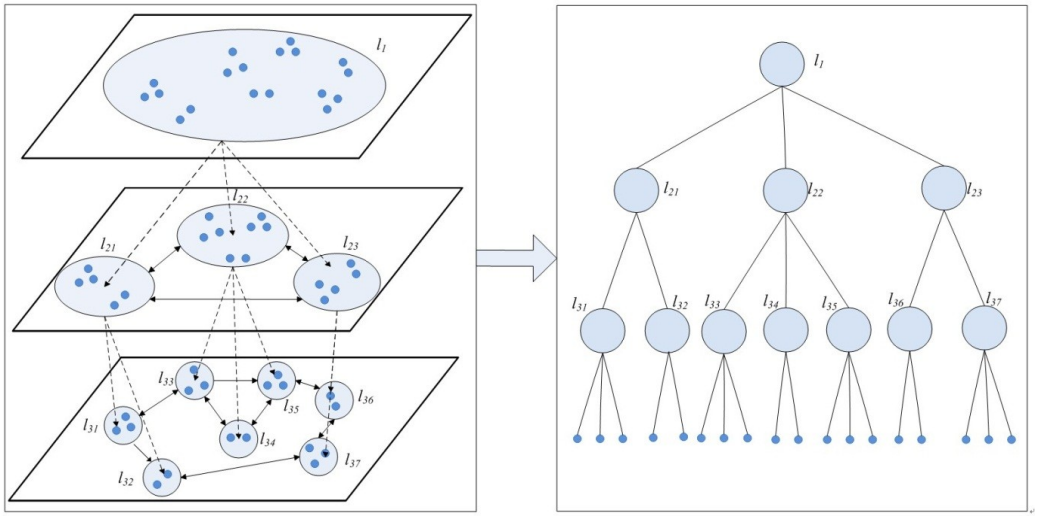


Figure 3. Hierarchical Clustering in RT-tree

V. IMPLEMENTATION

RFIDSim is designed to rely on a discrete event simulator. A discrete simulation is a form of simulation where all actions within the simulation can be modeled in discrete points in time. For example, a signal is broadcasted from the reader at time t, and is received at time t+k by a tag. Though the movements of tags are continuous in real world, we can simulate all the movements as discrete events at a proper predefined frequency to ensure the validity of the simulation.

To implement RFIDSim, we chose to use Eclipse RCP which is a platform for building and deploying rich client applications. It includes the ability to deploy native GUI applications to a variety of desktop operating systems, such as Windows, Linux and Mac OSX. It also poses an integrated update mechanism for deploying desktop applications from a central server. This plug-in based development produces a modular structure and allows selected modules to be put integrated together in different software versions.

This RFIDSim consists of three plug-ins, each of which implements a special function. The first plug-in is the core layer which builds the abstract model and defines the extension points of reader, tag, obstruction, signal propagation and etc. The second plug-in is the implementation layer which implements multiple entity

models by loading the extension points from the core layer. The third plug-in is the GUI layer which provides users a visual developing platform by using GEF (Graphical Editing Framework).

GEF allows us to easily develop graphical representations for existing models. Thus, we choose to use GEF to develop a feature rich graphical editor here. With this editor, users can modify models, like changing element properties, by using very common functions like the drag and drop, copy and paste, and actions invoked from menus or toolbars.

The relationship between core layer and implementation layer is shown in Fig. 4. By loading the extension points from the core layer, users can even develop their own plug-in to implement new types of entities. Thus, this RFIDSim has a strong expansibility.

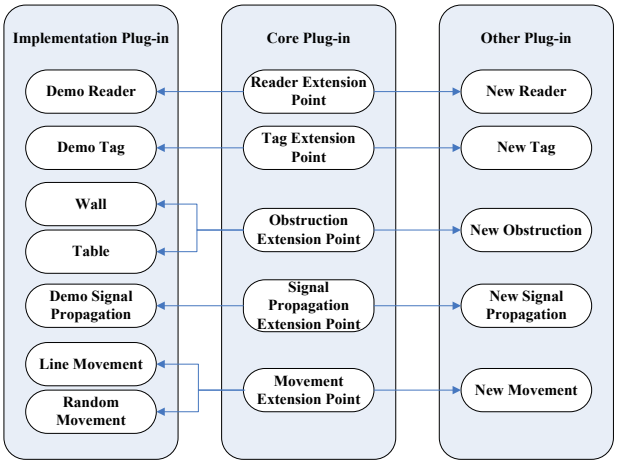


Figure 4. Expansibility of RFIDSim

TABLE II
ENTITIES IMPLEMENTED IN RFIDSIM

Entity	Description
Application	initiates readers and generates proper command sequences according to the pre-input programme and stores all the data collected during a simulation process and presents it to the user on the console
Reader Logical Layer	generates the main ISO 18000-6C commands
Reader Physical Layer	implements capture model
Tag Logical Layer	receives reader commands, updates state and generates appropriate replies
Tag Physical Layer	implements capture and backscatter model
Scenario Obstruction	obstructs tag movement and signal transmittance
Signal Propagation	implement the path loss model
Movement	implement different types of tag movements
Radio Field	changes location of RFID tags and deliver datapackages between readers and tags

The RFIDSim implements the entities shown in Table II. At the beginning of a simulation, users need to build their own scenario or choose a default scenario (such as an intellectual museum) offered by the system. The default programme implements the basic tag identification process. If users want to implement other functions such as tag memory access, they can write a special programme to control the simulation process. Then, the application initiates readers and generates proper command sequences according to the pre-input programme to control the behavior of readers. And RFID readers and tags communicate with each other by datapackages delivered by the Radio Field. Whenever a simulation finishes, the application would store the data collected during the simulation for further processing. The architecture of RFIDSim is shown in Fig. 5.

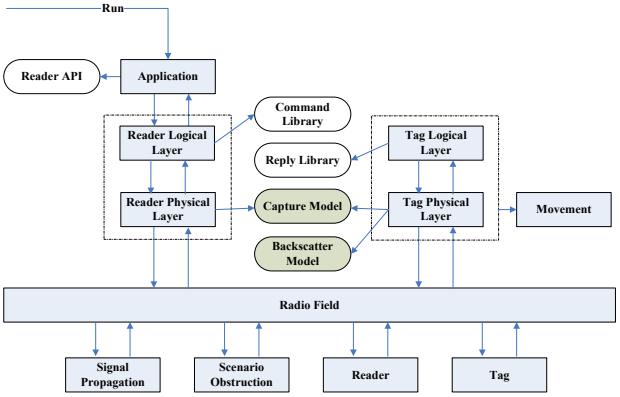


Figure 5. Architecture of RFIDSim

In order to control the behavior of readers as the real ones, we abstract some common reader APIs (cf. Table III) by which users can write a programme to control the simulation process.

TABLE III
READER APIS AND THEIR DESCRIPTION

Category	API	Decription
Reader Administration	OpenReader	to open a reader
	CloseReader	to close a reader
	BeepControl	to control a reader buzzer
	Power	to set a reader's transmiting power
Tag Manipulation	SingleTagIdentify	to identify a single tag
	MultipleTagIdentify	to identify multiple tags
	ReadTag	to read a tag's memory
	ReadTag0	to read a certain tag's memory
	WriteTag	to write a tag's memory
	WriteTag0	to write a certain tag's memory
	LockTag	to lock a tag
	LockTag0	to lock a certain tag

VI. EXPERIMENTS OF RFIDSIM

The objective we implement RFIDSim is to provide users a visual developing platform for RFID facility deployment in multiple scenarios. To evaluate the effectiveness of this system, we carried out a series of experiments. In the next section, we present one of basic

experiments with the purpose of figuring out a proper deployment in an intellectual museum.

In an intellectual museum scenario, tags appear as exhibits and visitors. The exhibits are displayed in different rooms. Several rooms compose an exhibition hall. Different exhibition halls are connected by channels. Readers are placed next to exhibits for the use of supervisory control. Visitors can walk around in the intellectual museum. Once a visitor walks into the accessible range of a reader, it would be read immediately. Information of the visitor such as the identification number, the location area and the exact time of this identification process would be generated. Based on this information, we can track visitors, analyze their interests, optimize the exhibition deployment and even deal with the abnormal conditions.

Table IV shows the use case for the experiment. And Table V shows the simulation results. As all the exhibits remain static in this experiment, here we only record the data which are related to the visitors in Table V.

TABLE IV
USES CASE OF RFIDSIM

Use Case	Test of RFIDSim
Level	High
Input	(a) Choose the default scenario of intellectual museum. (b) Deploy readers and tags. (c) Use the default programme with the function of tag identification.
Steps	(a) Run the system.
	(b) Choose the intellectual museum as the simulation scenario.
	(c) Deploy tag0 to tag 5 as the exhibit0 to exhibit5.
	(d) Deploy tag6 to tag8 as the visitor0 to visitor2.
	(e) Deploy reader0 to reader5 next to the exhibits.
	(f)) Add random motion to tag 6.
	(g) Add rectilinear motion to tag7 and tag8.
	(h) Choose the default programme with the function of tag identification.
	(i) Open a console and run the simulation.
	(j) Use the simulation results to analyze the rationality of the deployment.
	(k) If the deployment is irrational, go to (c); else, finish the simulation.
Expected Results	When a tag is in the accessible range of a reader, it would be read by the reader immediately. The data collected during simulation would be stored in the database for further processing, and also be outputted on the console to users.

Using a proper location algorithm, users could achieve the target tracking with the data collected during the simulation. They can also figure out whether all the RFID facilities are properly deployed at the right places and make the corresponding adjustment.

Further, RFIDSim supports the users to select different location scales according to their different simulation requirements for the further data cleaning. The cleaning method is as follows: the system partitions the simulation space into equal square regions by using the scale as the side length of the squares. All the coordinates in a square region are substituted by the coordinate of the central point of the square, which means the smaller the scale is, the finer the grain of the location information will be. On the contrary, the larger the scale is, the coarser the grain of the location information will be. In some outdoor RFID simulation scenarios, it's necessary to select a larger scale.

After executing the location algorithm and the data cleaning, we could obtain a series of trajectories composed of the coordinate points with timestamp for each label in the simulation scenario for supporting the further trajectory analysis. By adopting the adaptive clustering algorithm, the trajectories of different targets could be mapped into different levels in RT-tree. And we could get different graph models by connecting different clusters accordingly.

TABLE V
SIMULATION RESULTS

Time	Data	Location of Tag
1-32	No data.	Visitor0 wanders between exhibit0 and exhibit1. Visitor1 is on the way to the room where exhibit5 is displayed. Visitor2 is on the way to the room where exhibit3 is displayed.
33-56	Visitor0 is read by reader0.	Visitor0 is at exhibit0. Visitor1 is on the way to the room where exhibit5 is displayed. Visitor2 enters the room where exhibit3 is displayed.
57-136	No data.	Visitor0 wanders off exhibit0. Visitor1 enters the room where exhibit5 is displayed. Visitor2 is in the room where exhibit3 is displayed.
137-148	Visitor2 is read by reader3.	Visitor0 wanders between exhibit0 and exhibit1. Visitor1 is in the room where exhibit5 is displayed. Visitor2 is at exhibit3.
149-160	Visitor1 is read by reader5. Visitor2 is read by reader3.	Visitor0 wanders between exhibit0 and exhibit1. Visitor1 is at exhibit5. Visitor2 is at exhibit3 .
161-188	Visitor0 is read by reader1. Visitor1 is read by reader5. Visitor2 is read by reader3.	Visitor0 is at exhibit1. Visitor1 is at exhibit5. Visitor2 is at exhibit3.
189-200	Visitor1 is read by reader5. Visitor2 is read by reader3.	Visitor0 wanders off exhibit1. Visitor1 is at exhibit5. Visitor2 is at exhibit3.

VII. CONCLUSION

In traditional RFID applications such as keyless entry badges, all the readers are sparsely deployed. However, today's RFID applications usually require readers to be densely deployed. Thus, the deployment problem of the RFID devices arises in real scenario. To solve this problem, we developed the RFIDSim.

RFIDSim is an improved simulation platform for the RFID application deployment which implements part of ISO 18000-6C communication protocol and supports the path loss, backscatter, capture and tag mobility models as well. It is driven by a discrete event simulator and has strong expansibility. To control readers' performances, we also abstract some common reader APIs. From the test results, we can conclude that the RFIDSim provides users a visual developing platform for RFID facility deployment in multiple scenarios. And from the data collected during the simulation, users can judge whether a certain deployment is fairly appropriate or not. Further more, in the simulation platform, we store the data by combining R-Tree with TSB-Tree to support the RFID object location and the trajectory analysis.

For future work, we will try to perfect reader commands, tag replies and tag states, making them perfectly accord with ISO 18000-6C protocol. We will also impove the reader APIs to make models work just as the real ones. Limited by the experiment condition, we didn't comparison testing between the models and the real devices. Thus, more tests on this system would be performed in the near future.

REFERENCES

[1] S. Lewis, "A basic introduction to RFID technology and its use in the supply chain" Jan 2004. [Online]. Available: http:// www.idii.com/wp/LaranRFID.pdf.

[2] Philips Semiconductor and TAGSYS and Texas Instruments Inc., "Item-level visibility in the pharmaceutical supply chain: a comparison of HF and UHF RFID technology" July 2004. [Online]. Available: http://www.hibcc-au.com.au/RFID%20Website/RFID%20 Reference%20 Files/jointPharma.pdf.

[3] C. Floerkemeier and S. Sarma, "RFIDSim-a physical and logical layer simulation engine for passive RFID" IEEE Transactions On Automation Science and Engineering, vol. 6, no. 1, pp. 33-43, Jan 2009.

[4] XIA Tian, ZENG Juan-fang and LIU Yu. "A configurable simulation platform for RFID application deployment" Microcomputer Information, vol. 25, no. 1-2, pp. 224-226, 2009.

[5] Gilles Fritz, Vincent Beroulle, et, al. "SystemC Modeling of RFID Systems for Robustness Analysis" in Proceeding of the 19th International Conference on Software, Telecommunications and Computer Network(SoftCOM), pp. 1-5, 2011

[6] Matthieu-P. Schapranow, Cindy Faehnrich, Alexander Zeier, et, al. "Simulation of RFID-aided Supply Chains: Case Study of the Pharmaceutical Industry" in Proceeding of the Third International Conference on Computational Intelligence, Modelling & Simulation, pp. 340-345, 2011

[7] M. Zorzi and R. Rao, "Capture and retransmission control in mobile radio" IEEE J.Sel. Areas Commun, vol. 12, no. 8, pp. 1289-1298, Oct. 1994.

[8] "Class 1 generation 2 UHF air interface protocol standard version 1.0.9, EPCglobal, 2005". [Online]. Avaliable: http:// www.epcglobalus. org.

[9] H. Hashemi, "The indoor radio propagation channel" Proceedings of IEEE, vol. 81, no. 7, pp. 943-968, Jul. 1993.

[10] K. S. Leong, M L Ng and P. H. Cole, "Operational considerations in simulation and deployment of RFID systems" in Proceeding of 17th Int. Zurich Symp. Electromagnetic Compatibility, pp. 521-524, 2006

[11] Yu Zheng, Lizhu Zhang, Xing Xie, Wei-Ying Ma. Mining interesting locations and travel sequences from GPS trajectories. In Proceedings of International conference on World Wild Web (WWW 2009), Madrid Spain. ACM Press: 791-800.

Tiancheng Zhang received his Ph.D. degree in computer science from the Northeastern University (China) in 2008. He is currently an associate professor of computer science at Northeastern University. His major interests include RFID data management and data stream analysis.

Yifang Yin received her B.S. degree in computer science from Northeastern University(China) in July 2011. She is the major co-auther of this work. She is currently a Ph.D candidate at the National University of Singapore. Her main research interest is multimedia data analysis.

Dejun Yue received his B.S and M.S. degrees both in computer science from the Northeastern University(China) in July 2005 and March 2008. He is currently a Ph.D candidate at the Northeastern University. His major interests include data stream analysis and XML data management.

Xirui Wang received his B.S degree in computer science from the Fuzhou University in July 2011. He is currently a graduate student of computer science at Northeastern University(China). His major interest is RFID data analysis.

Ge Yu received his Ph.D. degree in information science from the department of engineering at Kyushu University (Japan) in 1996. He is currently an professor of computer science at Northeastern University(China). His major interests include database theory and applications, data mining, deep web, wireless sensor network.

Duality of Multi-objective Programming

Xiangyou Li, Qingxiang Zhang
College of Mathematics and Computer Science
Yanan University, Yanan, China,
yadxlxy@163.com, ydzqx@yahoo.com.cn

***Absteact*—In this paper, a class of multi-objective programming is considered, in which related functions are-B–(p,r,a)-invex functions, Mond-Weir dual problem is researched, many duality theorems are proved under weaker convexity.**

***Index Term*— B–(p,r,a)-invex function， multi-objective programming，duality**

I. INTRODUCTION

The convexity theory plays an important role in many aspects of mathematical programming. In recent years, in order to relax convexity assumption, various generalized convexity notions have been obtained. One of them is the concept of B–(p,r)invexity defined by T.Antczak [1], which extended the class of $B-$ invex functions with respect to η and b and the classes of (p,r)invex functions with respect to η [2][3]. He proved some necessary and sufficient conditions for- B–(p,r) invexity and showed the relationships between the defined B–(p,r)-invex functions and other classes of invex functions. Later Antczak defined a classes of generalized invex functions[4], that is B–(p,r) pseudo-invex functions, strictly B–(p,r) pseudo-invex functions, and B–(p,r) quasi-invex functions, considered single objective mathe -matical programming problem involving B–(p,r) pseudo-invex functions, B–(p,r) quasi-invex functions and obtained some sufficient optimality conditions. Qing xing Zhang[5][6]defined B -arcwise connected functions, $(v,\rho)_{h,\varphi}$-type I functions, studied multiobjective progra -mming problem in which involving functions belong to the introduced classes of functions, Xiangyou Li[7] discussed saddle-point conditions for multi-objective fractional programming.

Under different assumption of convexity, several auth -ors establish various duality results. Zhang Ying, Zhu Bo and Xu yingtao discussed nonsmooth programming by a class of Lipschitz B–(p,r) invex function, studied Mond-Weir type dual and Wolfe type dual, derived many dual conditions, Liang Zhi'an, Zhang Zhenhua [9] considered duality for uniform invex multi-objective programming, derived many dual conditions, MorganA. Hanson, Rita Pini and Chanchal Singh [10] researched multiobjective programming problem, using Lagrange multiplier conditions, established many sufficiency results, proved weak, strong and converse duality theorems in the Mond-Weir setting by V-type I-invex functions, Mohamed Hachimi, Brahim Aghezzaf [11] introduced generalized (F,ρ,α,d) type I functions, researched differentiable multi-objective programming, obtained several sufficient optimality conditions, proved weak and strong duality theorems for mixed type duality.

In this paper, we introduce new classes of generalized invex function, classes of B–(p,r,a)-invex functions, B–(p,r,a)quasi-invex functions, B–(p,r,a)pseudo-invex functions and strictly B–(p,r,a) pesudo-invex functions. In this way, we extend B–(p,r) -invex functions, B–(p,r) quasi-invex functions, B–(p,r) pesudo-invex functions and strictly B–(p,r) pesudo-invex functions. Then we research multiobjective programming problem in which corresponding functions belong to the introduced classes of functions, obtain many duality conditions under weaker convexity.

II . DEFINITIONS AND EXAMPLES

Throughout this paper, let R^n be the n-dimensional Eu -clidean space and R^n_+ be its non negative subset, X be a nonempty open subset of R^n. For the benefit of the reader, we recall concept of B–(p,r)-invexity introduced by Antczak in [2] and concept of B–(p,r,a)- invexity intr -oduced by Xiangyou Li in [7] .

Definition 2.1[2] Let $u \in X$, The differentiable funct -ion $f: X \to R$ is said to be (strictly) B–(p,r)-invex fun -ction with respect to η and b at u on X if there exist fun -ctions $\eta: X \times X \to R^n$, $b: X \times X \to R_+$, $0 \le b(.,.) \le 1$, for all $x \in X$, the inequality

$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1) \ge \frac{1}{p}\nabla f(u)(e^{p\eta(x,u)}-I),$$

$$(> if x \ne u),\ for (p \ne 0, r \ne 0),$$

This research was supported by special fund of Shaanxi Provincial high-level university building(2012sxts07),

doi:10.4304/jsw.9.1.169-176

$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1)\geq \nabla f(u)\eta(x,u),$$
$$(>ifx\neq u),\ for(p=0,r\neq 0),$$
$$b(x,u)(f(x)-f(u))\geq \frac{1}{p}\nabla f(u)(e^{p\eta(x,u)}-I),$$
$$(>ifx\neq u),\ for(p\neq 0,r=0),$$
$$b(x,u)(f(x)-f(u))\geq \nabla f(u)\eta(x,u),$$
$$(>ifx\neq u),\ for(p=0,r=0),$$

holds.

Now, we introduce a definition B–(p,r,a)-invex func -tion with respect to η and b at u .

Definition 2.2[7] Let $X\subset R^n$ is a nonempty open set, $u\in X$, the differentiable function $f:X\to R$ is said to be (strictly) B–(p,r,a)-invex function with respect to η and b at u if there exist functions $\eta: X\times X\to R^n$, $b: X\times X\to R_+$, $0\leq b(.,.)\leq 1$, $a: X\times X\to R$ for all $x\in X$, the inequality

$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1)\geq \frac{1}{p}\nabla f(u)(e^{p\eta(x,u)}-I)$$
$$+a(x,u),(>ifx\neq u),\ for(p\neq 0,r\neq 0),$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1)\geq \nabla f(u)\eta(x,u)$$
$$+a(x,u),(>ifx\neq u),\ for(p=0,r\neq 0),$$
$$b(x,u)(f(x)-f(u))\geq \frac{1}{p}\nabla f(u)(e^{p\eta(x,u)}-I)$$
$$+a(x,u),(>ifx\neq u),\ for(p\neq 0,r=0),$$
$$b(x,u)(f(x)-f(u))\geq \nabla f(u)\eta(x,u)$$
$$+a(x,u),(>ifx\neq u),\ for(p=0,r=0),$$

holds.

Function $f:X\to R$ is said to be B–(p,r,a)-invex function with respect to η and b on X if it is B–(p,r,a)-invex function with respect to the same η and b at each u on X .

Now, we introduce a definition B–(p,r,a) quasi-inv -ex function with respect to η and b at u .

Definition 2.3[7] Let $X\subset R^n$ is a nonempty open set, $u\in X$, the differentiable function $f:X\to R$ is said to be B–(p,r,a) quasi-invex function with respect to η and b at u if there exist functions $\eta: X\times X\to R^n$, $b: X\times X\to R_+$, $0\leq b(.,.)\leq 1$, $a: X\times X\to R$ for all $x\in X$, the inequality

$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1)\leq 0\Rightarrow \frac{1}{p}\nabla f(u)$$
$$(e^{p\eta(x,u)}-I)+a(x,u)\leq 0,\ for(p\neq 0,r\neq 0),$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1)\leq 0\Rightarrow \nabla f(u)\eta(x,u)$$
$$+a(x,u)\leq 0,\ for(p=0,r\neq 0),$$
$$b(x,u)(f(x)-f(u))\leq 0\Rightarrow \frac{1}{p}\nabla f(u)(e^{p\eta(x,u)}-I)$$
$$+a(x,u)\leq 0,\ for(p\neq 0,r=0),$$
$$b(x,u)(f(x)-f(u))\leq 0\Rightarrow \nabla f(u)\eta(x,u)$$
$$+a(x,u)\leq 0,\ for(p=0,r=0),$$

holds.

Function $f:X\to R$ is said to be B–(p,r,a) quasi-invex function with respect to η and b on X if it is B–(p,r,a) quasi-invex function with respect to the same η and b at each u on X .

Now, we introduce a definition B–(p,r,a) pseudo-invex function with respect to η and b at u .

Definition 2.4 [7] Let $X\subset R^n$ is a nonempty open set, $u\in X$, the differentiable function $f:X\to R$ is said to be B–(p,r,a) pseudo-invex function with resp -ect to η and b at u if there exist functions $\eta: X\times X\to R^n$, $b: X\times X\to R_+$, $0\leq b(.,.)\leq 1$, $a: X\times X\to R$, for all $x\in X$, the inequality

$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)}-I)+a(x,u)\geq 0\Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1)\geq 0,\ for(p\neq 0,r\neq 0),$$
$$\nabla f(u)\eta(x,u)+a(x,u)\geq 0\Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))}-1)\geq 0,\ for(p=0,r\neq 0),$$
$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)}-I)+a(x,u)\geq 0\Rightarrow$$
$$b(x,u)(f(x)-f(u))\geq 0,\ for(p\neq 0,r=0),$$
$$\nabla f(u)\eta(x,u)+a(x,u)\geq 0\Rightarrow$$
$$b(x,u)(f(x)-f(u))\geq 0,\ for(p=0,r=0),$$

holds.

Function $f:X\to R$ is said to be B–(p,r,a) pesudo-invex function with respect to η and b on X if it is B–(p,r,a) pesudo-invex function with respect to the sa -me η and b at each u on X .

Now, we introduce a definition strictly B–(p,r,a) pse -udo-invex function with respect to η and b at u .

Definition 2.5 [7] Let $X \subset R^n$ is a nonempty open set, $u \in X$, the differentiable function $f: X \to R$ is said to be strictly B–(p,r,a) pseudo-invex function with resp -ect to η and b at u if there exist functions $\eta: X \times X \to R^n$, $b: X \times X \to R_+$, $0 \le b(.,.) \le 1$, $a: X \times X \to R$, for all $x \in X$, the inequality

$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)} - I) + a(x,u) \ge 0 \Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) > 0, \ for(p \ne 0, r \ne 0),$$
$$\nabla f(u)\eta(x,u) + a(x,u) \ge 0 \Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) > 0, \ for(p = 0, r \ne 0),$$
$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)} - I) + a(x,u) \ge 0 \Rightarrow$$
$$b(x,u)(f(x) - f(u)) > 0, \ for(p \ne 0, r = 0),$$
$$\nabla f(u)\eta(x,u) + a(x,u) \ge 0 \Rightarrow$$
$$b(x,u)(f(x) - f(u)) > 0, \ for(p = 0, r = 0),$$

hold or equivalently have

$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) \le 0 \Rightarrow \frac{1}{p}\nabla f(u)$$
$$(e^{p\eta(x,u)} - I) + a(x,u) < 0, \ for(p \ne 0, r \ne 0),$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) \le 0 \Rightarrow \nabla f(u)\eta(x,u)$$
$$+ a(x,u) < 0, \ for(p = 0, r \ne 0),$$
$$b(x,u)(f(x) - f(u)) \le 0 \Rightarrow \frac{1}{p}\nabla f(u)(e^{p\eta(x,u)} - I)$$
$$+ a(x,u) < 0, \ for(p \ne 0, r = 0),$$
$$b(x,u)(f(x) - f(u)) \le 0 \Rightarrow \nabla f(u)\eta(x,u)$$
$$+ a(x,u) < 0, \ for(p = 0, r = 0),$$

hold.

Function $f: X \to R$ is said to be strictly B–(p,r,a) pesudo-invex function with respect to η and b on X if it is B–(p,r,a) pseudo-invex function with respect to the same η and b at each u on X.

Definition 2.6 Let $X \subset R^n$ is a nonempty open set, $u \in X$, the differentiable function $f: X \to R$ is said to be strong B–(p,r,a) pseudo-invex function with respect to η and b at u if there exist functions $\eta: X \times X \to R^n$, $b: X \times X \to R_+$, $0 \le b(.,.) \le 1$, $a: X \times X \to R$, for all $x \in X$, the inequality

$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)} - I) + a(x,u) > 0 \Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) > 0, \ for(p \ne 0, r \ne 0),$$
$$\nabla f(u)\eta(x,u) + a(x,u) > 0 \Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) > 0, \ for(p = 0, r \ne 0),$$
$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)} - I) + a(x,u) > 0 \Rightarrow$$
$$b(x,u)(f(x) - f(u)) > 0, \ for(p \ne 0, r = 0),$$
$$\nabla f(u)\eta(x,u) + a(x,u) > 0 \Rightarrow$$
$$b(x,u)(f(x) - f(u)) > 0, \ for(p = 0, r = 0),$$

hold.

Function $f: X \to R$ is said to be strong B–(p,r,a) pesudo-invex function with respect to η and b on X if it is B–(p,r,a) pesudo-invex function with respect to the same η and b at each u on X.

Definition 2.7 Let $X \subset R^n$ is a nonempty open set, $u \in X$, the differentiable function $f: X \to R$ is said to be weak B–(p,r,a) pseudo-invex function with respect to η and b at u if there exist functions $\eta: X \times X \to R^n$, $b: X \times X \to R_+$, $0 \le b(.,.) \le 1$, $a: X \times X \to R$, for all $x \in X$, the inequality

$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)} - I) + a(x,u) > 0 \Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) \ge 0, \ for(p \ne 0, r \ne 0),$$
$$\nabla f(u)\eta(x,u) + a(x,u) > 0 \Rightarrow$$
$$\frac{1}{r}b(x,u)(e^{r(f(x)-f(u))} - 1) \ge 0, \ for(p = 0, r \ne 0),$$
$$\frac{1}{p}\nabla f(u)(e^{p\eta(x,u)} - I) + a(x,u) > 0 \Rightarrow$$
$$b(x,u)(f(x) - f(u)) \ge 0, \ for(p \ne 0, r = 0),$$
$$\nabla f(u)\eta(x,u) + a(x,u) > 0 \Rightarrow$$
$$b(x,u)(f(x) - f(u)) \ge 0, \ for(p = 0, r = 0),$$

hold.

Function $f: X \to R$ is said to be weak B–(p,r,a) pse -udo-invex function with respect to η and b at X if it is weak B–(p,r,a) pesudo-invex function with respect to the same η and b at each u on X.

In above section, $I = (1, \cdots, 1) \in R^n$, $e^{(a,\cdots,a_n)} = (e^{a_1}, \cdots, e^{a_n}) \in R^n$.

When $a(x,u) \ge 0$, B–(p,r,a) -invex function is $B-(p,r)$-invex function, but if $a(x,u) < 0$, B–(p,r,a) invex function may not be $B-(p,r)$-invex function.

Therefore, adding a parameter $a(x,u)$ means that the $B-(p,r)$ invexity maybe lost.

Now we give several examples about B–(p,r,a)-invex function, B–(p,r,a) quasi-invex function, B–(p,r,a) pesudo-invex function with respect to the same η and b.

Example 2.8 We consider a differentiable function $f:R\to R$, defined by $f(x)=\ln(\ln(x^2+e))$, let $\eta(x,u)=-u$, $b(x,u)=\begin{cases}0, x^2<u^2\\ 1, x^2\geq u^2\end{cases}$, then it is not difficult to prove that $f:X\to R$ is B–(p,r,a)-invex function with respect to η and b when

$$a(x,u)\leq \frac{1}{\ln(u^2+e)}\frac{2u}{(u^2+e)p}(1-e^{-pu}) \text{ for } p\neq 0,$$

(when $a(x,u)\leq \dfrac{1}{\ln(u^2+e)}\dfrac{2u^2}{u^2+e}$ for $p=0$).

Example 2.9 We consider a differentiable function $f:R\to R$, defined by $f(x)=\ln(e^{(x^2-1)}+1)$, let $\eta(x,u)=ux^2$, $b(x,u)=\begin{cases}0, x^2<u^2\\ 1, x^2\geq u^2\end{cases}$, then it is not difficult to prove that $f:X\to R$ is B–(p,r,a) pseudo-invex function with respect to η and b when

$$a(x,u)\geq \frac{e^{(u^2-1)}}{e^{(u^2-1)}+1}\frac{2u}{p}(1-e^{-pux^2}) \text{ for } p\neq 0,$$

(when $a(x,u)\geq \dfrac{-2u^2x^2e^{(u^2-1)}}{e^{(u^2-1)}+1}$ for $p=0$).

Example 2.10 We consider a differentiable function, $f:R\to R$, defined by $f(x)=\ln(x^2+1)$, let $\eta(x,u)=-u$, $b(x,u)=\begin{cases}1, x^2<u^2,\\ 0, x^2\geq u^2,\end{cases}$ then it is not difficult to prove that $f:X\to R$ is B–(p,r,a) quasi-invex function with respect to η and b when

$$a(x,u)\leq \frac{2u}{(u^2+1)p}(1-e^{-pu}) \text{ for } p\neq 0,$$

(when $a(x,u)\leq \dfrac{2u^2}{u^2+1}$ for $p=0$).

Now, we give a useful lemma whose simple proof is omitted in the paper.

Lemma 2.11 Let $f:X\to R$ be a differentiable function defined on a nonempty subset X of R^n.

(a) If f is B–(p,r,a) pseudo-invex function with respect to η and b on X, and k is any positive real number, then the function kf is B–$(p,\frac{r}{k},a)$ pseudo-invex functions with respect to the same η and b on X.

(b) If f is B–(p,r,a) quasi-invex function with respect to η and b on X, and k is any positive real number, then the function kf is $B-(p,\dfrac{r}{k},a)$ quasi-invex functions with respect to the same functions η and b on X.

In following section, B–(p,r,a)-invex functions, B–(p,r,a) quasi- invex functions and B–(p,r,a) pesudo-invex functions are discussed only when $p\neq 0, r\neq 0$, other cases will be deal with likewise because the only changes arise from the form of inequality. The proofs in the other cases are easier than in this one. Moreover,with-out limiting generality of considerations, we shall assu-me that $r>0$ (in the case when $r<0$, the direction of some of the inequalities in the proofs of theorems should be changed to the opposite one).

III. MOND-WEIR TYPE DUALITY

In this section, we consider Mond–weir type dual and establish some duality results for multiobjective problem in which corresponding functions belong to classes of B–(p,r,a)-invex functions, B–(p,r,a) quasi-invex func-tions, B–(p,r,a) pseudo-invex functions with respect to η and b.

We consider below vector programming

$$(VP)\ \min\ f(x)=(f_1(x),\cdots,f_k(x))$$
$$s.t.\quad g(x)=(g_1(x),\cdots,g_m(x)), x\in X\subset R^n.$$

where $f_i(x):X\to R, i=1,\cdots,k$, $g_j(x):X\to R$, $j=1,\cdots,m$ are differentiable, its Mond-Weir dual progra-mming defined as below

$$(VD)\ \max\ f(y)=(f_1(y),\cdots,f_k(y))$$
$$s.t.\quad \sum_{i=1}^{k}\lambda_i\nabla f_i(y)+\sum_{j=1}^{m}\mu_j\nabla g_j(y)=0; \quad (1)$$
$$\sum_{j=1}^{m}\mu_j g_j(y)\geq 0; \quad (2)$$

$$\lambda=(\lambda_1,\cdots,\lambda_k)^{\mathrm{T}}\geq 0,\ \mu=(\mu_1,\cdots,\mu_m)^{\mathrm{T}}\geq 0.$$

Theorem 3.1 (Weak duality).Suppose that

(i) x is a feasible solution of (VP), (λ,μ,y) is a feas-ible solution of (VD);

(ii) $\sum_{i=1}^{k}\lambda_i f_i$ is B–(p,r,a)-invex function with respect to η and b_0 at y, $\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,a) quasi- invex

function with respect to η and b_1 at y ;

(iii) $b_0(x,y)>0$ when $x\neq y$, $a(x,y)+c(x,y)\geq 0$.

Then $f(x) \leqq f(y)$ not hold.

Proof Since $g_j(x)\leq 0, \mu_j \geq 0,$ so $\sum_{j=1}^{m}\mu_j g_j(x)\leq 0,$ consider (2), we can get $\sum_{j=1}^{m}\mu_j g_j(x)\leq \sum_{j=1}^{m}\mu_j g_j(y),$ obviously have

$$\frac{1}{r}b_1(x,y)(e^{r(\sum_{j=1}^{m}\mu_j g_j(x)-\sum_{j=1}^{m}\mu_j g_j(y))}-1)\leq 0.$$

Using $\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,a)-quasi-invex function with respect to η and b_1 at y, we have

$$\frac{1}{p}\sum_{j=1}^{m}\mu_j\nabla g_j(y)(e^{p\eta(x,u)}-I)+c(x,u)\leq 0, \qquad (3)$$

relation (1), (3) along with $a(x,y)+c(x,y)\geq 0$, we can get $\frac{1}{p}\sum_{i=1}^{k}\lambda_i\nabla f_i(y)(e^{p\eta(x,u)}-I)+a(x,u)\geq 0$, since $\sum_{i=1}^{k}\lambda_i f_i$ is B–(p,r,a)-invex function with resp -ect to η and b_0 at y, we can get

$$\frac{1}{r}b_0(x,y)(e^{r(\sum_{i=1}^{k}\lambda_i(f_i(x)-f_i(y)))}-1)\geq 0.$$ by $b_0(x,y)>0,$ we get $\sum_{i=1}^{k}\lambda_i(f_i(x)-f_i(y))\geq 0,$ so $f(x) \leqq f(y)$ not hold.

Theorem 3.2 (Weak duality).Suppose that

(i) x is a feasible solution of (VP), (λ,μ,y) is a fea -sible solution of (VD);

(ii) $\sum_{i=1}^{k}\lambda_i f_i+\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,a)-invex function with respect to η and b_0 at y ;

(iii) $b_0(x,y)>0$ when $x\neq y$, $a(x,y)>0$.

Then $f(x) \leqq f(y)$ not hold.

Proof Suppose $f(x) \leqq f(y)$, then there exists $\lambda\in R^k{}_+$ such that $\sum_{i=1}^{k}\lambda_i f_i(x)\leq \sum_{i=1}^{k}\lambda_i f_i(y)$, also x is a feasible solution of (VP), (λ,μ,y) is a feasible solution of (VD), so there exists a $\mu\in R^m{}_+$ such that $\sum_{j=1}^{m}\mu_j g_j(x) \leq 0\leq \sum_{j=1}^{m}\mu_j g_j(y)$ so, $\sum_{i=1}^{k}\lambda_i f_i(x)+\sum_{j=1}^{m}\mu_j g_j(x)\leq \sum_{i=1}^{k}\lambda_i f_i(y)+\sum_{j=1}^{m}\mu_j g_j(y)$. easily get

$$\frac{1}{r}b_0(x,y)(e^{r[(\sum_{i=1}^{k}\lambda_i(f_i(x)+\sum_{j=1}^{m}\mu_j g_j(x))-(\sum_{i=1}^{k}\lambda_i(f_i(y)+\sum_{j=1}^{m}\mu_j g_j(y))]}-1)\leq 0.$$

using $\sum_{i=1}^{k}\lambda_i f_i+\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,a)-invex function with respect to η and b_0 at y, we have

$$\frac{1}{p}(\sum_{i=1}^{k}\lambda_i\nabla f_i(y)+\sum_{j=1}^{m}\mu_j\nabla g_j(y))(e^{p\eta(x,y)}-I)+a(x,y)\leq 0.$$

relation (1) along with $a(x,y)>0$, we can get a contr -adiction, so $f(x) \leqq f(y)$ not hold.

Lemma 3.3[4] We say that *g* satisfies the generalized Slater type constraint qualification at a feasible point *x* if there exists a feasible point *x* such that *g*(*x*) < 0.

Lemma 3.4[4] Suppose that x is an efficient solution of (VP), assume that the Slater type constraint qualificat-ion is satisfied at x. Then, there exist $\lambda\in R^k, \lambda\geq 0$, $\mu\in R^m, \mu\geq 0,$ such that

$$\sum_{i=1}^{k}\lambda_i\nabla f_i(x)+\sum_{j=1}^{m}\mu_j\nabla g_j(x)=0;$$

$$\sum_{j=1}^{m}\mu_j g_j(x)=0.$$

Theorem 3.5(Strong duality).Suppose that x is an effi -cient solution of (VP), (λ^0,μ^0,y) is a feasible solution of (VD), and the generalized Slater type constraint qualifica -tion is satisfied at x, then exist $\lambda\in R^k,\lambda>0$, $\mu\in R^m$, $\mu\geq 0$, such that (λ,μ,x) is a feasible solution of (VD) and the objective functions of (VP) and (VD) are equal at x. If the hypotheses of the weak duality theorem 3.1 are fulfilled, then (λ,μ,x) is a efficient solution of (VD).

Proof from lemma 3 we can get $\exists\lambda\in R^k, \lambda\geq 0$, $\mu\in R^m, \mu\geq 0,$ such that(4), (5) hold, so (λ,μ,x) is a feasible solution of (VD), from result of theorem 3.1, we can get $f(x) \leqq f(y)$ not hold for all feasible soluti -on of (VD), so (λ,μ,x) is an efficient solution of (VD).

Theorem 3.6(Strict Duality). Suppose that

(i) x and (λ,μ,y) be efficient solutions of problems (VP) and (VD), respectively;

(ii) $\sum_{i=1}^{k}\lambda_i f_i$ is B–(p,r,a) invex with respect to η and

b_0 at y, and $\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,c)quasi-invex function with respect to η and b_1 at y;

(iii) $b_0(x,y)>0$ when $x\neq y$, $a(x,y)+c(x,y)\geq 0$.

Then $x=y$.

Proof Suppose that $x\neq y$, since x is an efficient solutions of (VP), so $\sum_{i=1}^{k}\lambda_i f_i(x)<\sum_{i=1}^{k}\lambda_i f_i(y)$ for λ (appear in (λ,μ,y)). easily get

$\frac{1}{r}b_0(x,y)(e^{r(\sum_{i=1}^{k}\lambda_i(f_i(x)-f_i(y)))}-1)<0.$ Also since $\sum_{i=1}^{k}\lambda_i f_i$ is B–(p,r,a) -invex function with respect to η and b_0 at y, we can get

$$\frac{1}{p}\sum_{i=1}^{k}\lambda_i\nabla f_i(y)(e^{p\eta(x,u)}-I)+a(x,u)<0. \quad (4)$$

Since x and (λ,μ,y) be efficient solutions of problems (VP) and (VD), respectively, so

$\sum_{j=1}^{m}\mu_j g_j(x)\leq 0\leq\sum_{j=1}^{m}\mu_j g_j(y)$ for μ (appear in (λ,μ,y)), so

$\frac{1}{r}b_1(x,y)(e^{r(\sum_{j=1}^{m}\mu_j g_j(x)-\sum_{j=1}^{m}\mu_j g_j(y))}-1)\leq 0.$

Also $\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,a) quasi-invex function with respect to η and b_1 at y, we can get

$\frac{1}{p}\sum_{j=1}^{m}\mu_j\nabla g_j(y)(e^{p\eta(x,u)}-I)+c(x,u)\leq 0,$ relatio(1) along with $a(x,y)+c(x,y)\geq 0$, we can get

$\frac{1}{p}\sum_{i=1}^{k}\lambda_i\nabla f_i(y)(e^{p\eta(x,u)}-I)+a(x,u)\geq 0,$ it is a contradiction with (4), so $x=y$.

Theorem 3.7(Converse Duality). Suppose that

(i) x and (λ,μ,y) be efficient solutions of problems (VP) and (VD), respectively;

(ii) any one of the following conditions is satisfied:

(a) $\sum_{i=1}^{k}\lambda_i f_i$ is strictly B–(p,r,a) invex with respect to η and b_0 at y, and $\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,c) quasi-invex function with respect to η and b_1 at y;

(b) $\sum_{i=1}^{k}\lambda_i f_i+\sum_{j=1}^{m}\mu_j g_j$ is strictly B–(p,r,a) pseudo -invex function with respect to η and b_0 at y;

(iii) $b_0(x,y)>0$ when $x\neq y$, $a(x,y)+c(x,y)\geq 0$.

Then y be efficient solutions in problems (VP).

Proof Assume that the condition (a) is fulfilled. We proceed by contradiction. Suppose that y is not an effici -ent solution of (VP). Then there exists a feasible soluti-on of (VP) x such that $\sum_{i=1}^{k}\lambda_i(x)\leq\sum_{i=1}^{k}\lambda_i f_i(y)$, for λ (appear in (λ,μ,y)), easily get

$$\frac{1}{r}b_0(x,y)(e^{r(\sum_{i=1}^{k}\lambda_i(f_i(x)-f_i(y)))}-1)\leq 0.$$

Also $\sum_{i=1}^{k}\lambda_i f_i$ is strictly B–(p,r,a)- invex with respect to η and b_0 at y, we can get

$$\frac{1}{p}\sum_{i=1}^{k}\lambda_i\nabla f_i(y)(e^{p\eta(x,u)}-I)+a(x,u)<0.$$

Since x and (λ,μ,y) be efficient solutions of probl-ems (VP) and (VD), respectively, so $\sum_{j=1}^{m}\mu_j g_j(x)\leq 0\leq\sum_{j=1}^{m}\mu_j g_j(y)$ for μ (appear in (λ,μ,y)), so

$\frac{1}{r}b_1(x,y)(e^{r(\sum_{j=1}^{m}\mu_j g_j(x)-\sum_{j=1}^{m}\mu_j g_j(y))}-1)\leq 0.$

Also $\sum_{j=1}^{m}\mu_j g_j$ is B–(p,r,a)-quasi-invex function with respect to η and b_1 at y, we can get $\frac{1}{p}\sum_{j=1}^{m}\mu_j\nabla g_j(y)(e^{p\eta(x,u)}-I)+c(x,u)\leq 0,$ relation (1) along with $a(x,y)+c(x,y)\geq 0$, we can get $\frac{1}{p}\sum_{i=1}^{k}\lambda_i\nabla f_i(y)(e^{p\eta(x,u)}-I)+a(x,u)\geq 0,$ it is a contradiction with (4), so y be efficient solutions of prob -lems (VP).

When the condition (b) is fulfilled. We proceed by con -tradiction. If y isn't an efficient solution of (VP), there exists a feasible solution of (VP) x, $x\neq y$ such that

$\sum_{i=1}^{k}\lambda_i(x)\leq\sum_{i=1}^{k}\lambda_i f_i(y)$,by $\sum_{j=1}^{m}\mu_j g_j(x)\leq 0$, and $0\leq\sum_{j=1}^{m}\mu_j g_j(y)$, we have

$$\sum_{i=1}^{k}\lambda_i f_i(x)+\sum_{j=1}^{m}\mu_j g_j(x)\le$$

$$\sum_{i=1}^{k}\lambda_i f_i(y)+\sum_{j=1}^{m}\mu_j g_j(y)\ ,\text{by}\quad \sum_{i=1}^{k}\lambda_i f_i+\sum_{j=1}^{m}\mu_j g_j$$

is strictly B–(p,r,a)-pesudo-invex function with respect to η and b_0 at y, we obtain

$$\frac{1}{p}(\sum_{i=1}^{k}\lambda_i\nabla f_i(y)+\sum_{j=1}^{m}\mu_j\nabla g_j(y))(e^{p\eta(x,y)}-I)$$

$$+a(x,y)<0$$

It's a contradiction with (2) and (iii). Thus, *y* is an effic –ient solution of (VP).

Theorem 3.8(strictly converse duality) Suppose that

(i) x is a feasible solution of (VP), (λ,μ,y) is a feasible solution of (VD);

(ii) $\lambda^{\mathrm{T}} f(x)\le\lambda^{\mathrm{T}} f(y)+\mu^{\mathrm{T}} g(y)$, $\sum_{i=1}^{k}\lambda_i f_i+$

$\sum_{j=1}^{m}\mu_j g_j$ is strictly B–(p,r,a) pesudo-invex function with respect to η and b_0 at y;

(iii) $a(x,y)>0$, $b_0(x,y)>0$ when $x\neq y$.

Then $x=y$ and y is an efficient solution of (VD).

Proof Suppose that $x\neq y$,accordering to $\sum_{i=1}^{k}\lambda_i f_i+\sum_{j=1}^{m}\mu_j g_j$ is strictly B–(p,r,a) pesudo-invex function with respect to η and b_0 at y, we can get

$$\frac{1}{r}b_0(x,y)(e^{r[(\sum_{i=1}^{k}\lambda_i(f_i(x)+\sum_{j=1}^{m}\mu_j g_j(x))-(\sum_{i=1}^{k}\lambda_i(f_i(y)+\sum_{j=1}^{m}\mu_j g_j(y))]}$$

$$-1)\ge\frac{1}{p}(\sum_{i=1}^{k}\lambda_i\nabla f_i(y)+\sum_{j=1}^{m}\mu_j\nabla g_j(y))$$

$$(e^{p\eta(x,y)}-I)+a(x,y)>0$$

by $b_0(x,u)>0$, we can get

$$\sum_{i=1}^{k}\lambda_i f_i(x)+\sum_{j=1}^{m}\mu_j g_j(x)-\sum_{i=1}^{k}\lambda_i f_i(y)-$$

$\sum_{j=1}^{m}\mu_j g_j(y)>0$,consider $\sum_{j=1}^{m}\mu_j g_j(x)\le 0$, so

$\sum_{i=1}^{k}\lambda_i f_i(x)>\sum_{i=1}^{k}\lambda_i f_i(y)+\sum_{j=1}^{m}\mu_j g_j(y)$, it's a cont -radiction with (ii), so $x=y$.

If x isn't an efficient solution of (VP), then follow the proof of [Theorem 3.7], we can obtain *x* is an effici -ent solution of (VP).

IV. CONCLUSION

In this paper, we introduce new classes of generalized invex function, that is, classes of B–(p,r,a)-invex functions, B–(p,r,a) quasi-invex functions, B–(p,r,a) pseudo -invex functions and strictly B–(p,r,a) pesudo-invex functions, establish Mond-Weir dual problem multi- obje -ctive programming in which corresponding functions be -long to the introduced classes of functions, obtain many duality conditions under weaker convexity, which extend many results of [4].

Finally, duality problems of minimax fractional prog-ramming involving the introduced functions should be considered, Wolfe dual problem also should be consider -ed in the future.

REFERENCES

[1] T.Antczak, A class of $B-(p,r)$-invex functions and ma -thematical programming. J.Math.Anal.Appl. Vol.286, pp.187-206, 2003.

[2] C.R.Bector and C.singh, B-vexfunctions.J.Optim.Theory.Appl. Vol.71, pp. 237-253, 1991.

[3] T.Antczak, (p,r)-invex sets and functions. J.Math.Anal. Appl. Vol.263, pp. 355-379, 2001.

[4] T.Antczak,Generalized $B-(p,r)$ -invexity functions and nonlinear mathematical programming. Numerical functional Analysis and Optimazation.. Vol.30,pp. 1-22,2009.

[5] Qingxiang Zhang, Optimality conditions and duality for se-mi-infinite programming involving B-arcwise connected functions, Journal of Global Optimization ,Vol 45(4), pp 615-629.2009.

[6] Qingxiang Zhang, Yan Jiang , Ruirui Kang, Suffcient opti-mality conditions for multiobjective programming involving $(v,\rho)_{h,\varphi}-$ type I functions, Chinese Quarterly Journal of Mathematics, Vol.27,No.3, pp 409-416,2012.

[7] XiangYou Li, Saddle point condition for fractional program-ming. Preceedings of the 2012eighten international conference on computational intelligence and security. pp.82-85, Guang zh -ou.china Nov, 2012.

[8] Zhang Ying, Zhu bo, Xu Yingtao, A class of Lipschitz $B-(p,r)$ -invex functions and nonsmooth programming.OR Transactions. Vol.13, pp. 62-71, 2009.

[9] Liang Zhi'an, Zhang Zhenhua, The efficiency conditions and duality for uniform invex multiobjective program. OR Tran-sactions. Vol.13, pp.44-50, 2009.

[10] Morgan A. Hanson, Rita Pini and Chanchal singh, Multi-objective programming under generalized type I invexity. J. Math. Anal. Appl. Vol.261, pp.562-577, 2001.

[11] Yu guolin, Zhanng Suling, Efficient and duality for genera-lized convex multi-objective programming. Journal of Jilin uni -versity(natural science edition). Vol.45(5), pp.707-712, 2007 (in Chinese).

[12] Mohamed Hachimi, Brahim Aghezzaf, Sufficiency and duality in differentiable multi-objective programming involving generalized type I functions. J. Math. Anal. Appl. Vol.296,pp.382-392, 2004.

[13] Lin CuoYun, Dong Jiali, Theory and Methond of multi-obj -ective optimalition. Beijing. 1992.

[14] A.M. Hanson, Proper efficiency and theory of vector maxi-mization. J. Math. Anal. Appl. 22, 618-630, 1968.

Xiangyou Li was born in 1976, he received his master degree in Yanan University in 2004. Now he works in College of Math -ematics and Computer Science of Yanan University, engages in optimization theory, algorithm and application.

Qingxiang Zhang was born in 1954, a professor of Yanan University, engages in optimization theory, algorithm and Application.

Application Study on Intrusion Detection System Using IRBF

Yichun Peng[1,2,3], Yunpeng Wang[1,3] , Yi Niu[2] , Qiwei Hu[2]
[1]Guangzhou Institute of Geochemistry Chinese Academy of Sciences, Guangzhou, China
Email: yichunpeng678@hotmail.com
[2] City College of Dongguan University of Technology Dongguan, China
[3] University of Chinese Academy of Sciences, Beijing, China
Email: wangyp@gig.ac.cn, ny3388@163.com

***Abstract*—As an active and dynamic security-defense technique, intrusion detection can detect the interior and exterior attacks, and it plays an important role in assuring the network security. Based on immune recognition algorithm, a Radial Basis Function (RBF) neural network learning algorithm was studied. In this algorithm, the input data is regarded as antigens and antibodies are regarded as the hidden layer centers, the weights of the output layer are determined by adopting the Recursive Least Square method, which can improve convergence speed and precision of the RBF neural network, using Snort to establish innate antibody and using negative selection algorithm to generate detectors. This algorithm was applied to Intrusion Detection Systems. Theory and experiment show that this algorithm has better ability in intrusion detection, and can be used to improve the efficiency of intrusion detection, and reduce the false alarm rate.**

***Index Terms*—Intrusion Detection; Radial Basis Function Neural Network; Clonal Selection; Immune Algorithm; Snort; Negative Selection**

I. INTRODUCTION

Network, especially Internet, has brought unprecedented chances and challenges to the society in the 21st century. On one hand, the normal running of network has brought great progresses and wealth to the society. On the other hand, it has caused unexpected disasters and losses by the insecurity of network. The relationship between security threats and ensured safety is just like the spear and the shield. Nowadays, in order to deal with all kinds of infinite changing attacks, people have taken a variety of anti-attack means, among which intrusion detection system (IDS) is the second security gate behind the firewall. IDS can be used to detect all kinds of intrusion behaviors, active intercept, and dynamic reacts to the vicious intrusions before the network system is jeopardized. However, the promotion of network bandwidth, the diversity of attacking forms, the diversification of attacking means, and intelligence of attacking technologies have increased the difficulty of intrusion detection, which has greatly reduced the practicability of the intrusion detection system. The disadvantages include high rates of incorrectness of detection intrusion, high rates of false positive, and bad activations. The following are the biggest disadvantages:1) the high missing rate of detection 2) the high false detecting rate 3) poor autonomous and less intelligent detection 4) mainly by human activities not automatically action after detecting invasions. In order to overcome the deficiencies of the existing IDS, in this paper, Radial Basis Function (RBF) neural network and Immune Algorithm (IA) are combined to form a kind of Immune Radial Basis RBF (IRBF) network training Algorithm, which can not only distinguish normal and abnormal data in the network, but also diagnose invasion types, take special precautions and further respond to specific invasions as well. The experimental results showed that IRBF based intrusion detection technology can accurately distinguish and identify a variety of parallel invasion. It has faster processing speed, enough fault-tolerant and the powerful ability of self-learning and self-adjusting. Therefore, intrusion detection systems can be a truly intelligent security gate in network.

II. RELATED TECHNOLOGIES

A. RBF Neural Network

RBF neural network is a kind of local approximation neural network, which has very strong approximation ability, classification ability and learning speed. Its working principle is to put the network as the approximation of unknown function, which means any functions can be expressed as weighted sum for a set of basis functions. That is to say, it chooses transfer functions of each hidden layer's neurons to form a set of basis function which approximate the unknown function. The structure of RBF neural network is shown in Figure 1. It is a three-layer feed forward neural network: input layer, hidden layer and output layer, and the number of their respective units are m, q, p.

This work was supported in part by a grant from the Scientific and Technological Projects of Guangdong (No. 2009B010800042), and in part by Projects of Science and Technology of Dongguan(No. 201110825100119).

doi:10.4304/jsw.9.1.177-183

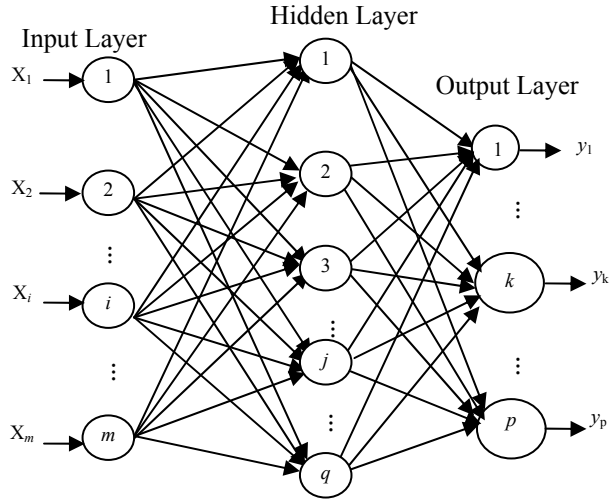


Figure 1. The Structure of RBF Neural Network

The hidden layer of RBF neural network chooses the function of Gauss as the basis function, which sets the input of the input layer as $X=(x_1,x_2,...,x_j,...,x_n)$, but the actual output is $Y=(y_1,y_2,...,y_k,...,y_p)$., Input layer is to achieve non-linear mapping of $X \to R_i(x)$, output layer is to realize linear mapping of $R_i(x) \to y_k$, network output of the K-th neuron of output layer is:

$$\hat{y}_k = \sum_{i=1}^{m} \omega_{ik} R_i(x) \qquad (k=1,2,...,p) \tag{1}$$

Where, n is the input layer nodes, m is the hidden layer nodes, and p is the output layer nodes; ω_{ik} is the connection weight between the i-th neuron of hidden layer and the K-th neuron of output layer. $R_i(x)$ is an action function of the i-th neuron of hidden layer, just as formula (2) below:

$$R_i(x) = \exp(-\|x-c_i\|^2 / 2\sigma_i^2), (i=1,2,\mathrm{L},m) \tag{2}$$

Where, x is an n-dimensional input vector, ci is the center of the k-th basis function, the same dimension vector as x, σi, which determines the width of the basis function around the center point, is the i-th perception variables; m is the number of perception unit (hidden node number). $\|x-c_i\|$ is the norm of vector x-ci, and it usually indicates the distance between x and ci; $R_i(x)$ has a unique maximum value in ci, with the increasing of $\|x-c_i\|$, $R_i(x)$ rapidly decays to zero. For a given input, only a small portion near the centre of x is activated. When the cluster center ci of RBF network and weights ω_{ik} are determined, we can obtain the network output value according to a certain input.

It is critical to select the center ci of RBF neural network. The following are the two main ways: according to the experience and using the clustering method (such as K means clustering method). However, these two ways are more difficult to achieve the network global optimal value of the center and width of basic function. In this paper, we use immune recognition algorithm which is based on clonal selection to determine the center of RBF neural network.

B. Immune Algorithm

The concept of modern immunity refers to the function that the body distinguishes between self and non-self, even excludes non-self, and the purpose is to maintain its own physiological balance and stability. Immune algorithm is a new kind of intelligent learning algorithm which simulates the biology immunity systems; it is one of the main content of the Artificial Immune System (AIS). Immune algorithm has a good system response, dynamic and autonomy, and has the strong ability to maintain self-balancing when the system is interfered. In addition, immune algorithm also simulates some special functions of immune system such as learning, memory and recognition. It has the very strong ability to classify the pattern, especially for multi-modal problem analysis, processing and solving, which exhibits a higher intelligence and robustness. Immune algorithm has been applied to a variety of single target, multi-objective optimization and engineering optimization, for example, automatic control, abnormal and fault diagnosis, the robot behavior simulation, robot control, network intrusion detection, neural network design and other fields, and has shown more excellent performance and efficiency. In addition, immune algorithm has been applied in pattern recognition, image recognition, design optimization, data mining, information processing, associative memory, bank identification for mortgage fraud, etc.

III. Research on Intrusion Detection System Based on IRBF Neural Network Learning Algorithm

In this paper, the IRBF neural network training algorithm is that it uses immune recognition algorithm which is based on clonal selection to determine the data center of hidden layer of RBF neural network, and then uses the formula (2) to calculate the output of hidden layer after the center of hidden layer is determined. Furthermore, it uses the least squares method to calculate the weighted between hidden layer nodes and output nodes. Finally, we can get the final output of the RBF neural network.

A. Uses Immune Recognition Algorithm Which is Based on Clonal Selection to Determine the Data Center of Hidden Layer of RBF Neural Network

In the course of development of immune algorithm, immune recognition algorithm based on clonal selection has been investigated by many scholars. It is an evolutionary algorithm which simulates the learning process of the biological immune systems. its essence is Darwinian selection and mutation theory, using the strategy of antibody set population updating.

The input data as antigen, RBF network of the hidden layer center is corresponding to antibody, using this algorithm to get the diversity of antibody memory set as the hidden layer data center. The algorithm's steps are as follows:

(1) Initializing. Input antigen and determining the size of the initial population N, the total number of clone M, randomly generated N antibodies that constitute the initial antibody population A_0, which is defined as the problem of possible solutions (or random solution).

(2) Calculate affinity. Calculate the affinity of each antibody in the A_0, and A_0 will be decomposed into A_m and A_r, wherein, A_m represents an antibody memory set in which the affinity of antibody is higher, A_r represents the remainder of the antibody set. The computation formula of the affinity is as follows:

The matching degree between antigen x_i and antibody c_j is called affinity degree:

$$a_{ij} = \frac{1}{1+\left\|x_i - c_j\right\|} \tag{3}$$

When $x_i = c_j$, affinity degree a_{ij}=1 is maximum;

The matching degree between antigen c_i and c_j is called similarity degree:

$$s_{ij} = \frac{1}{1+\left\|c_i - c_j\right\|} \tag{4}$$

When c_i=c_j, similarity degree s_{ij}=1 is maximum;

(3) Cloning. To choose k antibodies whose affinity degree is the highest for cloning, the number of cloning is proportional to the affinity degree of antibody, that is, the higher affinity antibodies have a higher chance to be searched.

(4) Variation. Each clone cell is mutated according to its affinity mutation operator, the mutation bit number is inversely proportional to the affinity of its antigen, to get cloning set C_n, cloning inhibition operator acting on C_n and to get the cloning set C_n^*, and to calculate the affinity of each new antibody and antigen.

(5) Excellent antibodies screening. In C_n^*, if the highest affinity antibody whose affinity is even higher than the affinity of its parent antibody, then using it to replace the original antibody, and form a new memory set D_m.

(6) Clone inhibition. Calculating the similarity degree among those antibodies, the higher the similarity degree of antibody, the greater the antibiotic activity, . Selecting the inhibition threshold and exclude those high similarity degree antibody according to the formula below:

$$t_s = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} s_{ij}}{M(M-1)} \times 2 \tag{5}$$

Where, M represents the total number of antibody in the current antibody set.

(7) Generate memory set. Detecting all antigen whether they have learned completely, if yes, then merging all antibody memory sets which including all antibodies generated by antigen; otherwise, turn to step 2), restart.

(8) Immune depression. Calculating the similarity degree among each memory cell, and excluding those high similarity degree antibody according to formula (5) .

(9) Checking whether it reaches the maximum evolution generation. If so, the current memory set is the optimal solution of the problem, then to output results and end, otherwise, turn to step 2), restart.

B. Least Squares Recursive Method to Adjust Weights

There are three methods to calculate the weight between the hidden layer nodes and the output nodes, which are negative gradient descent direction of minimum variance method, recursive least squares method (RLS) and mirrored the least squares method. Among them, the RLS is often used because it has good global convergences. Define the objective function:

$$j(t) = \sum_{p=1}^{L} E_p(t) = \frac{1}{2}\sum_{p=1}^{L} \lambda(p)[d_p(t) - y_p(t)]^2 \tag{6}$$

Where, L is the length of the sample, $\lambda(p)$ is the weighting factor($0< \lambda(p) <1$), d_p is the target output sample, y_p is the actual output sample.

Through $\frac{\partial j(t)}{\partial w} = 0$ to calculate W, which makes $j(t)$ get minimum value, then, this w is the required weight.

$$\begin{aligned} w_p(t) &= w_p(t-1) + k(t)[d_p(t) - q_p^T(t)w_p(t-1)] \\ k(t) &= p(t-1)q_p(t)[q_p^T(t)p(t-1)q_p(t) + \frac{1}{\lambda(p)}]^{-1} \\ p(t) &= [L - k(t)q_p^T(t)]p(t-1) \end{aligned} \tag{7}$$

Where, $q_p(t) = [q_{1p}(t), q_{2p}(t), ..., q_{Lp}(t)]^T$, L is the number of hidden layer nodes.

Because the weight only exists between the hidden nodes and the output nodes, the computational requirements for the RBF network training are very less. Neural network is trained to generate the appropriate structures and parameters, and will be able to detect the network data in intrusion detection.

C. IRBF based on Intrusion Detection Model

The structure of intrusion detection model based on IRBF is shown in Figure 2:

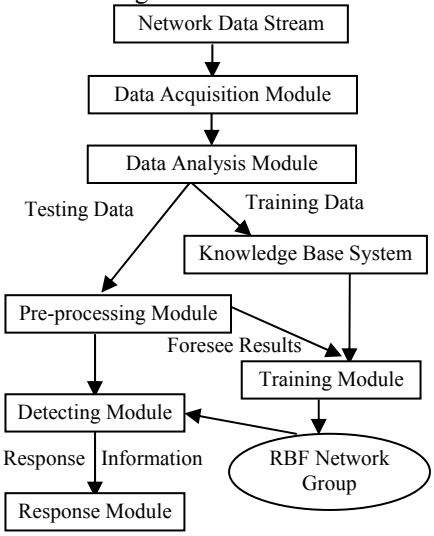


Figure 2. The Structure of Intrusion Detection Model Based on IRBF

Each module is described as follows:

(1) Data acquisition modules. It's responsible for

grasping network packets, and sends them into data analysis module.

(2) Data analysis module. Data analysis module can be snort, TCP dump or development packet protocol analysis program, its function is packet filtering and classification, then it obtains the required data header information, and stores it. Firstly, preliminary filtering, checking the format of IP packets, restructuring if it is subdivision. Secondly, distinguishing IP packet, UDP packet, or ICMP packet event, and then calling and semantic analyzing different analyzer program segment according to the different protocol type of the packet. Finally, sending the information of the packet which meets the requirement to the pre-processing module.

(3) Pre-processing module. In the process of generating detector, the received training samples will be transformed into binary format by TCPdump For detecting process, the received pocket header information, which will be transformed into binary format by TCPdump, and as the input of RBF neural network, the processed data can also be directly sent into the detector module, but if attack types of the current data has been identified, then the processed data can be send into the training module for RBF neural network training, in order to achieve the real-time monitoring and continuous self-learning.

(4) Knowledge base system. Knowledge base system can be replaced with a simply including abnormal behavior rules set and it is used to decide what kind of packets and session will be monitored and accessed. The existence of these rules has two functions. One corresponds to the congenital antibody of biological immune system, and can accurately detect some known intrusions; the other puts forth some limit condition when the detector is generated to reduce the generating time and the occupied space of the detector.

(5) Training module. Combined with knowledge base system and foresee results, using the above algorithm to train the pre-processed data and generate RBF network group.

(6) RBF network group. It is the core part of intrusion detection, and used for detecting data and outputting the result. RBF network group pertinently enters the detecting module to detect data, and at the same time, it is also continuously updated, with the arrival of the new learning data and detecting continuously, the number and internal structure of the RBF network group will also be changed.

(7) Detecting module. Containing the most affinity RBF network relative to the data waiting for detecting, final discriminating the output of the RBF network group, and sending the result to the response module for processing

(8) Response module. Determining the intrusion behavior and alarm information to notify the network administrator or take corresponding measures, such as cutting off connections, tracking the attacker, etc.

Among them, the detector module plays a vital role in the intrusion detection system, and at the same time, without response module, the intrusion detection system will lose the value of its existence. The following are the further study on these two modules.

1) Generation of the Detector

The human immune system can be divided into innate and acquired immune by the immune response. Therefore, this system also be designed two kinds of detector: one kind is innate detector, is to establish detection rules based on expert knowledge to realize the same known intrusion detection, the other kind is acquired detector, which is to be established by negative selection to achieve the unknown intrusion detection.

While the system is running, its antibody vaccine is produced by the antibody gene library which includes expert antibody library and adaptive antibody gene library, among which:

Expert antibody library consists of created rules, which is equivalent to the body's innate immunity. As the body's immune system can't resist all allogenic attacks, networks may also contain some new form of attacks, which may escape detection range of the detection system, in this case, establishing a new detection rule based on this attack to implement the intrusion detection. To establish an expert antibody library not only can improve some known intrusion detection efficiency and accuracy bat also can decrease the expenditure of time and space to generate adaptive antibody library.

The adaptive antibody library is a new antibody library which is formed by the immune genetic computing mechanism. The antibody of adaptive antibody library was formed after the field (i.e. the antibody gene) which represents the characteristics of the invasion in the network data packet header to be encoded. And each antibody has an adaptive value A, if some antibody (detector) has successfully detected corresponding intrusion behavior, then A value is added 1; Conversely, if some detector has not detected the invasion for long time (survival period), then the A value is misused 1.When the value of A is less than 0, the detector will be deleted from the adaptive antibody library, which is equivalent to the biological cell death. This mechanism can ensure that the adaptive antibody library saves its most active antibody, which is also consistent with the biology of natural selection, namely the principle of survival of the fittest. In the intrusion detection system, which generates candidate antibody library after the existing alien mode (namely antigen) has been mutated, and there is a negative selection on each new candidate antibody with existing alien pattern. If they are completely matched then new candidate antibody will be deleted, the last remaining effective antibody is stored in the adaptive antibody library, and is used for the detector to detect intrusion.

i. THE ESTABLISHMENT OF INNATE ANTIBODY

The establishment of innate antibody is based on misuse intrusion detection method. Here, we adopted Snort-based intrusion behavior description method, which is simple, easy to implement, detection rapidly and can describe the vast majority of intrusion behavior.

Snort stored all known attacks in the form of rules in the rule library. Each rule is composed of the rule header and the rule option. Rule header is corresponding to the

Rule Tree Node (RTN), including action, protocol, source (destination) address, port and data flow direction; Rule option is corresponding to the Optional Tree Node (OTN), including alarm information (MSG), matching content options. It is not an essential part of the rule and it is only used to define and collect specific characteristics of specific data packets. When Snort initialize and parse rules, TCP, UDP, ICMP and IP four different rules tree are established respectively, each rule tree contains independent 3D linked list: RTN (rule head), OTN (rule option) and point matching function pointer.

Here is an example to illustrate the composition of the rules:

alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg:"mounted access";)

Description: data packets of 111 port of any host that uses the TCP protocol to connect to 192.168.1.0/24 network, if in which a binary data “00 01 86 a5” has appeared, then the system will issue a warning message” mounted access”.

In this rule: "alert TCP any any->192.168.1.0/24 111" is the rule header; "content:’|00 0186 a5|’;msg:’mounted access’;" is the rule option, in front of colon phrases is called the option keyword. A rule only to be executed when different parts of it must be satisfied simultaneously which is equivalent to the "and" operation, and among all rules is equivalent to an "or" operation in a same rule database file.

The first part of rule header is action, which indicates what should be done when it finds the data pocket that is suitable for its conditions. There are five predefined action: Alert, Log, Pass Activate and Dynamic, and can also customize action; The second part is protocol, which shows what type of pocket will be compared with the rule. At present, Snort supports the following protocols: TCP, the IP, UDP, and ICMP; The third part is data packet's source and destination IP address and port, behind the IP address, it specifies the network mask, for example, /16 specify the class B network, /24 specify the class C network, and /32 specify a particular host, the port number can be specified in several ways: "ANY", digital, ":" (range) and "!" (not), where "ANY" specify any port, number specifies a single port, such as 80 for HTTP, 23 for telnet, etc, between these two address and port is direction section, which determine the source and destination, "->" indicates a direction from left to right, "<-" indicates a direction from right to left , and "<>" indicates the rule will be used in both directions. You can use it when the system must monitor server and client simultaneously, for example, monitoring the data flow of POP or Telnet server that comes and goes.

Rule option may include more than one option, there use ";" to separate different options, and use logic operator "AND" to express it. Option consisted of keywords and parameters, each keyword and its parameters using ":" to separate. At present, those following keywords can be explained: msg,logto, ttl, id, dsize, content, offset, depth, nocase, flags, seq, ack, itype, icode, session, icmp_id, icmp_seq, ipoption, rpc and resp, etc.

ii. THE FORMATION OF ADAPTIVE ANTIBODY

Gene and encoding are very important in the intrusion detection system based on biological immune. According to expert the knowledge and experience, we have extracted some intrusion detection features from all fields of network data packet as the gene that will be encoded and be generated antibody (namely detector). Since the operation must be accomplished by reorganization, selection and quantitative calculation of individuals with a certain structure form in the population, it needs a direct digital representation, namely, encoding. Encoding refers to a process that images phenotype into genotype, among them, phenotype refers to readable rules directly received by joining records, genotype means an internal form in proceeding antibody evolution, negative selection and clonal selection, the corresponding relationship between the phenotype and the genotype as shown in Table I.

TABLE I.
THE CORRESPONDING RELATIONSHIP BETWEEN THE PHENOTYPE AND THE GENOTYPE

The phenotype of detector	*ScrIP DesIP ProType Scrport Desport flag …*
The genotype of detector	110011… 011111000… 00000110…00101000

In the paper, we have consulted the principle of using negative selection algorithm to generate detectors, which was proposed by Stephanie Forrest group of Department of Computer at New Mexico University, USA. This principle is shown as in figure 3.

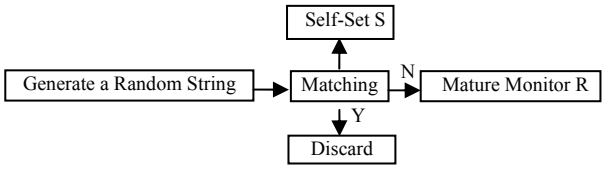


Figure 3. The Generation of Effective monitor

The model was originally used to generate detector set for detecting viruses, and achieve success, later, to be applied in the UNIX operating system which can detect several intrusion, such as sendmail, lpr, however, for the generation of the detector in intrusion detection system, using purely random string (that is, the candidate antibody) to produce effective antibody which is low-efficiency and time consuming. In this paper, we make some improvements to this method. Firstly, encoding the known intrusion patterns, then evolving the genetic operator. Finally, generating candidate antibody library. The steps of algorithm are as follows:

Step 1) Generating self set and non-self set, and encoding.

Step 2) Evolving non-self set through mutation, generating the initial candidate antibody library.

Step 3) Detecting the candidate antibody with expert rules, if in accordance with the rule then delete it, otherwise, turn to Step 4.

Step 4) Matching the candidate antibody generated by mutation with the original antigen, if they are matching then delete the candidate antibody, otherwise, turn to Step 5.

Step 5) Matching those remaining candidate antibodies after selected by Steps 2 and Step 3 with

normal set, if they are matching then delete the candidate antibody, if not, the candidate antibody become mature antibody, and will be used to detect intrusion behavior.

Compared to the original algorithm, this algorithm has some advantages as follows: the newly generated candidate detector is based on the existing abnormal mode based, and is not an impossible mode. Thus, it can make the number of candidate detector not need so much like the original algorithm, and these candidate detectors are effective, which will be helpful for protecting the detection efficiency and saving storage space.

2) Intrusion Response and Confrontation

The most simple automatic intrusion response of intrusion detection system is to inform: when the system detects intrusion occurs. It will send an E-mail or a message to the administrator. An initiative response is to prevent the ongoing attacks, make the attacker unable to continue to access. For example, truncating the connection between the attacker and the target host through injecting reset datagram, restricting the access of an intruder through updating the configuration of firewall, and so on; A more initiative response is to counterattack the attacker, but this method is very dangerous, it may affect innocent users in the network, but also is illegal. Automatic response is the cheapest and the easiest response way, as long as can be wise and carefully implemented. It is still relatively safe. However, it has two problems: for one thing，since the system has the potential to create false alarm, there may response to a network node which never attacks us by mistake; for another, if an attacker determines our system with automatic response, he might take advantage of this to attack us, for example, he may connect two network nodes with automatic response intrusion detection system to establish a feedback loop which is equivalent to echo-charged, then makes address spoofing attack to those two nodes.

Take different response mechanisms for different types of "non-self": for connection-oriented protocol (such as illegal TCP connection), directly reset it; for non-connection-oriented protocols (such as illegal UDP data), alarm and timely notify the system administrator. If it is found that other unknown protocol (e.g., the system's own non-standard protocol) can also alarm and notify the system administrator, the administrator check system alarm and log, if it is the system normal data then confirm its legality in safety rules and become a member of "self" set, otherwise, there need timely adjustment of the firewall rules (e.g., using linkage method) to perfect object security rules and trace intrusions.

The process of alarm decision-making is as follows:

The response module receives alarm information from the detector module, firstly, alarm information will be analyzed locally, if it can't be determine, this response module requests other node's response module to determine local analysis by requisition-coordination, which is based on cooperative mechanism of biological immune. Its basic principle is: if more than a certain number of detector modules detect the behavior and administrators also confirm that it is intrusion behavior, the behavior is an intrusion behavior; Then, in determining the alarm is a kind of intrusion behavior, response module makes general response, but also converts alarm into memory antibody, the administrator can also generates memory detector through the features generator of the detection module; Finally, the response module distributes memory detector to other nodes, so that other nodes can rapidly response to the same invasion in the future, which draw lessons from biological immune secondary response mechanism.

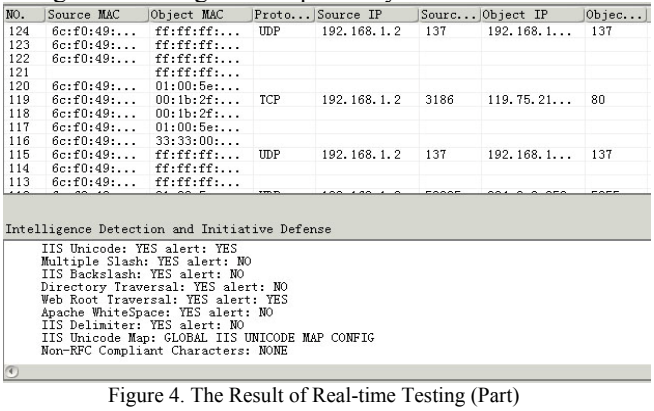
IV. Experimental Results and Analysis

The experiment adopts KDD Cup 1999 data set released by the Lincoln Laboratory of the United States. This data set consists of 4 categories (PROBE, DoS, U2R, R2L) , and 39 attack types for a total of 5000000 records; it also provides a 10 percent training subset and testing subset, there are 22 of attacks in the training subset and 17 types remained in the testing set. The purpose of this design is to test the generalization ability of the classifier model. The ability to detect the unknown attack types is an important index to evaluate whether the intrusion detection system is good or not

As to selecting samples, selecting Dos and Normal types data, and only choosing R2L, Probe types data records mixed with R2L type data. There are 494021 records in the selected 10 percent data subset, which includes 97278 normal data records and 396473 abnormal data records. The proportion of normal data to abnormal data is 9:1, which is in conformity with general rules of intrusion detection.

We selected 11 representative vector elements in RBF neural network's input layer: source IP address, destination IP address, the IP packet flag, the total length of the IP packet, IP header length, protocol code, source port number, destination port number, TCP flags, TCP window size, and the first byte of the data segment. These data are input into RBF network after they have been normalized.

In order to make "own" library development perfect, firstly, the intrusion detection system should learn in safety network flow. The system will gradually produce antibodies in the training process. Experiments are made on each type of attack, and each type uses 10 records. There are two ways for experiments to test: real-time testing and off-line testing. The results (part) are shown in Figure 4 and Figure 5 respectively:



NO.	Source MAC	Object MAC	Proto...	Source IP	Sourc...	Object IP	Objec...
124	6c:f0:49:...	ff:ff:ff:...	UDP	192.168.1.2	137	192.168.1...	137
123	6c:f0:49:...	ff:ff:ff:...					
122	6c:f0:49:...	ff:ff:ff:...					
121		ff:ff:ff:...					
120	6c:f0:49:...	01:00:5e:...					
119	6c:f0:49:...	00:1b:2f:...	TCP	192.168.1.2	3186	119.75.21...	80
118	6c:f0:49:...	00:1b:2f:...					
117	6c:f0:49:...	01:00:5e:...					
116	6c:f0:49:...	33:33:00:...					
115	6c:f0:49:...	ff:ff:ff:...	UDP	192.168.1.2	137	192.168.1...	137
114	6c:f0:49:...	ff:ff:ff:...					
113	6c:f0:49:...	ff:ff:ff:...					

Figure 4. The Result of Real-time Testing (Part)

```
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 152.163.210.24:80 -> 172.16.113.105:17341
[**] [1:384:5] ICMP PING [**] [Priority: 0] {ICMP} 192.168.1.2 -> 192.168.1.1
[**] [1:408:5] ICMP Echo Reply [**] [Priority: 0] {ICMP} 192.168.1.1 -> 192.168.1.2
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 207.25.71.141:80 -> 172.16.116.194:17873
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 205.181.112.65:80 -> 172.16.114.207:18499
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 205.181.112.65:80 -> 172.16.114.207:18500
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 205.181.112.65:80 -> 172.16.114.207:18507
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 205.181.112.65:80 -> 172.16.114.207:18513
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 209.143.225.42:80 -> 172.16.116.194:18524
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 209.143.225.42:80 -> 172.16.116.194:18525
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 209.143.225.42:80 -> 172.16.116.194:18562
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 209.143.225.42:80 -> 172.16.116.194:18571
[**] [1:648:8] SHELLCODE x86 NOOP [**] [Priority: 0] {TCP} 172.16.114.148:20 -> 195.115.218.108:8255
[**] [1:648:8] SHELLCODE x86 NOOP [**] [Priority: 0] {TCP} 172.16.114.148:20 -> 195.115.218.108:8255
[**] [1:648:8] SHELLCODE x86 NOOP [**] [Priority: 0] {TCP} 172.16.114.148:20 -> 195.115.218.108:8255
[**] [1:648:8] SHELLCODE x86 NOOP [**] [Priority: 0] {TCP} 172.16.114.148:20 -> 195.115.218.108:8255
[**] [1:648:8] SHELLCODE x86 NOOP [**] [Priority: 0] {TCP} 172.16.114.148:20 -> 195.115.218.108:8255
[**] [1:648:8] SHELLCODE x86 NOOP [**] [Priority: 0] {TCP} 172.16.114.148:20 -> 195.115.218.108:8255
[**] [1:648:8] SHELLCODE x86 NOOP [**] [Priority: 0] {TCP} 172.16.114.148:20 -> 195.115.218.108:8255
[**] [1:1463:7] CHAT IRC message [**] [Priority: 0] {TCP} 194.7.248.153:8034 -> 192.168.1.20:6667
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 205.181.112.65:80 -> 172.16.114.207:19262
[**] [1:2925:4] INFO web bug 1x1 gif attempt [**] [Priority: 0] {TCP} 205.181.112.65:80 -> 172.16.114.207:19908
[**] [1:1463:7] CHAT IRC message [**] [Priority: 0] {TCP} 194.7.248.153:8034 -> 192.168.1.20:6667
[**] [1:895:7] WEB-CGI redirect access [**] [Priority: 0] {TCP} 172.16.116.194:20415 -> 207.46.176.50:80
[**] [1:1463:7] CHAT IRC message [**] [Priority: 0] {TCP} 194.27.251.21:4257 -> 192.168.1.20:6667
[**] [1:1463:7] CHAT IRC message [**] [Priority: 0] {TCP} 194.7.248.153:8034 -> 192.168.1.20:6667
[**] [1:1463:7] CHAT IRC message [**] [Priority: 0] {TCP} 194.27.251.21:6117 -> 192.168.1.20:6667
[**] [1:1463:7] CHAT IRC message [**] [Priority: 0] {TCP} 194.27.251.21:6117 -> 192.168.1.20:6667
[**] [1:1463:7] CHAT IRC message [**] [Priority: 0] {TCP} 194.7.248.153:6957 -> 192.168.1.20:6667
```

Figure 5. The Result of Off-line Testing (Part)

In the last experiment, we have sampled all types of data records by interval sampling, and observed the detection precision as shown in Table II in four experiments:

TABLE II.
THE OFF-LINE DETECTION RESULT

Sample Type	*Detection Precision*
Dos+Normal	98.6%
R2L+Normal	69.5%
Probe+Normal	75.7%
All Types	83.7%

The experiments showed that it is not only able to distinguish between "self" and "non-self" network data, but also to identify those four types of known intrusion: DoS, R2L, U2R, and probing. However, nowadays no intrusion detection system can find all the invasion, and still exist false positive and false negative. IRBF algorithm also contains such defects.

V. CONCLUSIONS

This paper presents an intrusion detection system model based on IRBF neural network learning algorithm, and the model determines the center of RBF neural network by means of cloning, mutation and suppression immune algorithm, and uses the recursive least square method to adjust the weight between hidden layer and output layer of RBF network. Moreover, the model has advantages of less computation, faster convergence speed, high precision, and good real-time performance. The model is applied to intrusion detection system, and the experiments showed that it can not only detect the known intrusion, but also detect unknown intrusion to some extent, which reduces the rate of false positives and false negative rate of traditional intrusion detection systems, and improves the system learning efficiency and intelligence.

REFERENCES

[1] Li Xin-yu, Zhou Tie-jun, "Research of Intrusion Detection Optimization Algorithm based on RBF Neural Network," *Computer Security*, no.4, 2011,pp.29-32.

[2] Liu Dihua, Yu Bin, Wang Xiaofen, "Research on Intrusion Detection Model based on RBF Neural Network," *Network Security Technology & Application*, no.12,2008,pp.36-38.

[3] Huang Yuanjiang, "Prediction of debris flow based on IRBF neural network," *Journal of Central South University of Forestry & Technology*, no.3,2010,pp.159-163.

[4] Deng Guanghui, Jing Dongxing, Ye Jixiang, "Emotion Recognition of Speech Signals Based on the Immune Radial Basis Function Networks," *Computer Engineering & Science*,no.9,2009,pp.153-159.

[5] Qiu Chuchu, You Dade,Ma Ye, Wang Weiyan, "Prediction of carrier UAV based on IRBF neural network,", *Ship Science and Technology*,2011(11):109-111.

[6] Bao Wensheng, Liu Xiaogang, "Structure Optimization Algorithm of RBF Neural Networks based on Adaptive Genetic Algorithem," *Journal of Shandong Normal University(Natural Science)*,no.3,2007,pp.37-39.

[7] Yang Shu-yuan , Jiao Li-cheng, Liu Fang, "An immune RBF neural network MUD method," *Journal of XIDIAN University (Natural Science)*,no.4,2004,pp.209-213.

[8] Niu Yi, Zhang Quanju, Zheng QiLun, Peng Hong, "Security Operation Center Based on Immune System," *Workshops International Conference on Computational Intellignece and Security. Harbin,China: IEEE Computer Seciety Press*, no.11,2007,pp.97-103.

[9] Niu Yi, Zheng QiLun, Peng Hong, "Security Operation Center Design Based on Radial Basis Function Neural Network," *Dynamics of Continuous, Discrete and Impulsive Systems*, no3,2007,pp.1133-1140

[10] Paul K Harmer, Paul D Williams, Gregg H Gunsch, Gray B Lamont, "An Artificial Immune System Architecture for Computer Security Applications," *IEEE Transactions on Evolutionary Computation*, no.3,2002,pp.252-280.

[11] Lei Wang, Beat Hirsbrunner, "Immune Mechanism Based Computer Security Design," *Proceeding of the First International Conference on Machine Learning and Cybernetics*, no.11,2002, pp.1887-1893.

[12] Hamid Reza Golmakani, Elnaz Jalilipour Alishah, "Portfolio Selection Using An Artificial Immune System," *IEEE Congress on Information Reuse and Integrations*, vol.28, no.3, 2008, pp.65-72.

A Fast Algorithm for Undedetermined Mixing Matrix Identification Based on Mixture of Guassian (MoG) Sources Model

Jiechang Wen[1]
[1] School of Applied Mathematics, Guangdong University of Technology, Guangzhou, China
Email: wjcpig@126.com

Suxian Zhang [2], Junjie Yang[3]
[2] School of Information Engineering, Guangdong University of Technology, Guangzhou, China
Email: zsxchn@yahoo.cn
[3] School of Automation, Guangdong University of Technology, Guangzhou, China
Email: yangjunjie0807@163.com

***Abstract*— This paper proposes a new fast method for identifying the mixing matrix based on a binary state mixture of Gaussian (MoG) source model. First, a necessary discussion for solving the mixing matrix detection is offered under the multiple dominant circumstance. Second, a density detection method is presented to improve the identification performance. Simulations are given to demonstrate the effectiveness of our proposed approach.**

***Index Terms*— blind source separation (BSS); sparse component analysisSCA; density detection; mixture of Gaussian (MoG) model.**

I. INTRODUCTION

As a result of the widely application in the area of speech recognition, wireless communication and biological medical signal processing, Blind Source Separation (BSS) [1-6] is becoming one of the hottest spots in the signal processing field. The linear model of BSS can be stated as follows:

$$x(t) = As(t) + e(t) \tag{1}$$

where $t = 1, 2, ...T$ and $A = [\alpha_1 ... \alpha_n] \in R^{m \times n}$ is the mixing matrix. The sample of sources $s(t) \in R^{n \times 1}$, the observed signals sample $x(t) \in R^{m \times 1}$ and the white Gaussian noise sample $e(t) \in R^{m \times 1}$. If $m < n$, which means that the number of sources is greater than the number of observed signals, then the separation problem is degenerated to the Underdetermined Blind Source Separation (UBSS) [7] problem. In this case, traditional independent component analysis (ICA) cannot be directly applied again. However, since signals are sparse in the real environment or in the frequency domain through Fourier or Wavelet transform, therefore we can solve the UBSS problem using sparse component analysis (SCA) [8]. According to the sparsity assumption of sources, model (1) can rewrite as follows:

$$x(t) = \sum_{j=1}^{k} \alpha_{i,(t)} s_{i,(t)}(t) + e(t), i_j(t) \in \{1, 2, ...n\} \tag{2}$$

where $t = 1, 2, ...T$ and k is the number of active source components at each instant.

Typically, a two-stage "clustering-then-l_1-optimization" approach is often used in SCA, which is included by the mixing matrix estimation stage and sources recovery stage. According to the difference of active components number of sources, the problem of mixing matrix estimation can be categorized into two types: $k = 1$ and $k > 1$. To the one single dominant SCA problem [7] $(k = 1)$, several linear orientation-based algorithms [7-9] are addressed to solve this single dominant SCA problem; To the second case $k > 1$, this problem, which is called as multiple dominant SCA problem [10-12], can be solved by two steps: concentration hyperplanes clustering and mixing vectors identification. Although these hyperplane methods can effectively improve the precision of mixing matrix identification, they may not be applied in practice because of high computational costs. For overcoming this problem, we propose a novel method to reduce the time cost in the identification of A. First, we discuss the geometrical distribution feature of the observed sample. Second, we give a simple density detection method to reduce the complexity of algorithm by avoiding traditional concentration hyperplane clustering step.

This paper is organized as follows: we make an intuitive and heuristic analysis of new algorithms in section 2. The binary state mixture of Gaussians (MoG) mode [13] is introduced in section 3. The complete algorithm is given in section 4. Section 5 provides some numerical simulations to demonstrate the effectiveness of our new algorithm. Then we discuss and conclude in section 6.

II. THEORETICAL ANALYSIS OF THE ALGORITHM

A. Evolutionary Algorithm

From the k-sparse mixture model of (2) , there are $c(c = C_n^k)$ k-dimensional hyperplanes to the observed data samples. And each column of lies in the hyperplanesn

doi:10.4304/jsw.9.1.184-189

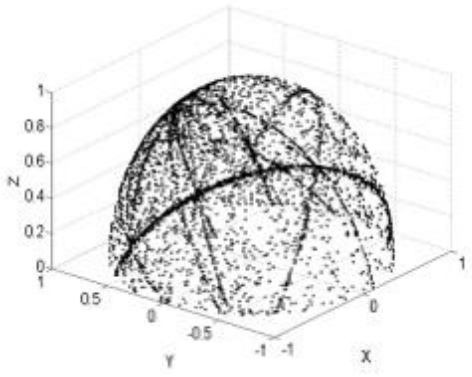


Figure 1. The scatter plot of observed signal samples on a unit 3-dimensional space.

of $q(q = C_{n-1}^{k-1})$ hyperplanes. By the normalization process for each $x(t)$, data samples are projected onto a unit n-dimensional sphere (as is shown in Fig.1). In other words, the directions of vectors in mixing matrix A can be detected by the directions of data sample intersections. Therefore, we can estimate the columns of mixing matrix A by detecting these intersections instead of hyperplane clustering.

Since the amplitude of sources is limited, then each hyperplane is bounded in a fixed region in which the area is considered as s. Suppose the probability of data points located in a hyperplane is f_x and one hyperplane can be equally devided into several hyperplanes; Without loss of generality, the probability of data points locating in a hyperplane, which is denoted as φ, can be calculated as $\oint f_x dx_1 dx_2 ... dx_m$. For simplicity, we assume that each hyperplane has the same area. If the number of hyperplanes is l and the number hyperplanesnis denotedyperplanes are denoted as $N_1, ..., N_c$, hyperplaneprobability of points in the same hyperplane (which is denoted as ϕ) is approximately as $f_x \times \frac{s}{l}$. As is stated in section 2.1, there are n intersections on the hypersphere. The probability of the hyperplane containing intersection point is denoted as $p_i (i \in \{1...n\})$, which is intersected by q hyperplanes $B_{i1}, ...B_{iq}$. Therefore, the number of points in this hyperplane can be calculated by the following equation:

$$N_{p_i} = (N_{B_{i1}} \times f_{B_{i1}}(P_i) + ...N_{B_{iq}} \times f_{B_{iq}}(P_i)) \times s/l \quad (3)$$

We assume that all the hyperplanes have the same number of points, and this total number equals to N. Then (3) can be changed as

$$N_{p_i} = (f_{B_{i1}}(P_i) + ...f_{B_{iq}}(P_i)) \times N \times s/l \quad (4)$$

But the other hyperplanes which do not contain intersection points would contain less than than $N \times f_{B_{i1}}(\overline{p}_i) \times s/l$ numbers of point, $i \in \{1...c\}$, where $f_{B_{i1}}(\overline{p}_i)$ refers to probability density functions of other points in an arbitrary hyperplane B_i, $i \in \{1...c\}$. In other words, the number of points in the two kinds of hyperplane (one contains the intersection point and the other does not) is greatly different. So the ratio between them is given as:

$$\frac{N_{p_i}}{N_{\overline{p}_i}} = \frac{f_{B_{i1}}(P_i) + ...f_{B_{iq}}(P_i)}{f_{B_i}(\overline{p}_i)} \quad (5)$$

Note that if the distribution of points in every hyperplane is previously known, there may be some methods to distinguish the difference between intersection regions and other regions. For example, consider points in all hyperplanes are identically distributed with a uniform distribution. Then the ratio value of these two kind regions is

$$\frac{N_{p_i}}{N_{\overline{p}_i}} = \frac{f_{B_{i1}}(P_i) + ...f_{B_{iq}}(P_i)}{f_{B_i}(\overline{p}_i)} = q \quad (6)$$

As is shown in (6), the number of data points in the intersection regions is q times larger than other regions which do not contain intersection poiintersectionn detect the intedensens points from the density regions.

III. SYSTEM MODEL AND THE DISTRIBUTION FEATURE OF DATA SAMPLES

From the analysis above, we found that the distribution of observed data points in m-dimensional space is decided by the distribution of observed signal points in one hyperplane. In this section, our major job is to study the distribution of observed signals in a hyperplane.

A. The mathematical model of one hyperplane

Still review the model of (2), suppose that there are N obshyperplaneals in the same hyperplane. Then the system model is:

$$x_{t_i} = \sum_{j}^{k} \alpha_{i_j} s_{i_j}(t_i) + e(t_i), l \in 1...N, i_j \in 1, 2, ...n \quad (7)$$

As is stated in (7), it is very important to study the source model. In order to depict the distribution of source, we will introduce the following source models.

B. Binary state MoG source model

The mixture of Gaussian model [13] is one of the non-Gaussian signal model. A p-th order of MoG is given as:

$$p(s_i) = \sum_{k=1}^{p} \pi_{i,k} N_{s_i}(0, \delta_{i,k}^2) \quad (8)$$

where $\sum_{k=1}^{p} \pi_{i,k} = 1$. The MoG model is often used for depicting non-Gaussian signals like speech/audio signals. To the binary state of MoG model, which is the simplest MoG model, is widely applied in image processing and modeling sparsity in wavelet decomposition [13-16]. This model is provided as follows:

$$p(s_i) = \pi_{i,1} N_{s_i}(0, \delta_{i,1}^2) + \pi_{i,2} N_{s_i}(0, \delta_{i,2}^2) \quad (9)$$

where $\delta_{i,1} \approx 0$, $\delta_{i,2} \gg \delta_{i,1}$, $\pi_{i,1} \in [0, 1]$ and $\pi_{i,1} + \pi_{i,2} = 1$. In other words, we can rewrite model (9) as follows:

$$p_{s_i} = \begin{cases} N_{s_i}(0, \delta_{i,1}^2), & s_i \text{ is inactive with probability of } \pi_{i,1} \\ N_{s_i}(0, \delta_{i,2}^2), & s_i \text{ is inactive with probability of } \pi_{i,2} \end{cases} \quad (10)$$

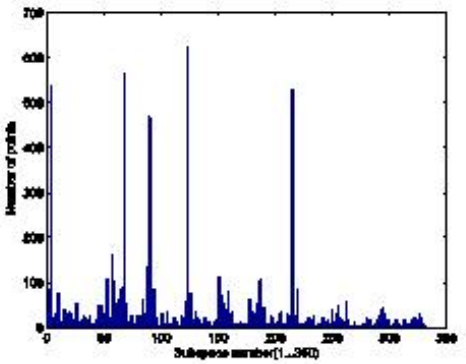


Figure 2. The histogram of the point number in 350 hyperplanes.

C. Distribution of data points in one hyperplane

Suppose the components of source signals are independent with the same distribution, then the distribution of observed signals is:

$$P(x|A,s)=\sum_{i=1}^{k}N_k(0,\alpha_i\alpha_i^T\delta_2^2)=N_k(0,\sum_{i=1}^{k}\alpha_i\alpha_i^T\delta_2^2) \tag{11}$$

Therefore, we can know that the distribution of the observed signals also satisfies the Gaussian distribution. To the Gaussian signals, the values of probability density function in the interval $[-\delta,\delta]$ are close to each other. When the variance is large enough, especially when $\delta\to\infty$, the probability of hypersphere points in a hypersphere can be viewed as a constant in the interval $[-\delta,\delta]$. Therefore, the value of (5) is close to q which is large enough to distinguish intersection regions from others. For example, assuming that 5 sources are generated by the model of binary state sparse MoG and the parameter $\delta_2=1$, then produce 10000 observed points in a 3-dimensional space. We divide the data sample space into 350 hyperplanes and calculate the number of each hyperplane. As is shown in Fig.2, it is obvious that there are 5 indices are more significant than others.

With the discussion above, we can make a conclusion. If the source signal satisfies the distribution of binary-state sparse Gaussian model, the density of points of the intersections is larger than others. As a result, we can estimate the columns of mixing matrix A by the detection of intersected region.

IV. COMPLETE MIXING MATRIX IDENTIFICATION ALGORITHM

Here we summarize the complete algorithm of mixing matrix identification:

1) Remove the sample that are close to origin.

2) Normalize and symmetric the sample $x(t)$ by the following process:

$$x(t)=\begin{cases}\frac{x(t)}{\|x(t)\|}, & x(t)>0\\ -\frac{x(t)}{\|x(t)\|}, & x(t)<0\end{cases} \tag{12}$$

3) Divide the m-dimensional Euclidean space into hyperplanes, where $l_i=\frac{\max(x_i)(t)-\min(x_i)(t)}{\eta}$, η is an interval length.

4) Assign sample $x(t)$ into different spaces by the following method. Define a partition matrix $U\in R^{L\times T}$, $u_{i,j}\in[0,1]$, $i\in 0...L$, $j\in 0...T$.

For $j=1:T$

For$q=1:m$

$$Loc=ceil(\frac{x_q(j)}{\eta})$$

$$Set=u_{\sum_{k=1}^{q-1}l_k+Loc,j}$$

End

End

5) Calculate the number of points in each hyperplane. Choose the first n largest hyperplanes and estimate the center of each hyperplane by the following equations:

$$\begin{cases}\widetilde{\alpha}_1=\frac{\sum_{i=1}^{K_1}x_{1_i}(i)}{K_1},\\ ...\\ \widetilde{\alpha}_m=\frac{\sum_{i=1}^{K_m}x_{m_i}(i)}{K_m}.\end{cases} \tag{13}$$

Where K_i is the number of the data points in the i-th data hyperplane.

6) Finally, construct vectors [$\widetilde{\alpha}_1$,...$\widetilde{\alpha}_m$] as the estimated matrix $\widetilde{A}$.

V. SIMULATION EXAMPLES

In all experiences, source samples are generated independently and satisfy the distribution of the binary state MoG model which is also used in paper [13]. All the simulations were performed in MTALAB7 environment using Intel Pentium 42.4GHz processor with 512M RAM under Microsoft Window XP operating system.

A. Experiment 1

Set $n=5$, $m=4$, $k=3$, the mixing matrix A are randomly generated and normalized as follows:

$$\text{A=}\begin{pmatrix}0.7930 & 0.7428 & 0.1410 & 0.9021 & 0.3281\\ 0.1480 & 0.5901 & 0.7010 & -0.3691 & -0.4419\\ -0.5910 & 0.3161 & -0.6992 & -0.2235 & -0.8349\end{pmatrix}$$

The Procedures of our algorithm are shown in Fig.3 and we obtained the estimated mixing matrix as follows:

$$\widetilde{A}\text{=}\begin{pmatrix}0.7890 & 0.9030 & 0.7441 & 0.3244 & 0.1434\\ 0.1546 & -0.3665 & 0.5888 & -0.4454 & 0.7000\\ -0.5941 & -0.2231 & 0.3152 & -0.8343 & -0.6995\end{pmatrix}$$

For demonstrating the validity of our algorithm, the criterion which is presented in paper [11] and paper [12] is used:

$$\xi=\min_{P\in\rho}\|A-\widetilde{A}P\|_2 \tag{14}$$

Where ρ is the set of al.Permutation matrices. We calculate estimation error is 0.0089, and the result is 0.0066 using the algorithm in paper [13] and 0.2018 with paper [17]. The process took about 160s when the source sample

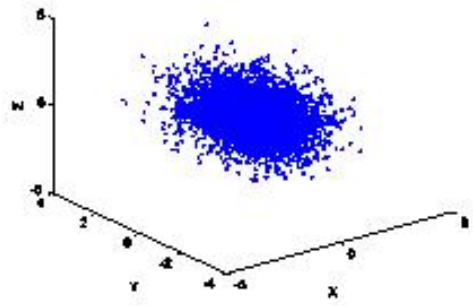


Figure 3. Scatter plot of the mixed sources

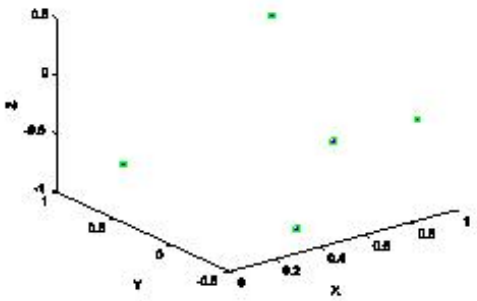


Figure 6. Procedures of the algorithm

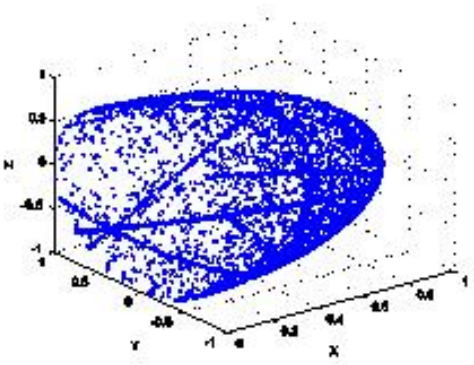


Figure 4. Normalize and symmetric the matrix X

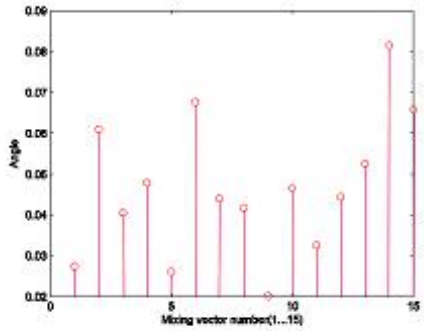


Figure 7. The angle (in radian) between the mixing vectors and their corresponding estimation in middle scale problems(n=15,m=7,k=3).

number is 1000 and 25s when the source sample number is 400, while the algorithm in this paper only took less than 1s to finish the computing process.

B. Experiment 2

In order to demonstrate our fast detection algorithm is capable of solving large scale problems, we compared our algorithm to the existing method proposed in paper [13] by using two simulations. In the first simulation, the parameters are set as $n = 15$, $m = 7$, $k = 3$, $T = 9000$; In the second experiment, parameters are set as $n = 30$, $m = 15$, $k = 2$, $T = 8500$. Our method took less than 6 seconds in this two simulation while it took about 40 minutes for the first case and two hours for the second case by using the algorithm in paper [13].

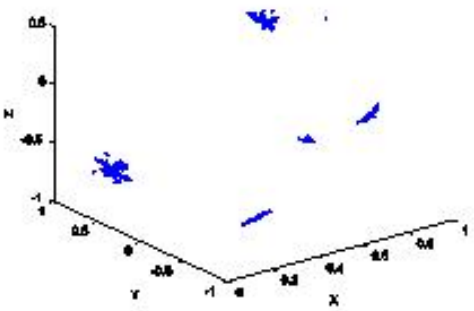


Figure 5. Regions that contain first and largest points were detected.

TABLE 1.

Parameters	our algorithm	algorithm in paper[13]
n=15,m=7,k=3,T=9000	6 Sec	About 40 minutes
n=30,m=15,k=2,T=8500	4 Sec	About 2 hours

Table 1 The performance comparison between our algorithm and the algorithm in paper [13] To measure the precision of identification, the angle between each estimated vector and its corresponding actual mixing vector (inverse cosine of their dot product) is calculated, the result is shown in Fig.4, the accuracy is close to that presented in paper [17], which shows the proposed method can also estimate the mixing matrix successfully.

As is seen in this experiment, the proposed algorithm can estimate mixing matrix very fast with higher accuracy and do not change much when the parameters get larger. It means that the proposed algorithm can be used for dealing with middle scale problems.

VI. DISCUSSION AND CONCLUSION

In this paper, we propose a fast algorithm to estimate the mixing matrix A in multi-dominant SCA based on a binary state sparse MoG model. There are some aspects we need to discuss to our algorithm.

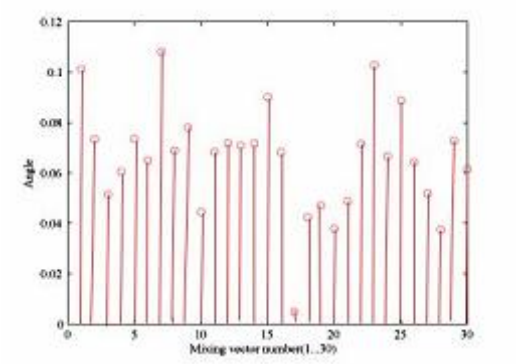


Figure 8. The angle (in radian) between the mixing vectors and their corresponding estimation in middle scale problems(n=30,m=15,k=2).

A. Comparison with existing algorithms in accuracy and speed efficiency

The existing algorithms to estimate the mixing matrix is based on the hyperplanes clustering idea. There are several factors that traditional method need to take into account, such as the number of samples, observations and active source component. These algorithms would suffer from an exponential growth in the computation cost like in [13]. Furthermore, if experimental data contain noises, the algorithm would convergence much slower. But our algorithm only takes few seconds to finish this process and the computation cost doesn't change much with the growth of sample number. As observed in the simulation results, the location of mixing vector is less precise when there is noise-free, because the proposed algorithm regards the center of the intersection point region as the estimation of the mixing vector. However, the existing algorithms can estimate the mixing vector precisely if the system is noise-free. But it should be mentioned that, the estimation result is imprecisely or even worse when noise exists by using existing algorithms. In contrast, the proposed algorithm in this paper can smooth the noise effect and achieve a good accuracy.

B. Comments on choosing the parameter

In the proposed algorithm, the parameter η dhyperplanethe size of hyperplane should choose a suitable value according to the situation of reality. Generally, when η is shyperplanee number of hyperplane is increasing, which will improve the identification accuracy of mixing matrix. And if η gets lhyperplanee number of hyperplane is deleading, which will leads a bad performance.

C. Comments on prior knowledge

Another previous knowledge is that the source signals should distribute in the binary state sparse distribution model. Although such a source model might be considered too simple, it has sufficient complexity to capture the salient features for very sparse data. In fact, binary state mixture models have been used very successfully by Olshausen and Millman [12] to estimate overcomplete bases for images. Fortunately, it will be possible to solve all kinds of BSS problem of different kinds of source models if the probability density function of observed data points is given in advance. These issues are currently under study. Meanwhile, the construction of the sparse signal model is still an open problem that remained to be solved.

ACKNOWLEDGMENT

This work was jointly supported by the Natural Science Foundation of Guangdong Province (S2011010005075) and Guangzhou technology projects (11C42110781).

REFERENCES

[1] C. Jutten, J. Herault. "Blind separation of sources, Part I: An adaptive algorithm based on neuromimetic." *Signal Processing*, 1991, vol. 24(1), pp. 1-10.

[2] Tianqi Zhang, Shaosheng Dai, Guoning Ma, Wei Zhang, and Pu Miao. "Approach to blind estimation of the PN sequence in DS-SS signals with residual carrier," *Journal of Systems Engineering and Electronics*, 2010, Vol. 21(1), pp. 1-8.

[3] Hai-lin Liu, Xie Sheng-li. "Nonlinear blind separation algorithm based on multi objective evolutionary algorithm." *Journal of Systems Engineering and Electronics*, 2005, Vol. 9, pp. 5176-5179.(In Chinese)

[4] A, DelormeT. SejnowskiS. "MakeigImproved rejection of artifacts from EEG data using high-order statistics and independent component analysis." *Neuroimage*, 2007, Vol. 34, pp. 1443-1449.

[5] Hai-Lin Liu. "A blind deconvolution parallel algorithm based on a simplified mixing model" *Journal of Systems Engineering and Electronics*, 2007, Vol. 4, pp. 651-654. (In Chinese)

[6] Z.S. He, S.L. Xie, S.X. Ding, A. Cichocki. "Convolutive Blind Source Separation in Frequency Domain Based on Sparse Representation," it IEEE Transactions on Audio, Speech and Language Processing, 2007, Vol. 15 (5), pp. 1551-1563.

[7] Georgiev P, Theis F, Cichocki A. "Sparse component analysis and blind source separation of underdetermined mixtures." it IEEE Transactions of Neural Network, 2005, Vol. 16 (4), pp. 992-996.

[8] Z. He, and A. Cichocki. "K-EVD Clustering and its Applications to Sparse Component Analysis.6th International Conference on Independent Component Analysis and Blind Signal Separation," it Charleston SC, USA, March 5-8, 2006, Springer LNCS 3889, pp. 90-97.

[9] Hai-Lin Liu, Chu-Jun Yao and Jia-Xun Hou. "A new algorithm for the underdetermined blind source separation based on sparse component analysis." *International journal of pattern recognition and artifcial*, 2009, Vol. 23 (1), pp. 71-85.

[10] Gao Ying, Xie Sheng-li, Xu Ruo-ning, Li Zhao-hui. "Blind Sparse Source Separation Based on Particle Swarm Optimization." *Journal of System Simulation*, 2006, Vol. 18 (8), pp.2264-2266.(In Chinese)

[11] Z.S.He, A. Cichocki, Y.Q.Li, S.L. Xie and Saeid Sanei. "K-hyperline clustering learning for sparse component analysis," *IEEE Transactions on Signal Processing*, 2009, Vol. 89, pp. 1011-1022.

[12] M. Aharon, M. Elad, A. Bruckstein. "The K-SVD: an algorithm for designing of overcomplete dictionaries for sparse representation," *IEEE Trans. Signal Process*. 2006, Vol. 54 (11), pp. 4311-4322.

[13] Movahedi N.F, Hosein M. G., Babaie-Zadeh, M.,Jutten C. "Estimating the mixing matrix in Sparse Component Analysis (SCA) based on partial k-dimensional hyperplane clustering." *Neurocomputing*, 2008, Vol.71 (10), pp. 2330-2343.
[14] B. A. Olshausen and K.J. Millman. "Learning sparse codes with a mixture-of-Gaussians prior." *In Advances in Neural Information Processing Systems, 12, MIT Press*, 2000, pp. 841-847.
[15] H. Zayyani, M. Babaie-Zadeh, and C. Jutten. "Source estimation in noisy sparse component analysis." *In Proc. DSP07*, 2007, pp. 219-222.
[16] L. Vielva, D. Erdogmus, and C. Principe. "Underdetermined blind source separation using a probabilistic source sparsity model." it ICA01, 2001, pp. 675-6.
[17] Y. Washizawa, A. Cichocki. "On-Line k-plane clustering learning algorithm for sparse component analysis," *in Proceedings of ICASSP'06, Toulouse, France*, 2006, pp. 681-684.

Jiechang Wen Female, was born in 1964, Master, Professor. The major research covers Optimization Method and its Application, Intelligent Computation.

Suxian Zhang received his Master degree in Chongqing University of Posts and Telecommunications. He is a M.S.candidate at the school of applied mathematics, Guangdong University of Technology, Guangzhou, China.

Jun-Jie Yang received his Master degree in Applied Mathematics from Guangdong University of Technology, China, in 2011. He is now pursuing his Ph.D degree in Automation of Guangdong University of Technology. His current research interests include Sparse Component Analysis, Physical Layer Security and Smart Grid Security.

Reliable Enhanced Secure Code Dissemination with Rateless Erasure Codes in WSNs

Yong Zeng[1]
[1]School of Computer Science and Technology, Xidian University, Xi'an, China
yzeng@mail.xidian.edu.cn

Xin Wang[1,2], Zhihong Liu[1], Jianfeng Ma[1] and Lihua Dong[3]
[2]Education Technology Center, Changchun Institute of Engineering Technology, ChangChun,China
[3]School of Telecommunication Engineering, Xidian University, Xi'an, China
{wangxin, lih_dong, jfma, zhliu}@mail.xidian.edu.cn

***Abstract*—Code dissemination is very useful to remotely fix bugs or add now functions in wireless sensor networks (WSNs) after sensors deployed. Hostile environments keep the secure code dissemination a major concern. The Deluge-based protocols are the widely used code disseminations, however, which have to take much energy and memory to deal with the problem caused by out of order delivery of packets in WSNs. Rateless erasure codes based approaches can reduce the overhead, while failed in defeating DoS attacks. This paper proposed a novel code dissemination scheme, which integrates immediately authentication into rateless erasure codes. The analysis shows that proposed scheme can provide code image confidentiality, bogus code image protection, DoS protection and reliable enhanced property.**

***Index Terms*—wireless sensor networks, code dissemination, reliability, security, rateless erasure codes**

I. INTRODUCTION

Wireless sensor networks (WSNs) can provide wonderful sensing and actuation. WSNs are considered ideal candidates for a wide range of applications, such as industry monitoring, data acquisition in hazardous environments, and military operations [1]. It is often necessary to remotely update sensor nodes' configuration after deployment. For example, it has to fix bugs or add new functionalities. It is very hard to update sensors' softwares one by one due to the large-scale and embedded nature of WSNs. An efficient way is to wirelessly disseminate a code update image and remotely manage the code images on sensor nodes. Such process is so called over the air reprogramming or remote code update. There are two significant steps in over the air reprogramming: code dissemination and code implementation. This paper focuses on how to provide secure and reliable code dissemination.

Deluge[2] is the most well-known code dissemination protocol in WSNs, which is a de facto standard in TinyOS, though, other protocols [3-5] have been suggested. In Deluge the code image is divided into pages, the size of which depends on that of RAM. Each page is split up into packets. Generally speaking the size of packets is about equal to that of frame. The packets are propagated in a pipelined fashion.

However, sensors worked on a hazardous environment. The packets are delivered not in the well defined pipelined fashion due to collisions or multiple parallel transmissions of the same content. It often takes much time and energy to process out-of-order received packets. This is so-called out-of-order-delivery problem, which significantly reduced the reliability of WSNs.

Rateless erasure codes based approaches can reduce the overhead caused by out-of-order-delivery problem. Hgedorn [6] and Rossi [7] proposed efficient code image dissemination scheme based on random linear codes and digital Fountain codes, respectively. In their approaches, the sender generates arbitrarily number of encoded packets using rateless erasure code. Any receivers can get the original code image from any subset of encoded packets, the size of which is equal to or slightly larger than the number of source packets. Note that "any subset of encoded packets" means the receiver can recover the image using out-of-order received packets. As a result their protocols can significantly reduce latency, retransmission, and communication overhead cased by out-of-order received packets. Moreover, due to the rateless property, it is possible to adaptively change the code rate according to the local neighbors' requests or link quality.

However, none of above approaches took security into consideration. The security of Rossi's approach [7] is improved by Bohli [8]. In their approach, the integrity and authentication, two security properties, of each page is achieved by using a digital signature and hash chains closely follows Seluge [1] and [9], which are security extensions from Deluge. However, this approach cannot immediate authenticate each received packets, hence may suffer from DoS attacks by authentication delays of bogus encoded packets. The authors gave a possible

This work is supported by Major national S&T program (No. 2011ZX03005-002), National Natural Science Foundation of China (No.61100235, No.61173135) and the Fundamental Research Funds for the Central Universities.

doi:10.4304/jsw.9.1.190-194

improvement by filtering bogus packets, however, they did not provide detailed effectiveness discussion. LR-Seluge gave another solution by using fixed-rate erasure code and attentively creating hash chains between original and encoded packets using lightweight cryptographic hash functions [10]. However, only receiving sufficient encoded packets to recover one page can the hash images of the next page be recovered. As a result LR-Seluge does not effectively reduce overhead dissemination delays [11].

The above security and reliability enhanced code dissemination schemes are based on rateless erasure codes. Their basic ideas are to bootstrap the code image authentication using a digital signature and to propagate the security of the signature through the code packets by means of hash chains or Merkle hash tree, which is used in Deluge-based protocols. The structure of chains or tree is to keep the packets verifying in order under out-of-order delivery scenarios. For example, in hash tree based proposals, only after successfully receiving *j*th packet of the (*i*+1)th page and successfully verifying its integrity by comparing a hash value, can the integrity of *j*th packet's of the *i*th page can be verified. And the whole code image will be authenticated by a signature of these hash values. The out-of-order delivery will delay the processes of integrity verifying and authentication. However, the rateless erasure code can avoid the out-of-order problem. As a result they cannot take full advantage of erasure codes, and consequently does not immediately authenticate packets.

Our contribution: To the best of our knowledge, available code dissemination schemes do not take their work to be of the interest in immediately authentication with out-of-order-delivery-tolerant property. This paper extends our result [18], which studies a Fountain code using both by Rossi and Bohli, namely the LT code [12]. Our scheme, a reliable enhanced secure code dissemination protocol with immediately authentication property, is achieved by integrating authenticating into LT encoding.

II. PRELIMINARIES

A. Digital Fountain Codes

The basic principle of digital fountain codes, or LT codes, one of rateless erasure Codes, for data transmission can be described as follows. The original data is separated into k packets. Then the source generates a potential unlimited sequence (generally two sizes larger than original data) of code words as follows.

1) To get a code word C_i, a packet degree d_i is randomly chosen following a given distribution function.

2) The encoded packet is d_i packets choosing uniformly randomly out of the k source packets. The d_i packets are successively XORed to get a code word C_i.

Figure 1 illustrates the encoding procedure of LT codes. The encoding is done for at least $n(n>k)$ encoded packets. The coding vector X_i means that packets are XORed for each code word C_i. For example, X_4=(1, 1,0,…,0,1), X_1=(1, 0,1,0…,0,1). X_i may be computed simultaneously by sender and receiver using a pseudo-random number generator with the same seed. However, it will require a strict synchronization between sender and receiver. The alternative scheme is that X_i is appended to each packet.

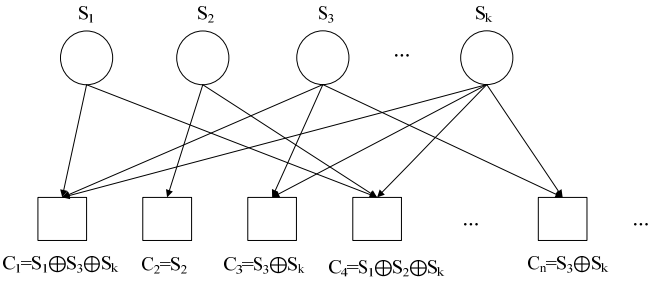


Figure 1. An illustration of LT codes

The receiver extracts the pair (C_i, X_i) from the packet. Then the decoding follows iterative procedure.

1) Find a code word C_i with degree 1. Then it is actually a source packet S_i. If there are none such code words, stop.

2) Find all the other code words containing S_i, then XOR them with S_i, and remove packet i from their coding vectors, i.e., set the coding vector's 'i^{th}' bit 1 as 0 respectively. Goto step 1).

We illustrate the decoding process using the example in Fig.1. Receiver finds that code C_2 is actually source packet S_2. Then set the 2nd bit '1' in X_4 equals to '0' and get new X_4=(1, 0,0,…,0,1) and $C_4=S_1 \oplus S_k$.

The decoding procedure is equivalent to soling a linear equation system $Ax=b$ for x, where $k*k$ matrix A consists of k linear independent coefficient vectors of successfully received codes, and vector b contains the corresponding incoming encoded packets C. The detailed decoding algorithm can be seen in [13].

B. Seluge

The Seluge [1] is considered as one of the most well-known security extension to Deluge. The Figure 2 depicts the Seluge.

Each packet packet $Pkti,j$ in page P_i is augmented to form $p_{i,j}$ by appending the hash value $h(p_{i+1},j)$ of the packet page P_{i+1} (so a hash chain or tree is setup to verify orderly all the packets), where $h()$ is a secure hash function with eight bytes. In Seluge a so-called Merkle hash tree is constructed with M hash values of page P_1. And the page P_0 is created by appending all the authentication hash paths. The root of the Merkle hash tree including some headers is given by a signature packet of code image. Then the packets are disseminated in orders: signature packet first (waiting a few time to make sure that it may arrive majority of all the sensors), then page $P_i(1<i<N+1)$ one by one. If the signature packet and pages arrive in order, then any accepted packets can be immediately authenticated. However, the out-of-order property in WSNs may significantly delay the authentication.

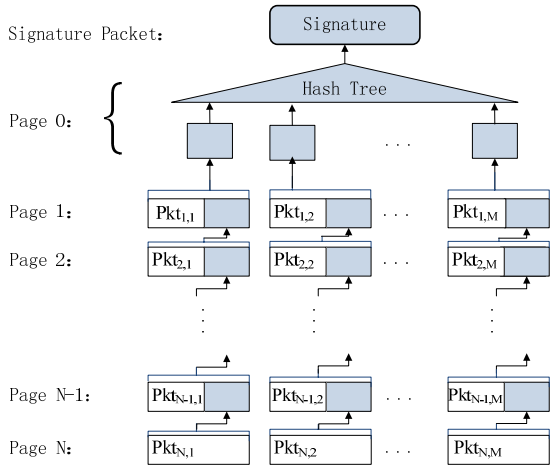


Figure 2. The Seluge code authentication architecture

III. PROPESED CODE DISSEMINATION

We assume that a base station BS is responsible to disseminate update code image on the sensor nodes. It will take multi-hops communication over several sensor nodes to reach all nodes. Sensors are deployed in a untrusted or hostile area.

A. Security Model

We consider the scenario where a code image update takes place in a large scale WSNs with a full and a limited adversary. The limited adversary can eavesdrop or insert packets. The full adversary can eavesdrop, modify and insert packets. The code update process should satisfy the following security requirements:

1) **Code image confidentiality**: the update code image has to be kept secret to prevent eavesdroppers from gaining information for a given time window.

2) **Bogus code image protection**: the unauthenticated update code image should not be written into sensors' memory. This amounts to ensuring authenticity and integrity of the code image.

3) **Denail of Service protoction by immediately authentication**: when an adversary sends modified packets, the honest sensor nodes should not perform unnecessary energy consumption operations. In this paper we focus on the DoS attacks due to the non-immediately authentication problem, which may cause two possible attacks effects: authentication delays or expensive signature verifications.

It is assumed that there is a shared or broadcast key between BS and sensors, which can be distributed by using delayed key disclosure such as μTESLA[14] or pre-distribution[15]. An attacker is supposed keep away from the key.

B. Integrating Authentication into LT Encoding

The basic principle is to integrate authentication code into LT codes so as to immediately verify the integrity and confidentiality of encoded packets arrived in an out-of-order way. More specifically, our proposal differs from existing schemes in that it uses an *authentication code* to verify the integrity. The code is also used to achieve immediately authentication.

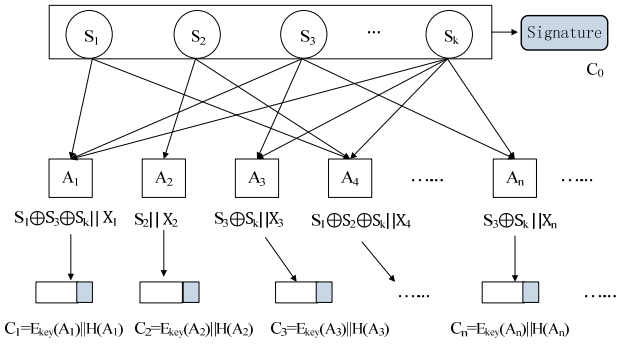


Figure 3. An illustration of LT codes with authentication code

Figure 3 gives an illustration of proposed scheme. In the first step, The update code image is divided into k source packets S_1, …, S_k, then all the k hash values will be signed with a signature scheme to produce signature, i.e., sign($H(S1)||…||H(S_k)$. So a signature packet C_0 is generated, C_0= sign($H(S_1)||…||H(S_k)$). Then they are encoded to A_1, …, A_n using LT code.

Then an *authentication code* C_j of each code is calculated as in equation (1)

$$C_j = E_{key}(A_j)||H(A_j) \quad (1)$$

where $E_{key}()$ is a lightweight encryption algorithm and $H()$ is a secure hash function. In literature conflicting results about encryption algorithm for WSNs have been obtained considering memory requirements, performance or energy consumption [16]. In the code update scenario, the majority amount of ROM is already taken by the reprogramming protocol, so the encryption algorithm should take less ROM memory and execution time. So as to we refer to the hardware ASE-128 block cipher provided by the CC2420 RF chip in the TelosB platform. Then C_j is created by appending plain packet's hash value $H(A_j)$ to encrypted packet $E_{key}(A_j)$. We call C_j an *authentication code*. The confidentiality and integrity of packets can be verified by the authentication code. The detailed security analysis will be shown in Section IV.

C. Transmission , Authentication and Decoding

The signature packet C_0 will be transmitted with Deluge, in which no LT codes are applied. After the signature packet C_0 have been successfully received, the C_1, …, C_k, … will be encoded using the method above. Then the base station will send $n>k$ packets C_i.

When a node received a code, say C_j, then it calculates $D_{key}(E_{key}(A_j))$ to get A'_j, where $D_{key}()$ is the decryption algorithm. If $H(A_j)= H(A'_j)$, then it accepts the packet A_j, it drop the code as a bogus code.

If a node accepts enough corrected codes, say, A'_1, A'_n, then it stops listening and decodes these codes using the nounce and LT decoding algorithm to recover code update image packets, say, S'_1, …, S'_k. Then it calculates C'_0= sign ($H(S'_1)||…||H(S'_k)$). If $C'_0= C_0$, then the code update image is successfully recovered.

If a node has not received enough packets to recover code update image, then it keeps listening. If n packets

have been transmitted, nodes still have not successfully recover code update image, then they send a *NACK* and BS or their neighbors continue sending another n' encoded packets.

IV. ANYLYSIS

This section analyses the features of proposed secure codes dissemination. The LT encoder and decoder are the same with that in [7,8]. So we focus on the security and overhead analysis.

A. Code Image Confidentiality Protection

The plain code is encoded by LT method, and then encrypted using AES-128 block cipher with the shared key. To the best of our knowledge, the best method to break the security of AES-128 without key is the exhaustive search, i.e., brute force attack. In our scheme the attacker is supposed that he or she do not know the key. Thus, the AES-128 encryption of the CC2420 RF chip can provide enough code image confidentiality protection.

This security level is achieved under the consumption that an attacker is keep from the key. However, if an attacker physically captures a sensor node, he or she could compromise the key from its memory. Then the data may be decrypted using the key. However, the compromising key problem can be overcome through the key distribution and updating schemes, which is beyond the scope of this paper. The compromising key does not impair the bogus code image protection and immediate authentication which are our main security goals.

B. Bogus Code Image Protection

The code image is protected by authentication codes. An authentication code C_j, say, $C_j = E_{key}(A_j)||H(A_j)$, is a cascade of the encrypted and hash values of A_j. When a sensor node received C_j, then it calculates $D_{key}(E_{key}(A_j))$ to get A'_j. If $H(A_j)= H(A'_j)$, then it accepts the packet A_j, it drop the code as a bogus code. As a result the code image is secure when the key is secret.

The code image is also protected by the signature packet C_0 transmitted in the first step. The private key to generate the signature is only known to the trusted base station which is responsible for the code dissemination. An adversary cannot get the private key to generate a correct signature. As a result the bogus code image can also be found in the step of signature verification.

Due to the limited memory of sensor nodes, the signature algorithm should take less memory and execution time. The efficient short-lived Rabin-Williams signature scheme [17] is adopted in our scheme.

C. DoS Protection by immediately authentication

The proposed scheme is resistant to the DoS attacks shown in Section IIII from external attackers.

Due to the Authenticate-code-by-Authenticate-code dissemination strategy, upon receiving a code, each sensor node can verify whether the code is a corrected code or not simply by a decryption and a hash operations. Thus, it can immediately authenticate any code it receives, and successfully defeat DoS attacks exploiting authentication delays.

Due to the use of efficient short-lived Rabin-Williams signature scheme, each node can performing a single modular squaring (comparable to a singe hash for RSA-512) and a simple decoding requiring 3-4 hash operations [17] to detect fake signature packets. Thus our scheme provides resistance to DoS attack exploiting expensive signature verifications.

D. Out-of-Order-Delivery-Tolerant

Some works may take much time and memory to process out-of-order received packets. Proposed scheme integrated authentication into LT encoding. Upon detect a correct code from a received packet, each sensor node can simply keep listening until receiving enough packets to recover code update image, where these packets do not need keep order. Thus, proposed scheme is out-of-order-delivery-tolerant.

E. Security Comparison with Previous Approaches

The available code dissemination schemes as Deluge or Deluge-based way do not fully defeat DoS attacks exploiting authentication delays. The reason follows. The Deluge-base schemes need a tree-like structure to keep the packets verifying in order under out-of-order delivery scenarios. Figure 2 has shown the architecture of Seluge(one of Deluge-based schemes). It shows that only after successfully receiving jth packet of the (i+1)th page and successfully verifying its integrity by comparing a hash value, can the integrity of jth packet's of the ith page can be verified. And the whole code image will be authenticated by a signature of these hash values. The out-of-order delivery will delay the processes of integrity verifying and authentication. As a result it cannot fully defeat DoS attacks exploiting authentication delays.

TABLE I.
COMPARISON WITH PREVIOUS APPROACHES

	Code image confidentiality	***Bogus code image protection***	***DoS Protection***		***Out-of-Order-Delivery-Tolerant***
			delays	***verify***	
Seluge[1]	N	Y	N	Y	N
[17]	N	Y	N	Y	N
R-deluge[6]	N	Y	N	N	Y
SYNAPSE++[7]	N	Y	N	Y	Y
[8]	N	Y	N	Y	Y
Our Scheme	Y	Y	Y	Y	Y

Delay: authentication delays; verify: expensive signature verifications

The Fountain code based schemes in [6-8] have the out-of-order-delivery-tolerant property. However, the signature verification of code image is completed after that they receive enough encoded packets and decode them. Since the encoded packets are delivered in plaintext without authentication, an adversary can easily forge fake packets and send to WSNs. If nodes receive fake packets, they know the truth after all the packets are decoded. As a

result they do not defeat DoS attacks exploiting authentication delays.

Table I gives the security comparison with previous approaches. It shows that our scheme not only has the out-of-order-delivery-tolerant property, but also has better security than available.

F. Data Overhead Comparison

The overhead of our scheme should compare with that in [6-8] with out-of-order-delivery-tolerant under the same hash and signature functions.

The communication overhead of our scheme is smaller than those in [6-8]. The reason follows. The sizes of first signature packet C_0 in four schemes are equal if the schemes [6-8] use the same short-lived Rabin-Williams signature efficient as us. Each packet holds one hash value in all the schemes. However, the schemes [6-8] need an additional hash value in the last packet of each page. Let P the number of pages. Then they need transmit more P hash values than us.

The computation overhead of our scheme is smaller than those in [6-8] under DoS attacks. When there are DoS attacks, node must perform more computation in all the schemes. The actual computation depends on the number of fake packets injected by the attacks. Our scheme can immediately judge whether a packets is a fake one or not. However, they [6-8] know after that enough packets are decoded and the signature is computed. As a result, our scheme is the better one under DoS attacks. However, our scheme needs an additional AES-128 operation in each packet, which is to keep the confidentiality of a code image.

V. CONCLUSION

This paper proposed an efficient secure code dissemination scheme with out-of-order-delivery-tolerant property. Proposed scheme can protect code image confidentiality, code image integrity, code image authentication, and defeat external DoS attacks. It has better data overhead than available schemes. The experiment comparison is in hand targeted at the current sensor platforms MicaZ and Imote2. Our scheme can provide security under external attacks. In the future we will discuss the inside attack scenarios.

ACKNOWLEDGMENT

This work was supported in part by a grant from Major national S&T program (No. 2011ZX03005-002), National Natural Science Foundation of China (No.61100235, No.61173135) and the Fundamental Research Funds for the Central Universities.

REFERENCES

[1] S. Hyun, P.Ning, A. Liu, and W.Du. “Seluge: Secure and dosresistant code dissemination in wireless sensor networks. In Information Processing in Sensor Networks,” IPSN 2008, pp.445–456. *IEEE*, 2008.

[2] J. W. Hui and D. Culler, “The dynamic behavior of a data dissemination protocol for network programming at scale,” In *Embedded networked sensor systems*, *SenSys ’04*, pp.81–94. ACM, 2004.

[3] D. Estrin, T. Stathopoulos, and J. Heidemann, “A remote code update mechanism for wireless sensor networks,” *Technical Report 30, Center for Embedded Networked Sensing*, UCLA, November 2003.

[4] S.S. Kulkarni and L.M. Wang, “MNP: Multihop network reprogramming service for sensor networks,” In ICDCS ’05: *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pp.7–16, Washington, DC, USA, 2005.

[5] N. Reijers and K. Langendoen, “Efficient code distribution in wireless sensor networks,” In *WSNA ’03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pp.60–67, New York, NY, USA, 2003. ACM.

[6] A.Hagedorn, D. Starobinski, and A. Trachtenberg, “Rateless deluge: Over-the-air programming of wireless sensor networks using random linear codes,” In *IPSN ’08: Proceedings of the 7th international conference on Information processing in sensor networks*, pp.457–466, Washington, DC, USA, 2008. IEEE Computer Society.

[7] M. Rossi, N.Bui, G. Zanca, L. Stabellini, R. Crepaldi, and M. Zorzi, “SYNAPSE++: Code dissemination in Wireless Sensor Networks using Fountain Codes,” *IEEE Trans. On Mobile Computing*, Vol.9, No.12, pp.1749-1765, 2010.

[8] J.M. Bohli, A. Hessler, O. Ugus, and D. Westhoff, “Security enhangced multi-hop over the air reprogramming with fountain codes,” in *SenseApp 2009*, Zurich, Switzerland, pp.850-857, October 2009.

[9] O.Ugus, D. Westhoff, and J.M. Bohli, “A ROM-friendly Secure Code Update mechanism for WSNs using a stateful-verifier T-time Signature Scheme,” In *ACM Conference on Wireless Network Security*, *WiSec’09*, pp.29–40. ACM, 2009.

[10] R. Zhang and Y.C. Zhang, “LR-Seluge: Loss-resilient and secure code dissemination in wireless sensor networks,” In *Proceedings of IEEE ICDCS*, 2011.

[11] H. Sangwon, “Secure and reliable code dissemination for wireless sensor networks”, *Ph.D. thesis*, *Raleigh*, North Carolina, 2011.

[12] M. Luby, “LT Codes,” In *Foundations of Computer Science*, *FOCS 2002*, pp.271–282. IEEE, 2002.

[13] M. Mitzenmacher, “Digital fountains: a survey and look forward,” in *IEEE ITW’04*, *San Antonio, TX*, Oct. 2004.

[14] Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. “SPINS: security protocols for sensor networks”, *Wireless Networks*, 8(5):521–534, 2002.

[15] K. J. Lu, Y. Qian, M. Guizani, and H.H Chen, “A framework for a distributed key management scheme in heterogeneous wireless sensor networks”, *IEEE Transactions on Wireless Communications.2008*, 7(2):639-647

[16] Y.W. Law, J. Doumen, and P. Hartel, “Survey and benchmark of block ciphers for wireless sensor networks”, *ACM Trans. on Sensor Networks*, Vol.2, No.1, pp.65-93, Feb, 2006.

[17] Chae Hoon Lim, “Secure Code Dissemination and Remote Image Management Using Short-Lived Signatures in WSNs”, *IEEE Communication Letters*, Vol.15, No.4, pp.362-364, 2011.

[18] Yong Zeng, Xin Wang, Lihua Dong, Jianfeng Ma, and Zhihong Liu, “Out-of-Order-Delivery-Tolerant Secure Code Dissemination with Fountain Codes in Wireless Sensor Networks”, in CIS’2012: *Proceedings of the 2012 Eighth International Conference on Computer Intelligence and Security*, pp.683-686, Guangzhou, China, November, 2012.

A New Prediction Method of Gold Price: EMD-PSO-SVM

Jian-hui Yang
School of Business Administration, South China University of Technology, Guangzhou , China
Email: bmjhyang@scut.edu.cn

Wei Dou
School of Business Administration, South China University of Technology, Guangzhou , China
Email: dauwile@qq.com

***Abstract*—The current gold market shows a high degree of nonlinearity and uncertainty. In order to predict the gold price, Empirical Mode Decomposition (EMD) was introduced into Support vector machine (SVM). Firstly, we used the EMD method to decompose the original gold price series into a finite number of independent intrinsic mode functions (IMFs), and then grouped the IMFs according to different frequencies. Secondly, SVM was used to predict each IMF in which particle swarm optimization (PSO) was applied to optimize the parameters of SVM. Finally, the sum of each IMF's forecasting result will be the final prediction. In order to validate the accuracy of the proposed combination model, the London spot gold price and the Shanghai Futures gold price series were employed. Empirical studies indicated that the EMD-PSO-SVM model outperformed the WT-PSO-SVM model, and was feasible and effective in gold price prediction. We can promote the EMD-PSO-SVM to other related financial areas.**

***Index Terms*— empirical mode decomposition, independent intrinsic mode functions, support vector regression, wavelet transform, PSO, gold price**

I. INTRODUCTION

Gold is a symbol of wealth since from the ancient times. Since the disintegration of the Bretton Woods system in 1973, the gold is non-monetary which makes it become an important tool of financial market. The current gold market has high-yield and high risks. After long-term practice, a gold price theory gradually formed. However, due to the price of gold market is affected by many factors, there are a variety of uncertainties. Many scholars have done researches on it. Qian chose a fuzzy time series model to determine the initial parameters of the fuzzy system, and used Type -2 Fuzzy Systems and Type-1 fuzzy system to train and forecast the price of gold [1]. According to the basic principles of the gray prediction model and the Markov chain, Qin and Chen constructed gray Markov model to predict the price of gold, in which two methods can complement each other, making the predictions more reasonable and reliable[2]. Zhang, Yu and Li predicted the gold price on model based on wavelet neural network [3]. Summarize previous studies, we find that the gold price shows a high degree of nonlinearity and uncertainty, and currently, a variety of model results is not satisfactory.

Support vector machine (SVM), a novel learning machine based on statistical learning theory, was developed by Vapnik etc. in 1995 [4]. SVM can be used to solve problems in pattern recognition and makes out decision-making rules on generalization performance. SVM is attar-ctive and has widely been applied to various different fields [5,6]. Meanwhile, many scholars have studied the combination of innovative methods of SVM. Abdulhamit proposed that hybridized the particle swarm optimization and SVM method to improve the EMG signal classification accuracy [7]. Jazebi combined SVM and wavelet transforms, and used on a power transformer in PSCAD/EMTDC soft-ware [8]. Wei etc. studied wavelet decomposition, EMD and R / S valuation process, and finally got a fast, high-precision method of valuation of the Hurst exponent [9].

In this paper, empirical mode decomposition (EMD) and particle swarm optimization (PSO) are introduced into the SVM model to establish the gold price forecasting model. We used the London spot gold price and the Shang-hai Futures gold prices to validate the innovative method. The EMD-PSO-SVM model is expected to be more accu-rate and feasible in gold price prediction.

II. METHODOLOGY FORMULATION

Support vector machine (SVM) is a new and promising technique for data classification, regression and forecasting. In this section we give a brief description of SVM. Assume $\{(x_1,y_1),...,(x_l,y_l)\}$ is the given training data sets, where each $x_i \subset R_n$ shows the input date of the sample and has a corresponding target value $y_i \subset R$ for i=1, . . . ,l. where l represents the size of the training data. The support vector machine solves an optimization problem:

$$\min \quad \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{l}\xi_i$$

China National Natural Science Foundation (71073056). Authors: YANG Jian-hui(1960-),male, professor, postdoctoral, the main research direction : the investment decision-making and risk management; DOU Wei(1989-),male, graduate student, the main research direction: finan-ceial decision-making ,corresponding author' E-mail adderss :dauwile @foxmail.com;

doi:10.4304/jsw.9.1.195-202

$$\text{Subjected to}\begin{cases} y_i - < w, x_i > -b \le \epsilon_i + \xi \\ < w, x_i > +b - y_i \le \epsilon_i + \xi^* \\ \xi_i, \xi_i^* \ge \quad i = \quad \ldots l \end{cases}$$

Where x_i is mapped to a higher dimensional space by the function Φ,ξ_i is the upper training error(ξ_i^* is the lower) subject to the ε insensitive tube $y_i - < w, x_i > -b \le \varepsilon$. The parameters which control the regression quality are the cost of error C, the width of the tube E, and the mapping function Φ. The constraints imply that we would like to put most data x_i in the tube $y_i - < w, x_i > -b \le \varepsilon$. If x_i is not in the range, there is an error ξ_i or ξ_i^* which we would like to minimize in the objective function. SVM avoids under fitting and over fitting the training data by minimizing the training error $\sum_{i=0}^{l}(\xi \text{ or } \xi^*)$, as well as the regularization term $\frac{1}{2}\|w\|^2$. By contrast, traditional least square regression ε is always 0, and data are not mapped into a higher dimensional spaces. Therefore, SVM is a more general and flexible model on regression problems.

Many works in forecasting have demonstrated the favorable performance of SVM before. Therefore, SVM is adopted in this paper. The selection of the three parameters γ, ε and C of SVM will influence the accuracy of the forecasting result. However, there is no standard method of selection of these parameters. In the paper, particle swarm optimization technique is used in the proposed model to optimize parameter selection.

A. WT-PSO-SVM Forecasting Model

Let $\Psi(t) \in L^2(R)$, its Fourier transform as $\Psi(\omega)$, to meet permit conditions $C_\Phi = \int_R^d |\Psi(\omega)|^2 / |\omega| d\omega < \infty$. $\Psi(\omega)$ is basic wavelet, in continuous case,

$$\Psi_{ab}(t) = a^{(-1/2)}\ \Psi(\frac{(1-b)}{a}),$$

Where a is the dilation factor, b is the translation factor. Given any function $f(x) \in L^2(R)$, the continuous wavelet transform and its reconstruction formula is:

$$W_f(a,b) = (f, \Psi_{ab}) = |a|^{-1/2} \int_R^d f(t)\Psi(\frac{t-b}{a})dt$$

$$f(t) = \frac{1}{C_\Psi}\int_{-\infty-\infty}^{+\infty+\infty}\frac{1}{a^2}W_f(a,b)\Psi\left(\frac{t-b}{a}\right)dadb$$

Decomposition contains a signal of lower frequency component, while details contain higher frequency components. After wavelet decomposition and reconstruction, we can get a different frequency component. The original signal Y will be decomposed into $Y=D_1+D_2+\ldots+D_N+A_N$, Where $D_1,D_2,\ldots,D_N$, respectively, for the first layer, second layer to the N-tier decomposition of high-frequency signal (i.e., the detail signal). Then plus D_1 to D_N, and using PSO to optimize SVM's parameters to get the prediction result of the signals. Using PSO method to train the parameter of SVM again, and get the prediction result of A_N. Plusing the two prediction results, we can get the final prediction [9] [10].

Nowadays, the WT is a mature model to decompose the signal, and will get a good performance. WT method decomposed the signal into approximation signal and detail signals, then we use a combination of PSO and SVM model to predict the signals that WT decompose the original signal, finally can get a better result. Its prediction accuracy is higher than the traditional SVM method. EMD is a new type of signal decomposition tool, so we combine EMD, PSO and SVM together, and expect to have a higher accuracy and reduce errors. Therefore, comparing the WT-PSO-SVM method, we can test whether EMD-PSO-SVM is affective or not. In our next section, we will introduce EMD-PSO-SVM method.

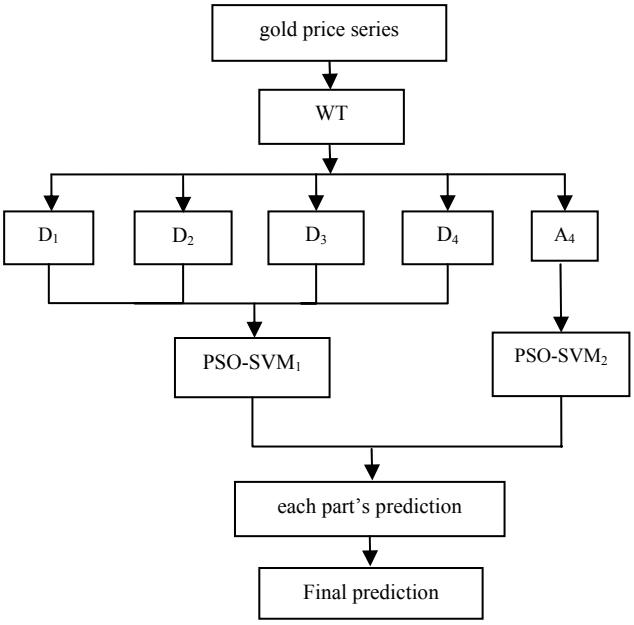


Figure 1. The construction of Gold price forecasting model by WT-PSO-SVM

B. EMD-PSO-SVM Prediction Model

EMD is a generally nonlinear, non-stationary data processing method developed by Huang et al. (1998) [11],[12]. It assumes that the data, depending on its complexity, may have many different coexisting modes of oscillations at the same time. EMD can extract these intrinsic modes from the original time series, based on the local characteristic scale of data itself, and represent each intrinsic mode as an intrinsic mode function (IMF), which meets the following two conditions:

1) The functions have the same numbers of extreme and zero-crossings or differ at the most by one;

2) The functions are symmetric with respect to local zero mean.

The two conditions ensure that an IMF is a nearly periodic function and the mean is set to zero.IMF is a harmonic-like function, but with variable amplitude and

frequency at different times. In practice, the IMFs are extracted through a sifting process.

The EMD algorithm is described as follows:

1) Identify all the maxima and minima of time series x(t);

2) Generate its upper and lower envelopes, $e_{min}(t)$ and $e_{max}(t)$, with cubic spline interpolation.

3) Calculate the point-by-point mean (m(t)) from upper and lower envelopes:

$$m(t) = \frac{e_{min}(t) + e_{max}(t)}{2}$$

4) Extract the mean from the time series and define the difference of x (t) and m (t) as d (t): $d(t) = x(t) - m(t)$

5) Check the properties of d (t):

If it is an IMF, denote d (t) as the ith IMF and replace x (t) with the residual $r(t) = x(t) - d(t)$.

The ith IMF is often denoted as ci(t) and the i is called its index;

If it is not, replace x (t) with d (t);

6) Repeat steps 1)-5) until the residual satisfies some stopping criterion.

The original time series can be expressed as the sum of some IMFs and a residue:

$$x(t) = \sum_{j=1}^{N} c_j(t) + r(t)$$

Similar with the wavelet decomposition, the price series is decomposed into a number of different frequencies IMFs. Based on fine-to-coarse reconstruction rule, the IMFs are composed into high-frequency sequence, low-frequency sequence and trend series. Then we choose the right kernel functions to build different SVM to predict each IMF. Finally, we plus the prediction of the high-frequency sequence, low-frequency sequence and trend series to get the final result[13].

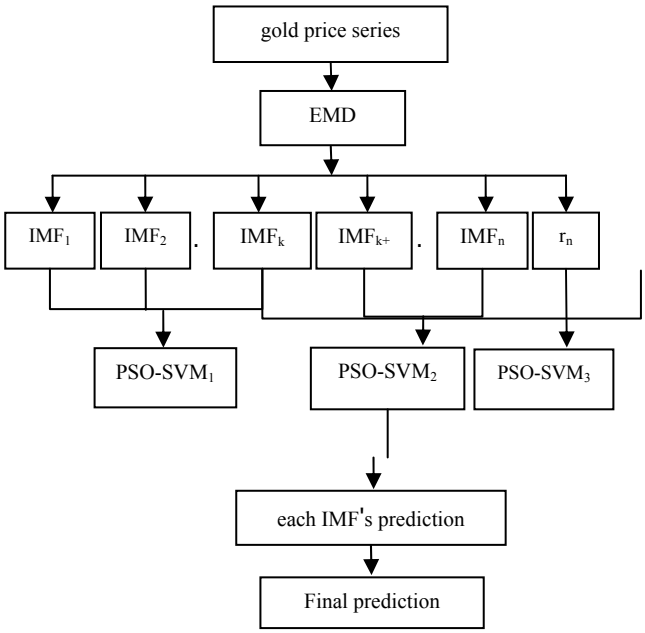


Figure 2. The construction of Gold price forecasting model by EMD-PSO-SVM

III. Experimental Results and Analysis

A. Research Data

The experimental data set comes from the London gold market's afternoon fixing price from January 4, 2005 to November, 28, 2011 which consists of a total of 1860 data. All data from http://www.lbma.org.uk, the London Bullion Market Association. For the missing data, we use the interpolation method to fill. In the London gold price series, the data from January 4, 2005 to February 21, 2011 are used as the training data, while February 22, 2011 to November 28, 2011 as the testing data.

At the same time, we chose the Shanghai gold futures closing price as another experimental data to test whether the combination method has good adaptability and stability. The time span is from January 8, 2008 to December.28 2011. The data from January 8, 2008 to September 15, 2011 are used as training samples, while the data from September 16, 2011 to December 28, 2011 as the testing data.

B. Wavelet Decomposition and Prediction

First of all, using wavelet method, we decomposed the gold price series in the London market to a detail signal and an approximation signal. Then continue to decompose the approaching signal, and get the next level of approximation and details signals. Repeat the above steps until we get four detail signals Di and an approximation signal A4, as illustrated in Fig. 3.

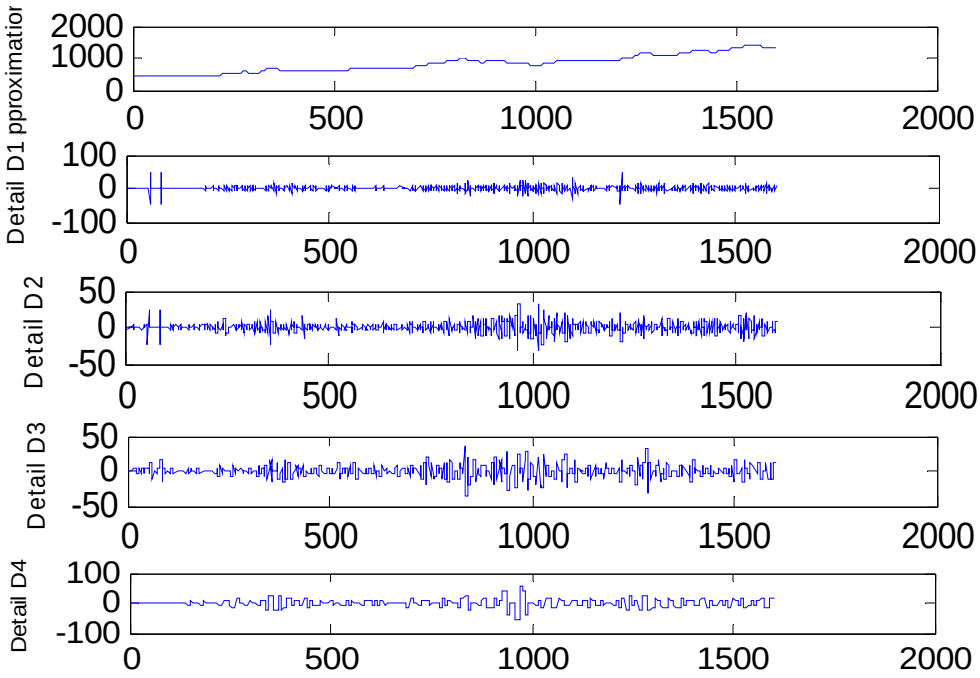
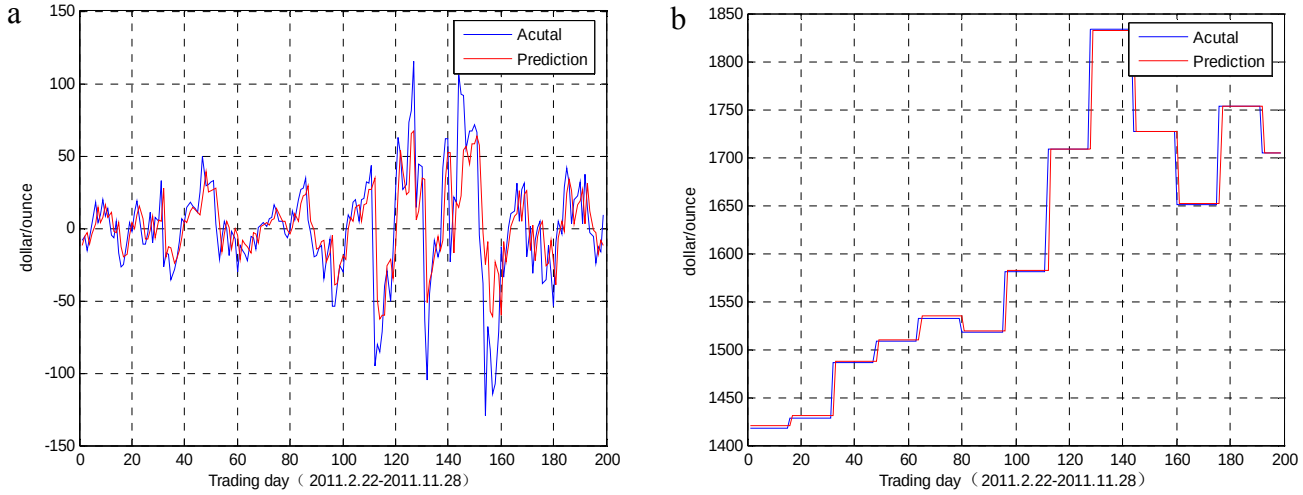


Figure 3. The decomposed using WT in London market

Adding the four details signal Di together, we can get the detail part of the entire sequence, representing the fluctuations in the market. While approaching signal indicates the direction of the market trend. We use the PSO-SVM method to predict the approximation signal and detail signal. The detail signal is in a short period of time, and has high frequency fluctuations, but less volatile. The detail signal basically fluctuates to 0 and prediction deviation is a little large. While the approaching signal's change frequency is low, but significant, showing a trend of change. The prediction deviation of the approaching signal is small. The predicted data of the details signal are plotted in Fig. 4(a) while the predicted approaching signal is shown in Fig. 4(b). The final prediction of WT-PSO-SVM is given in Fig. 4(c).



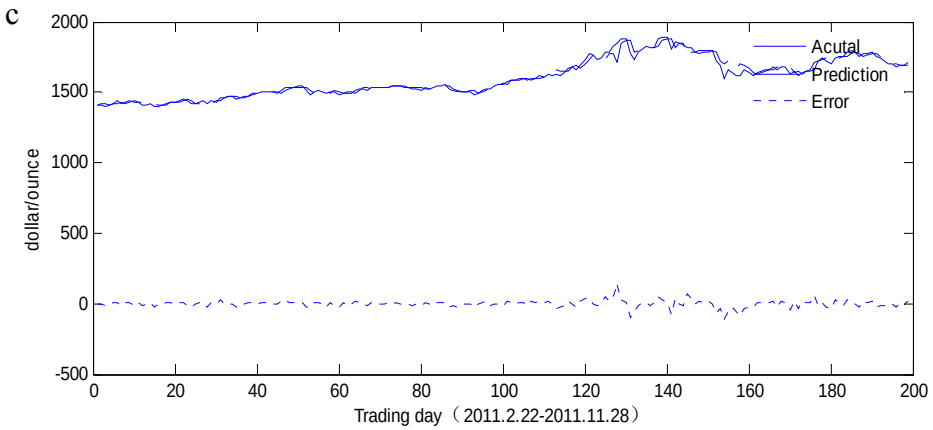


Figure 4. Forecasting results by WT-PSO-SVM in London market

As shown in the previous method, we have chosen the Shanghai gold futures market data to analyze. And we can get the final forecasting result that is substantially the same with the London market prediction, as illustrated in Fig 5.

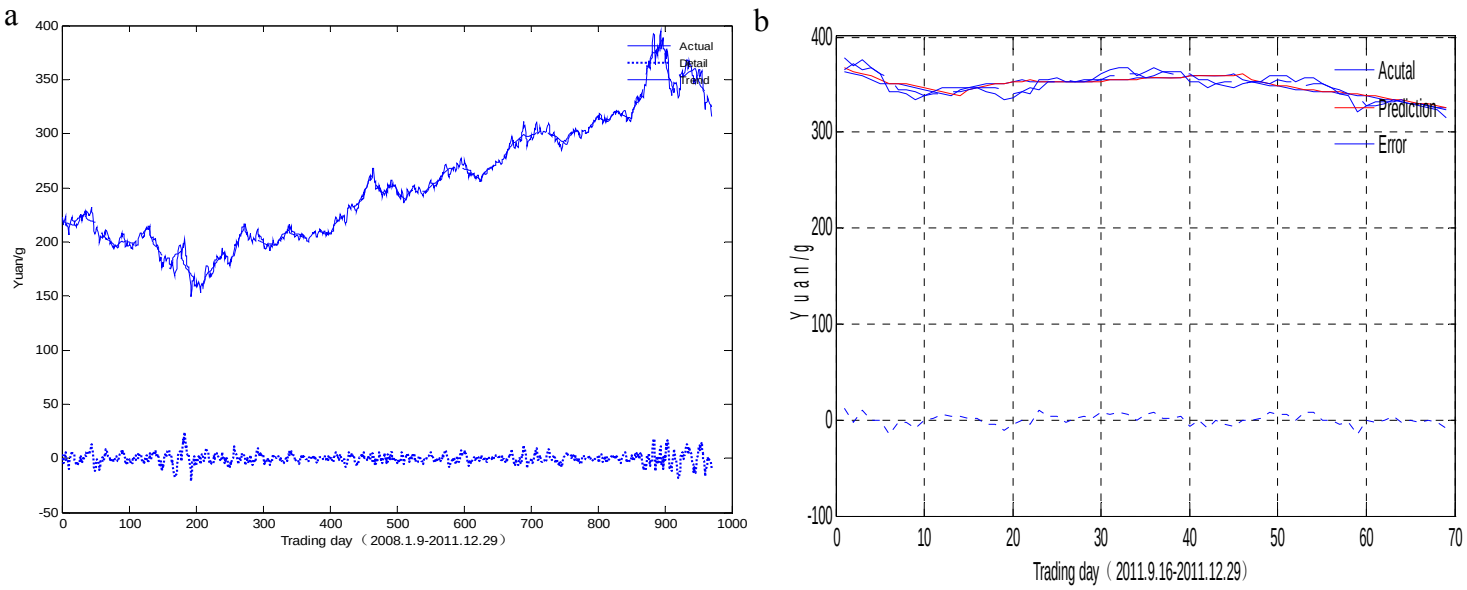
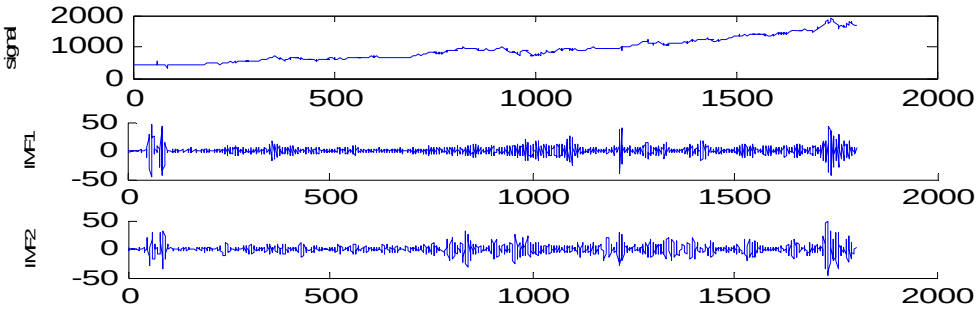


Figure 5. Forecasting results by WT-PSO-SVM in shanghai market

C. *EMD Decomposition and Prediction*

Firstly, using EMD method, we decomposed the gold price series in the London market. Unlike the wavelet composition, EMD method directly divided the gold price series into many IMFs and a residual component R. It can be seen from Fig. 6 that we finally get 7 IMFs and a residual component R.



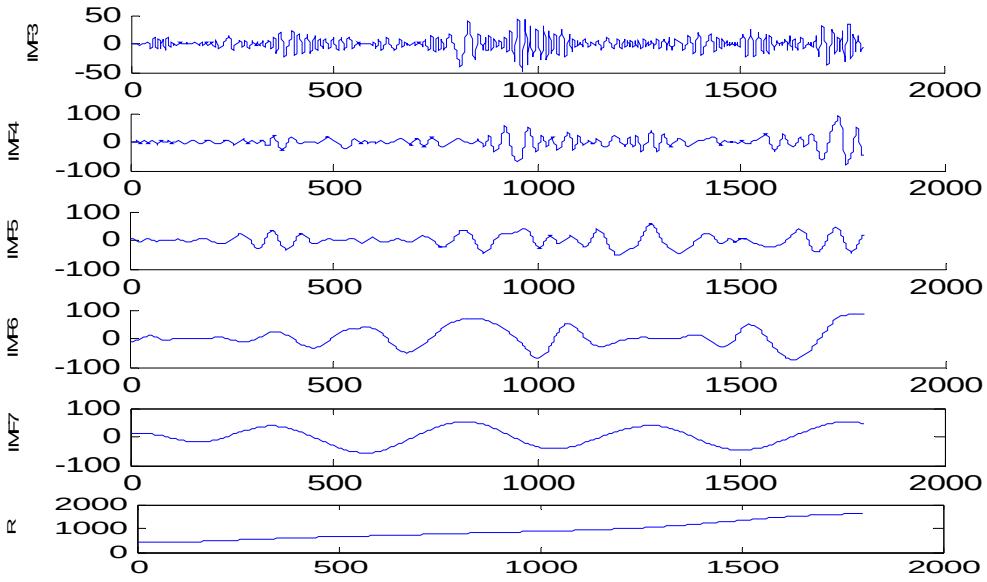
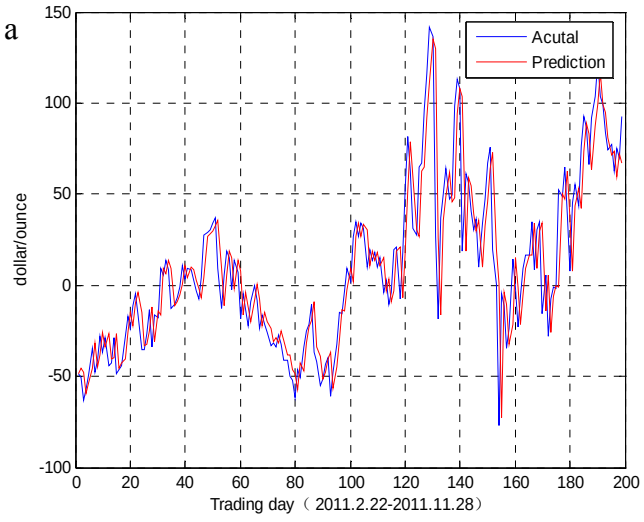
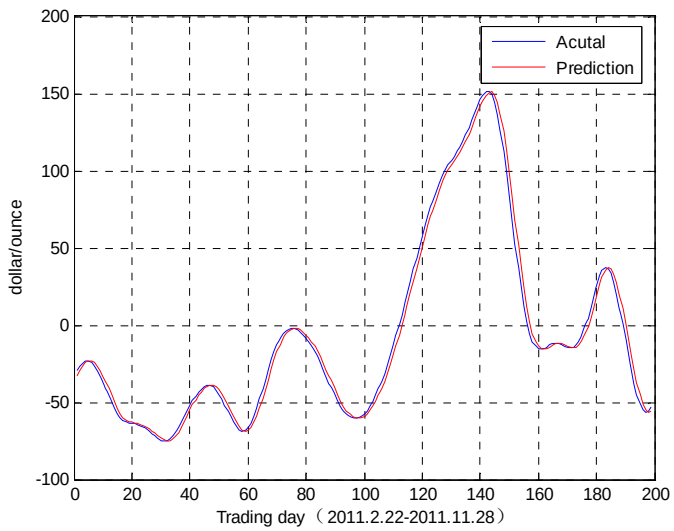


Figure 6. The decomposed using EMD decomposition

From Fig. 6, we can find that the average value of IMF1-IMF4 is approximately equal to zero and presents a very dramatic fluctuation. Group IMF1-IMF4 into a high-frequency sequence part, representing minor changes in the market, for example, some fabricated rumors. At the same time, the average value of IMF5-IMF7 is significantly greater than zero and presents a smaller frequency fluctuations, but long life cycle and impact. Group IMF5-IMF7 into a low-frequency sequence,representing big changes in the market which have long-term and stable affection to gold price, for example, raising interest rates by the central bank or enhancing the deposit reserve ratio. Finally, R represents the trend in the market, considered the impact of the global nature of the entire financial industry. For example, central banks around the world increase e-currency launch, causing the devaluation of the local currency. So gold as a hard currency, presents a continuous uplink irreversible trend. Then we use PSO-SVM method to predict different frequency sequences. The sum of each forecasting value will be the final prediction. The actual data and predicted data of different frequency sequences are shown in Fig. 7(a) to Fig. 7(c). And the final prediction of EMD-PSO-SVM method is given in Fig. 7(d).





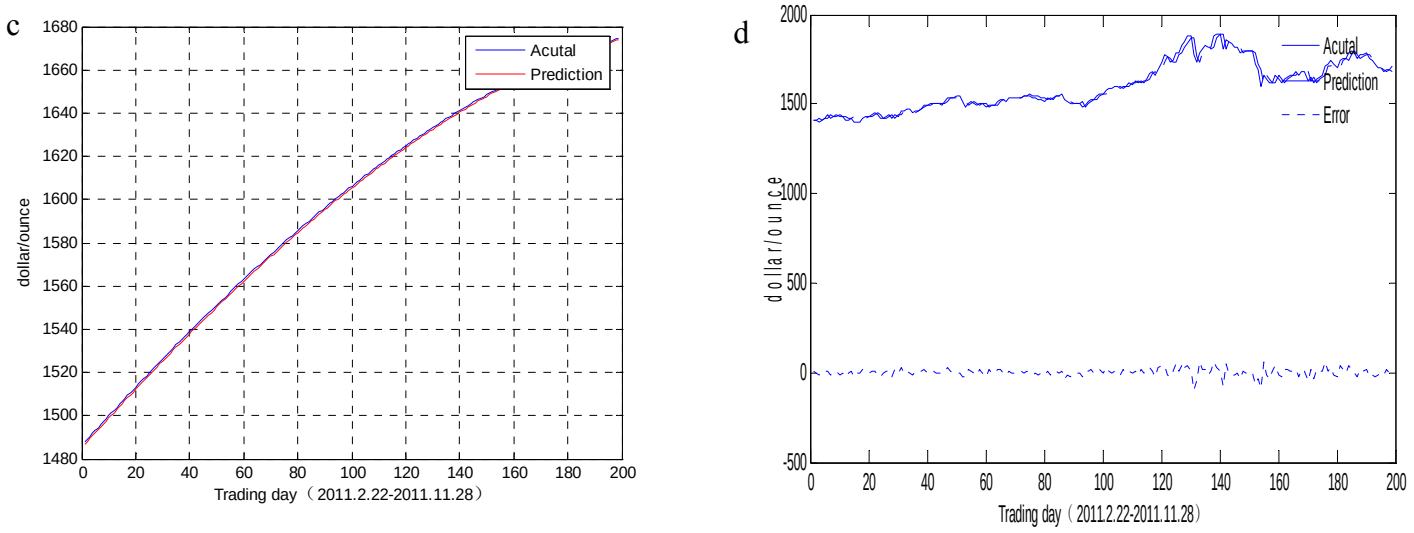


Figure 7. Forecasting results by EMD-PSO-SVM and details enlargement

As shown in the previous method, we have chosen the Shanghai gold futures market data to analyze. We can find that the gold price movements and error are substantially the same with the London market prediction, as illustrated in Fig 8. This shows that EMD-PSO-SVM model has stability and strong adaptability, and can be applied in different markets.

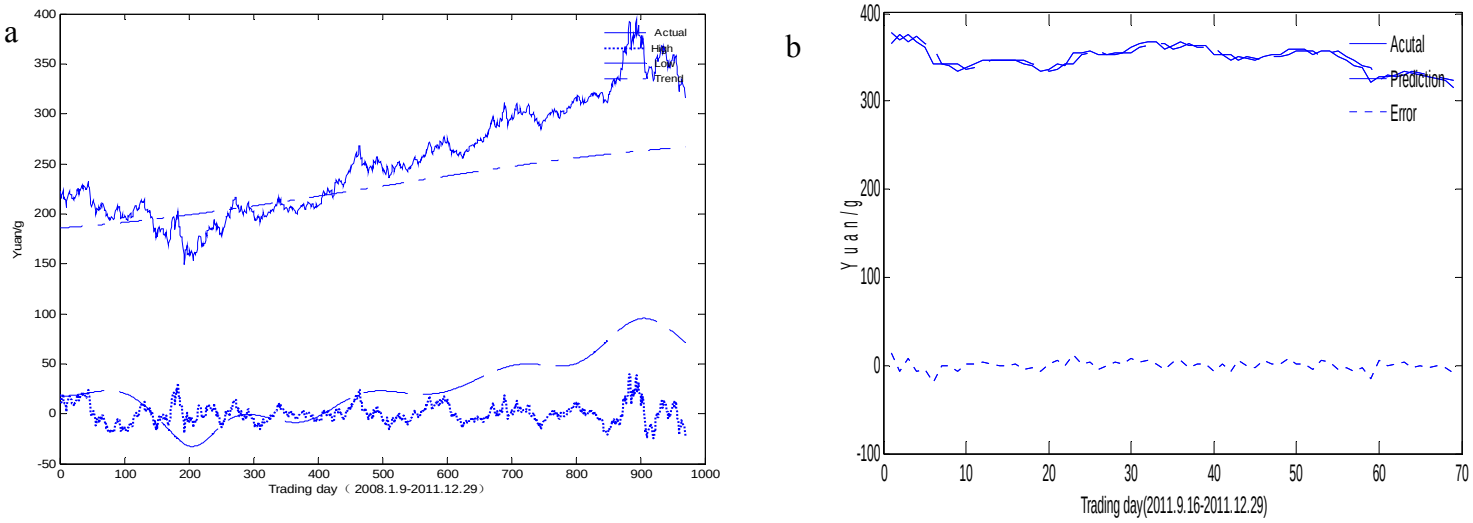


Figure 8. Forecasting results by EMD-PSO-SVM in shanghai market

D. The Comparison of the Two Methods' Results

The training errors of the two methods are all small. But we can still see that, the average error of WT-PSO-SVM method is 1.09% in London market. While in shanghai market, the error is 1.13%; the average error of EMD-PSO-SVM method is 0.46% in London market. While in shanghai market, the error is 0.49%. As a result, the EMD-PSO-SVM model outperformed the WT-PSO-SVM model, and was feasible and effective in gold price prediction.

E. Discussion

The results in the above experimental studies prove that comparing to the WT-PSO-SVM method, EMD-PSO-SVM has achieved a significant improvement in prediction accuracy. The accurate rate is at a high level. The reason is the following:

(1)The EMD is a better signal decomposition tool than the WT model, but it was generally used in industrial and oceanography field before. We introduce EMD into the financial sector, and the practice has proved that it is also effective. In particular, EMD portrays the characteristics of the series more accurately. Through analyzing the IMFs, we can find economic factors which affect the gold market movements and provide decision-making for investment.

(2) In the paper, SVM was used to predict each IMF in which PSO method was applied to optimize the

parameters of SVM. The most suitable parameters directly decide the prediction accuracy of SVM.

(3) Since gold price is non-stationary, using EMD method decompose the series, then regroup the sequence in accordance with the different frequency which avoid the errors of accumulation in the respective segments in the prediction process.

(4) Comparing to the London gold market, the prediction error is larger in Shanghai gold market. It mainly manifests in the short-term high frequency part. Because when influenced by some market fluctuations, the gold price in Shanghai market will appear a larger fluctuation, showing that the Shanghai gold market is not as mature as the London gold market, and it has poorer resistance to shock. Nowadays, the investors are also sensitive to market noise impact. Long-term value investment idea has not deeply rooted.

IV. Concluding Remarks

In this article, we study the London and Shanghai gold market price data, and successfully establish the prediction model. Firstly, we use the EMD method and wavelet method to decompose each set of data, and then reconstruct them. Add the predicted data together respectively and obtain our final results. In the forecasting part, we combine the PSO and the SVM together. In order to improve the prediction accuracy of the SVM, the PSO is used to optimize the parameters. Empirical studies showed that: comparing the EMD method to the traditional wavelet method, the prediction accuracy is significantly improved. Especially when processing nonlinear and non-stationary data, EMD has its own superiority. EMD method will be as much as possible to retain the basic features of the original data. The PSO combined with SVM method can effectively improve the prediction accuracy. The combination of EMD, PSO and SVM can decompose the data into several layers which we can analyze the characteristics of each time series data to get better explanatory of the prediction results. Also, through the analysis of each sequence prediction results, we can know short and long term trend of fluctuations of the gold price, and find the influencing factors which can guide our investment. The EMD-PSO-SVM method has a wide range of practical value, and can be promoted to other related financial areas.

References

[1] Qian Bingbing, "The Application of Type-2 Fuzzy System to Forecast the Price of Gold," Journal of Jiamusi University, vol. 25, pp. 397-399, 2007.

[2] Qin Sheng and Chen Yang, "Prediction Gold Price base on Grey Markov Model," China Economist, vol.10, pp. 29-31, 2010.

[3] Zhang Kun, Yu Yong and Li Tong, "Application of wavelet neural network in prediction of gold price," Computer Engineering and Applications, vol. 46(27), pp. 224-226,2010

[4] V.N. Vapnik, "The Nature of Statistical Learning Theory, " Springer, New York, 1995.

[5] Dongxiao Niua,Yongli Wanga,Desheng Dash Wu, "Power load forecasting using support vector machine and ant colony optimization," Expert Systems with Applications,2010, 37(3):2531-2539.

[6] Koknar-Tezel, LJ Latecki, "Improving SVM classification on imbalanced time series data sets with ghost points," Knowledge and information systems2011,28:1-23.

[7] Abdulhamit Subasi, "Classification of EMG signals using PSO optimized SVM for diagnosis of neuromuscular disorders," Computers in Biology and Medicine,2013,In Press.

[8] S. Jazebi ,B. Vahidi, M. Jannati, "A novel application of wavelet based SVM to transient phenomena identification of power transformers," Energy Conversion and Management,2011,52(2): 1354-1363.

[9] Wei Bin, Wu Chongqing and Shen Ping, "Fast Hurst Value Computation Base on Wavelet Transform and EMD," Computer Engineering, vol. 34, pp.1-3,2008

[10] Chen Wei, Wu Jiejun, Duan Weijun, "Model of Urban Air Pollution Concentration Forecast Based on Wavelet Decomposition and Support Vector Machine," Modern Electronics Technique, vol.34,pp145-148,2011

[11] HUANG N E,SHEN Z and LONG S R, "The Empirical Mode Decomposition and the Hilbert Spectrum for Nonlinear and Nonstationary Time Series Analysis, " The Royal Society A: Mathematical, Physical & Engineering Sciences, pp. 903-995, 1998

[12] HUANG N E,SHEN Z and LONG S R, "A New View of Nonlinear Water Waves: The Hilbert Spectrum, " Annual Review of Fluid Mechanics, vol. 31, pp. 417-457, 1999.

[13] Wang Wei, Zhao Hong, Liang Zhaohui and Ma Tao, "Hybrid intelligent prediction method based on EMD and SVM and its application," Computer Engineering and Applications, vol. 48,pp225-227,2012

Combining Local Binary Patterns for Scene Recognition

Minguang Song, Ping Guo*
Image Processing and Pattern Recognition Laboratory,
Beijing Normal University, Beijing 100875, China
Email: mgsongbnu@gmail.com; pguo@ieee.org

***Abstract*—Recently, spatial principal component analysis of census transform histograms (PACT) was proposed to recognize instance and categories of places or scenes in an image. An improved representation called Local Difference Binary Pattern (LDBP) also was proposed and performed better than that of PACT. LDBP is based on the comparisons between center pixel and its neighboring pixels, but the relationship among neighbor pixels is not considered. In this paper, we propose to combine Local Neighbor Binary Pattern (LNBP) with LDBP to construct a spatial representation for scene recognition, because that LNBP can provide complementary information regarding neighboring pixels for LDBP. Experiments on widely used datasets demonstrate that the performance of image recognition is further improved with proposed method.**

***Index Terms*—scene recognition, spatial pyramid matching, local binary pattern**

I. INTRODUCTION

Scene recognition is an important task in computer vision and has attracted considerable attention in recent years, it refers to the problem of recognizing the semantic category (e.g. bedroom, mountain, or coast) of a single image [1]. Scene recognition is widely used in many aspects, such as robotics path planning, video content analysis, content-based image retrieval, and video surveillance [2].

Compared with object recognition, scene recognition is more challenging because of ambiguity and variability in the content of scene images, which is further worsened by the variations in illumination and scale. Numerous efforts have been made to solve this kind of problem. Oliva and Torralba [3] proposed spatial envelope that represented the dominant spatial structure (naturalness, openness, roughness, expansion, ruggedness) of a scene, which achieved high accuracy in recognizing natural scenes. However, it performed bad about indoor scenes. Hoffman [4] put forward probabilistic latent semantic analysis (pLSA) model to perform probabilistic mixture decomposition. Bag of visual words (BoW) model [5, 6] becomes popular in recent years. BoW model represents an image as an unordered collection of local features, and has demonstrated impressive levels of performance [2]. But the spatial information is neglected in BoW model. To improve the BoW model, Lazebnik *et al.* [7] incorporated spatial information by using spatial pyramid matching (SPM) scheme, and uses scale in variant feature transform (SIFT) [8] descriptor as the local feature. SIFT becomes the most popular descriptor in recent years [5, 7, 9, 10, 16, 19, 20, 21, 22, 23, 24, 25, 26]. Yang *et al.* [9] proposed linear SPM based on sparse coding (ScSPM) which developed an extension of the SPM method by generalizing vector quantization to sparse coding of SIFT descriptors, and followed by multi-scale spatial max pooling. ScSPM remarkably reduces the complexity of training and testing task. Gao *et al.* [19] proposed a Laplacian sparse coding method, which exploited the dependence among the local features to alleviate the sensitiveness of quantization. Gemert *et al.* [10] introduce visual word ambiguity to model a soft assignment instead of hard assignment, profiting in high-dimensional feature spaces and receive higher benefits when increasing the number of image categories.

Research on non-parametric nearest neighbor (NN) classification has also made progresses in past years. Boiman *et al.* [20] proposed a trivial NN-based classifier, which was called Naive-Bayes Nearest-Neighbor (NBNN). NBNN computes direct image-to-class distances without descriptor quantization. Wang *et al.* [21] learned metric for each class using Mahalanobis distance. Behmo *et al.* [22] relaxed the incriminated assumption in NBNN and solve the parameter selection problem by hinge-loss minimization. Tuytelaars *et al.* [23] proposed the NBNN kernel which learned the classifier in a discriminative setting.

Although SIFT-based BoW model with SPM achieves remarkable performance, the computational complexity in both space and time is still a burden. Paris *et al.* [29, 30] combined Histogram of Local Binary Pattern with BoW, which outperforms SIFT-based methods. Recently, Wu and Rehg [1, 11] proposed spatial principal component analysis of census transform histograms (PACT), or Census Transform histogram (CENTRIST), which is an effective representation that fulfills the need for recognizing categories of places and scenes. CENTRIST captured local structures of an image by the Census Transform [13] and incorporated global structures with SPM. CENTRIST is superior to BoW model on scene recognition task for its simplicity and

* Corresponding author, email: pguo@ieee.org

doi:10.4304/jsw.9.1.203-210

efficiency. Hu *et al.* [12, 28] utilize a multi-level kernel machine to alleviate the difference existing in various levels. Meng *et al.* [2] introduced local difference magnitude information as complement and built spatial Local Different Binary Pattern (LDBP) representation.

CENTRIST and LDBP have achieved excellent performances. However, both of them are based on the comparisons between center pixel and neighbors; the relationship among neighbors is ignored. Under a large amount of conditions, there exist different local structures that have the same LDBP code. In such cases, the different local patterns are not clearly represented and cannot be differentiated. Some important information with respect to edges and gradients is lost. This information is significant for describing the structure of scenes. Consequently, different patterns are assigned into the same category, which decreases the discriminative power. To address this problem, Local Neighbor Binary Pattern (LNBP) [27] was proposed as an extension of local binary pattern. LNBP is a complement of CENTRIST and LDBP for describing local structures, and therefore could improve scene recognition task. We therefore propose to combine LDBP with LNBP, and it can preserve the advantages - easy to implement, nearly no parameter to tune and fast to evaluate.

The rest of this paper is organized as follows. Section II briefly describes spatial PACT and spatial LDBP. In Section III we introduced LNBP, and our proposed image representation is presented. In section IV, Experimental results on common datasets are given. A conclusion of this paper is drawn in Section V.

II. Related Works

A. Census Transfrom and Spatial PACT

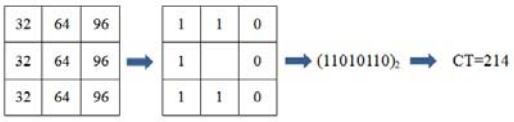


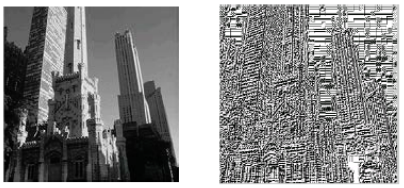
Figure 1. The Census Transform operation

Census Transform (CT) is a non-parametric local transform originally designed for establishing correspondence between local patches [13]. Census transform compares the intensity value of a pixel with its eight neighboring pixels, as illustrated in Fig. 1. If the center pixel is bigger than (or equal to) one of its neighbors, a bit 1 is set in the corresponding neighbor location. Otherwise a bit 0 is set, which only has a different bit order from the local binary pattern (LBP) code $LBP_{8,1}$ [18]:

$$CT = \sum_{i=0}^{P-1} g(I_i, T) \cdot 2^i ,$$
$$g(x,T) = \begin{cases} 1, x \le T \\ 0, x > T \end{cases}, \quad T = I_c, \tag{1}$$

where P is the number of neighboring pixels, *i.e.* 8.

Census transform is robust to illumination changes, gamma variations, etc. As a visualization method, a census transformed image is created by replacing a pixel with its CT value. Shown by the example in Fig. 2, the census transform retains global structures of the picture (especially discontinuities) besides capturing the local structures.



(a) original image (b) transformed image

Figure 2. An example of census transformed image.

One important property of the transform is that CT values of neighboring pixels are highly correlated [1]. In the example of Fig. 3, the Census Transform for pixels valued 36 and 37 are depicted in right, and the two circled bits are both comparing the two center pixels (in different orders). Thus the two bits must be strict complement to each other if the two pixels are not equal. More generally, bit 5 of CT(x, y) and bit 4 of CT(x + 1, y) must be complementary to each other, if the pixels at (x, y) and (x+1, y) are not equal. Generally, there are eight such constraints between one pixel and its eight neighboring pixels.

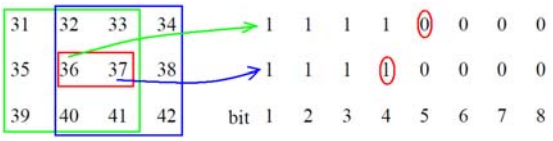


Figure 3. Illustration of constraints between CT values of neighboring pixels.

Besides these deterministic constraints, there also exist indirect constraints. For example, in Fig. 3, the pixel valued 32 compares with both center pixels when computing their CT values (bit 2 of CT(x, y) and bit 1 of CT(x + 1, y)). Depending on the comparison results between the center pixels, there are probabilistic relationships between these bits.

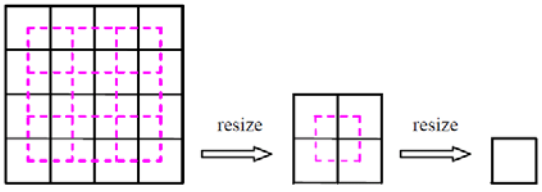


Figure 4. Illustration of the level 2, 1, and 0 spatial pyramid split of an image, from [1].

Wu *et al.* [1, 11] proposed Principal component Analysis of Census Transform histograms (PACT), that is, the principal component analysis (PCA) operation performs on the CT histograms, to remove these correlation effects, and to get a more compact representation. Because PACT can only encode global shape structure in a small image patch, in order to

capture the global structure of an image in larger scales, a spatial PACT representation based on the SPM scheme was proposed. A spatial pyramid, which divides an image into segments and concatenates correspondence results in these regions, encodes roughly spatial structure of an image and usually improves recognition rate. The level 2 split in a spatial pyramid divides the image into 4 × 4 =16 blocks. They also shift the division (dash line blocks) in order to avoid artifacts created by the non-overlapping division, which makes a total of 25 blocks in level 2. Similarly, level 1 and 0 have 5 and 1 block, respectively. The image is resized between different levels so that all blocks contain the same number of pixels. These blocks are shown in Fig. 4. PACT in all blocks is then concatenated to form an overall feature vector of 1240 dimensional.

B. Local Difference Binary Pattern and Spatial LDBP

Census transform concerns whether a center pixel is higher or lower than its neighboring pixels, resulting in some information loss of intensity contrast. It is not enough to discriminate different local structures using only census transform [2]. Meng *et al.* introduced local difference to better describe local structures.

Local difference is defined as the intensity difference between a center pixel and its neighboring pixels in a 3×3 image patch. Given a center pixel I_c and its neighbors I_i , i=0,1, …, 7. The local difference between I_c and I_i can be computed by $d_i = I_c - I_i$. Then the local difference d_i is decomposed into two components:

$$d_i = s_i \cdot m_i;\ s_i = \begin{cases} 1 & d_i \ge 0 \\ -1 & d_i < 0 \end{cases};\ m_i = |d_i|, \quad (2)$$

where s_i is the sign and m_i is the magnitude of d_i . Obviously, the sign and magnitude components contain complementary information of original local difference.

The sign and magnitude components are both converted into binary codes. The positive and negative elements in sign component are coded as 1 and 0. The 8-bit code is converted into a base-10 number called Local difference Sign Binary Pattern (LSBP). LSBP is equivalent to Census Transform.

The Local difference Magnitude Binary Pattern (LMBP) is defined as follows:

$$LMBP = \sum_{i=0}^{P-1} g(m_i, T) \cdot 2^i,$$
$$g(x,T) = \begin{cases} 1, x \ge T \\ 0, x < T \end{cases}, \quad T = \frac{1}{NP} \sum_{j=1}^{N} \sum_{i=0}^{P-1} m_{ij}, \quad (3)$$

where m_{ij} is m_i of the jth pixel, N is the number of pixels (excluding boundaries) in Image, and T is the mean m_i of the whole image. Finally, both LSBP and LMBP transform a 3×3 image block into an integer in [0, 255]. The coding process of LSBP and LMBP is shown in Fig. 5.

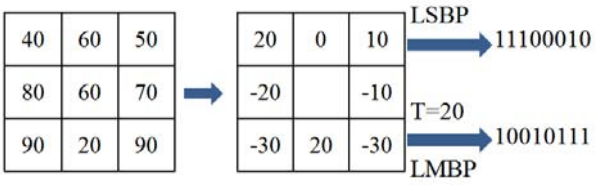


Figure 5. Coding process of LSBP and LMBP.

As shown in Fig. 6, the LMBP values of neighboring pixels are highly correlated. Similar to CT, Bit5 of LMBP at (x, y) and bit 4 of LMBP at (x+1, y) must be the same. There are eight such constraints between one pixel and its eight neighboring pixels. Applying the constraints to all pixels of an image, we can conclude that the number of pixels whose LMBP value's bit 5 is 1 must be equal to the number of pixels whose LMBP value's bit 4 is 1, and vice versa.

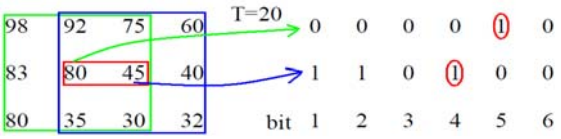
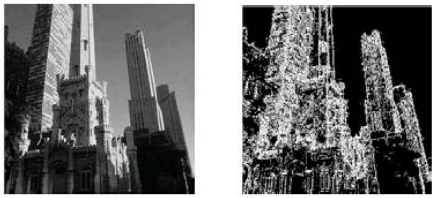


Figure 6. Illustration of constraints between LMBP values of neighboring pixels.

For visualization, a LMBP transformed image is created by replacing a pixel with its LMBP value. Shown by the example in Fig. 7, the LMBP transform also retains global structures of the picture.



(a) original image (b) transformed image

Figure 7. An example of LMBP transformed image

Because bins are strong correlated with each other in LSBP and LMBP, PCA is utilized to reduce the dimensionality. The LSBP and LMBP histograms perform PCA separately and then are concatenated to form the final feature vector, namely LDBP histogram. PACT only uses the sign component of LDBP.

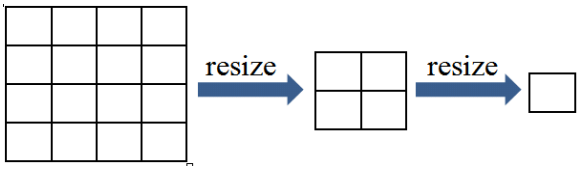


Figure 8. Illustration of the level 2, 1, and 0 spatial pyramid split of an image.(referred from [2])

The spatial pyramid scheme [2] is given in Fig. 8, the level 2 split in a spatial pyramid divides the image into 16 non-overlapping blocks. Similarly, level 1 has 4 blocks and level 0 has 1 block, respectively. The image

is resized between different levels so that all blocks contain the same number of pixels. In total, there are 21 blocks for each image. The vector representations in all blocks are concatenated to form an overall feature vector for each image as the global image representation. The dimension of final feature vector is 840.

III. Proposed Method

A. Local Neighbor Binary Pattern

LDBP are based on the comparisons between center pixel and its neighboring pixels, both the sign part and magnitude part. The relationship between neighbor pixel and center pixel is well described. However, there is some information loss concerning the relationship of neighbor pixels because the relationship of neighbor pixels is neglected.

Under a large number of circumstances, there exist different local structures that have the same LDBP code. In such cases, the local pattern is not clearly represented and cannot be differentiated. According to our statistics from popular datasets, there are more than 15% pixels in scene images belonging to this category. These local structures may contain important information for scenes, for example, edges and gradients; it is also possible that some of them are smooth areas. Nevertheless, in LDBP, these distinct patterns are treated as the same one. LDBP has no discriminative ability for these local structures. Therefore, it is necessary to distinguish these different local structures that LDBP is not capable to differentiate with. A new descriptor is demanded to characterize such local patterns.

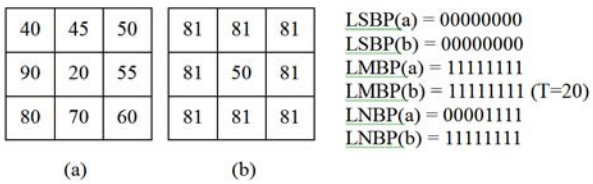


Figure 9. Example of complementary information from LNBP.

To address this problem, we propose an extension of local binary pattern, which only reflects local structure of neighboring pixels. The Local Neighbor Binary Pattern (LNBP) is defined as follows:

$$LNBP = \sum_{i=0}^{P-1} g(I_i, T) \cdot 2^i ,$$
$$g(x,T) = \begin{cases} 1, x \geq T \\ 0, x < T \end{cases}, \quad T = \frac{1}{P}\sum_{i=0}^{P-1} I_i, \tag{4}$$

LNBP is also computed on a 3×3 local neighborhood. Note that LNBP is different with Multimodal Invariant Local Binary Pattern (MILBP) [31], Local Gradient Pattern (LGP) [32], Modified Census Transform (MCT) [14], and Improved LBP (ILBP) [15]. Both MILBP and LGP use the absolute value of difference, therefore we cannot know whether the intensity of one pixel is higher than other ones. However, LNBP compares neighbor pixels with the mean of neighbors. Therefore we can know the relations of some neighbor pixels. This is the advantage of LNBP over MILBP or LGP. Compared with MCT and LBP, The center pixel is discarded to eliminate the influence of its intensity so that we can concentrate on the relationship of neighboring pixels. The threshold is set as the mean intensity value of eight neighbor pixels. Because the threshold is only related to neighboring pixels, the neighbor pattern can be described better. The local patch is transformed into an integer in [1, 255]. Note that 0 is not possible for that at least one neighbor pixel is larger than or equal to the mean value.

LNBP can provide useful complementary information for LSBP and LMBP. Fig. 9 shows an example which abounds in scene images. The patterns of the two example patches are different. However, they share the same LSBP and LMBP code. In other words, we cannot discriminate these patches only by LSBP and LMBP. With our LNBP code, the patches can be distinguished as different pattern. In the example we can know that the neighbors of block (b) are the same, while the neighbors of block (a) are different in intensities. LNBP can be used to describe the local structures about which

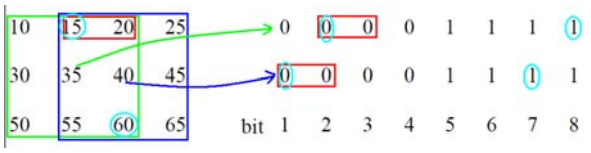


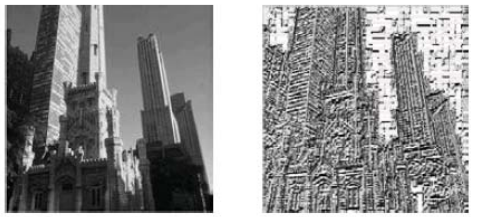
Figure 10. Illustration of constraints between LNBP values of neighboring pixels.

neighbors are larger than others. This also provides some information about gradient— how the intensity changed and the direction of gradient. LDBP may also provide this information for some local structures. But LDBP does not help much for the patches like those in Fig. 9. LNBP can always tell us such information. If the LNBP codes are all of 1, it tells us that this patch has neighbors having the same intensity. Therefore LNBP can provide useful complementary information for LDBP.

There are correlations between LNBP values. As shown in Fig. 10, when 15 and 20 are both smaller than the mean intensity in the neighboring patches, the bit 2 and bit 3 of the left patch are the same as well as the bit 1 and bit 2 in the right patch. Moreover, when the mean value is between 15 and 60, the bit 2 and bit 8 of the left block are identical to the bit 1 and bit 7 of the right block.

The transitive property of such constraints also makes them propagate to not only neighbor pixels, but also further ones. For example, in Fig. 10, the pixels valued 15 (coded as 0) and 55 (coded as 1) can be compared using various paths of comparisons. One path is $15 < 20 < 30 < 40 < 50 < 55$, the other is $15 < 20 < 25 < 35 < 45 < 55$. Similarly, although no deterministic comparisons can be deduced between some pixels (e.g. 55 and 60), probabilistic relationships can still be obtained. The propagated constraints make LNBP values and histograms implicitly contain information for describing global structures, just as CENTRIST.

To visualize the algorithm's effect, the LNBP transformed images are created by replacing a pixel with its LNBP transformed value. The examples shown in Fig. 11 demonstrate that LNBP, as well as LSBP and LMBP, not only captures local structures, but also retains the global structural information, especially discontinuities.



(a) original image (b) transformed image

Figure 11. An example of LNBP transformed image.

B. Spatial Image Representation by Combining LDBP with LNBP

A histogram of LNBP for an image or image block is computed. We kept the bin of zero, whose value is always 0. The dimension of LNBP histogram is 256. For each pair of adjacent pixels, they share four neighbors. The bins of LNBP histograms are implicitly correlated with each other. PCA was used to reduce the dimensionality of LNBP histogram to 20. Then the LDBP histogram was concatenated with the compressed LNBP histogram, and the dimension of the final feature vector is 60.

In our experiments the performance of 40 eigenvectors (an average of 13 or 14 eigenvectors for LSBP, LMBP and LNBP) was also evaluated. According to [2], when the number of eigenvectors is smaller than 20, the performance drops dramatically. In such case, the recognition rate was almost the same as spatial LDBP. Compared with 20 eigenvectors for both LSBP and LMBP, when there are only 13 or 14 eigenvectors for LSBP, LMBP, and LNBP, the benefit provided by LNBP is counteracted by the information loss of dimension reduction.

The spatial pyramid matching scheme in Fig. 8 is adopted. The final feature vector for an image is 1260 dimension. We used support vector machine (SVM) for classification.

IV. EXPERIMENTS

In this section, our approach is evaluated on three benchmark datasets: (1) 8 scene categories dataset [3], (2) 15 class scene category [7], and (3) 8 class sports event [16]. In each dataset, the available data are randomly split into a training set and a testing set following the published protocols on these datasets. The random splitting is repeated 5 times, and the average accuracy and standard deviation is reported.

In the experiments, following the same experiment procedure of the CENTRIST [1], only the intensity values and ignore color information was used. We normalized the LSBP, LMBP, and LNBP histograms and PCA eigenvectors such that they have zero mean and unit norm. LIBSVM [17] was utilized as the classifier and Radial Basis Function (RBF) kernel with recommended parameters $(C,\gamma)=(8,2^{-7})$ in [1] was adopted.

A. The 8 Class Scene Category Dataset

Figure 12. Sample images of 8 scenes. The categories are suburb, industrial, coast, forest, highway, inside city, mountain, open country, street, and tall building, respectively (from left to right, and from top to bottom).

TABLE I.
RECOGNITION RATES ON THE 8 CALSS SCENE DATASET

Method	Rates(%)
LSBP [2]	75.53
LDBP [2]	79.18
LDBP+LNBP	81.36

The 8 class scene category dataset contains total 2688 images with 8 outdoor categories. Images are 256x256 in resolution, varying from 260 to 360 images in each category. It is a subset of the 15 scene category dataset. These categories are coast (360 images), forest (328 images), mountain (274 images), open country (410 images), highway (260 images), inside city (308 images), tall building (356 images), and street (292 images). Fig. 12 gives example images of the 8 categories. This dataset is used to investigate the usefulness of LNBP. Different schemes, include LSBP, LDBP, and LDBP

combined with LNBP are compared. No PCA operation or SPM scheme were used on this dataset.

In the experiments, 100 images are drawn in each category for training, and the remaining images for testing. The SVM with RBF kernel was utilized to classify the images. The recognition results are shown in Table I. We can see that LNBP provides useful information and improves the recognition.

B. The 15 Class Scene Category Dataset

Figure 13. Sample images of 15 scenes. The categories are bedroom, suburb, industrial, kitchen, living room, coast, forest, highway, inside city, mountain, open country, street, tall building, office and store, respectively (from left to right, and from top to bottom).

The 15 class scene category dataset contains total 4485 images with 15 categories. Images are about 300×250 in average resolution, varying from 210 to 410 images in each category. This dataset contains a wide range of scene categories in both indoor and outdoor environments (scene classes including office, store, coast, etc. Fig. 13 gives example images of all 15 categories). Also, this is one of the most complete scene category dataset used in the literature so far.

According to previous works [1, 2, 11], the first 100 images in each category are used to calculate the PCA eigenvectors. The recognition results are shown in Table II. From that table we can see that our method achieves the highest recognition rate.

TABLE II.
RECOGNITION RATES ON THE 15 CALSS SCENE DATASET

Method	**Feature Type**	**Rates(%)**
SPM [7]	400 cluster centers	81.40 ± 0.50
ScSPM [8]	400 cluster centers	80.28 ± 0.93
Spatial PACT [1]	CENTRIST, 40 eigenvectors	83.88 ± 0.76
Spatial LDBP [2]	LDBP, 40 eigenvectors	83.58 ± 0.99
Our method	LDBP+LNBP, 60 eigenvectors	**84.09 ± 0.35**

Fig. 14 shows a confusion matrix from one run on this dataset using our approach. The biggest confusion happens between category pairs such as bedroom/living room, industrial/store, and coast/open country, which coincide well with the confusion distribution in [1, 2, 7, 11]. Our method achieves high recognition rates on forest, office, and suburb.

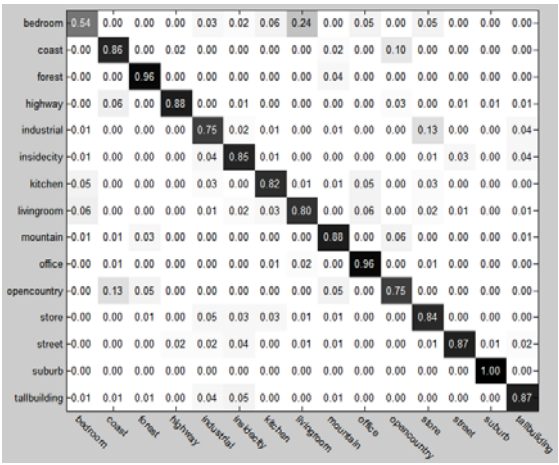


Figure 14. Confusion matrix from one run for 15 class scene category dataset recognition experiment.

TABLE III.
RESULTS OF DIFFERENT FEATURE AND CLASSIFIER ON THE 15 CALSS SCENE DATASET

Feature Type	**Classifier**	**Rates(%)**
LDBP+LNBP, 60 eigenvectors	Non-linear	84.09
LDBP+LNBP, 60 eigenvectors	Linear	83.02
LDBP+LNBP, non-PCA	Linear	72.24

Linear SVM classifiers are also applied to the scene dataset to test the PCA compact feature and the non-PCA concatenated histograms. The results are shown in Table III. The compact feature achieves the accuracy of 83.02%, obviously higher than 81.8% of spatial LDBP [2]. The difference in performance of RBF kernels and linear kernels is quite small. However, the performance of original non-PCA concatenated histogram on linear classifier is very poor. Therefore it is the PCA operation that turns the histograms into compact features. PCA is necessary. Because of the fast testing speed of linear classifiers and small performance difference, linear SVM classifiers could be used to ensure real-time classification.

C. The 8 Class Event Dataset

Figure 15. Sample images of 8 sport events. The categories are badminton, bocce, croquet, polo, rock climbing, rowing, sailing, and snowboarding (from left to right, top to bottom).

The event dataset contains images of eight sports: badminton, bocce, croquet, polo, rock climbing, rowing, sailing, and snowboarding. The images have high resolution (from 800x600 to thousands of pixels per dimension). The number of images in each category varies from 137 to 250. We used this dataset for scene recognition purposes only. Fig. 15 shows the example images.

TABLE IV.
RECOGNITION RATES ON THE 8 CALSS EVENT DATASET

Method	**Feature Type**	Rates(%)
Spatial PACT [1]	CENTRIST, 40 eigenvectors	78.25 ± 1.27
Spatial LDBP [2]	LDBP, 40 eigenvectors	82.96 ± 1.51
Our method	LDBP+LNBP, 60 eigenvectors	**83.66 ± 0.93**

Also, following the previous works of spatial PACT and spatial LDBP, we randomly select 70 images per category for training, and 60 ones for testing. The training images in each train/test split are used to compute the eigenvectors. The recognition results are shown in Table IV. Our method achieves best results outperforming spatial PACT and spatial LDBP.

We also compared the PCA feature with non-PCA concatenated histograms on linear classifier, and the results are similar to the experiment on the 15 scenes datasets, as is shown in Table V.

TABLE V.
RESULTS OF DIFFERENT FEATURE AND CLASSIFIER ON THE 8 CLASS EVENT DATASET

Feature Type	**Classifier**	**Rates(%)**
LDBP+LNBP, 60 eigenvectors	Non-linear	83.66
LDBP+LNBP, 60 eigenvectors	Linear	81.88
LDBP+LNBP, non-PCA	Linear	68.81

Fig. 16 shows the confusion matrix of one run on this dataset. The biggest confusion happens between bocce and croquet, which is coincident with previous works. From the example images in Fig. 15 we can see that the two categories are very similar in human vision. High recognition rates are achieved for rock climbing, rowing and sailing categories.

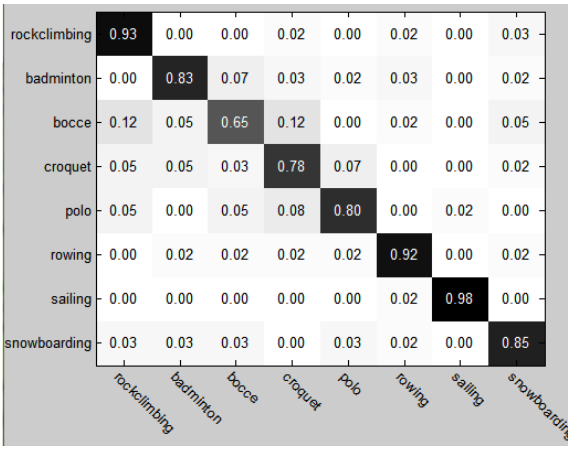


Figure 16. Confusion matrix from one run for 8 class event dataset recognition experiment .

V. CONCLUDSION

In this paper, we propose to combine LNBP with LDBP to build an effective representation for scene images. LNBP provides extra complementary information with respect to local neighbor structures, which is neglected in LDBP. The new feature provides stronger discriminative ability for local structures in improving scene recognition. Experiments conducted on common benchmark datasets demonstrate that our proposed scheme outperforms spatial PACT or spatial LDBP on scene recognition task. Moreover, proposed method preserves the advantages of spatial PACT and spatial LDBP. It is easy to implement, has nearly no parameter to tune. In all the datasets we experimented with, the difference in recognition rates between these two kernel types are less than 2%. This indicates that

images from the same category are compact in the feature space. It works well on linear classifiers, thus is very fast for evaluation.

ACKNOWLEDGMENT

The research work described in this paper was fully supported by the grants from the National Natural Science Foundation of China (Project No. 90820010, 60911130513).

REFERENCES

[1] J. Wu and J. M. Rehg, “CENTRIST: A Visual Descriptor for Scene Categorization,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 8, pp. 1489-1501, 2011.

[2] X. Meng, Z. Wang and L. Wu, “Building Global Image Features for Scene Recognition,” Pattern Recognition, vol. 45, pp. 373-380, 2012.

[3] A. Oliva and A. Torralba, “Modeling the Shape of the Scene: A Holistic Representation of the Spatial Envelope,” International Journal of Computer Vision, vol. 42, no. 3, pp. 145-175, 2001.

[4] T. Hofmann, “Unsupervised Learning by Probabilistic Latent Semantic Analysis,” Machine Learning, vol. 41, pp. 177-196, 2001.

[5] P. Quelhas, F. Monay, J. M. Odobez, D. Gatica-Perex, T. Tuytelaars and L.Van Gool, “Modeling scenes with local descriptors and latent aspects,” in Proceedings of IEEE International Conference on Computer Vision (ICCV), pp. 883-890, Oct. 2005.

[6] D. Gokalp and S. Aksoy, “Scene classification using bag-of-regions representations,” in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp.1-8, 2007.

[7] S. Lazebnik, C. Schmid and J. Ponce “Beyond Bags Of Features: Spatial Pyramid Matching for Recognizing Natural Scene Categories,” in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2169-2178, 2006.

[8] D. G. Lowe, “Distinctive Image Features from Scale-Invariant Keypoints,” International Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.

[9] J. Yang, K. Yu, Y. Gong, and T. Huang, “Linear Spatial Pyramid Matching Using Sparse Coding for Image Classification,” in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1794-1801, 2009.

[10] J. C. v. Gemert, C. J. Veenman, A. W. M. Smeulders, and J. M. Geusebroek, “Visual Word Ambiguity,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 7, pp. 1271-1283, 2010.

[11] J. Wu and J. M. Rehg, “Place Instance and Category Recognition Using Spatial PACT,” in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2008.

[12] J. Hu and P. Guo, "Multi-Level Kernel Machine for Scene Image Classification," in Proceedings of 2011 International Conference on Computational Intelligence and Security, pp. 1169-1173, 2011.

[13] R. Zabih and J. Woodfill, “Non-Parametric Local Transforms for Computing Visual Correspondence,” in Proceedings of European Conference on Computer Vision (ECCV), pp. 151-158, 1994.

[14] B. Fröba and Andreas Ernst, “Face Detection with The Modified Census Transform,” in Proceedings of the Sixth IEEE international conference on Automatic face and gesture recognition (FGC), 2004.

[15] H. Jin, Q. Liu, H. Lu, and X. Tong, “Face Detection Using Improved LBP Under Bayesian Framework,” in Proceedings of the International Conference on Image and Graphics (ICIG), pp. 306-309, 2004.

[16] L.-J. Li and L. Fei-Fei. “What, Where and Who? Classifying Events By Scene and Object Recognition,” in Proceedings of IEEE International Conference on Computer Vision (ICCV), 2007.

[17] C.-C. Chang and C.-J. Lin, "LIBSVM: A Library for Support Vector Machines," 2001, Software available at http: //www. csie. ntu. edu. tw/~cjlin/libsvm.

[18] T. Ojala, M. Pietikäinen, and T. Mäenpää, "Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 7, pp. 971-987, 2002

[19] S. Gao, I. Tsang, L. Chia, and P. Zhao, “Local Features Are Not Lonely – Laplacian Sparse Coding for Image Classification,” in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 3555-3561, 2010.

[20] O. Boiman, E. Shechtman, and Michal Irani, “In Defense of Nearest-Neighbor Based Image Classification,” in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1-8, 2010.

[21] Z. Wang, Y. Hu, and L. Chia, "Image-to-Class Distance Metric Learning for Image Classification," in Proceedings of European Conference on Computer Vision, 2010.

[22] R. Behmo, P. Marcombes, A. Dalalyan, and V. Prinet, "Towards Optimal Naive Bayes Nearest Neighbor", in Proceedings of European Conference on Computer Vision, 2010.

[23] T. Tuytelaars, M. Fritz, K. Saenko, and T. Darrell, "The NBNN Kernel," in Proceedings of IEEE International Conference on Computer Vision (ICCV), 2011

[24] Y. Jia C. Huang, and T. Darrell, "Beyond Spatial Pyramids: Receptive Field Learning for Pooled Image Features," in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2012.

[25] A. Bosch, A. Zisserman, and X. Muoz, “Scene Classification Using A Hybrid Generative/Discriminative Approach,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 30, no. 4, pp. 712–727, 2008.

[26] J. J. Kivinen, E. B. Sudderth, and M. I. Jordan, “Learning Multiscale Representaiton of Natural Scenes Using Dirichlet Processes,” in Proceedings of IEEE Conference on Computer Vision (ICCV), 2007.

[27] M. Song and P. Guo, "Scene Recognition via Combing Information of Neighbors," in Proceedings of International Conference on Computational Intelligence and Security (CIS), pp. 345-349, 2012.

[28] J. Hu, L. Wang, F. Duan, and P. Guo, “Adaptive Multi-level Kernel Machine for Scene Classification,” Mathematical Problems in Engineering, Volume 2013, Article ID, 324945.

[29] S. Paris, X. Halkias, H. Glotin, "Sparse Coding for Histograms of Local Binary Patterns Applied for Image Categorization: Toward A Bag-of-Scenes Analysis," in Proceedings of International Conference on Pattern Recognition (ICPR), pp. 1-4, 2012.

[30] S. Paris, X. Halkias, H. Glotin, "Efficient Bag of Scenes Analysis for Image Categorization," in Proceedings of International Conference on Pattern Recognition Applications and Methods (ICPRAM) pp. 10, 2013.

[31] R. M. N. Sadat, S. W. Teng, G. Lu and S. F. Hasan, "Texture Classification Using Multimodal Invariant Local Binary Pattern," in Workshop on the Applications of Computer Vision (WACV), 2011.

[32] B. Jun, D. Kim, “Robust Face Detection Using Local Gradient Patterns and Evidence Accumulation,” Pattern Recognition, vol.45, no.9, pp. 3304-3316, 2012.

Balanced Growth Solutions and Related Problems of Hua's Macroeconomic Model

Jing Zhang
DongGuan Polytechnic College/ Department of Continuous Education, DongGuan, China
Email: jingzhang0769@163.com

***Abstract*—In this paper, the balanced growth solution and relative stability of solution on Hua's macroeconomic model is studied. Firstly, by deriving the greatest eigenvalue and nonnegative eigenvector, and analyzing the range of the eigenvalue of nonnegative matrix, the existence of the balanced growth solution on a sort of Hua's macroeconomic model is proved, no matter whether direct consumption coefficient matrix is irreducible or reducible. Furthermore, the concept of balanced solution's relative stability is introduced to Hua's macroeconomic model and the necessary and sufficient condition for the existence of these solutions is obtained. Finally, based on the price equation proposed by Prof. Hua, the dynamic price system which is inclusive of the interest rate is proposed and the relationship between price and output on the basis of the relative stability of price system is illuminated.**

***Index Terms*—Hua's macroeconomic model, balanced growth solution, relative stability, price system**

I. Introduction

In the 1980s,Prof. Luogeng Hua established the well-known theory which called "mathematical theory of large-scale optimization in planned economy" in several papers. In these papers, he proposed the so-called Hua's macroeconomic model. Under the condition of enough large productivity elasticity, the model depicts the relationship between input and output. Compared with Leontief's macroeconomic model, Hua's model fits better in the current Chinese economy. Hence the model can be used to analyze and forecast effectively in China

Due to the causal indeterminacy, it is difficult to apply Hua's macroeconomic model into practice. Therefore it is necessary to study the model's output feature. Prof. Hua also introduced the balanced solution which is based on the nonnegative irreducible square matrix [1]. Recently, many researchers put forward to generalize Hua's macroeconomic model involving consumption and investment and gave the balanced solutions of these generalized models [8-11]. Furthermore, the positive eigenvector method was researched [13, 14]. Since all the generalized models can be simplified to Hua's macroeconomic model, so it is important to study the balanced growth solution on Hua's macroeconomic model.

II. Preliminaries

According to the input-output analysis method, national economy is divided into n production sectors. Let $A=(a_{ij})_{n\times n}$ stands for the direct consumption coefficient matrix. Here a_{ij} is the product quantity of sector i which sector j needs when sector j produces one unit product. obviously, $A=(a_{ij})_{n\times n}\geq 0$, that is $a_{ij}>0$ for some i, j. $X^{(t)}$ is an n-dimensional column vector, which stands for the output in period t. Then Hua's macroeconomic model is

$$X^{(t)}=AX^{(t+1)}, t\in T=\{0,1,2,\cdots\} \qquad (1)$$

Let A be an invertible matrix, then Hua's macroeconomic model can be defined as follow

$$X^{(t+1)}=A^{-1}X^{(t)}, t\in T=\{0,1,2,\cdots\} \qquad (2)$$

The balanced solution of the model is $X^{*(t)}=(1/\lambda_*{}^t)X_*$. Here, A is a nonnegative irreducible matrix, λ_* is the largest eigenvalue of A and X_* is the nonnegative eigenvector of λ_*.

Price equation is

$$(q_1 \quad \cdots \quad q_n)\lambda_*=(q_1 \quad \cdots \quad q_n)A \qquad (3)$$

Where, $q_i(i=1,2,\cdots,n)$ stand for the price of per unit product of sector i, λ_* is the price change rate which is also the largest eigenvalue of A.

Lemma 1 [2]. If A is a nonnegative irreducible square matrix, for any positive vector $X^{(0)}$ which is not an eigenvector of A, then there is a positive integer $l_0>0$, when a positive integer $l\geq l_0$, $X^{(l)}=A^{-l}X^{(0)}$ must be a variable vector, that is some entries of $X^{(l)}$ are positive, others are negative.

doi:10.4304/jsw.9.1.211-215

Lemma 1 shows that if initial input isn't a positive eigenvector of A, then some sectors' output will be negative in several years. In consequence, the economic system will collapse.

III. Balanced growth solution on Hua's Macroeconomic Model

Definition 1. On Hua's macroeconomic model, if there is $X^{(t)} = \alpha X^{(t-1)}$, then $X^{(t)}$ is called balanced solution. Here, $\forall t \in N$, $\alpha > 0$ is a constant and called growth coefficient.

By lemma 1, we know the balanced solution is the right positive eigenvector of A. Economic growth rate is $1/\lambda_*$, when the direct consumption coefficient matrix A is a nonnegative irreducible square matrix. However, the range of $1/\lambda_*$ was not given, which is an important index to show if the economic system will healthily develop. According to the definition 1, when $1/\lambda_* > 1$, economic gross increases and when $0 < 1/\lambda_* < 1$, economic gross decreases. If A is a reducible matrix, it is also possible that a balanced solution on the model may exist. For the two problems mentioned above, we are trying to get the balanced growth solution on a sort of Hua's macroeconomic model. So we suppose $I - A$ is a diagonal strictly dominant matrix.

Definition 2 [15]. If the relative structure of initial input does not meet any balanced solutions in an economic system, then for any solutions of the input-output economic model, it is possible at least one section's product output is negative. If it happens, the model has causal indeterminacy.

According to lemma 1, we know there is causal indeterminacy on Hua's macroeconomic model.

Lemma 2 ([16] Perron-Frobenius theorem on general nonnegative matrix). Let A be a $n \times n$ matrix with nonnegative real entries. Then,

(ⅰ) A has a nonnegative real eigenvalue $\lambda \geq 0$, which dominates the absolute values of all other eigenvalues λ_i of A, that is $\lambda \geq |\lambda_i|$.

(ⅱ)Exist a positive eigenvector $X \geq 0$ of λ. Here, $X \geq 0$ means that $\forall i, x_i \geq 0$ and $\exists j, x_j > 0$.

Lemma 3 [16]. Let A be a $n \times n$ matrix with nonnegative real entries, A has a nonnegative real eigenvalue $\lambda \geq 0$, which dominates the absolute values of other eigenvalues λ_i of A, that is $\lambda \geq |\lambda_i|$, then for any positive vector $x = (x_1, \cdots, x_n)^T > 0$, we have

$$\min_{1 \leq i \leq n} \left(\frac{1}{x_i} \sum_{j=1}^{n} a_{ij} x_j \right) \leq \lambda \leq \max_{1 \leq i \leq n} \left(\frac{1}{x_i} \sum_{j=1}^{n} a_{ij} x_j \right).$$

Theorem 1. Let A be a direct consumption coefficient matrix. Suppose $I - A$ is a diagonal strictly dominant matrix. Then there is a positive real $\hat{\lambda}$, $0 < \hat{\lambda} < 1$ and a positive vector $\hat{X} \geq 0$, which satisfy $A\hat{X} = \hat{\lambda}\hat{X}$.

Proof: For Hua's macroeconomic model $X^{(t)} = AX^{(t+1)}$, since $A \geq 0$, we know existing $\hat{\lambda} \geq 0$ and $\hat{X} \geq 0$, which satisfy $A\hat{X} = \hat{\lambda}\hat{X}$ by lemma 2. Since $I - A$ is a diagonal strictly dominant matrix, then $1 - a_{ii} > \sum_{j \neq i} a_{ij}$.

By Gerschgorin theorem, all the eigenvalues of A belong to the set

$$\bigcup_i \Omega_i = \left\{ \lambda \middle| \ |\lambda - a_{ii}| \leq \sum_{j \neq i} a_{ij} \right\}.$$

Since $1 - a_{ii} > \sum_{j \neq i} a_{ij}$, so $|\lambda - a_{ii}| \leq \sum_{j \neq i} a_{ij} \leq 1 - a_{ii} \Rightarrow$ $2a_{ii} - 1 < \lambda < 1$. Hence $\hat{\lambda} < 1$. According to lemma 3, let $x = (x_1, \cdots, x_n)^T = (1, \cdots, 1)^T$, then

$$\min_{1 \leq i \leq n} \left(\sum_{j=1}^{n} a_{ij} \right) \leq \hat{\lambda} \leq \max_{1 \leq i \leq n} \left(\sum_{j=1}^{n} a_{ij} \right).$$

Because A is a nonnegative matrix, therefore there exists $\sum_{j=1}^{n} a_{ij} \geq 0$. According to the economic means of A, it is impossible that one sector does not offer its product to others to produce, so $\sum_{j=1}^{n} a_{ij} > 0$, hence $0 < \hat{\lambda}$. Whence we obtain $0 < \hat{\lambda} < 1$ and $\hat{X} \geq 0$, which satisfy $A\hat{X} = \hat{\lambda}\hat{X}$.

For Hua's macroeconomic model

$$X^{(0)} = AX^{(1)}. \tag{4}$$

Suppose there is a balanced solution in the economic system, the growth rate is $1/\lambda$, that is

$$X^{(1)} = \frac{1}{\lambda} X^{(0)} \tag{5}$$

From (5) and (4), we obtain

$$\lambda X^{(0)} = AX^{(0)} \tag{6}$$

By inductive method, we obtain $X^{(t)} = (1/\lambda)^t X^{(0)}$. Let $X^{(0)}$ be $\hat{X}$, then the growth rate is $1/\hat{\lambda}$. Whence we have $X^{(t)} = (1/\hat{\lambda})^t \hat{X}$, that is if initial input is $\hat{X}$, the economic system could have a balanced solution. Since $0 < \hat{\lambda} < 1$, hence the balanced solution also is a balanced growth solution. By the analysis above, we obtain the following theorem.

Theorem 2. Let A be a direct consumption coefficient matrix, and satisfy $1 - a_{ii} > \sum_{j \neq i} a_{ij}$, then $X^{(t)} = (1/\hat{\lambda})^t \hat{X}$

is a balanced growth solution on Hua's macroeconomic model, the growth rate is $1/\hat{\lambda}$, here $0<\hat{\lambda}<1$ is the eigenvalue of A, $\hat{X}\geq 0$ is the eigenvector of $\hat{\lambda}$.

There is no restriction that the consumption coefficient matrix is irreducible and the balanced growth solution on a sort of Hua's macroeconomic model have been proposed in the theorem 2. It is illuminate when all sectors consume their own product less, it is impossible that the total amount of products that one sector consumes will be more than the total amount of products that it produces, which would result in a negative output in an economic system. Therefore this kind of model has no causal indeterminacy.

IV. Relative Stability of Balanced Solution

Definition 3. $A\geq 0$ is a direct consumption coefficient matrix and is invertible. For Hua's macroeconomic model, suppose $X^{*(t)}=(1/\lambda^t)X$ is a balanced solution, $\hat{X}^{(t)}$ is a general solution which is determined by any initial input $\hat{X}^{(0)}\geq 0$. If $\lim_{t\to\infty}(\hat{X}_i^{(t)}/X_i^{*(t)})=\sigma$, here, $\hat{X}_i^{(t)}$, $X_i^{*(t)}$ respectively stand for the i^{th} entry of $\hat{X}^{(t)}$, $X^{*(t)}$, $0<\sigma<\infty$ and there is no relation between σ and i, then the balanced solution is relatively stable.

Fig.1 shows the concept of relative stability in the two-dimensional situation. It means that $\hat{X}^{(t)}$ asymptotic approximation to a balanced solution $X^{*(t)}$ when $\lim_{t\to\infty}(\hat{X}_i^{(t)}/X_i^{*(t)})=\sigma\ i\in\{1,2\cdots\}$. Since $\hat{X}^{(t)}>0$, exist T, when $t>T$, we have $\hat{X}^{(t)}>0$. So when there is a relatively stable balanced solution on an economic model, the model's solution which is determined by any initial input is always greater than zero, so that there is no causal indeterminacy in the economic system.

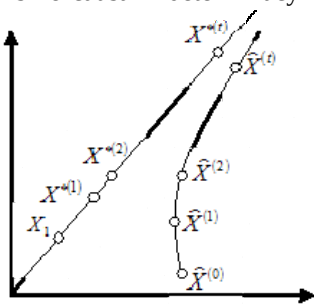


Figure 1. Diagram of two-dimensional relative stability.

Theorem 3. $A\geq 0$ is a direct consumption coefficient matrix, and is invertible, then exist a positive integer t, which satisfy $(A^{-1})^t>0$ if and only if $|\lambda_i|>\lambda_1>0$, $X_1>0$, here $\lambda_1,\lambda_i(i=2,3,\cdots,n)$ are the eigenvalue of A, X_1 is the eigenvector of λ_1.

Proof: ($\Rightarrow$) If the eigenvalue of A is λ_j, then the eigenvalue of A^{-1} is $1/\lambda_j$, and the eigenvalue of A^{-t} is $1/\lambda_j^t$. When there is a positive integer t, which satisfies $(A^{-1})^t>0$, then $(A^{-1})^t$ is irreducible matrix. According to Frobenius' theorem [16], there exists an eigenvalue $\mu_1>0$ and an eigenvector $Y_1>0$, which satisfies

$$\mu_1>|\mu_i|(i=2,\cdots,n),\ (A^{-1})^tY_1=\mu_1Y_1,$$

Here $\mu_i(i=2,\cdots,n)$ also are eigenvalue of $(A^{-1})^t$. Let λ_i be the eigenvalue of A and X_1 be the eigenvector of λ_1. Due to the relationship between A and $(A^{-1})^t$, we have

$$\mu_i=\frac{1}{\lambda_i^t}(i=1\cdots n),\ Y_1=X_1.$$

Then $(1/\lambda_1^t)>(1/|\lambda_i^t|)\ (i=2,\cdots n)$, therefore we obtain

$$|\lambda_i|>\lambda_1>0(i=2,\cdots n),\ X_1>0.$$

($\Leftarrow$) The general solution of difference equation (2) can be written as

$$\hat{X}^{(t)}=h_1\frac{1}{\lambda_1^{\ t}}X_1+h_2\frac{1}{\lambda_2^{\ t}}X_2+\cdots+h_n\frac{1}{\lambda_n^{\ t}}X_n \quad (7)$$

Here $\lambda_1,\cdots,\lambda_n$ are the eigenvalue of A, $X_1,\cdots,X_n$ are the eigenvector, $h_1,\cdots,h_n$ are determined by initial input vector.

Let e^i be an n-dimensional vector, its the i^{th} entry is 1, others are 0. Now let e^i be the initial input, we obtain

$$\hat{X}^{(0)}=e^i=h_1X_1+h_2X_2+\cdots+h_nX_n$$

$$(X_1\cdot e^i)=(X_1\cdot\hat{X}^{(0)})=\left(X_1\cdot\sum_{i=1}^{n}h_iX_i\right)$$

$$=\sum_{i=1}^{n}h_i(X_1\cdot X_i).$$

Since $AX_1=\lambda_1X_1$, we get $A^{-1}X_1=(1/\lambda_1)X_1$. So

$$\frac{1}{\lambda_1}(X_1\cdot X_i)=\left(\frac{1}{\lambda_i}X_1\cdot X_i\right)=(A^{-1}X_1\cdot X_i)$$

$$=(A^{-1}X_1)^TX_i=X_1^{\ T}(A^T)^{-1}X_i$$

$$=X_1^{\ T}\frac{1}{\lambda_i}X_i=\frac{1}{\lambda_i}X_1^{\ T}X_i$$

$$=\frac{1}{\lambda_i}(X_1\cdot X_i)$$

When $i\neq 1$, $\lambda_1\neq\lambda_i$, $(X_1\cdot X_i)=0$. Therefore $(X_1\cdot e^i)=h_1(X_1\cdot X_1)$, that is $h_1=X_1e^i/(X_1\cdot X_1)$. Since $(X_1\cdot X_1)>0$, $(X_1\cdot X_1)>0$, so $h_1>0$.

Since $|\lambda_i| > \lambda_1$, $(1/\lambda_1^t) > (1/|\lambda_i^t|)$, according to the following equation

$$\hat{X}^{(t)} = \left(A^{-1}\right)^t e^i = h_1 \frac{1}{\lambda_1^{\ t}} X_1 + h_2 \frac{1}{\lambda_2^{\ t}} X_2 + \cdots + h_n \frac{1}{\lambda_n^{\ t}} X_n,$$

we know there is a positive integer t, which satisfy $\left(A^{-1}\right)^t e^i > 0$. Because i is randomized, therefore $\left(A^{-1}\right)^t > 0$.

According to definition 3, if $X^{*(t)} = \left(1/\lambda_1^t\right)X_1$ is a relatively stable balanced solution, the general solution $\hat{X}^{(t)}$ which is determined by any initial input vector $\hat{X}^{(0)} \geq 0$ satisfies

$$\lim_{t\to\infty} \frac{\hat{X}_i^{(t)}}{X_i^{*(t)}} = \lim_{t\to\infty} \frac{h_1 \frac{1}{\lambda_1^{\ t}} X_{1i} + h_2 \frac{1}{\lambda_2^{\ t}} X_{2i} + \cdots + h_n \frac{1}{\lambda_n^{\ t}} X_{ni}}{\frac{1}{\lambda_1^{\ t}} X_{1i}}$$

$$= \lim_{t\to\infty} \left(h_1 + h_2 \frac{\lambda_1^{\ t}}{\lambda_2^{\ t}} \frac{X_{2i}}{X_{1i}} + \cdots + h_n \frac{\lambda_1^{\ t}}{\lambda_n^{\ t}} \frac{X_{ni}}{X_{1i}}\right) = \sigma$$

Since there isn't relation between σ and i, and $\sigma > 0$, we have $|\lambda_i| > \lambda_1 > 0$, that is the balanced solution is relatively stable if and only if $|\lambda_i| > \lambda_1 > 0$. We get the following theorem by the analyzing above.

Theorem 4. Suppose $A \geq 0$ is a direct consumption coefficient matrix and is invertible, then the balanced solution $X^{*(t)} = 1/\left(\lambda_1^t\right)X_1$ is relatively stable if and only if $|\lambda_i| > \lambda_1 > 0$, here λ_1, λ_i ($i = 2 \cdots n$) are the eigenvalue of A, X_1 is the eigenvector of λ_1.

Corollary. Suppose $A \geq 0$ is a direct consumption coefficient matrix and is invertible, then exist a positive integer t, which satisfy $\left(A^{-1}\right)^t > 0$ if and only if balanced solution $X^{*(t)} = \left(1/\lambda_1^t\right)X_1$ is a relatively stable solution.

By the theorem 4, we know , for Hua's macroeconomic model , the balanced solution $X^{*(t)} = (1/\lambda_1^t)X_1$ is relatively stable $\Leftrightarrow$ the eigenvalue and the eigenvector of A satisfy $|\lambda_i| > \lambda_1 > 0$ and $X_1 > 0$ $\Leftrightarrow$ exist a positive integer t, which satisfies $A^{-t} > 0$ $\Leftrightarrow$ there isn't the causal indeterminacy on Hua's macroeconomic model $\Leftrightarrow$ all sectors' output is not negative in several years.

V. Dynamic Price System

The price equation (3) doesn't include interest rate and was proposed under the presumption that products price changes proportionally in each period, that is $P^{(t+1)} = \lambda_* P^{(t)}$. Since interest rate has a direct impact on the product's sales and price, so it can't be disregarded. The product's price may not change proportionally. thus we suppose the price of i sector's per unit product is $P_i^{(t)}$ in t period, then $P^{(t)} = \left(P_1^{(t)} \ \cdots \ P_n^{(t)}\right)$ is the price vector in t period, and the price vector is a constant vector during each period, any product prices will not be affected by human factors, and the costs of raw material will be paid at the beginning of each period. The costs that j sector produce per unit j product in t period is

$$v_j^{(t)} = \sum_{i=1}^{n} P_j^{(t)} a_{ij} = P^{(t)}\ a_j \tag{8}$$

Here, a_j is the j^{th} column of the direct consumption coefficient matrix A, a_{ij} is the i^{th} entry of a_j. Then the net profit that j sector produce per unit j product in t period is

$$\pi_j^{(t)} = P_j^{(t+1)} - P^{(t)} a_j \tag{9}$$

Now there is an individual, who has an amount of money $v_j^{(t)}$ at the beginning of t period, we suppose this money can be lent out at an interest rate $r^{(t)}$, and then the interest who will get at the beginning of $t+1$ period is

$$R_j^{(t)} = r^{(t)} v_j^{(t)} = r^{(t)} P^{(t)} a_j \tag{10}$$

According to the competition arbitrage principle, the interest and the profit are the same in equilibrium, so we have

$$\pi_j^{(t)} = R_j^{(t)}$$

$$P_j^{(t+1)} - P^{(t)} a_j = r^{(t)} P^{(t)} a_j$$

$$P_j^{(t+1)} = (1 + r^{(t)}) P^{(t)} a_j \tag{11}$$

Obviously, for all $j = 1, \cdots, n$, (8) is right. Hence we obtain

$$P^{(t+1)} = (1 + r^{(t)}) P^{(t)} A \tag{12}$$

Let $(1 + r^{(t)})A = M$, (12) can be written as

$$P^{(t+1)} = P^{(t)} M \tag{13}$$

(13) is called dynamic price equation on Hua's macroeconomic model.

When the interest rate $r^{(t)}$ is 0, and the price changes proportionally in every period, (13) and (3) are the same. When the interest rate $r^{(t)}$ and the price vector $P^{(t)}$ are known in t period, we can get the price vector $P^{(t+1)}$ by (13), therefore (13) can also be called expected price equation.

VI. Relative Stability of Price System

In order to simplify, we suppose the interest rate r is a constant when we study the relative stability of the price system, thus $M = (1 + r)A$. The general solution of difference equation (13) can be written as

$$\widehat{P}^{(t)} = \alpha_1\zeta_1^t p_1 + \alpha_2\zeta_2^t p_2 + \cdots + \alpha_n\zeta_n^t p_n \qquad (14)$$

Here, $\zeta_1, \zeta_2, \cdots, \zeta_n$ are eigenvalue of M, $p_1, p_2, \cdots p_n$ are eigenvector of M, that is $p_i M = \zeta_i p_i$. $\alpha_1, \alpha_2, \cdots, \alpha_n$ are determined by initial price vector. Since $(1+r)A = M$, whence by the output balanced solution $X^{*(t)} = (1/\lambda_1^t)X_1$, we can get price balanced solution, that is

$$P^{*(t)} = \zeta_1^t p_1 \qquad (15)$$

Here, $\zeta_1 = (1+r)\lambda_1$.

Definition 4. For the dynamic price equation on Hua's macroeconomic model, suppose $P^{*(t)} = \zeta_1^t p_1$ is a balanced solution, $\widehat{P}^{(t)}$ is the price vector which is determined by any initial price vectors $\widehat{P}^{(0)} \geq 0$ by (13). If $\lim_{t\to\infty}\left(\widehat{P}_i^{(t)} / P_i^{*(t)}\right) = \sigma$, here $\widehat{P}_i^{(t)}$, $P_i^{*(t)}$ stand for the i^{th} entry of $\widehat{P}^{(t)}$, $P^{*(t)}$ respectively, $0 < \sigma < \infty$ and there is no relation between σ and i, then the price balanced solution is a relatively stable balanced solution.

Definition 4 illuminates when there is a relatively stable price balanced solution $P^{*(t)}$, the price vector $\widehat{P}^{(t)}$ which is determined by any initial price vectors $\widehat{P}^{(0)} \geq 0$ asymptotic approximation to the price balanced solution which is fit for the economic growth. According to definition 4, if $P^{*(t)} = \zeta_1^t p_1$ is relatively stable, then $\widehat{P}^{(t)}$ satisfies

$$\begin{aligned}
&\lim_{t\to\infty}\frac{\widehat{P}_i^{(t)}}{P_i^{*(t)}} \\
&= \lim_{t\to\infty}\left(\alpha_1 + \alpha_2\left(\frac{\zeta_2}{\zeta_1}\right)^t \frac{p_{2i}}{p_{1i}} + \cdots + \alpha_n\left(\frac{\zeta_n}{\zeta_1}\right)^t \frac{p_{ni}}{p_{1i}}\right) \\
&= \sigma
\end{aligned}$$

Because there is no relation between σ and i, and $\sigma > 0$, so $\zeta_1 > |\zeta_i|$, that is the price balanced solution is relatively stable if and only if $\zeta_1 > |\zeta_i|$. Hence we get the following theorem.

Theorem 5. Suppose $A \geq 0$ is a direct consumption coefficient matrix, r stands for the interest rate, let $M = (1+r)A$, then the price balanced solution $P^{*(t)} = \zeta_1^t p_1$ is relatively stable if and only if $\zeta_1 > |\zeta_i|$, here $\zeta_1, \zeta_2, \cdots, \zeta_n$ are n different eigenvalue of M, p_1 is the eigenvector of ζ_1.

According to $(1+r)A = M$, we know $\zeta_i = (1+r)\lambda_i$, when the price balanced solution is relatively stable, that is $\zeta_1 > |\zeta_i|$, we obtain $\lambda_1 > |\lambda_i|$, and then the output balanced solution is not relatively stable. On the contrary, when the output balanced solution is relatively stable, that is $|\lambda_i| > \lambda_1$, we obtain $|\zeta_i| > \zeta_1$, and then the price balanced solution isn't relatively stable.

REFERENCES

[1] Luogeng Hua, "Mathematical Theory of Large-scale Optimization in Planned Economy (I)", *Chinese Science Bulletin, China*, vol. 29, pp. 6–11, 1984(12).

[2] Luogeng Hua, "Mathematical Theory of Large-scale Optimization in Planned Economy (II-III)", *Chinese Science Bulletin,China*, vol. 29, pp. 769–772, 1984(13).

[3] Luogeng Hua, "Mathematical Theory of Large-scale Optimization in Planned Economy (IV-VI)", *Chinese Science Bulletin,China*, vol. 29, pp. 961–965, 1984(16).

[4] Luogeng Hua, "Mathematical Theory of Large-scale Optimization in Planned Economy (VII)", *Chinese Science Bulletin,China*, vol. 29, pp. 1089 –1092, 1984(18).

[5] Luogeng Hua, "Mathematical Theory of Large-scale Optimization in Planned Economy (VIII)", *Chinese Science Bulletin, China*, vol. 29, pp. 1281–1282, 1984(21).

[6] Luogeng Hua, "Mathematical Theory of Large-scale Optimization in Planned Economy (IX)", *Chinese Science Bulletin, China*, vol. 30, pp. 1–2,1985(1).

[7] Luogeng Hua, "Mathematical Theory of Large-scale Optimization in Planned Economy (X)", *Chinese Science Bulletin, China*, vol. 30, pp. 641–645, 1985(9).

[8] Fasheng Hu, "The Balanced Growth of a Sort of Macroeconomic Model", *Journal of Shandong University, China* , vol. 39, pp. 15–17, 2004(1).

[9] Xiaolan Chen, "The Dynamic Model Based on Investment Structure Optimization and Economy Equilibrium Growth Research", *Systems Engineering, China*, vol.21, pp.58–61, 2003(5).

[10] Daju Xu, Jiazhuang Liu, and Fangjun Dou, "Hua's Macroeconomic Models with Consumption or Investment", *Mathematics in Economics, China*, vol.20, pp.27–32, 2003(2).

[11] Daju Xu, Jiazhuang Liu, and Shulan Kong, "A Generalization of Hua's Macroeconomics Model", *Chinese Journal Management Science, China*, vol.11, pp.16–19, 2003(5).

[12] Daju Xu, "The Solution of Dynamic Input-output Model", *Chinese Journal Management Science, China*, vol.10, pp.134–136, 2002.

[13] Fasheng Hu and Jufang Zhang, "The Positive Character Vector Method to a Sort of Macroeconomic Model", *Journal of Shandong University, China*, vol.33, pp.7–11, 1998(1).

[14] Weidong Rong, Dali Yang, Liqun Dai, and Shulin Liu, "Macroeconomic Analytical New Method-Positive Character Vector Method", *Chinese Journal Management Science, China*, vol.1, pp.42–47, 1993.

[15] RM Solow and PA Samuelson, "Balanced Growth under Constant Returns to Scale", Econo-metrica. vol.21, pp.412–424, 1953.

[16] Gongning Chen, *Matrix Theory and Application. Second Edition, China*, Beijing, Science Press, 2007.

[17] Rongmei Xiang, *Input-Output system*, Southwest University of Finance and Economics Press, China, 2007.

Jing Zhang was born in 1981 in Xi'an, China. She obtained her Master's Degree in North West University in 2007. Her research interest is applied mathematics .

A New Image Denoising Method Based on Wave Atoms and Cycle Spinning

Wei-qiang Zhang
College of Mathematics and computational Science, Shenzhen University, Shenzhen 518060, China.
Email: wqzhang@szu.edu.cn

Yi-mei Song
School of Science, Xidian University, Xi'an 710071, China.
Email: songyimei0405@126.com

Ji-qiang Feng
Institute of Intelligent Computing Science, Shenzhen University, Shenzhen 518060, China.
Email: mathlove@126.com

***Abstract*—A new method for image denoising was presented，which colligated the strong point of wave atoms transform and Cycle Spinning. Due to lack of translation invariance of wave atoms transform，image denoising by coefficient thresholding would lead to Pseudo-Gibbs phenomena. Cycle Spinning was employed to avoid the artifacts. Experimental results show that the method can remove noisy and remain edges, while Pseudo-Gibbs phenomena are controlled efficiently, and can get better visual effect and PSNR gains compared with the methods like simplex wave atoms or wavelet denoising using Cycle Spinning.And in heavy background noise, this advantage is significant.**

***Index Terms*—image processing, denoising, wavelet transforms, wave atoms, translation invariance, Cycle Spinning**

I. INTRODUCTION

Wavelet theory is widely used in signal processing, but the traditional wavelet transformation showed some limitations in the processing of two-dimensional image[1,2]. The image processing method combined partial differential equations and wavelet theory can better retain the image edge information [3, 4]. In the past two years, Demanet and Ying proposed a variant of wavelet packet-wave atoms[5,6]. Wave atoms transformation is a new type of two-dimensional multi-scale transformation, and still meets the parabolic proportional scaling relation and anisotropic characteristics of curve wave. In the wave atoms, the oscillation function or director texture is sparser than that in the wavelet, Gabor atoms or curve wave [6]. Wave atoms applies to any local direction of the mode and can sparsely spread in the anisotropy mode in the axis direction. Compared with the curve wave, wave atoms can not only capture the vibration mode, but can characterize the pattern through the oscillation. Although wave atoms transformation can sparsely show the two-dimensional image, due to its lack of translation invariance, the artificial visual distortion will be introduced at the same time of being applied to image denoising; especially for the part of image edge, the Pseudo-Gibbs phenomenon is particularly obvious. The Cycle Spinning technology [7] proposed by Coifman and Donoho well avoided this visual distortion. Combined with the effective representation of the wave atoms on the oscillation texture, Cycle Spinning technology was introduced to improve the wave atoms hard threshold denoising, and a denoising algorithm based on the wave atoms transformation was proposed by this paper. The experimental results showed that, compared with traditional denoising method, the algorithm better improved the visual effect of image denoising and obtained a higher PSNR gain, especially had a better effect on the images with rich details and texture. In the strong noise level, this advantage was more apparent.

Project supported by National nature Science Foundation of China (No.61070087，61001183, 11101292).
Corresponding author: Ji-qiang Feng, mathlove@126.com.

II. WAVE ATOMS

We write wave atoms as $\phi_\mu(x)$，with subscript $\mu=(j,m,n)=(j,m_1,m_2,n_1,n_2)$， $j,m_1,m_2,n_1,n_2\in Z$，index a point (x_μ,w_μ) in phase space, as

$$x_\mu=2^{-j}n, w_\mu=2^j m\pi\ ,\quad C_1 2^j\le\max_{i=1,2}|m_i|\le C_2 2^j$$

where $C_1,C_2>0$ are two positive constants． x_μ and w_μ are the centers of $\phi_\mu(x)$ in spatial and frequency domain respectively.

Definition 1. The elements of a frame of wave packets $\{\phi_\mu(x)\}$ are called wave atoms when

$$|\phi_\mu(x)|\le C_M 2^j(1+2^j|x-x_\mu|)^{-M} \qquad (1)$$

$$\left|\hat{\phi}_\mu(w)\right|\le C_M 2^{-j}(1+2^{-j}|w-w_\mu|)^{-M} + C_M 2^{-j}(1+2^{-j}|w+w_\mu|)^{-M} \qquad (2)$$

for all $M>0$.

Definition 1 only presents a qualitative description for wave atoms with spatial frequency location restriction. In practice, Demanet uses the strategy of frequency localization given by Villemose to construct wave atoms from tensor products of adequately chosen 1D wave packets.

doi:10.4304/jsw.9.1.216-221

The trick consists in exhibiting adequate symmetric paris of compactly supported bumps in frequency, given by the formula

$$\hat{\psi}_m^0(w) = e^{-iw/2}[e^{i\alpha_m} g(\varepsilon_m(w-\pi(m+\frac{1}{2})))$$
$$+ e^{-i\alpha_m} g(\varepsilon_{m+1}(w+\pi(m+\frac{1}{2})))]$$

where $\varepsilon_m = (-1)^m$ and $\alpha_m = \frac{\pi}{2}(m+\frac{1}{2})$. The function g is an appropriate real-valued, C^∞ bump function, compactly supported on an interval of length 2π, and chosen such that $\sum_m \left|\hat{\psi}_m^0(w)\right|^2 = 1$. Let g supported on $[-7\pi/6, 5\pi/6]$,and such that for $|w| \le \pi/3$, $g(\pi/2-w)^2 + g(\pi/2+w)^2 = 1$ and $g(-2w-\pi/2) = g(\pi/2+w)$. Then the translates $\{\psi_m(x-n)\}$ form an orthonormal basis of $L^2(R)$ .This construction provides a uniform, or Gabor, tiling of the frequency axis. We need to introduce the subscript j to index scale, and write our basis functions as

$$\psi_{m,n}^j(x) = \psi_m^j(x-2^{-j}n) = 2^{j/2}\psi_m^0(2^j x - n)$$

Then the resulting basis of wavelet packets $\psi_{m,n}^j(x)$ form an orthonormal basis of $L^2(R)$. We emphasize here that these constructed basis functions have a good property, namely the uniformly bounded location in both time and frequency, which is the most important difference with wavelet packets from a standard multi-resolution analysis and plays a key role in designing wave atoms. For all $f(x) \in L^2(R)$, the coefficients can be seen as a decimated convolution at scale 2^{-j} ,

$$C_{j,m,n} = \int \psi_m^j(x-2^{-j}n) f(x)dx = \psi_m^j(x-2^{-j}n) * f(x)$$

By Plancherel,

$$C_{j,m,n} = \frac{1}{2\pi}\int e^{i2^{-j}nw}\,\overline{\hat{\psi}_m^j(w)}\,\hat{u}(w)dw$$

In two dimension, let us abbreviate $\mu = (j,m,n)$, where $m = (m_1, m_2)$ and $n = (n_1, n_2)$. H be Hilbert Transform. We define an orthonormal basis

$$\phi_\mu^+(x_1,x_2) = \psi_{m_1}^j(x_1-2^{-j}n_1)\psi_{m_2}^j(x_2-2^{-j}n_2)$$

A dual orthonormal basis can be defined from the "Hilbert-transformed" wavelet packets,

$$\phi_\mu^-(x_1,x_2) = H\psi_{m_1}^j(x_1-2^{-j}n_1)H\psi_{m_2}^j(x_2-2^{-j}n_2)$$

We denote $\phi_\mu^{(1)} = \frac{\phi_\mu^+ + \phi_\mu^-}{2}$ and $\phi_\mu^{(2)} = \frac{\phi_\mu^+ - \phi_\mu^-}{2}$, then $\{\phi_\mu\} = \{\phi_\mu^{(1)}, \phi_\mu^{(2)}\}$ form the wave atoms frame in two dimension, and satisfy

$$\sum_\mu \left|\langle \varphi_\mu^{(1)}, f\rangle\right|^2 + \sum_\mu \left|\langle \varphi_\mu^{(2)}, f\rangle\right|^2 = \|f\|^2$$

The coefficients of two-dimension wave atoms transform can be obtained as follows:

$$WA_\mu(f) = \langle f, \varphi_\mu^{(1)}\rangle + \langle f, \varphi_\mu^{(2)}\rangle$$

Figure 1 and figure 2 show the space-frequency domain forms of one-dimensional wave atoms at increasingly scales.

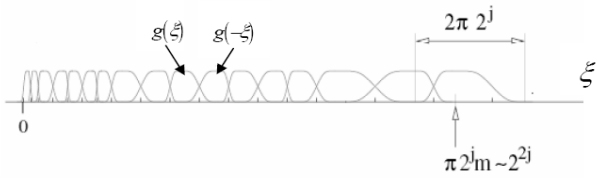
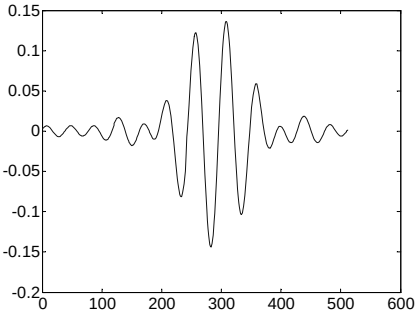
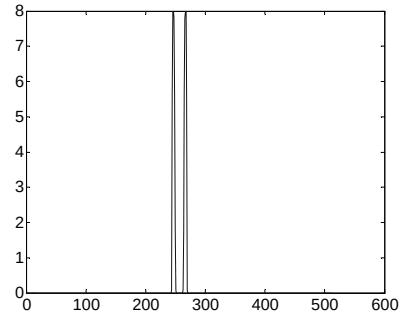
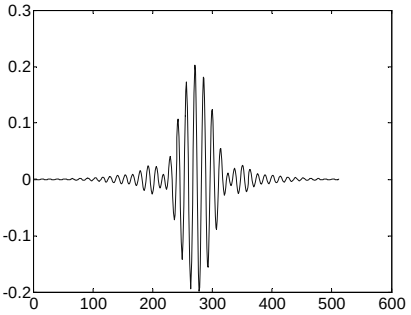


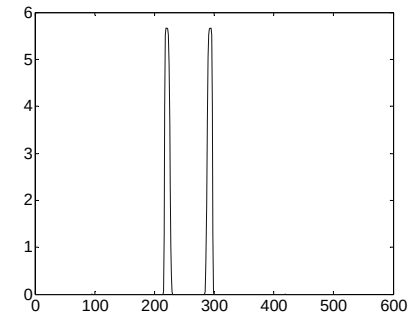
Figure 1. The frequency bands divide of one-dimensional wave atomes.



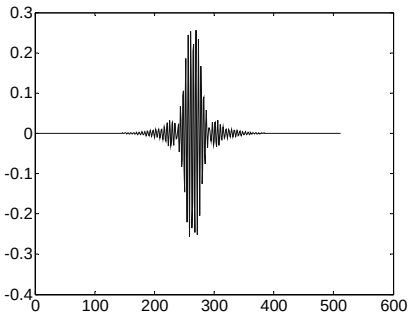


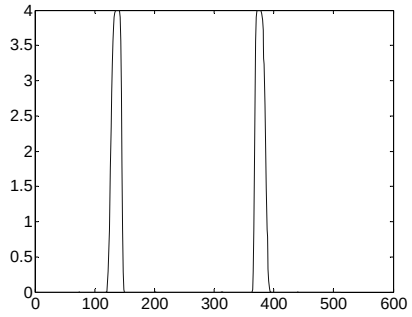
(a) j=3,m=3





(b) j=4,m=5

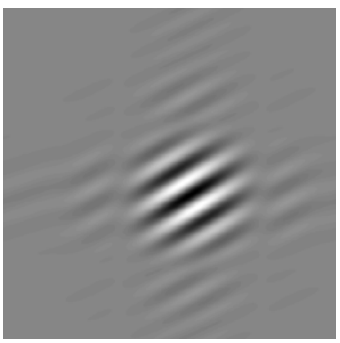




(c) j=5,m=8

Figure 2. One-dimensional wave atoms in space-frequency domain at increasingly scales.

Figure 3 shows two-dimensional wave atoms at increasingly scales. The upper panels represent wave atoms in the spatial domain and the nether panels show wave atoms in the frequency domain.



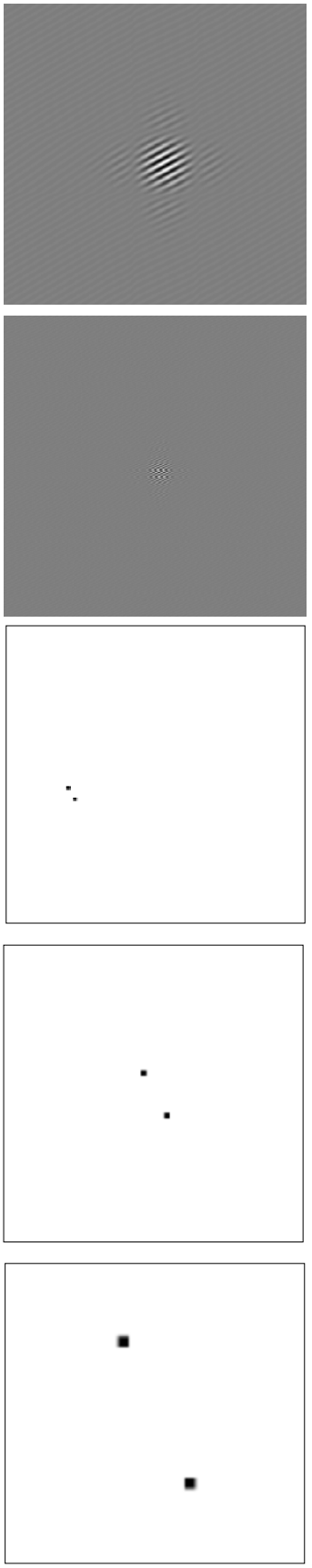


Figure 3. Two-dimensional wave atoms at increasingly scales.

III. Algorithm Description

A. Wave Atoms Hard Threshold Denoising

The basic idea of hard threshold denoising based on wave atoms transformation is consistent with the wavelet based denoising method. Assume the noisy image u can be expressed as $u = u_0 + \eta$, where u_0 is the noise clean image, η is the Gaussian noise of zero mean and variance σ^2; the purpose of image denoising is to recover a clear image from u_0. Soft threshold function because of its continuity makes the edge of the image denoising too vague, and too much detail is lost. However, hard threshold method can better retain the local characteristics of image edge, so this paper uses the method of wave atoms hard threshold denoising.

B. Cycle Spinning

In the threshold denoising process, if the transformation is lack of translation invariance, pseudo-Gibbs phenomenon will be produced in the image discontinuous point neighborhood area (edges and textures), leading to image distortion; this distortion is closely related to the location of image discontinuous points. For example, for Haar wavelet, the pseudo-Gibbs phenomenon will not be produced in the discontinuous point neighborhood area of $n/2$, but obvious pseudo-Gibbs phenomenon will occur in the discontinuous point neighborhood in other location (such as $n/3$). A method to prevent this phenomenon is to change the location of image discontinuous points via image translation, conduct threshold denoising on the translated image and then reversely translated the denoised image to avoid the pseudo-Gibbs phenomenon. If, however, the image to be analyzed contains a plurality of discontinuous points, the optimal translation of a certain discontinuous point may result in pseudo-Gibbs phenomenon in the neighborhood area of another discontinuous point. So it is difficult to find a translation amount that can satisfy the requirements of all discontinuous points. To inhibit the pseudo-Gibbs phenomenon occurred due to the lack of translation invariance in threshold denoising process, Coifman and Donoho proposed Cycle Spinning technology, that is, to carry out "cycle spinning-threshold denoising-reverse cycle spinning". As the threshold denoising on the image after each translation will make the occurrence of pseudo-Gibbs phenomenon in different places; therefore, single translation is not used, but a different denoising result $\hat{s}_{i,j}$ will be obtained from each translation in image rows and columns, and the denoising result $\hat{s}$ inhibiting pseudo-Gibbs phenomenon by linear average on all the denoising results, that is:

$$\hat{s}_{i,j} = S_{-i,-j}(T^{-1}(\Lambda[T(S_{i,j}(x))]),$$

$$\hat{s} = \frac{1}{K_1 K_2}\sum_{i=0}^{K_1}\sum_{j=0}^{K_2}\hat{s}_{i,j}.$$

K_1, K_2 is the maximum translation amount in the row and column direction, S is the cycle spinning operator, the subscript is the translation amount in the i, j row and column directions, T, T^{-1} is the transformation operator and its inverse operator respectively, and Λ is the threshold operator.

C. Cycle Spinning Based Wave Atoms Denoising Algorithm

Although the hard threshold can well preserve the image details, the processed image will have the vision distortions such as ringing, pseudo-Gibbs phenomenon; to inhibit pseudo-Gibbs phenomenon in the process of hard threshold denoising, the wave atoms based image denoising new algorithm is proposed by combining with Cycle Spinning technology; the specific algorithm steps are as follows:

1) Conduct cycle spinning on the noisy image u by the use of cycle spinning operator S, and obtain image $S(u)$;

2) Conduct wave atoms transformation T on the image $S(u)$ after cycle spinning and get the transformation coefficient $TS(u)$;

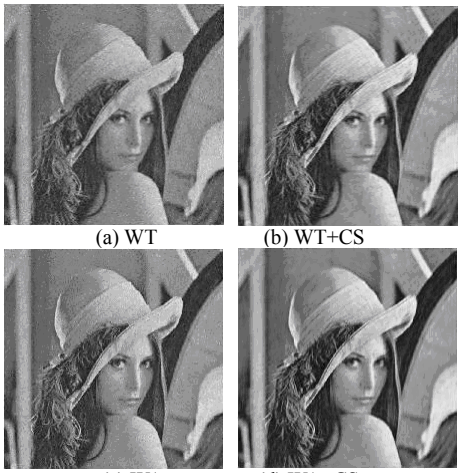
3) Process these coefficients by hard threshold operator Λ_h and obtain the transformation coefficient $\Lambda_h(TS(u))$ after denoising;

4) Carry out inverse wave atoms transformation on the wave atoms coefficient $\Lambda_h(TS(u))$ after hard threshold process and get the denoised image $T^{-1}(\Lambda_h(TS(u)))$;

5) The restored image $\tilde{u} = S^{-1}T^{-1}(\Lambda_h(TS(u)))$ can be obtained by conducting reverse cycle spinning on the denoised image $T^{-1}(\Lambda_h(TS(u)))$, where S^{-1} represents the reverse cycle spinning operator, and the final denoising results can be derived by averaging on all results.

IV. Experimental Results and Analysis

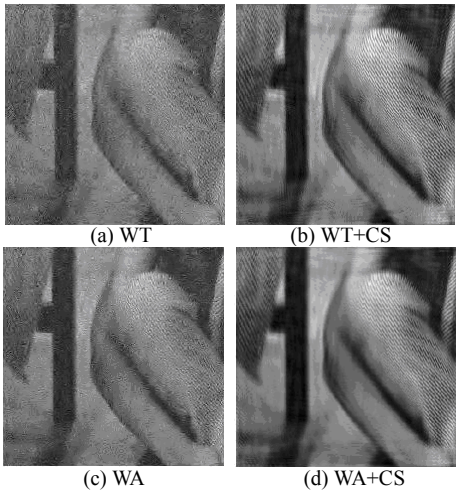
In order to verify the correctness and validity of the proposed algorithm, select some images with the size of about 512×512 and the white Gaussian noise with the mean of zero for experiments, such as the seismic profile with rich texture information, fingerprint image and Lena figure (figure 1) with rich edge details, and Barbara figure (figure 2), etc. Select 8 as the maximum translation amount in the image row and column direction. In the experiment, the comparison of denoising effects has been made of the wavelet hard threshold denoising (WT), cycle spinning wavelet hard threshold denoising (WT+ CS), wave atoms hard threshold denoising (WA) and the proposed method in this paper (WA + CS).



(a) WT (b) WT+CS

(c) WA (d) WA+CS

Figure 4. The comparison of denoising effects of Lena（σ=0.1，PSNR=19.99dB）.



(a) WT (b) WT+CS

(c) WA (d) WA+CS

Figure 5. The comparison of denoising effects of Barbara（σ=0.15，PSNR=16.50dB）.

From the visual effects, wave atoms denoising method can better retain the edge (the brim of Lena figure) and the texture information (hair of Lena figure and the pants stripes of Barbara figure). It indicates wave atoms can well retain the curved edge contour of the image, and is superior to the other two methods in terms of PSNR gain and characterization texture. The texture details in the figures such as the hair and pants stripes, figure (c) and figure (d) are much clearer than figure (a) and figure (b). In the edge area such as the hat brim, the effect of wave atoms method is better than that of the wavelet method. Moreover, the visual effect of the wave atoms denoising by the use of Cycle Spinning is significantly better than the traditional wave atoms denoising, and the peak signal to noise ratio has been improved by more than 1dB. Figure (d) has the highest peak signal to noise ratio of the image by the use of Cycle Spinning wave atoms denoising, which has more effectively inhibited the pseudo-Gibbs phenomenon caused by the lack of translation invariance in the process of threshold denoising, and significantly improved the visual quality of the image. The wave atoms anisotropy and its efficient representation of oscillation texture determine that the wave atoms is superior to traditional wavelet.

TABLE I.
THE COMPARISON ON THE PSNRS OF THE DENOISED IMAGES WITH DIFFERENT NOISE VARIANCES（DB）

Varian-ces	Lena				Barbara			
	WT	WT+CS	WA	WA+CS	WT	WT+CS	WA	WA+CS
0.10	24.75	27.58	28.41	29.53	23.00	25.45	27.24	28.27
0.15	21.81	24.75	26.43	27.57	20.30	22.86	25.36	26.43
0.20	19.58	22.58	24.94	26.17	18.58	21.24	24.03	25.14
0.25	17.84	20.91	23.78	25.04	17.05	19.80	22.86	24.12

To illustrate the algorithm proposed by this paper is significantly better than other methods in the objective performance, comparison has been made on the PSNRs of the denoised images with different noise variances (see Table 1). Whether the traditional wave atoms threshold denoising algorithm or the Cycle Spinning based wave atoms threshold denoising algorithm, the effect is better than the traditional wavelet threshold denoising, and even better than the cycle spinning wavelet denoising. Furthermore, in the strong noise level, this advantage is more obvious. The comparison of the CPU time consumed by the denoising of images with different noise variances has been made, and the results showed the wavelet method consumed less time than the wave atoms method. After the use of Cycle Spinning technology, the speeds of the algorithms are slower and the new algorithm is the most time consuming. This is due to the complexity of the wave atoms transformation computing; the repeated translation invariance will also increase the workload, so the cost of the new algorithm computing is great.

V. CONCLUSIONS

Wave atoms are an emerging new direction multi-scale transformation used for image processing and numerical analysis, with the oscillation cycle and support size satisfying the parabolic scaling relation. Its notable feature is the multi-scale and anisotropy, which can sparsely spread the smooth oscillation function (such as texture). In the processing of traditional image, pseudo-Gibbs phenomenon often arises from the lack of translation invariance and thus leading to image distortion, Cycle Spinning is an effective way to eliminate this distortion. On the basis of literature [6], this paper proposed an image denoising algorithm on the basis of wave atoms and Cycle Spinning. At the same time of effective removal of the image noise, this algorithm better retained the image edge and texture, and could effectively inhibit the pseudo-Gibbs phenomenon, making the denoised image look more realistic and natural, with better visual effects. The texture sharpness and contrast of the processed image were superior to the traditional wavelet threshold, cycle spinning wavelet threshold and wave atoms threshold methods. For images with rich texture information, particularly the texture

images, it has ideal denoising effect, and this advantage is more obvious in the context of strong noise. Due to the costly new algorithm computing, the fast algorithm of the given wave atoms transformation and the improvement of the computing speed of cycle spinning method will be the focus of research in the future.

REFERENCES

[1]. E.J. Candès, L. Demanet, "The curvelet representation of wave propagators is optimally sparse", Comm. Pure Appl. Math., Vol.58, No.11, pp. 1472–1528, 2005.

[2]. E.J. Candès, D.L. Donoho, "New tight frames of curvelets and optimal representations of objects with piecewise-C2 singularities", Comm. Pure Appl. Math., Vol.57, No.2, pp. 219–266, 2004.

[3]. Chen Lixia,Ding Xuanhao,Song Guoxiang, "Image Denoising algorithm based on total variation and wavelet transform", Journal of xidian university, Vol.35, No.6, pp. 1075-1079, 2008.

[4]. Lu Chengwu, "Multiscale Decomposition of Image Under (BV,E) Frame", Journal of xidian university, Vol.36, No.1, pp. 171-176, 2009.

[5]. L. Demanet, "Curvelets, wave atoms and wave equations", California: California Institute of Technology, 2006.

[6]. Demanet L, Ying L X, "Wave Atoms and Sparsity of Oscillatory Patterns", Appl.Comput. Harmon. Anal., Vol.23, No.3, pp. 368-387, 2007.

[7]. Coifman R R, Donoho D L, "Translation-invariant denoising", Lecture Notes in Statistics: Wavelets and Statistics, New York: Springer-verlag, pp. 125-150, 1995.

[8]. J.P. Antoine, R. Murenzi, "Two-dimensional directional wavelets and the scale-angle representation", Signal Processing, Vol.52, No.3, pp. 259–281,1996.

[9]. Guojun Liu, "Perona-Malik Model Based On Wave Atoms", Proceedings of the 3rd International Congress on Image and Signal Processing, pp. 1063-1066, 2010.

[10]. Ke Ding, "Wavelets, Curvelets and Wave Atoms for Image Denoising", Proceedings of the 3rd International Congress on Image and Signal Processing, pp. 782-786, 2010.

[11]. Anil A. Patil, Jyoti Singhai, "Image denoising using curvelet transform: an approach for edge preservation," Jounal of Scientific & Industrial Research, vol. 69, pp. 34-38, 2010.

[12]. M.O. Ulfarsson, J.R. Sveinsson, and J.A. Benediktsson, "Speckle Reduction of SAR Images in The Curvelet Domain," Proceeding of the International Geoscience and Remote Sensing (IGARSS), vol. 1, pp. 315-317, Toronto, Canada, 2002.

[13]. G. Plonka, J. Ma."Nonlinear regularized reaction-diffusion filters for denoising of images with textures", IEEE Trans. Image Process., 17, pp. 1283-1294, 2008.

[14]. J. Ma, G. Plonka."Combined curvelet shrinkage and nonlinear anisotropic diffusion", IEEE Trans. Image Process.,16, pp. 2198-2206, 2007.

Wei-qiang Zhang was born in 1977. He received the Ph.D. degree in applied mathematics from the Xidian University, Xi'an, Shanxi in 2006. Currently, he is an associate professor in Shenzhen University. His research interests include intelligent information processing and image processing.

Ji-qiang Feng was born in 1979. He received the Ph.D. degree in signal and information processing from the Shenzhen University, Shenzhen, Guangdong in 2011. Currently, he is an assistant professor in Shenzhen University. His research interests include intelligent information processing and optimization theory.

A Novel Multi-objective Evolutionary Algorithm Solving Portfolio Problem

Yuan Zhou
School of Applied Mathematics, Guangdong University of Technology, Guangzhou, China
Email: konoxx@126.com

Hai-Lin Liu*, Wenqin Chen, Jingqian Li
School of Applied Mathematics, Guangdong University of Technology, Guangzhou, China
Email: hlliu@gdut.edu.cn

Abstract— **With the improvement of complex and uncertain finance environment, the difficulty of portfolio problem is increasing. Whether or not the projects is successfully selected, directly affects the development of the investment companies. This paper firstly talks about the finance conditions in single term investment and then extends the investment from one term to many terms. After that, a multi-project and multi-term portfolio model through considering the remaining funds in different investment terms is proposed. The model is based on a new kind of Mean-Semi-covariance theory, which can describe the uncertainty of return and risk in investment. The portfolio investment is a multi-objective optimization problem with constraints. Multi-objective evolutionary algorithm (MOEA) with greedy repair strategy is used to deal with the infeasible individuals and makes the investment reasonable. Finally, computer simulation shows that the proposed algorithm can be considered as a viable alternative.**

Index Terms— **Multi-objective optimization, multi-project and multi-term portfolio, portfolio model, evolutionary algorithm**

I. Introduction

In the finance environment, portfolio investment actually faces a large number of risky assets. It is an open question how to distribute the limited funds reasonably. Generally speaking, the investment purpose is to get returns' maximum and risks' minimum. In order to quantify the risk, the Mean-Variance portfolio model first was proposed by Markowitz in literature [1]. This theory has become an important tool in coping the financial investment problem and decision-making.

A large number of portfolio models and algorithms have been proposed in literature [2-9]. Konno and Yamazaki proposed the mean-absolute deviation portfolio optimization model in literature [2]. Lin proposed an effective decision, he used genetic algorithm to deal with multi-objective portfolio optimization problem in literature [3]. In literature [4]. Gabriella Dellino used dynamic objectives aggregation method to solve the portfolio optimization problem. Kawakami made use of the genetic algorithm to deal with the dynamic asset portfolio optimization problem in literature [5]. Xu Bin put forward a general investment combination model and gave one solution of this model in his paper [6]. A new mean-variance model was proposed for optimal capital allocation and a fuzzy simulation was provided for solving the proposed optimization problem in literature [7]. Song Yuantao builded a model about staged investment and got the biggest benefit in literature [8]. In literature [9]. Wang Zhongye proposed a investment model based on information entropy and used genetic algorithm to make decision. Hou Linlin considered the investment sequence and introduced the combinatorial risk in his literature [10].

In the investment market, as shown in literature [11], we could find that investors confront more financial constraints than we have ever expected, if the technical resources and other factors are being considered. In fact, investors may have different investment preferences. Some of them prefer to take high risk in order to gain high return, while others incline to avoid high risk. In this case, its not proper if we only furnish one particular portfolio. Usually, investors want to obtain a series of investment portfolios and then they can choose the portfolio by their own preference. However, people must consider the funding constraints in the multi-term. The portfolio investment is a multi-objective optimization problem (MOP) with constraints in real life. In different investment terms, investors may have the remaining funds. It is not appropriate that we do not consider the remaining funds in investment. Thus this paper proposes a multi-project and multi-term portfolio model through considering the possible remaining funds in investment. Generally speaking, investment risk is closely related with the uncertainty. In general, investors would like to consider an investment as available one if the return is higher than they had expected. In other words, an investment will be regarded as so full of hazard if the investment return is lower than the expected return. It is quite common that people use variance to measure the investment risk in the proposed methods. However, the variance may exaggerate the risk in the investment. So, both of variance or absolute deviation is not the best approach to measure the investment risk. To solve this problem, this paper proposes a new method

*Corresponding author.

doi:10.4304/jsw.9.1.222-229

that can estimate the risk in investment more effectively: method of semi-covariance. It can describe the risk of investment and then makes the model more effective than some existing models.

Nowadays some methods are extremely difficult to solve multi-objective optimization problem if there are many constraints. For example, using the mutually-excluding method is complex to compute [12]. Due to the complexity of portfolio, traditional mathematical optimal methods would consume a lot of time and take too much EMS memory. Thus, we need to explore more effective algorithms. In fact, a large number of improved evolutionary algorithms have been given in literature [12-19]. Multi-objective evolutionary algorithm (MOEA) with greedy repair strategy is proposed in this paper. In investment market, the investment return always accompanies with the risk, and start-up investment funds of every project in investment need to be taken into account. The lost is denoted by the weighted sum of risk and start-up investment funds of every project in every term. Not all investment portfolios are feasible individuals. Therefore, greedy repair strategy considers ratio of the return and the loss of every project in investment which violate the constraint. It is used to repair the infeasible individuals during the evolutionary process and enlarge the return in investment as much as possible.

The remainder of the paper is organized as follows. First of all, measurement of return and risk is described in Section II. Then, investment problem is described in Section III. After that, the model of multi-project and multi-term portfolio and the framework of proposed algorithm are shown in Section IV and Section V. Finally, simulation results and conclusions are shown in Section VI and Section VII.

II. Investment Problem

A. Background

Most of paper only discuss single large project. However, there is not only single large project and the investment may last a long term in the actual investment environment. Sometimes it is difficult for investors to raise enough funds in a term. Nevertheless, it is necessary to extend the investment from one term to many terms in the field of the financial research. Investors may have many funding limitation, so it is important to take into account the remaining funds of each term. In addition, the modern financial environment is full of complexity and mutual influence. Investors may confront another finance constrains, for example, the administrative expenses. In the investment market, the unknown factors are obstructions on the road of seeking effective method for measuring the risk because it is always uncertain.

B. Single Term Investment

1) One Project: In the investment market which has only one project, we set the net cash flow in t ($t = 1, 2, ..., n$) duration as NCF_t, the cash flow bases on probability distribution as follows:

$$P(NCF_t) = p_t \quad and \quad \sum_{t=1}^{n} p_t = 1$$

The start-up investment funds of project is denoted by K in the single term. If r is the risk-free interest rate, the net present value is denoted by

$$NPV = \sum_{t=1}^{n} NCF_t (1+r)^{\frac{-t}{365}} \tag{1}$$

and the net present value index is denoted by

$$NPVI = \frac{1}{K} \cdot NPV = \frac{1}{K} \cdot \sum_{t=1}^{n} NCF_t (1+r)^{\frac{-t}{365}} \tag{2}$$

Then the return and risk of the project in the term can be given as follows:

$$E(NPVI) = \frac{1}{K} \cdot \sum_{t=1}^{n} E(NCF_t)(1+r)^{\frac{-t}{365}} \tag{3}$$

$$D(NPVI) = \frac{1}{K^2} \cdot \sum_{t=1}^{n} D(NCF_t)(1+r)^{-2(\frac{t}{365})} \tag{4}$$

In equation(3), we know that $E(NCF_t) = NCF_t \cdot p_t$.

2) Multi-Project: In the investment market, there are k projects. If these projects can be marked as $x_1, x_2, ..., x_k$, we try to select some available projects for the investment. Taking project k for example, we want to invest it in the Tth investment term ($T = 0, 1, ..., m$). We mark the net cash flow in t duration as NCF_{k^t} ($t = 1, 2, ..., n$), the cash flow abides by probability distribution as follows:

$$P(NCF_{k^t}) = p_{k^t} \quad and \quad \sum_{t=1}^{n} p_{k^t} = 1$$

The start-up investment funds of project i in the Tth term is denoted by K_i. Afterwards, the return and risk of projects in the single term can be given as follows:

$$R = \sum_{i=1}^{k} \frac{x_i K_i}{\sum_i x_i K_i} \cdot E(NPVI_i) \tag{5}$$

$$\Sigma(NPVI_i, NPVI_j) = E(NPVI_i - E(NPVI_i))(NPVI_j - E(NPVI_j)) \tag{6}$$

In equation (5), we know that

$$E(NPVI_i) = \frac{1}{K_i} \cdot \sum_{t=1}^{n} E(NCF_{k^t})(1+r)^{\frac{-t}{365}}$$

C. Multi-Term and Multi-project Investment

1) Assumptions and Symbols: In the investment market, if each large project i ($i = 1, 2, ..., k$) is prepared to be invested in many terms, we mark project i in the Tth term as $x_{i,T}$ ($T = 0, 1, ..., m$). Generally speaking, every project in different terms need the start-up investment funds and the funds of project i in the Tth term can be

denoted by $K_{i,T}$. Furthermore, $K_{i,T}$ is different in every investment term. In every investment term, it is no needs to have the same duration t $(t = t_1, t_2, ..., t_i, ..., t_n)$. For instance, if we plan to invest the project k in its 2nd term, the term has 30 days, so it means that the duration $t = 30$.

Suppose that we mark the net cash flow of project i in its t duration as NCF_{it} in the Tth term. For example, the net cash flow of project 1 in the multi-term investment can be given as:

$NCF_{11} \rightarrow NCF_{12} \rightarrow ... \rightarrow NCF_{1t_1}, NCF_{1t_1+1} \rightarrow NCF_{1t_1+2} \rightarrow ... \rightarrow NCF_{1t_2}, ..., NCF_{1t_{n-1}+1} \rightarrow NCF_{1t_{n-1}+2} \rightarrow ... \rightarrow NCF_{1t_n}$.

The net cash flow of project k in multi-term investment is given as:

$NCF_{k1} \rightarrow NCF_{k2} \rightarrow ... \rightarrow NCF_{kt_1}, NCF_{kt_1+1} \rightarrow NCF_{kt_1+2} \rightarrow ... \rightarrow NCF_{kt_2}, ..., NCF_{kt_{n-1}+1} \rightarrow NCF_{kt_{n-1}+2} \rightarrow ... \rightarrow NCF_{kt_n}$.

In the investment, we have the total capital limits of each investment term. The total capital limits in the Tth term is denoted by Q_T and it is various in different investment term. Moreover, because the project is integrative, it means that the project can't be separated. Hence, investors may have the remaining funds in some investment term. The remaining funds in the Tth term is denoted by U_T. It is not appropriate that investors do not consider the remaining funds in the investment or treat them as the return directly.

2) Measurement of Return and Risk: Suppose that $NCF_{i,T^{t_i}}$ is the cash flow of the project i in the Tth term and the term has t_i duration. The cash flow obeys probability distribution as follows

$$P(NCF_{i,T^{t_i}}) = p_{i,T^{t_i}} \quad (i = 1, 2, ..., k)$$

$$\sum_{T^{t_i}=1}^{t_i} p_{i,T^{t_i}} = 1$$

The mathematical expectation of project i in the Tth term is

$$E(NCF_{iT}) = \textstyle\sum_{T^{t_i}=1} NCF_{i,T^{t_i}} \cdot p_{i,T^{t_i}} \qquad (7)$$

If r is the risk-free interest rate as a specified value, investors can obtain the net present value index of project i in the Tth term as follows:

$$E(NPVI_{iT}) = \tfrac{1}{K_{i,T}} \cdot E(NPV_{iT}) \qquad (8)$$

In the equation (8), the net present value is

$$NPV_{iT} = \sum_{T^{t_i}=1} NCF_{i,T^{t_i}} (1 + r)^{\frac{-t_i}{365}}$$

The return of the project i in the Tth term is

$$R_{i,T} = \tfrac{x_{i,T} K_{i,T}}{\sum_{i=1}^{k} x_{i,T} K_{j,T}} \cdot E(NPVI_{iT})$$

Then the return and the risk of projects in the multi-term can be given as follows:

$$R = \sum_{T=0}^{m} \sum_{i=1}^{k} \tfrac{x_{i,T} K_{i,T}}{\sum_{i}^{k} x_{i,T} K_{j,T}} \cdot E(NPVI_{iT}) \qquad (9)$$

$$\Sigma(NPVI_{iT}, NPVI_{jT}) =$$

$$E(NPVI_{iT} - E(NPVI_{iT}))(NPVI_{jT} - E(NPVI_{jT})) \qquad (10)$$

As shown in Section II, it is not proper to use variance or absolute deviation for risk measuring. Thus, a new optimized method is given. The method is that let the semi-covariance be a measure which estimate the investment risk. We use $\Sigma(NPVI_{iT}, NPVI_{jT})$ to represent the covariance matrix. After the correction, the covariance matrix can be divided into two parts. The lower semi-covariance is denoted by $\Sigma(NPVI_{iT}, NPVI_{jT})^-$. The upper semi-covariance is denoted by $\Sigma(NPVI_{iT}, NPVI_{jT})^+$. They can be shown as follows:

$$\Sigma(NPVI_{iT}, NPVI_{jT})^- =$$

$$E(NPVI_{iT} - E(NPVI_{iT})^-)(NPVI_{jT} - E(NPVI_{jT})^-) \qquad (11)$$

$$\Sigma(NPVI_{iT}, NPVI_{jT})^+ =$$

$$E(NPVI_{iT} - E(NPVI_{iT})^+)(NPVI_{jT} - E(NPVI_{jT})^+) \qquad (12)$$

In the equation (11), we have

$$(NPVI_{iT}, NPVI_{iT})^- = \max(0, E(NPVI_{jT}) - NPVI_{jT})$$

In the equation (12), we have

$$(NPVI_{iT}, NPVI_{iT})^+ = \max(0, NPVI_{jT} - E(NPVI_{jT}))$$

III. Model Of Multi-project And Multi-term Portfolio

In the multi-project and multi-term investment, investors may consider the return and the risk of projects in the multi-term. Usually, Generally speaking, they want to get the high returns with the low risk. So the portfolio optimization model is based on maximizing the return and minimizing the risk.

If $x_{i,T} = 1$, it means that we select project i to be invested in the Tth investment term; if $x_{i,T} = 0$, it means that we will not plan to select project i to be invested in the Tth investment term.

So if we want to get the maximization of return and minimization of risk, the MOP model can be given as follows:

$$\max(R) = \sum_{T=0}^{m} \sum_{i=1}^{k} \tfrac{x_{i,T} K_{i,T}}{\sum_{i}^{k} x_{i,T} K_{i,T}} E(NPVI_{iT})$$

$$\min(V) = \frac{\sum_{T}^{m} \sum_{i}^{k} \sum_{j}^{k} \frac{x_{i,T} K_{i,T}}{\sum_{i}^{k} x_{i,T} K_{i,T}} \Sigma(NPVI_{iT}, NPVI_{jT})^- \frac{x_{j,T} K_{j,T}}{\sum_{j}^{k} x_{j,T} K_{j,T}}}{\sum_{T}^{m} \sum_{i}^{k} \sum_{j}^{k} \frac{x_{i,T} K_{i,T}}{\sum_{i}^{k} x_{i,T} K_{i,T}} \Sigma(NPVI_{iT}, NPVI_{jT})^+ \frac{x_{j,T} K_{j,T}}{\sum_{j}^{k} x_{j,T} K_{j,T}}}$$

$$s.t \quad x_{1,0}K_{1,0} + x_{2,0}K_{2,0} + x_{3,0}K_{3,0} + ... + x_{k,0}K_{k,0} + x_{k+1,0}U_0 = Q_0 \tag{13}$$

$$x_{1,1}K_{1,1} + x_{2,1}K_{2,1} + x_{3,1}K_{3,1} + ... + x_{k,1}K_{k,1} + x_{k+1,1}U_1 \le Q_1 + U_0(1+r)^{\frac{t_1}{365}} \tag{14}$$

$$x_{1,2}K_{1,2} + x_{2,2}K_{2,2} + x_{3,2}K_{3,2} + ... + x_{k,2}K_{k,2} + x_{k+1,2}U_2 \le Q_2 + U_1(1+r)^{\frac{t_2-t_1}{365}} \tag{15}$$

$$... \ ... \ ...$$

$$x_{1,T}K_{1,T} + x_{2,T}K_{2,T} + x_{3,T}K_{3,T} + ... + x_{k,T}K_{k,T} + x_{k+1,T}U_T \le Q_T + U_{T-1}(1+r)^{\frac{t_n-t_{n-1}}{365}} \tag{16}$$

$$\sum_{T}^{m}\sum_{i}^{k} x_{i,T}K_{i,T} \le \sum_{T}^{m} Q_T \tag{17}$$

where equation (13) is capital funding constraint of the initial term in the investment, equation (14) and (15) are the funding constraints of all projects in the 1st investment term and the 2nd investment term, equation (16) and (17) are the funding constraints of all projects in the Tth investment term and the whole investment terms respectively.

Besides, we consider the minimization problem and denote it by $f(x) \in (0,1)$. If the constant value $\gamma \ge 1$, the problem of minimizing $f(x)$ can be turned to obtain the maximization of $(\gamma - f(x))$.

IV. The Framework Of Proposed Algorithm

A. Encoding

Suppose that we plan to select some projects from projects $1, 2, ..., k$, which will be invested in the T investment terms. In this algorithm, every individual is a composed of $T \times k$ matrix. The number of the row and the number of the column correspond to the project and investment term, elements of the matrix are 0 or 1.

For example, suppose $k = 25, T = 5$, it means that we plan to select some projects to invest in five investment terms. An individual is represented by a transposed matrix of 25 rows and 5 columns, we can denote it by X. In the matrix, $x_{0,4} = 0$ means project 4 is not selected in the first term ; $x_{1,10} = 1$ means project 10 is selected in the second term and $x_{2,2} = 0$ means project 2 isn't selected in the third term.

$$X = \begin{pmatrix} 1110000101100001010001010 \\ 0110011011010010100101110 \\ 0001111000000000110101100 \\ 1000101000000000110001010 \\ 0001111000000000110001111 \end{pmatrix}$$

X is a 5×25 matrix as follows

$$X = \begin{pmatrix} x_{0,1}x_{0,2}x_{0,3}...x_{0,25} \\ x_{1,1}x_{1,2}x_{1,3}...x_{1,25} \\ ..... \\ ..... \\ x_{4,1}x_{4,2}x_{4,3}...x_{4,25} \end{pmatrix}$$

In order to simplify the operation of the proposed algorithm, the encoding of X in this paper is as follows

$$X = \left(\ x_{0,1}, ..., x_{0,25}, x_{1,1}, ..., x_{1,25}, ...x_{4,1}, ..., x_{4,25} \ \right)$$

where $x_{1,1}$ also indicates project 1 in the second investment term.

B. Proposed Algorithm

1) Subregion Strategy: As is well known, evolutionary algorithm has the problem of premature. It is important to maintain the diversity of population. If we do not consider to use the subregion strategy, some points will be easy to be eliminated in the evolution process. The increasing investment return has accompanied with risk in finical investment. It is difficult to furnish portfolios which may have the maximization of return with a reasonable value of relative risk. If we utilize the subregion strategy, points will be divided into different subregion so that they can be preserved. Thus it is necessary to use the subregion strategy to preserve these points, and the points in the same subregion may have the maximization of return with reasonable value of risk. Then they may offer help in furnishing the Pareto optimal solution. In addition, the number of individuals in every subregion is less than the population size. Therefore, the subregion strategy can be used to decrease the complexity of algorithm.

The objective space is divided into M subregions by using the subregion strategy, refer to literature [16]and M center vectors are distribute uniformly in the space. Then every subregion is independently optimized and corresponds to an external set, the set is denoted by H_h and is employed to preserve some individuals ever found in this subregion $(h = 1, 2, ..., M)$. In this paper, two main objectives are denoted by $f_s(X)$, where $s = 1, 2$. The weight of individual X was denoted by set $W^s = ({w_1}^s, {w_2}^s, ..., {w_{popsize}}^s)$. We classify the weight vectors by Tchebycheff method. We can express the fitness function $G(X) = max\{W^s g_s(X)\}$, where $g_s(X) = {f_s}^* - f_s(X)$ and ${f_s}^* = max\{f_s(X)\}$. The subregion strategy is used to maintain the diversity of population with a purpose of preventing premature in the evolutionary process.

2) Greedy Repair Strategy: It is important to deal with the infeasible individuals in multi-objective optimization problem with constraints. So we choose greedy repair strategy to repair the infeasible individuals in order to effectively deal with the constraint.

Suppose that X is a set of infeasible individual such that $\sum_{T}^{m}\sum_{i}^{k} x_{i,T}K_{i,T} > \sum_{T}^{m} Q_T$, $T = 0, 1, ..., m$. The start-up investment funds of project i in the Tth investment term is denoted by $K_{i,T}$. If $\sum_{T}^{m}\sum_{i}^{k} x_{i,T}K_{i,T} > \sum_{T}^{m} Q_T$, a way to make X as a feasible individual is to remove some projects from the investment term regularly. But not all investment portfolios are the infeasible individuals, the individuals which don't violate the constraint do not

need to be considered in the investment. The greedy repair strategy is used frequently and described as follows

Step 1) If X is infeasible individual, then go to Step 2.

Step 2) Set $X = \{(i,T) \mid x_{i,T} = 1\}$.

Step 3) Select $x \in X$ such that:

$$x = max\frac{x_{i,T}R_{i,T}}{K_{i,T}} \tag{18}$$

Step 4) Set $x_{i,T} = 1$ and Stop .

If one project is removed from the investment term, in investment market, the return and risk of the investment must be changed. Because the investment return has always accompanied with risk. Some investors may want to get high returns but they do not like the risk. And at the same time, investors may pay some attention on the start-up investment funds of every project in each investment term. So only project is selected to be invested in one investment term, the investment portfolio will be affected by the project's risk, the return and start-up investment funds. Hence the greedy repair strategy is based on the ratio between profit and loss of every individuals. The lost funding of project i in Tth term is denoted by the sum of start-up investment funds and risk. According to this idea, an improved greedy repair strategy can be given and transformed formula as

$$x = max\frac{x_{i,T}R_{i,T}}{aK_{i,T} + bV_{i,T}} \tag{19}$$

In equation (19), $(aK_{i,T} + bV_{i,T})$ denotes the lost funding in the investment, where $a + b = 1$ and $a, b \in (0,1)$. The lost funding of project i in Tth term is denoted by the sum of start-up investment funds and risk. As is known, $R_{i,T}$ is the return of project j in Tth investment term, $V_{i,T}$ is the risk of project j in Tth investment term.

Additionally, investors can evaluate a and b by their own preferences. In this paper, we provide $a = 0.8$, $b = 0.2$. It means investors like considering about the start-up investment funds of every project in every investment term. Considering the start-up investment funds an risk could allow the portfolios to become more feasible. As a consequence, the major purpose of using greedy repair strategy is to repair the infeasible individuals, and keep the higher return in every investment term as much as possible. Feasible individuals are penetrated into the next generation, and the proposed greedy repair strategy can improve the quality of population individuals.

3) Crossover Operator and Mutation Operator: We perform the crossover between an individual and an individual which is randomly selected from the corresponding external set. It is helpful in exploring great individuals and wide area. The crossover operator uses one-point crossover strategy. Crossover probability is denoted by p_c. Individuals are selected to perform the crossover according to a random number in $[0,1]$. $popsize$ denote the population size. A random number pos denote the crossover point, where $pos \in [1,j]$ and j is the length of chromosome. There are $j-1$ crossover positions. The coupled individuals exchange partial chromosomes with each other at the crossover point. So we can get the new offsprings.

The individuals which from the same subregion and the corresponding external set are selected for mutation operator. It exchanges the information among different subregions to discover the new individuals. The mutation operator uses uniform mutation strategy. It selects a single parent $X = (x_1, ..., x_w, ..., x_p)$ and generates a single offspring $X' = (x_1, ..., x_w', ..., x_p)$, where $w \in (1,p)$. Mutation probability is smaller than crossover probability, and it is denoted by p_m. Individuals are selected to perform the mutation. In this paper, if $x_w = 1$, after the mutation, $x_w' = 0$; if $x_w = 0$, after the mutation, $x_w' = 1$. Then we can obtain the new offsprings. Mutation operator plays an important part in the evolution process as the solutions are allowed to shift freely in the search space. It can enhance the search ability and exploit the optimum offspring avoiding a local optimum.

4) Selection Strategy: This paper adopts selection strategy, refer to [17]. An external set is introduced for each subregion and is used to store individuals ever found in this subregion. The dominated individuals are eliminated at once in some algorithms. But it is not helpful to utilize the dominated individuals to construct the simulative descent direction. We generate new individuals and update the external sets and subregions in the evolutionary process.

C. Steps For The Proposed Algorithm

(1) Setting parameter: set size of the population $popsize$, the number of subregions M and iterations $maxgen$, crosser probability p_c and mutation probability p_m.

(2) Initialization: generate weight vectors W^s and initial population randomly, repair infeasible individuals by formula (19), divide population into M subregions, calculate fitness value of individuals and select individuals of having the best value into sub population.

(3) Performing crosser and mutation: modify the population and generate new offspring, classify them into different subregions.

(4) Updating: update the current population and external sets.

(5) Stopping criteria: repeat (3) until satisfy the stopping criteria.

V. Computer Simulation

This paper uses similar examples as literature [6] and literature [20]. Example I: there is an investment company. The company plan to select some projects to be invested in the investment market. According to the method: coefficient of variation, where $C.V \leq 1.0$, we have 10 large projects successfully passed the assessment. If these projects can be invested in five investment terms, we can suppose $T = 0,1,2,3,4$. Every term contains $\triangle t_1/365 = 2$, $\triangle t_i/365 = 3, i = 2,3,4,5$. Inputs

are given at the beginning and outputs are furnished at the end. The cash flows $NCF_{11}, NCF_{12}, ...$, in different terms have been completely given. The risk-free rate is denoted by r, where $r = 0.05$. Assume that the rate will not be changed in the multi-term investment. The total investment funds Q_T in the multi-term investment and start-up investment funds $K_{i,T}$ of every project are given by Table I and Table II.

TABLE I.
TOTAL INVESTMENT FUNDS

$Term$	$Initial$	$1st$	$2nd$	$3rd$	$4th$
$Funds$	84	120	253	98	161

TABLE II.
START-UP INVESTMENT FUNDS

$Project$	$Initial\ term$	$1st$	$2nd$	$3rd$	$4th$
1	10	15	20	18	25
2	20	23	24	25	30
3	30	35	40	45	40
4	08	10	12	06	15
5	15	20	25	30	15
6	18	25	27	20	25
7	25	30	35	35	40
8	40	38	40	45	55
9	35	40	45	38	37
10	30	33	38	35	48

In this paper, according to the equation in Section III , Table I and Table II, we can get Table III, IV and V by using the tool of EXCEL. Upper semi-covariance is given by Table III, lower semi-covariance is given by Table IV and the net present value index is given by Table V.

TABLE III.
UPPER SEMI-COVARIANCE

$Term$	$Initial$	$1st$	$2nd$	$3rd$	$4th$
$Initial$	1.56001	0.00000	0.0	0.05281	0.00000
$1st$	0.00000	0.06056	0.00000	0.04503	0.06621
$2nd$	0.00000	0.00000	1.20978	0.00000	0.00000
$3rd$	0.05281	0.04503	0.00000	0.16843	0.22450
$4th$	0.00000	0.06621	0.00000	0.22450	1.65436

TABLE IV.
LOWER SEMI-COVARIANCE

$Term$	$Initial$	$1st$	$2nd$	$3rd$	$4th$
$Initial$	0.00000	0.05061	0.30898	0.00000	0.26439
$1st$	0.05061	0.00000	0.01126	0.00000	0.00000
$2nd$	0.30898	0.01126	0.00000	0.31654	0.51689
$3rd$	0.00000	0.00000	0.31654	0.00000	0.00000
$4th$	0.26439	0.00000	0.51689	0.00000	0.00000

With the help of Matlab7.0, we can use the parameters as follows: the number of iterations is given as $maxgen = 1500$, the population size is given as $popsize = 300$, crossover probability is given as $p_c = 0.8$, and mutation probability is given as $p_m = 0.05$.

This paper considers the structure of model in Section IV and Section V, we can get Figure 1. We consider

TABLE V.
NET PRESENT VALUE INDEX

$Project$	$Initial$	$1st$	$2nd$	$3rd$	$4th$
1	1.36594	1.07845	0.90055	1.39878	1.23368
2	2.45204	1.11645	1.55111	1.24839	1.14300
3	1.06478	1.12471	5.03689	1.12561	0.98967
4	1.13109	1.37653	1.50422	1.51784	1.53480
5	0.84234	1.12734	1.08757	1.21720	2.21834
6	1.15826	1.08426	1.33762	1.36065	1.13004
7	1.11121	1.14391	1.16814	1.15824	0.81519
8	1.09338	1.19024	1.16193	1.13716	0.74639
9	1.19343	1.13267	1.14291	1.05786	0.96679
10	1.17438	1.10146	1.14136	1.16192	0.69489

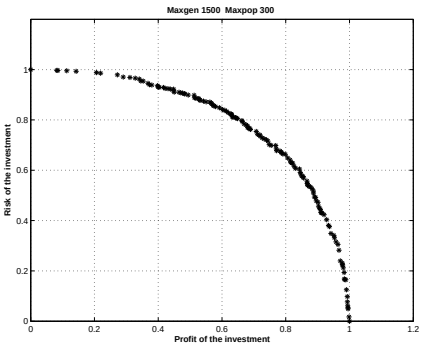


Figure 1. Return and risk in the investment

horizontal and vertical coordinates as the return of investment and risk of investment. In this situation, we can observe the investment return is increasing and the investment risk is increasing. It is able to get a series of investment portfolios, and the portfolios constitute Pareto effective surface. In the investment, investors may have different attitude to the risk and return of projects. Some of them may want to get high return even with high risk, while others may dislike high risk and they can accept the low return. So from Figure 1, they can choose portfolio which they prefer. Before investors determine the investment decision-making, it is better to talk with them and find out their preference. If investor wants to get high return and does not mind to take the high risk, he can choose the point which is the longest distance with vertical coordinate. If the investor doesn't like the high risk, he can choose the point which is the longest distance with horizontal coordinate.

In addition, from Figure 1, for example, we take two portfolios in the investment.

TABLE VI.
INVESTMENT PORTFOLIO

$Term$	$Portfolio1$	$Portfolio2$
$Inital$	1100110000	1001100010
$1st$	0101110100	1010101000
$2nd$	1001101101	0100110110
$3rd$	1100110000	0000100011
$4th$	1101110010	1011110010
$Return$	0.532061	0.530556
$Risk$	0.429770	0.423282

As shown in Table VI, the number of invested projects

in portfolio1 is more than portfolio2, but their return and risk are the same. In other words, the return and risk of portfolio do not change greatly with numbers of projects in the investment. However, portfolio1 may produces more administrative expenses than portfolio2. If an identity matrix is denoted by $I_{i,T}$, we give an account of another objective $\min(N) = \sum_{T}^{m}\sum_{i}^{k} x_{i,T} \cdot I_{i,T}$ into account.

This situation will obviously be seen when the number of invested projects increase more. We will try to research this situation in more detail on another paper.

Example II: One company plan to select some projects to be invested in the investment market. We have 15 large projects successfully passed the assessment. If these projects can be invested in four investment terms, we can suppose $T = 0, 1, 2, 3$. Inputs are given at the beginning and outputs are furnished at the end. The risk-free rate is denoted by $r = 0.05$ and the rate will not be changed in the investment. We give the parameters as shown in Table VII, Table VIII, TableIX, TableX. In addition, duration t in each investment term is different.

TABLE VII.
RELATED COEFFICIENT

$Term$	$Initial$	$1st$	$2nd$	$3rd$
$Initial$	0.00000	0.25000	0.30000	-0.50000
$1st$	0.25000	0.00000	0.70000	0.10000
$2nd$	0.30000	0.70000	0.00000	-0.50000
$3rd$	-0.50000	0.10000	-0.5000	0.00000

TABLE VIII.
START-UP INVESTMENT FUNDS

$Project$	$Initial\ term$	$1st$	$2nd$	$3rd$
1	20	30	35	00
2	20	35	20	00
3	30	35	40	00
4	25	18	00	00
5	15	30	00	00
6	28	25	27	20
7	25	30	35	35
8	40	38	00	45
9	35	40	45	38
10	30	33	38	35
11	10	15	20	18
12	20	23	24	25
13	20	35	40	45
14	08	00	12	06
15	15	20	00	30

As shown in Example I, with the help of Matlab7.0, we use the parameters as follows: the number of iterations is given as $maxgen = 1500$, the population size is given as $popsize = 300$, crossover probability is given as $p_c = 0.7$, and mutation probability is given as $p_m = 0.06$.

Besides, we are able to get a series of investment portfolios and we also can find the investment return is increasing and the investment risk is increasing too. We can get a series of investment portfolios, and the portfolios constitute Pareto effective surface as shown in Figure II. In the investment, investors can choose portfolio which they prefer. For example, if investor wants to get high return and does not mind high risk, he can choose the portfolio1 as shown in Table XI; if the investor doesnt accept the high risk, he can choose the portfolio2 as shown in Table XI.

TABLE IX.
DURATION IN INVESTMENT TERMS

$Project$	$\triangle t_1/365$	$\triangle t_2/365$	$\triangle t_3/365$	$\triangle t_4/365$
1	2	3	2	0
2	3	2	2	0
3	2	2	2	0
4	3	3	0	0
5	3	2	0	0
6	2	2	2	2
7	2	3	3	2
8	3	2	0	2
9	3	2	2	3
10	3	3	2	2
11	2	2	2	2
12	2	2	2	2
13	3	3	2	2
14	2	0	2	3
15	2	2	0	3

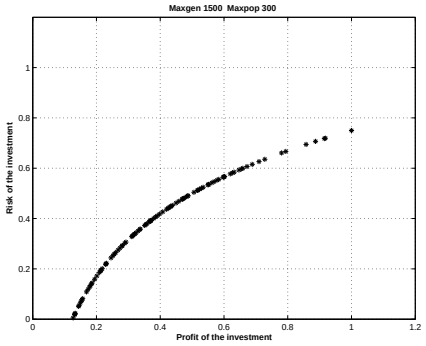


Figure 2. Return and risk in the investment

VI. CONCLUSIONS

This paper firstly talks about conditions in the single term investment and then extends the investment from one term to many terms in the field of the financial research. After that, it considers the funding constraints in finance environment and proposes a new multi-project and multi-term portfolio model. The model is about multi-objective optimization problem through considering the possible remaining funds in every investment term. Besides, it is not appropriate that we do not consider them in investment. Generally speaking, the investment risk is closely related with uncertainty. It is not appropriate to use variance to measure the investment risk. So in this paper, the model is based on a new kind of Mean-Semi-covariance theory. Then multi-objective evolutionary algorithm with greedy repair strategy is used to deal with the infeasible individuals. Finally, computer simulation proofs that the algorithm can be consider as a viable alternative. However, the influencing factors of investment may do changes all the time. We must think about variety of finance conditions in investment and we should develop another effective way to measure the investment risk. On

TABLE X.
INVESTMENT PORTFOLIO

$Term$	$Portfolio1$	$Portfolio2$
$Inital$	110011001011011	100110001011101
$1st$	010101010011001	101010100100000
$2nd$	110000100111010	010001001011010
$3rd$	000001101111110	000001010111101
$Return$	0.72158	0.34583
$Risk$	0.69353	0.30452

the whole, further research is required to the investment model and algorithm.

ACKNOWLEDGMENT

This work was supported in part by the Natural Science Foundation of China (60974077), and in part by the Natural Science Foundation of Guangdong Province (S2011030002886, S2012010008813), and in part by projects of science and technology of the department of education of Guangdong province (2012KJCX0042), and in part by Zhongshan projects of science and technology (20114A223).

REFERENCES

[1] H. Markowitz, "Portfolio Selection," *Journal of Finance*, vol.1, no.7, 1952, pp. 77-91.
[2] H. Konno, H. Yamazaki, "Mean-Absolute Deviation Portfolio Optimization Model and Its Application to Tokyo Stock Marcher," *Management Sicence*, vol.37, no.5, 1991, pp.519-531.
[3] C. MI lin, "An Effective Decision-Based Genetic Algorithm Approach to Multi-objective Portfolio Optimization Problem," *Applied Mathematical Sciences*, vol.3, no.5, 2007, pp.201-210.
[4] G. Delino, M. Fedele, C. Meloni, "Doam for Evolutionary Portfolio Optimization: A Computional Study," *Applied New Economics Paper*, 2008, pp.253-266.
[5] A. Kawakami,et al, "Dynamic Aseet Portfolio Optimization by Using Genetic Algorithm," *Information and Systema*, vol.129, no.7, 2009, pp.1348–1355.
[6] Xu Bin, Fang Weiguo, Liu Lu, "Optimization of Discrete Multi-term and Multi-project Investment Combination Model Based on NPV," *Mathematics in Practice and Theory*, vol.37, no.22, 2007, pp.6-12.
[7] HUANG X. X, "Mean-Variance Model for Fuzzy Capital Budgeting," *IEEE Computer and Industrial Engineering*, vol.55, no.1, 2008, pp.34-47.
[8] Song Yuantao, Wu Shanjie, Huang Jun, "Research on the Selection of Staged Investment In Project Group," *Science Technology Progress and Policy*, vol.26, no.21, 2009, pp.50-52.
[9] Wang Zhongye, Fang Lina, "Project Investment Decision Based on Genetic Algorithm," *Vehicular Science Technology Progress and Policy*, vol.23, no.5, 2006, pp.109-112.
[10] Hou Linlin, Chen Liwen, Qiu Wanhua, "Research on Construction and Application of Risk Decision Model for Project Investment Investment," *Chinese Journal of Management Science*, vol.15, no.10, 2007, pp.252-257.
[11] P. Skolpadungket, K. Dahal, N. Hampornchai, "Portfolio Optimization Using Multi-objective Genetic Algorithms," *In Proceedings of IEEE Congress on Evolutionary Computation*, Singapore, vol.516, no.5, 2007, pp.53-62.
[12] Coello C.A.C,et al. "Evolutionary Algorithms for solving Multiobjective Problems," *2010 New York: Kluwer Academic*, 2002.
[13] Ma Guadulupe, Castillo Tapia, Carlos Coello, "Applications of Multiobjective Evolutionary Algorithms in Economics and Finance: A Survey," *In Proceedings of IEEE Congress on Evolutionary Computation*, Singapore, vol.116, no.3, 2007, pp.28-34.
[14] Reza Golmakani, Hamid Jalilipour Alishah, "Portfolio Selection Using An Artificial Immune System. Information Reuse and Iintegration," *IEEE International Conference*, vol.28, no.3, 2008, pp.65-72.
[15] H. Liu, X. LI, "The Multiobjective Evolutionary Algorithm Based on Determined Weight and Sub-regional Search," *IEEE Congresson Evolutionary Computation*, 2009, pp.1928-1934.
[16] H-L. Liu, F. Gu and Q. Zhang, "Decomposition of a Multiobjective Optimization Problem into a Number of Simple Multiobjective Subproblems,"*IEEE Trans. Evol. Comput.,* 2013, in press
[17] H. Liu, W. Chen, F. Gu, "A Novel Multiobjective Differential Evolutionary Algorithm Based on Subregional Search," *IEEE Congress on Digital Object Identifier*, 2012, pp.1-6.
[18] H.Liu, Y.Wang, Y.Cheung, "A Multiobjective Evolutionary Algorithm Using Min-max Strategy and Sphere Coordinate Transformation," *Intelligent Automation and Soft Computing*, vol.15, no.3, pp.361–384, 2009.
[19] E.Zitzler, M.Laumanns, L.Thiele, "SPEA2:Improving The Strengh Pareto Evolutionary Algorithm for Multiobjective Optimization," *Evolutionary Methods for Design, Optimization and Control with Application to Industrial Problems*, pp.95–100, 2001.
[20] Chen Zhiwen, Yang Jianhui, L.Thiele, "SPEA2:Improving The Strengh Pareto Evolutionary Algorithm for Multiobjective Optimization," *Science and Technology Management Research*, no.4, pp.193–196, 2011.

Yuan Zhou was born in 1987. She is a M.S.candidate at the school of applied mathematics, Guangdong University of Technology, Guangzhou, China. Her current research interest includes multi-objective decision making and optimization.

Hai-Lin Liu received the BS degree in mathematics from Henan Normal University, Xinxiang, China, the MS degree in applied mathematics from Xidian University, Xi' an, China, the Ph.D degree in control theory and engineering from South China University of Technology, Guangzhou, China, and Post-doctor in the Institute of Electronic and Information, South China University of Technology, Guangzhou, China. He is currently a Professor at the school of applied mathematics, Guangdong University of Technology. His research interest includes computational intelligence, wireless network planning, optimization, and blind source separation.

Optimal Classification of Epileptic EEG Signals Using Neural Networks and Harmony Search Methods

[1, 2] Xiao-Zhi Gao, [3, 5]Jing Wang, [4] Jarno M. A. Tanskanen, [3]Rongfang Bie, [2] Xiaolei Wang, [3]Ping Guo, [2] Kai Zenger

[1]College of Information Engineering, Shanghai Maritime University, China
[2]Department of Automation and Systems Technology, Aalto University School of Electrical Engineering, Finland
[3]Laboratory of Image Processing and Pattern Recognition, Beijing Normal University, China
[4]Department of Biomedical Engineering, Tampere University of Technology, Finland
[5]School of Foundational Education, Peking University Health Science Center, China
xiao-zhi.gao@aalto.fi, wang_jing@bjmu.edu.cn, tanskanen@ieee.org,
rfbie@bnu.edu.cn, xiaolei.wang@aalto.fi, pguo@ieee.org, kai.zenger@aalto.fi

***Abstract*—In this paper, the Harmony Search (HS)-aided BP neural networks are used for the classification of the epileptic electroencephalogram (EEG) signals. It is well known that the gradient descent-based learning method can result in local optima in the training of BP neural networks, which may significantly affect their approximation performances. Three HS methods, the original version and two new variations recently proposed by the authors of the present paper, are applied here to optimize the weights in the BP neural networks for the classification of the epileptic EEG signals. Simulations have demonstrated that the classification accuracy of the BP neural networks can be remarkably improved by the HS method-based training.**

***Index Terms*—Harmony Search (HS) method, ElectroEncephaloGram (EEG), BP neural networks, optimization, Opposition-Based Learning (OBL), memetic computing, bee foraging algorithm, signal classification.**

I. INTRODUCTION

Epilepsy is a chronic neurological disorder that affects approximately 1% of the world's population, which is characterized by recurrent unprovoked seizures caused by abnormal electrical discharges in the brain. The ElectroEncephaloGram (EEG) is an electrical signal recorded from the scalp or intracranial, and reflects the mass activity of neurons and their interactions. The EEG is widely used by physicians to assist diagnosing many neurological disorders, especially the epilepsy. The detection of epileptic seizures in the EEG signals is very important in the diagnosis of epilepsy. In the past decade, interpretation of the EEG has been limited to only visual inspection by neurophysiologists, individuals trained to qualitatively make a distinction between normal and abnormal EEG. Unfortunately, detection of epilepsy that needs visual inspection of long recordings of the EEG is usually a time-consuming and high-cost process. Therefore, several diagnostic aid approaches for automatically detecting epileptic seizures from the EEG signals have been proposed and studied during the recent years.

Various techniques have been developed in the literature for the detection of epileptic seizures in the EEG [1-14]. All of the seizure detection schemes generally consist of two principal stages. In the first phase, features are extracted from the raw EEG data in the time domain, frequency domain, or time-frequency domain. In the second phase, the features extracted from the EEG are used for training classifiers that differentiate between the normal and epileptic EEG. Actually, numerous classifiers have been proposed and employed, including the Bayesian classifiers [1], Support Vector Machine (SVM), and different kinds of artificial Neural Networks (NNs) [2-6], artificial neuro-fuzzy inference system and dynamic fuzzy NN [7, 8]. In addition to the features for classification, the performance of the epilepsy detection is heavily dependent on the classifiers deployed.

The Harmony Search (HS) method is inspired by the underlying principles of the harmony improvisation [15]. Similar to the Genetic Algorithms (GA) [16], Particle Swarm Optimization (PSO) [17], Differential Evolution (DE) [18] and other computational swarm intelligence systems [19], the HS method is a stochastic search technique. It does not require any prior domain information beforehand, such as the gradient of the objective functions. However, different from many population-based evolutionary approaches, it only utilizes a single search memory to evolve. Thus, the HS method has the interesting characteristics of algorithm simplicity. In the HS, the harmony memory is used to store potential solution candidates, which can considerably reduce the possibility of being trapped into local optima.

The BP neural networks have been extensively employed in such important areas as control, optimization, signal processing, prediction, data classification, etc. Unfortunately, the gradient descent-based learning algorithm used usually results in the local optima of the weights in

doi:10.4304/jsw.9.1.230-239

the BP neural networks. Hence, it is always advantageous to apply some global optimization methods in order to acquire the optimal weights so that the training performances can be enhanced. Motivated by this idea, we apply the HS-based training method of the BP neural networks to classify the epilepsy and normal signals in the paper.

The structure of this paper is as follows: the principles of the HS method together with two modified versions are given in Sections II, III, and IV, respectively. In Section V, the epileptic EEG signal classification using the HS-based BP neural networks is proposed and discussed in details. Section VI demonstrates the numerical simulation results of applying our signal classification scheme. Finally, a few remarks and conclusions are given in Section VII.

II. Principles of HS Method

As we know that when musicians compose the harmony, they usually try various possible combinations of the music pitches stored in their memory. This kind of efficient search for a perfect harmony is indeed analogous to the procedure of finding the optimal solutions to many engineering problems. Hence, the HS method is inspired by the underlying principles of the harmony improvisation [15]. Figure 1 shows the flowchart of the basic HS method, in which there are four principal steps involved.

Step 1. Initialize the HS Memory (HM). The initial HM consists of a given number of randomly generated solutions to the optimization problems under consideration. For an *n*-dimension problem, an HM with the size of HMS can be represented as follows:

$$\mathrm{HM}=\begin{bmatrix} x_1^1, x_2^1, \cdots, x_n^1 \\ x_1^2, x_2^2, \cdots, x_n^2 \\ \vdots \\ x_1^{HMS}, x_2^{HMS}, \cdots, x_n^{HMS} \end{bmatrix}, \quad (1)$$

where n is the dimension of the problem, $\left[x_1^i, x_2^i, \cdots, x_n^i\right]$ ($i=1,2,\cdots,HMS$) is a solution candidate, and HMS is typically set to be between 50 and 100.

Step 2. Improvise a new solution $\left[x_1', x_2', \cdots, x_n'\right]$ from the HM. Each component of this solution, x_j' , is obtained based on the Harmony Memory Considering Rate (HMCR). The HMCR is defined as the probability of selecting a component from the present HM members, and 1-HMCR is, therefore, the probability of generating it randomly. If x_j' comes from the HM, it is chosen from the j^{th} dimension of a random HM member, and it can be further mutated according to the Pitching Adjust Rate (PAR). The PAR determines the probability of a candidate from the HM to be mutated. Obviously, the improvisation of $\left[x_1', x_2', \cdots, x_n'\right]$ is quite similar to the production of the offspring in the GA [16] with the mutation and crossover operations. However, the GA usually create fresh chromosomes using only one (mutation operator) or two (simple crossover operator) existing ones, while the generation of the new solutions in the HS method makes full use of all the HM members on a probability basis.

Step 3. Update the HM. The new solution from Step 2 is evaluated. If it yields a better fitness than that of the worst member in the HM, it will replace that one. Otherwise, it is eliminated.

Step 4. Repeat Step 2 to Step 3 until a preset termination criterion, e.g., the maximal number of iterations, is met.

The HS method is a random search technique. It does not require any prior domain information beforehand, such as the gradient of the objective functions. However, different from those population-based evolutionary approaches, it only utilizes a single search memory to evolve. Thus, the HS method has the interesting characteristics of computation simplicity.

A few modified HS methods have been developed and reported in the literature. For example, the authors of the present paper study a fusion of the HS and Cultural Algorithm (CA), HS-CA, in which the search knowledge stored in the CA is utilized to guide the mutation direction and size of the HS. This HS-CA is further used to effectively cope with an optimal wind generator design problem [20].

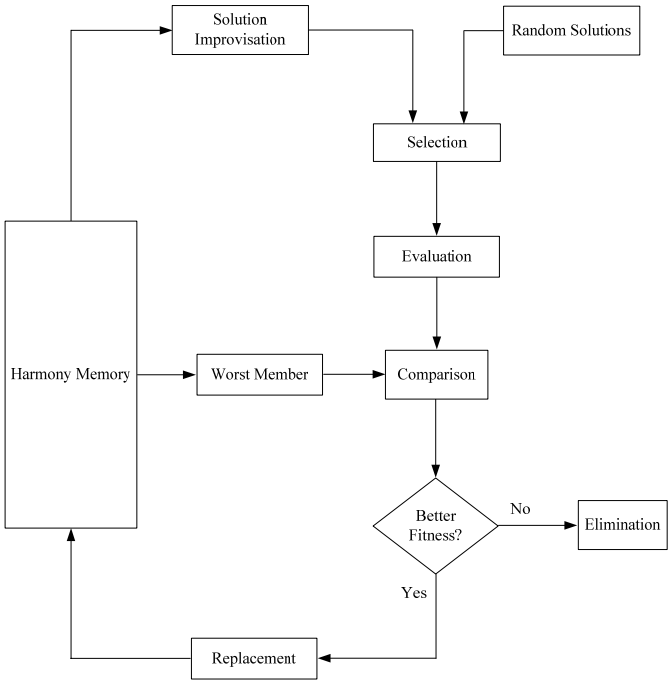


Fig. 1. HS method.

III. A Modified HS Method Based on Opposition-Based Learning (OBL)

A. Opposition-Based Learning (Obl)

Proposed by Tizhoosh, the OBL is a new approach to machine intelligence, which has been extensively employed in optimization, neural networks training, and reinforcement learning [21]. For dealing with optimization problems, the OBL is based on the utilization of the opposition numbers of the current search directions. More precisely, suppose $\mathbf{x}=(x_1, x_2, \cdots, x_n)$ is a single search point in the *n*-dimension solution space, and $x_i \in [a_i, b_i]$,

$i = 1,2,\cdots,n$. Only the continuous variables $\mathbf{x}$ are considered here. The opposition number $\mathbf{x}^* = (x_1^*, x_2^*, \cdots, x_n^*)$ of $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ is defined as:

$$x_i^* = a_i + b_i - x_i \,,\ i = 1,2,\cdots,n \,. \tag{2}$$

The principle of the OBL for optimization is that the search for the optimal solutions should be on the basis of both $\mathbf{x}$ and $\mathbf{x}^*$ as follows:

In every iteration, $\mathbf{x}^*$ is calculated from $\mathbf{x}$, and let $\mathrm{f}(\mathbf{x})$ and $\mathrm{f}(\mathbf{x}^*)$ represent the fitness of $\mathbf{x}$ and $\mathbf{x}^*$, respectively. The iterations proceed with $\mathbf{x}$, if $\mathrm{f}(\mathbf{x}) \geq \mathrm{f}(\mathbf{x}^*)$, otherwise, with $\mathbf{x}^*$. Note that "$\geq$" here means "better than or equal to with regard to the objective function $\mathrm{f}(\mathbf{x})$". An illustrate example of the OBL in the simple one-dimension ($n = 1$) optimization case is given in Fig. 2, where k is the iteration step.

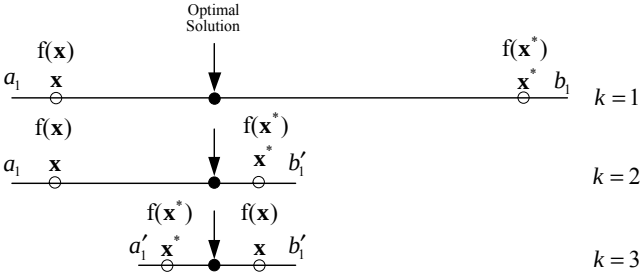


Fig. 2. Opposition-based Learning (OBL) in one-dimension ($n = 1$) optimization.

As Fig. 2 shows, with the growth of OBL iterations, the search interval can be *recursively* shrunk by half by choosing the solution candidate as the better one between $\mathbf{x}$ and $\mathbf{x}^*$. This procedure will ultimately converge, when $\mathbf{x}$ has approached to be close enough with $\mathbf{x}^*$. From these descriptions, it is concluded that the counterpart of $\mathbf{x}$ is utilized in the OBL so that the efficiency of search can be improved. Particularly, the employment of the OBL in the GA, reinforcement learning, DE, and HS method has been investigated in [22]-[24], respectively.

As a matter of fact, hybridization of different optimization schemes has shown to converge drastically faster than the standalone algorithms under certain application circumstances [25]. Inspired by this idea, we propose a hybrid HS method, so called DUAL-HS, by merging the HS and OBL together. A secondary memory is introduced in the DUAL-HS, and the OBL is incorporated for the evolution of this auxiliary memory so that the overall convergence speed can be accelerated [26].

B. A Hybrid HS Method with Dual Memory: DUAL-HS

As previously discussed, the quality of the HM members plays an important role in the convergence of the original HS method. Therefore, we introduce an OBL-based secondary harmony memory for providing alternative solution candidates in our hybrid HS method: DUAL-HS. Figure 3 illustrates the structure and evolution procedure of our DUAL-HS, and its principles can be explained as follows. At the beginning of the DUAL-HS search, a counterpart of the initial harmony memory HM_0, HM_0^*, is obtained using the OBL according to (2). Note that $[a, b]$ used here are the originally given variable ranges of the optimization problems. HM_0^* is first evaluated in the same way as HM_0, and it is then combined with HM_0. Only the top HMS members of $HM_0 + HM_0^*$ are selected as the initial HM to be started with. Actually, the use of HM_0^* results in an improved starting point for our DUAL-HS. In Fig. 3, N is the number of the iterations in the evolution interval of the DUAL-HS. Suppose there are N iterations in the evolution from the harmony memories HM_k to HM_{k+N}. For HM_{k+N}, we first compare the members in HM_{k+N} and HM_k, and merely choose those new members to compose a temporary memory $\overline{HM}_{k+N}$. That is to say, the high-quality fresh HM members created by the HS search during N iterations are employed. Note that the size of $\overline{HM}_{k+N}$ is usually much smaller than that of HM_{k+N}, especially when the DUAL-HS approaches to convergence. Next, the secondary memory in the DUAL-HS is built up by applying the OBL to $\overline{HM}_{k+N}$. It should be emphasized that $[a, b]$ used this time to calculate $\overline{HM}_{k+N}^*$ is based on the present ranges of the members in $\overline{HM}_{k+N}$. In other words, with the shrinkage of the solution candidates in $\overline{HM}_{k+N}$, the convergence of the DUAL-HS can be guaranteed. Similarly, $\overline{HM}_{k+N}^*$ is evaluated and combined together with HM_{k+N}. Similarly to $HM_0 + HM_0^*$, only the best HMS members from the combination of $\overline{HM}_{k+N}^*$ and HM_{k+N} are retained to replace HM_{k+N} so as to continue the search of the DUAL-HS. The above iteration procedure is repeated until a preset termination criterion is satisfied.

It can be observed from these descriptions that the secondary memory in the DUAL-HS, $\overline{HM}_k^*$, acts as an auxiliary storage to the primary harmony memory HM_k. The members generated by the OBL in $\overline{HM}_k^*$ can provide alternative solution candidates for the DUAL-HS to utilize, which may result in a superior convergence property over the regular HS method.

IV. A MEMETIC-INSPIRED HARMONY SEARCH METHOD: m-HS

The memetic computing has recently gained growing interest from different communities. The past decade has witnessed the great successes of applying the memetic algorithms in coping with large-scale, combinatorial, constrained, and multi-objective optimization problems [27]. As a matter of fact, the memetic algorithms represent a wide class of evolutionary computation methods with an inherent local search capability. More precisely, in the memetic algorithms, some local search techniques are incorporated into the meta-heuristics framework, and they operate only at certain cycles of the main-stream computation. The interesting characteristics of the memetic algorithms are that the local search used can efficiently improve the overall quality of the solution candidates, thus accelerating the convergence procedure. Indeed, the memetic computing can provide a useful guideline for researchers to modify the existing evolutionary computation schemes so as to design alternative optimization methods. However, the following important issues

have to be carefully addressed when developing a memetic algorithm:

(1) Types of the local search strategies utilized.
(2) Components in the memetic algorithms chosen for the local search.
(3) Frequency of applying the local search.
(4) Depth size (search range) of the local search.

Among all these issues, selecting an appropriate local search method can significantly affect the optimization performance of the memetic algorithms.

As we know that the swarm of bees can simultaneous explore various directions from their nests and find a lot of food sources. However, they are well capable of successfully locating the nearest flower patches with the largest amount of nectar or pollen. Actually, the bee foraging starts with randomly sending out a colony of scout bees for searching for potential flower patches. Based on the information (directions, distances, and qualities of the flower patches) collected by the returned scout bees, the bee colony evaluates the merits of different patches, and then send more scout bees to those more promising areas. During this positive feedback procedure, the bee swarm can gradually find the best food sources to harvest.

The bee foraging algorithm is a kind of popular population-based search method, which is inspired by the aforementioned food foraging behavior of honey bees [28]. In the bee foraging algorithm, the scout bees that return back with the best fitness are first chosen. The sites explored by these bees are considered as the most potential areas, where the optimal solutions may exist. Therefore, the local search is next performed on such sites in order to obtain more promising solution candidates. In the local search, a given number of bees are assigned to the selected sites according to their fitness for neighborhood search. That is to say, the sites with better fitness are going to receive more scouted bees to explore. Among all the scouted bees, only the best bee is selected from each patch as the representative local search result. Nevertheless, at the same time, some bees are also randomly scouted in the whole solution space. With this unique local search capability, the bee foraging algorithm has been proved to be an effective optimization method [29]. In the next section, we propose a memetic HS method, so-called m-HS, by incorporating the bee foraging-based local search strategy into the regular HS method.

A few interesting approaches to merging the HS method and bee foraging algorithm so as to develop novel memetic algorithms have been proposed and studied in the literature. For example, in [30], the authors propose a hybrid HS method, namely HHSABC, by incorporating the Artificial Bee Colony (ABC) algorithm and its variants. The harmony memory of the HHSABC is optimized by the ABC so that both the overall optimization accuracy and convergence rate can be significantly enhanced. The uniform design experiment is employed to verify and demonstrate the superiority of this hybrid HS. Based on the fusion of the HS method, hill climbing, and PSO, another hybrid version, HHSA, is developed [31]. In the HHSA, the local optimizer of the hill climbing and global-best approach of the PSO are complementary to each other, which can strike an appropriate balance between the exploration and exploitation in the search space. Compared with a total of 27 published methods, it is well capable of achieving the best results for most of the data sets for dealing with the popular benchmark problem of the university course timetabling. The hybrid HS method introduced by the authors in [32] combines the HS and bee algorithm together. It actually involves two serial optimization phases of the neighborhood search and global search implemented by the bee algorithm and HS, respectively. The effectiveness of their hybrid technique is examined using 14 real-world data instances of the university course timetabling problem. It can indeed outperform a few famous meta-heuristics methods, such as the variable neighborhood search, Tabu search as well as the original bee algorithm.

We propose and study a new memetic HS algorithm, m-HS, by incorporating the bee foraging like search strategy into the HS method [33]. In our m-HS, the bee foraging-inspired local search technique is applied periodically to improve the quality of the harmony memory. The structure of this m-HS is shown in Fig. 4. More precisely, after N steps of the HS evolution, the neighborhood search is performed on only some selected HM members, as illustrated in Fig. 5. Suppose $\mathbf{x}'$ is one of the top e members $[\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_e]$ chosen from HM_{K+N}. The neighborhood search can produce ne offspring from $\mathbf{x}'$ as follows:

$$\begin{aligned} \mathbf{x}'_1 &= \mathbf{x}' \pm rand \times ngh \\ \mathbf{x}'_2 &= \mathbf{x}' \pm rand \times ngh \\ &\vdots \\ \mathbf{x}'_{ne} &= \mathbf{x}' \pm rand \times ngh \end{aligned}, \tag{3}$$

where $rand$ is a random number within $[-1,1]$, and ngh is the local search range applied. $[\mathbf{x}'_1, \mathbf{x}'_2, \cdots, \mathbf{x}'_{ne}]$ are then evaluated, and only the one with the best fitness is retained. Note, to simplify our presentation here, the search performed by the randomly scouted bees is not used, and ne is chosen to be fixed. In other words, it is not proportional to the fitness of those selected HM members. This neighborhood search and selection applies to every member of $[\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_e]$. Therefore, there are a total of e solution candidates with better fitness resulted from the local search, which may replace $[\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_e]$ and enter the harmony memory HM_{K+N}. The above evolution procedure is terminated when a preset criterion is met.

It is concluded that the bee foraging like local search approach employed in the m-HS can indeed lead to enhanced solution candidates. That is to say, the quality of the harmony memory is improved by exploring the neighborhood of the top members. Additionally, the choices of parameters of e, ne, and ngh provide desired flexibilities to the m-HS so that its performance can be

further fine-tuned. However, the local search used might increase the computational complexity of the HS method.

V. Epileptic EEG Signal Classification with HS-based BP Neural Networks

A. BP Neural Networks

The BP neural networks, also named multi-layer perceptron networks, are an important class of neural networks, due to their simple topology and powerful approximation capability [34]. A simplified BP neural network with only three layers, i.e., input, hidden, and output layer, is illustrated in Fig. 6. There are adjustable weights connecting each two adjacent layers. The back-propagation of approximation error is utilized to train these weights. In general, one iteration of the back-propagation learning algorithm can be written as:

$$\mathbf{w}_{k+1} = \mathbf{w}_k - \alpha_k g_k , \tag{4}$$

where $\mathbf{w}_k$ is a vector of the weights at iteration k, α_k is the learning rate, and g_k is the calculated error gradient. It has been proved that a BP neural network with sufficient hidden nodes can approximate any nonlinear function to arbitrary degree of accuracy [35]. Therefore, the BP neural networks are usually regarded as universal function approximators as well as good candidates for classification, modeling, and prediction.

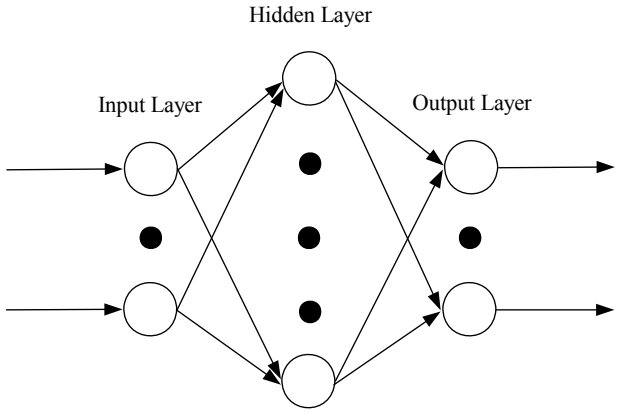


Fig. 6. A BP neural network with three layers.

B. EEG Signal Classification Using BP Neural Networks with HS Method-based Training

In this study, the epileptic seizure detection in the EEG signals can be considered as a classification problem. It includes the data acquisition, feature extraction, and classification steps [36]. With the consideration of the fact that EEG is sparse in Gabor dictionary, feature extraction method described in paper [1] is applied here. The HS-based BP neural networks are used as data classifiers to differentiate the normal EEG from the epilepsy signal [37]. The procedure of our method can be summarized as follows:

Step 1: Divide every EEG signal into segments.

Step 2: Extract feature vector based on the sparse representation [1].

Step 3: Formulate the training and testing signal sets for classification.

Step 4: Obtain the optimal weights of the BP neural networks using the HS method.

Step 5: Examine the classification performance of the BP neural networks using the testing set.

The simulation results of the proposed epileptic EEG signal classification scheme are demonstrated in the following section.

VI. Simulations

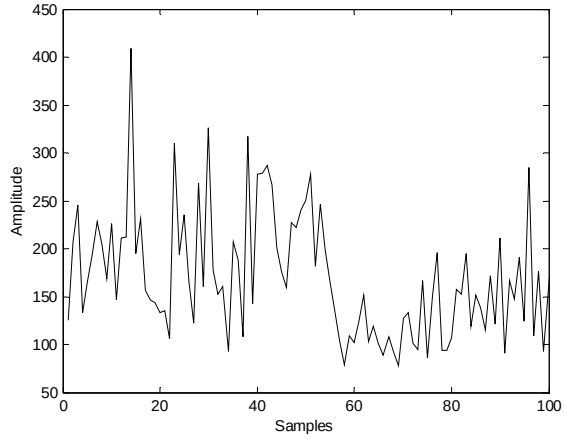
A. Data Sets

The public available data described in [38] is deployed. The complete data set consists of five sets (denoted as Z, O, N, F and S), and each contains 100 single-channel EEG segments. The dimension of the raw data is 4,096. Sets Z and O consist of segments, which are taken from the surface EEG recordings that are carried out on five healthy volunteers using a standardized electrode placement scheme. Volunteers are relaxed in an awake state with eyes open (Z) and eyes closed (O), respectively. Sets N, F and S originate from the EEG archive of presurgical diagnosis. Segments in set F are recorded from the epileptogenic zone, and those in set N from the hippocampal formation of the opposite hemisphere of the brain. While set N and F contain only the activity measured during seizure free intervals, set S only contains the seizure activity. Here, the segments are selected from all the recording sites exhibiting ictal activity.

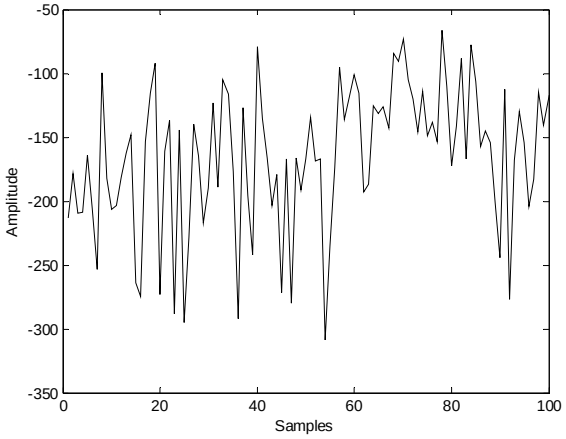
The above data are digitized at 173.61 samples per second using 12 bit resolution. The band-pass filter settings are 0.53-40 Hz (12dB/oct). The dataset Z includes the signals from normal people and S contains signals with epileptic patient's seizure activity. In this paper, two data sets (Z and S) of the complete data set are used.

B. Simulation Results

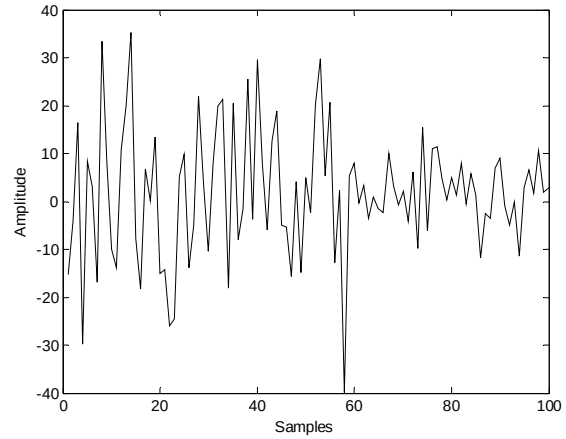
In our simulations, because the dimension of the raw data set is very high, every sample is divided into 17 subsamples. Thus, the dimension of 4,096 is reduced to 241. The parameters needed in feature extraction based on the sparse representation are the same as in [38]. The normal EEG signals from healthy volunteers and epileptic EEG signals from patients are shown in Figs. 7 and 8, respectively. Note that to simplify our presentation, only the first three sub-samples are given here (in (a), (b), and (c)). The desired classification outputs of the normal and abnormal EEG signals are denoted as -1 and 1, respectively, as illustrated in Fig. 9.



(a)

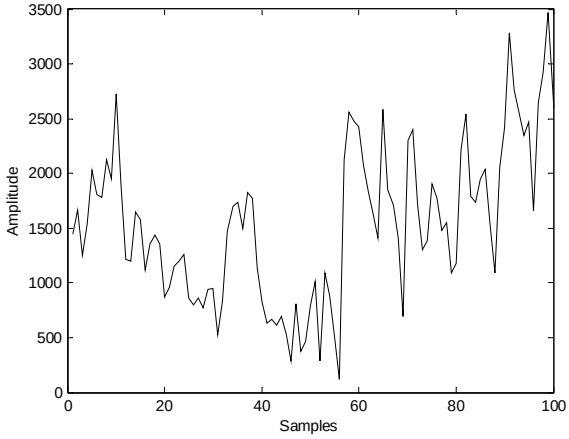


(b)

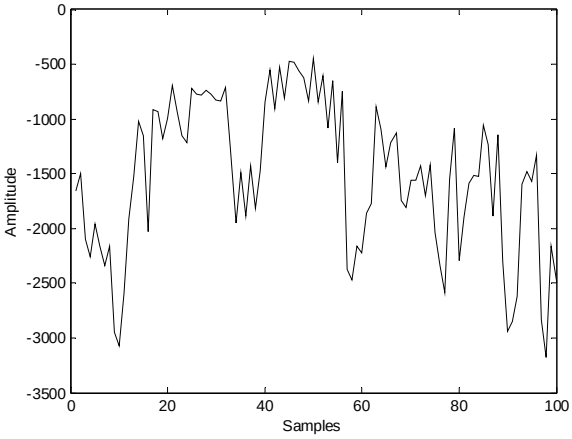


(c)

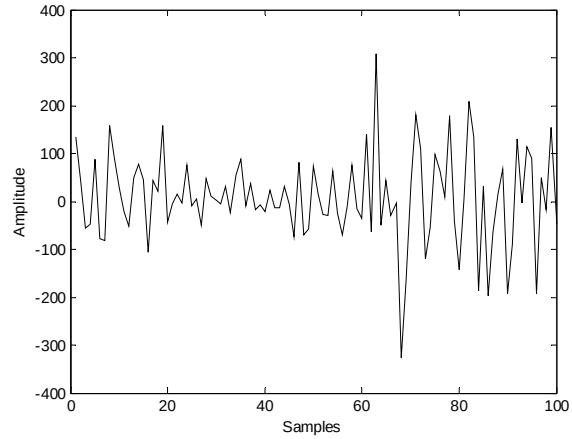
Fig. 7. Normal EEG signals from healthy people.



(a)



(b)



(c)

Fig. 8. Epileptic EEG signals from patients.

The structure of the BP neural network used is 3-5-1. That is, there are three, five, and one nodes in the input layer, hidden layer, and output layer, respectively. Therefore, a total of 26 weights/biases need to be optimized. We first compare the optimization performances of the original HS method, DUAL-HS, and m-HS, all of which have 100 HM members, i.e., $HMS = 100$. Their common parameters are given as follows: $\mathrm{HMCR} = 0.8$, and $\mathrm{PAR} = 0.6$. However, in the DUAL-HS, the OBL coeffi-

cient, P^{OBL}, is chosen to be $P^{OBL}=0.35$, and $N=10$. In the m-HS, $N=100$, $e=10$, $ne=10$. It is also pointed out that all the optimization results presented are based on the average of 100 independent trials.

The classification error of the epileptic EEG signals is used as the fitness for the HS method to optimize. A targeted optimization goal is chosen for the HS, DUAL-HS, and m-HS, which are all terminated after the goals, as given in Table 1, are reached. The iteration steps used by these three algorithms are compared with each other, and the comparison results are presented in Table 1. Obviously, compared with the original HS method, both the DUAL-HS and m-HS use less iterations to achieve the same targeted optimization goals. In other words, the enhanced convergence of these two modified HS methods results in an improved optimization capability. It is also worth pointing out that the m-HS can converge slightly faster than the DUAL-HS. The classification results of the BP neural networks with the HS-based training are further shown in Fig. 10. The testing EEG signals instead of training signals are used this time to examine their generalization capability. It is clearly visible that they are well capable of separating the epileptic EEG signals from the normal EEG signals.

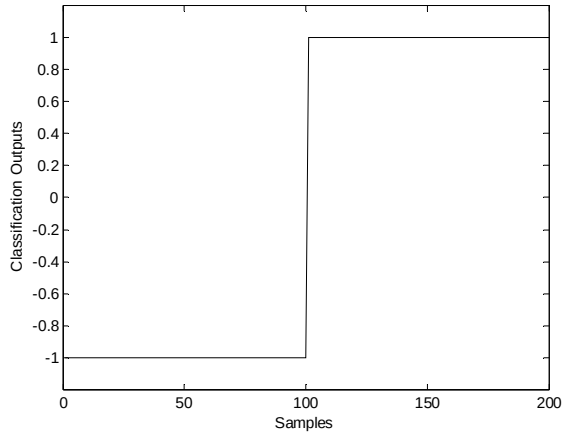


Fig. 9. Desired classification outputs of EEG signals.

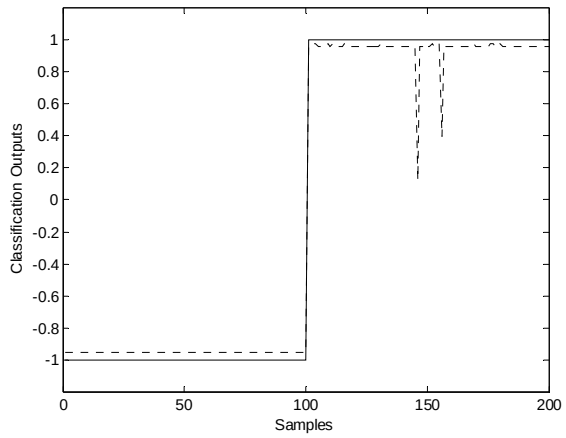


Fig. 10. Classification results of EEG signals using HS-optimized BP neural networks (solid line: desired classification outputs, dotted line: BP neural networks classification outputs).

VII. Conclusions

In this paper, the HS method together with two variants are used to acquire the optimal weights in the BP neural networks, which are employed as efficient data classifiers for the classification of the EEG signals. The performances of the regular HS method, DUAL-HS, and m-HS are compared in this case-study. Simulations show that both the two modified HS methods can yield an improved optimization accuracy in the training of the BP neural networks. With the proposed HS-based training strategies, the BP neural networks are capable of classifying the epilepsy EEG signals in a satisfactory way. Our future work includes how to apply the HS method in optimizing other kinds of data classifiers so that their performances can be enhanced.

Acknowledgments

The research work in this paper was supported by the grants from a joint call by the National Natural Science Foundation of China (Project No. 60911130513) and Academy of Finland (Grants 135225, 127299, and 137837). X. Z. Gao's research is also supported by the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning.

References

[1] J. Wang and P. Guo, "Epileptic electroencephalogram signal classification based on sparse representation," in *Proceedings of the International Conference on Neural Computation Theory and Applications*, Paris, France, pp. 24-26, October 2011.

[2] P. Guo, J. Wang, X. Z. Gao, and J. Tanskanen, "Epileptic EEG signal classification with marching pursuit based on harmony search method," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, Seoul, Korea, October, 2012, pp. 283-288.

[3] V. Nigam and D. Graupe, "A neural-network-based detection of epilepsy," *Neurological Research*, vol. 26, pp. 55-60, 2004.

[4] V. Srinivasan, C. Eswaran, and N. Sriraam, "Artificial neural network based epileptic detection using time-domain and frequency-domain features," *Journal of Medical Systems*, vol. 29, (6), pp. 647-660, 2005.

[5] N. Guler, E. D. Ubeyli, and I. Guler, "Recurrent neural networks employing Lyapunov exponents for EEG signals classification," *Expert Systems with Applications*, vol. 29(3), pp. 506-514, 2005.

[6] A. Subasi, "Automatic recognition of alertness level from EEG by using neural network and wavelet coefficients," *Expert Systems with Applications*, vol. 28(4), pp. 701-711, 2005.

[7] A. Subasi, "Epileptic seizure detection using dynamic wavelet network," *Expert Systems with Applications*, vol. 29, pp. 343-355, 2005.

[8] A. Subasi, "Automatic detection of epileptic seizure using dynamic fuzzy neural networks," *Expert Systems with Applications*, vol. 31(2), pp. 320-326, 2006.

[9] A. Subasi, "Application of adaptive neuro-fuzzy inference system for epileptic seizure detection using wavelet feature extraction," *Computers in Biology and Medicine*, vol. 37(2), pp. 227-244, 2007.

[10] A. Subasi, "EEG signal classification using wavelet feature extraction and a mixture of expert model," *Expert Systems with Applications*, vol. 32 (4), pp. 1084-1093, 2007.
[11] E. Ubeyli, "Combined neural network model employing wavelet coefficients for EEG signals classification," *Digital Signal Processing*, vol. 19(2), pp. 297-308, 2009.
[12] H. Ocak, "Automatic detection of epileptic seizures in EEG using discrete wavelet transform and approximate entropy," *Expert Systems with Applications*, vol. 36(2), pp. 2027-2036, 2009.
[13] E. D. Ubeyli, "Lyapunov exponents/probabilistic neural networks for analysis of EEG signals," *Expert Systems with Applications*, vol. 37(2), pp. 985-992, 2010.
[14] L. Guo, D. Rivero, J. Dorado, C. R. Munteanu, and A. Pazos, "Automatic feature extraction using genetic programming: An application to epileptic EEG classification," *Expert Systems with Applications*, vol. 38(8), pp. 10425-10436, 2011.
[15] Z. W. Geem, J. H. Kim, and G. V. Loganathan, "A new heuristic optimization algorithm: harmony search," *Simulation*, vol. 76 (2), pp. 60-68, 2001.
[16] R. Poli and W. B. Langdon, *Foundations of Genetic Programming*, Berlin, Germany: Springer-Verlag, 2002.
[17] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of the IEEE International Conference on Neural Networks*, Perth, Australia, December 1995, pp. 1942-1945.
[18] R. Storn and K. Price, "Differential evolution: A simple and efficient adaptive scheme for global optimization over continuous spaces," *Journal of Global Optimization*, vol. 11, pp. 341-359, 1997.
[19] A. P. Engelbrecht, *Fundamentals of Computational Swarm Intelligence*. West Sussex: John Wiley & Sons Ltd, 2005.
[20] X. Z. Gao, X. Wang, T. Jokinen, S. J. Ovaska, A. Arkkio, and K. Zenger, "A hybrid optimization method for wind generator design," *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 6, pp. 4347-4373, 2012.
[21] H. R. Tizhoosh, "Opposition-based learning: a new scheme for machine intelligence," in *Proceedings of the International Conference on Computational Intelligence for Modelling Control and Automation*, Vienna, Austria, November, 2005, pp. 695-701.
[22] S. Rahnamayn, H. R. Tizhoosh, and M. Salama, "A novel population initialization method for accelerating evolutionary algorithms," *Computers and Mathematics with Applications*, vol. 53, no. 10, pp. 1605-1614, 2007.
[23] H. R. Tizhoosh, "Opposition-based reinforcement learning," *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 10, no. 5, pp. 578-585, 2006.
[24] S. Rahnamayan, H. R. Tizhoosh, M. M. A. Salama, "Opposition-based differential evolution," *IEEE Transactions on Evolutionary Computation*, vol. 12, no. 1, pp. 64-79, 2008.
[25] X. Z. Gao, X. Wang, S. J. Ovaska, and K. Zenger, "A hybrid optimization method of harmony search and opposition-based learning," *Engineering Optimization*, vol. 44, no. 8, pp. 895-914, 2012.
[26] X. Z. Gao, X. Wang, K. Zenger, and Xiaofeng Wang, "A novel harmony search method with dual memory," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, Seoul, Korea, October 2012, pp. 177-183.
[27] F. Neria and C. Cottab, "Memetic algorithms and memetic computing optimization: A literature review," *Swarm and Evolutionary Computation*, vol. 2, pp. 1-14, 2012.
[28] D. T. Pham and M. Castellani, "The bees algorithm: modelling foraging behaviour to solve continuous optimization problems," *Proceedings of Institution of Mechanical Engineers*, Part C, vol. 223, pp. 2919-2938, 2009.
[29] D. Karaboga and B. Basturk, "On the performance of artificial bee colony algorithm," *Applied Soft Computing*, vol. 8, no. 1, pp. 687-697, 2008.
[30] B. Wu, C. Qian, W. Ni, and S. Fan, "Hybrid harmony search and artificial bee colony algorithm for global optimization problems," *Computers and Mathematics with Applications*, vol. 64, no. 8, pp. 2621-2634, October 2012.
[31] M. A. Al-Betar, A. T. Khader, and M. Zaman, "University course timetabling using a hybrid harmony search metaheuristic algorithm," *IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews*, vol. 42, no. 5, pp. 664-681, September 2012.
[32] K. Nguyen, P. Nguyen, and N. Tran, "A hybrid algorithm of harmony search and bees algorithm for a university course timetabling problem," *International Journal of Computer Science Issues*, vol. 9, no. 1, pp. 12-17, January 2012.
[33] X. Z. Gao, X. Wang, K. Zenger, and Xiaofeng Wang, "A bee foraging-based memetic harmony search method," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, Seoul, Korea, October 2012, pp. 184-189.
[34] S. Haykin, *Neural Networks, A Comprehensive Foundation*. Second Edition, Upper Saddle River, NJ: Prentice-Hall, 1999.
[35] K. Hornik, M. Stinchcommbe, and H. White, "Multilayer feedforward networks are universal approximators," *Neural Networks*, vol. 2, pp. 359-366, 1989.
[36] X. Z. Gao, J. Wang, J. Tanskanen, R. Bie, and P. Guo, "BP neural networks with harmony search method-based training for epileptic EEG signal classification," in *Proceedings of the International Conference on Computational Intelligence and Security*, Guangzhou, China, November 2012, pp. 252-257.
[37] K. C. Zikidis and A. V. Vasilakos, "ASAFES2: A novel, neuro-fuzzy architecture for fuzzy computing, based on functional reasoning," *Fuzzy Sets and Systems*, vol. 83, no. 1, pp. 63-84, 1996.
[38] R. Andrzejak, K. Lehnertz, F. Mormann, C. Rieke, P. David, and C. Elger, "Indications of nonlinear deterministic and finite-dimensional structures in time series of brain electrical activity: Dependence on recording region and brain state," *Physical Review E*, vol. 64, 2001.

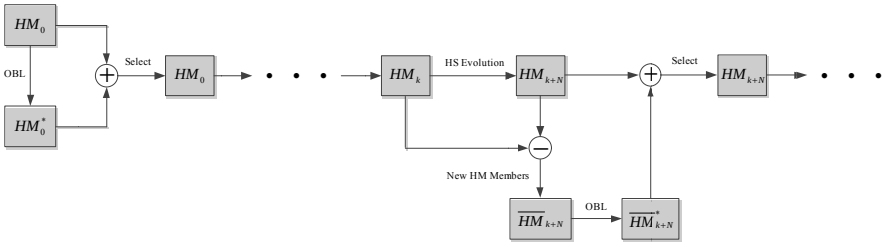


Fig. 3. A new HS method with dual memory: DUAL-HS.

Fig. 4. A memetic HS method: m-HS.

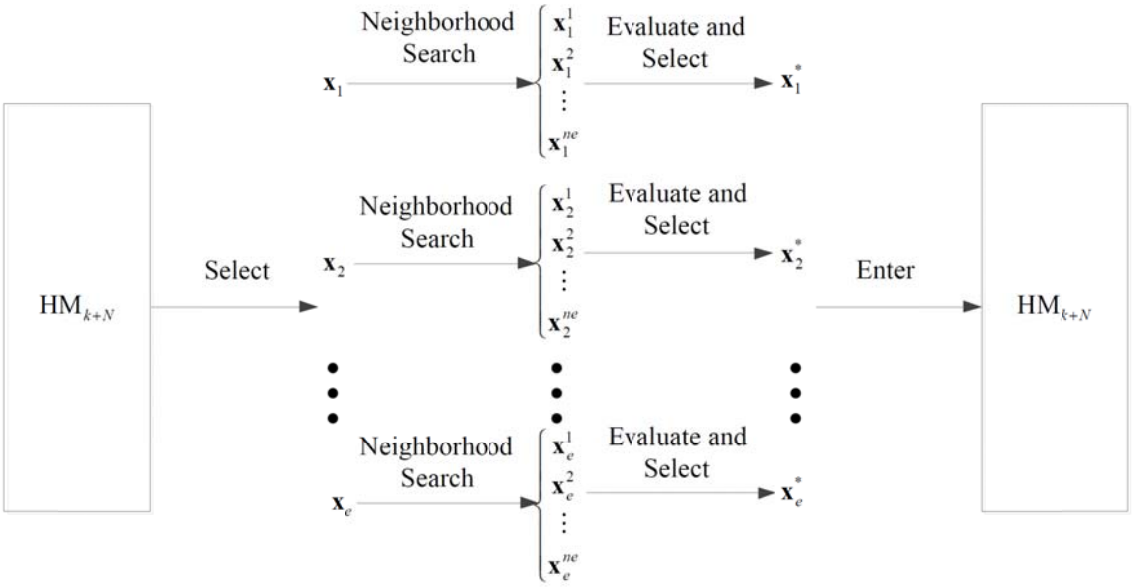


Fig. 5. Local search in m-HS.

TABLE 1.
ITERATIONS USED BY HS, DUAL-HS, AND M-HS IN BP NEURAL NETWORKS TRAINING FOR ACHIEVING OPTIMIZATION GOALS.

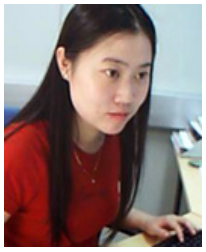
Optimization Goals	HS	DUAL-HS	m-HS
0.25	3.5316×10^4	3.0738×10^4	3.0228×10^4
0.5	2.6097×10^4	2.4230×10^4	2.1780×10^4
0.75	2.1423×10^4	1.9011×10^4	1.7347×10^4
1	1.7869×10^4	1.5792×10^4	1.5202×10^4
1.25	1.7359×10^4	1.5669×10^4	1.4014×10^4
1.5	1.3840×10^4	1.2188×10^4	1.1275×10^4

Xiao-Zhi Gao received his D.Sc. (Tech.) degree from the Helsinki University of Technology (HUT), Finland in 1999. Since 2004, he has been appointed as a Docent of Soft Computing Methods and Applications at the Aalto University (formerly HUT). His current research interests are nature-inspired computing methods with applications in optimization, prediction, data mining, signal processing, and control. He has published more than 260 technical papers in refereed journals and international conferences.

Jing Wang received the M.Sc. degree in computer software theory and applications from the Beijing Normal University, China in 2004. She is currently a Ph.D. student at the same university. Her research interests include computational intelligence methods with applications in medical signal processing.

Jarno M. A. Tanskanen received his D.Sc. (Tech.) degree from the Helsinki University of Technology (HUT), Finland in 2000. He is now working as a Senior Research Fellow at the Department of Electronics and Communications Engineering, Tampere University of Technology (TUT), Finland. His main research interests are biomedical and electrophysiological signal processing and analysis.

Rongfang Bie is the leader of IReG Group on the Internet of Things (IoT) at the College of Information Science and Technology of the Beijing Normal University (BNU), China. She received her M.Sc. degree in 1993 and Ph.D. degree in 1996 in Mathematics from the Beijing Normal University. She was with the Computer Laboratory at the University of Cambridge as a visiting faculty from March 2003 for one year. She is the author or co-author of more than 40 academic papers. Her current research aims to establish theories and models on database management model, knowledge representation, knowledge automatic acquisition, and knowledge sharing for the IoT, to develop the corresponding platforms, and to develop some typical applications on IoT education, health monitoring methods for civilians, and mechanical structures using the proposed theoretical models and IoT related technologies, such as sensing systems.



Xiaolei Wang received her D.Sc. (Tech.) degree from the Helsinki University of Technology (HUT), Finland in 2009. She is now working as a Postdoc Research Fellow at the Aalto University School of Electrical Engineering (formerly HUT). Her research interests are hybrid computational intelligence methods for optimization.

Ping Guo is an IEEE Senior Member and Professor at the College of Information Science and Technology of the Beijing Normal University (BNU), China. From 1980 to 1983, he studied at the Physics Department of the Peking University for M.Sc. degree, majoring in Optics. From 1997 to 2001, he studied at the Computer Science and Engineering Department of the Chinese University of Hong Kong for his Ph.D. degree. From 1993 to 1994, he was a visiting faculty at Computer Science and Engineering Department of Wright State University in the United States. He is a PC member of several international conferences, such as the ISNN and ICIC. As an author or co-author, he has published over 200 academic papers.

Kai Zenger received his M.Sc., L.Sc. and D.Sc. degrees in electrical engineering, computer technology, and automation and systems technology in 1986, 1992, and 2003, respectively. From 1983 to 1989, he worked as an automation engineer in MKT Finland and HT Automation. Since 1989, he had several positions related to teaching and research in the Control Engineering Laboratory at the Helsinki University of Technology, Finland. Currently, he is working as a Professor of Automation Technology in the Aalto University School of Electrical Engineering, Finland. Prof. Zenger's main research areas are Control Engineering and System Theory with applications in chemical process engineering, power electronics and mechanical engineering. He has specialized in the research of time-varying linear systems, periodic systems, and adaptive and robust control methods.

A Fractional Order Integral Approach for Reconstructing from Noisy Data

Dongjiang Ji
The School of Science, Tianjin University of Technology and Education, Tianjin 300222, P. R. China
zjkjdj@126.com

Wenzhang He
The School of Science, Tianjin University of Technology and Education, Tianjin300222, P. R. China
hewenzhang@sina.com

***Abstract*—Computed tomography (CT) plays an important role in many applications.Recently,total variation(TV) minimization has become a main topic in image reconstruction. This paper focuses on iterative algorithm: SART and EM in both of TV and ordered subset. Iterative reconstruction is an improved algorithm for reconstructing image from noisy projection data. However,image noise will increase after some iterations while the image quality does not meet the requirement. In order to improve the quality of the reconstructed image, for three dimensional cone-beam CT, a new iterative algorithm via fractional order integral is researched. Experimental results show that the proposed method has faster convergence speed and achieve higher PSNR**

***Index Terms*—Cone-beam CT; noise projection data; total variation ;iterative algorithm ; fractional order integral**

I. INTRODUCTION

The iterative reconstruction (IR) algorithm is the key component of computed tomography imaging technology. Iterative algorithms are able to generate higher quality CT images,with the rapid development of computer technology, more and more attention has been given to iterative algorithm [1,2] .

Compared with two-dimensional (2D) CT, in which fan-beam rays are used to scan the object, the three-dimensional (3D) CT, in which cone-beam rays are used to scan the object, has a much shorter scan time because it can make use of the rays more efficiently. So it has attracted increased attention, and is gradually being used in medical diagnosis and engineering [3,4].

For noise projection data, image quality will be worse after the certain number of iteration. There is no method which can completely change this problem, the common method is that we adjust the key factors of iterative algorithm or adopt regularization method enhancement algorithm stability[5]. Total variation ordered subsets iterative algorithm also has this problem, TV-OS-SART algorithm with fractional order integral filtering is researched handle this problem[6], this paper will study two methods TV-OS-SART and TV-OSEM algorithm combined with fractional order integral to enhancement algorithm stability,In order to test those method is possible,Peak Signal to Noise Ratio (PSNR) is adopted.These two methods are addressed as TV-OS-IR-FOI (TV-OS-Iterative reconstruction-fractional order integral).

The rest of the paper is organized as follows.In the next section, we will introduce the cone-beam CT model. In section Ⅲ,TV-OS-IR via fractional order integral will be presented.In section Ⅳ,we present the reconstructed quality evaluation criteria.In section Ⅴ,numerical results will be described to support our method.Finally,we will give a conclusion.

Ⅱ. 3D CONE-BEAM CT

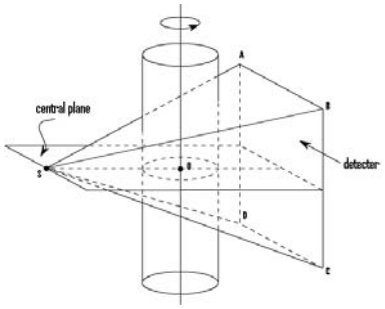


Figure 1. Cone-beam CT

In 3D cone beam scanning (see Fig .1), S is the ray source,the cylinder indicates the object that will be reconstructed,the plane ABCE represents the detector. Source runs around the object on a circle,together with a 2D detector .The scanning process provides us with the line integral of the reconstruct object along each of the lines. From all these integrals we have to reconstruct object.

Ⅲ. ITERATIVE RECONSTRUCTION ALGORITHM

An imaging system can be modeled as follows:

$$Wf = p \tag{1}$$

where $W = (w_{ij})$ denotes an $M \times N$ matrix, projection data is $p = [p_1, p_2, ..., p_M]^T \in R^M$, $f = (f_1, ... f_N) \in R^N$ is the

doi:10.4304/jsw.9.1.240-245

image space.The problem is to reconstruct the image space f according to W and p.

3.1 TV-OS-IR

The CT reconstruction problem of the system (1) can be solved by the CS-based reconstruction method to minimize the image TV regularized by the projections. It is equal to solving the following optimization program [7]

$$\arg\min_{f\in H(f)} TV(f), \quad s.t. Wf = p. \tag{2}$$

For the sake of discussion,let's just call this algorithm a TV-IR,this algorithm includes two major steps: in the first step,an iteration algorithm is used to reconstruct a rough image.In this paper,the OS-SART and OSEM are used to reconstruct the image respectively.

Iterative formulas of the OS-SART can be expressed as follows[8]:

$$f_n^{(k+1)} = f_n^{(k)} + \lambda_k \sum_{m\in\phi_l} \frac{w_{mn}}{\sum_{m'\in\phi_l} w_{m'n}} \frac{p_m - \tilde{p}_m}{W_{m+}}, k = 0,1,2..., \tag{3}$$

Iterative formulas of the OSEM can be expressed as follows[9]:

$$f_n^{(k+1)} = f_n^{(k)} \lambda_k \sum_{m\in\phi_l} \frac{w_{mn} p_m}{\tilde{p}_m} \frac{1}{\sum_{m'\in\phi_l} w_{m'n}}, k = 0,1,2..., \tag{4}$$

where k indicates the iteration number, $f_n^{(k)}$ means the (n)th 3D pixels, w_{mn} indicates that the (n)th 3D pixels contribution along the (m)th ray, p_m is the measured projection, $\tilde{p}_m$ is the simulated projection. λ_k is relaxation parameter, ϕ_l represents the set of ray indexes in the (l)th view.In the second step,a searching method is used to minimize the TV of the reconstruction image[10].

3.2 Fractional order integral for TV-OS-IR

The real projection data contain many kinds of noises, so the image quality will be worse after some iterations. We adopted TV-OS-SART and TV-OSEM algorithm to reconstruct image and denoise the image using fractional order integral before the image quality become worse. Those method are addressed as TV-OS-IR-FOI (TV-OS-Iterative reconstruction-fractional order integral) .

The general definition form of factional order calculus follows, let $f(t)\in(a,t)$,it has the $m+1$ order continual derivative, when $a\in R, a>0$, m is the integer part of a[11]

$$d^a f(t) = \lim_{h\to 0} \frac{1}{h^a} \sum_{m=0}^{n} (-1)^m \binom{a}{m} f(t-mh) = \lim_{h\to 0} \frac{1}{h^a} \sum_{m=0}^{\frac{t-a}{h}} (-1)^m \frac{\Gamma(a+1)}{\Gamma(a-m+1)} f(t-mh) \tag{5}$$

$$\Gamma(a) = \lim_{x\to\infty} \int_0^{\infty} e^{-x} t^{a-1} dt = (a-1)! \tag{6}$$

$d^a f(t)$ differential expression as follows:

$$\frac{d^a f(t)}{dt^a} \approx f(t) + (-a) f(t-1) + \frac{(-a)(-a+1)}{2!} f(t-2) + \frac{(-a)(-a+1)(-a+2)}{3!} f(t-3) + ... + \frac{\Gamma(-a+1)}{n!\Gamma(-a+n+1)} f(t-n) \tag{7}$$

where $n = [t-n]$.

The one-dimensional differential expression is extended to that of two dimensions, which is applied to image reconstruction[12]:

$$\frac{\partial^a f(x,y)}{\partial x^a} \approx f(x,y) + (-a) f(x-1,y) + \frac{(-a)(-a+1)}{2} f(x-2,y) \tag{8}$$

$$\frac{\partial^a f(x,y)}{\partial y^a} \approx f(x,y) + (-a) f(x,y-1) + \frac{(-a)(-a+1)}{2} f(x,y-2) \tag{9}$$

Fractional order of integral template along the x axis and y axis are defined in [13],where $a<0$.

The TV-OS-IR-FOI can be summarized as the following pseudo-code:

a) Initialization parameters: iteration number n ; relaxation parameter λ_k ;the number of subsets; initial value $f_0 = 1$; fractional order of integral operator;

b) it counts nth iterations of the loop by TV-OS-IR to reconstruct f_n , then f_n is normalized to $0 \le f_n \le 255$ and decomposing f_n along the vertical direction coordinates to get slice sequence; finally, along the x axis and y axis ,convolution operations are performed between fractional order of integral template and f_n to get f_n^x and f_n^y ;

c) Computing $f_n^{TV-OS-IR-FOI}$:

$$f_n^{TV-OS-IR-FOI} = a\times f_n + a_x \times f_n^x + a_y \times f_n^y, \tag{10}$$

where $\{(a,a_x,a_y) | a>0, a_x>0, a_y>0\}$

d)Until the stopping criteria are satisfied; else increment n and return to step b).

IV. EVALUATION CRITERIA

In order to test the method is possible, Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) are adopted to evaluate the reconstructed image.

Their formula are defined as[14]:

$$MSE = \frac{1}{I\times J\times K} \sum_{k=1}^{K}\sum_{j=1}^{J}\sum_{i=1}^{I} (t_{i,j,k} - r_{i,j,k})^2, \tag{11}$$

$$PSNR = 10 * \log[\frac{I\times J\times K\times 255^2}{\sum_{k=1}^{K}\sum_{j=1}^{J}\sum_{i=1}^{I} (t_{i,j,k} - r_{i,j,k})^2}], \tag{12}$$

where the image size is $I\times J\times K$, $r_{i,j,k}$ is the gray of voxel in original image, $t_{i,j,k}$ is the gray of voxel in reconstructed image.

V. EXPERIMENTAL RESULTS

TABLE Ⅰ.
3D CONE-BEAM SCANNING PARAMETERS

Parameter	value
Model size	128×128×128
Distance between Source and rotation center distance /mm	3000
Detector number	128×128
Projection sampling number	128

A 3D model is adopted to verify the TV-OS-IR-FOI and has much faster convergence speed and can achieve

higher PSNR than TV-OS-IR.Update f_n by TV-OS-IR-FOI at 4th and 8th iteration.

The parameters of 3D Cone-beam Scanning are listed in Table Ⅰ,8% Poisson noise was added to the simulated projection data; Relaxation parameter λ_k is 1;The numbers of subsets are 8 and 4;Fractional order of integral operator is -0.0001, iteration number *n* is 8.

5.1 The Number of Subsets is 8 for TV-OS-SART-FOI

At the 4th iteration,in which the reconstruction images were shown in Fig.2,we adopt weight coefficient $a_x = a_y = 2$, $a = 0.9$,it can be seen in figure 2 that TV-OS-SART-FIO can improve the brightness of the background and spherical area,while MSE becomes greater, just as shown in Fig .3.

After the 4th iteration .TV-OS-SART-FIO has faster convergence speed than TV-OS-SART is shown in Fig. 3.

At the 8th iteration,we adopt weight coefficients $a_x = a_y = 0.9$ $a = 2$ .The reconstruction images are shown in Fig. 4,it can be seen in Fig.4 that the reconstructed image using our proposed TV-OS-SART-FOI is in excellent agreement with the original model.

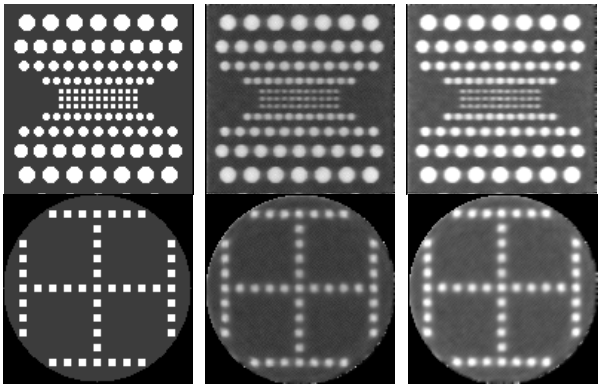


Figure2.Slice of image at x=64 and z=86
Left: original model; middle: reconstruction by TV-OS-SART
Right: reconstruction by TV-OS-SART-FOI

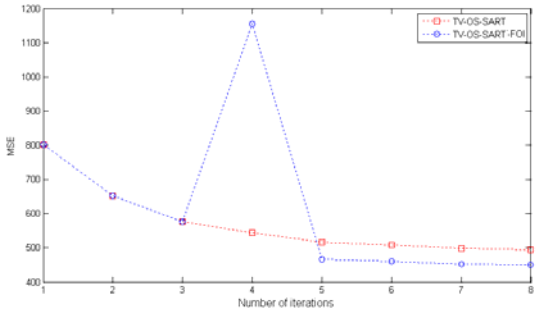


Figure 3. Mean Squared Error

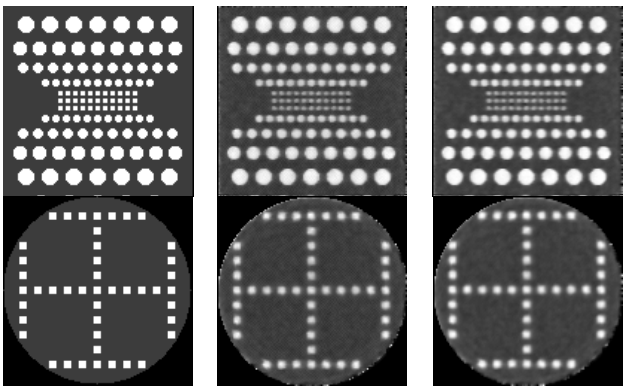


Figure4.Slice of image at x=64and z=86
Left: original model; middle: reconstruction by TV-OS-SART
Right: reconstruction by TV-OS-SART-FOI

TABLE Ⅱ.
PEAK SIGNAL TO NOISE RATIO

Number of Iterations	1	2	3	4
TV-OS-SART	19.0914	19.9864	20.5224	20.7765
TV- OS-SART-FOI	19.0914	19.9864	20.5224	17.5022
Number of Iterations	5	6	7	8
TV-OS-SART	21.0064	21.0586	21.1584	21.1421
TV- OS-SART-FOI	21.4336	21.4934	21.5768	21.5923

In order to evaluate the reconstruction results objectively,PSNR is adopted to evaluate the reconstructed image,just as in Table Ⅱ. From Table Ⅱ, we can see that the TV-OS-SART-FOI performs better than TV-OS-SART in the aspects of PSNR after 4th iteration .

5.2. The number of subsets is 4 for TV-OS-SART-FOI

At the 4th iteration,we adopt weight coefficients $a_x = a_y = 1.8$, $a = 0.9$ .The reconstruction images were shown in Fig. 5,it can be seen in Fig.5 that TV-OS-SART-FOI can improve the brightness of the background and spherical area,while MSE becomes greater, just as shown in Fig.6.

After the 4th iteration,TV-OS-SART-FOI has faster convergence speed than TV-OS-SART is shown in Fig.6.

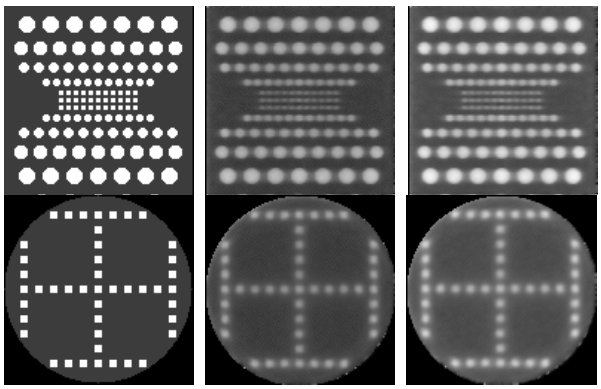


Figure 5. Slice of image at x=64 and z=86
Left: original model; middle: reconstruction by TV-OS-SART
Right: reconstruction by TV-OS-SART-FOI

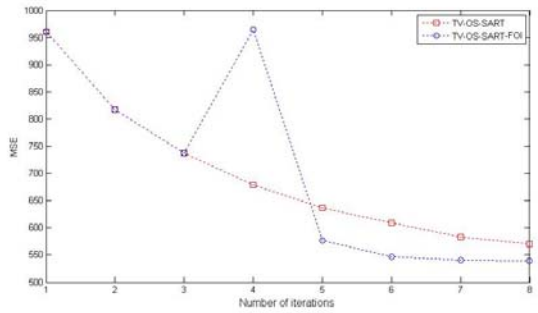


Figure 6 . Mean Squared Error

At the 8th iteration,we adopt weight coefficients $a_x = a_y = 0.7$, $a = 2.4$ .The reconstruction images were shown in Fig.7.It can be seen in Fig.7 that the reconstructed image using our proposed TV-OS-SART-FOI is in excellent agreement with the original model.

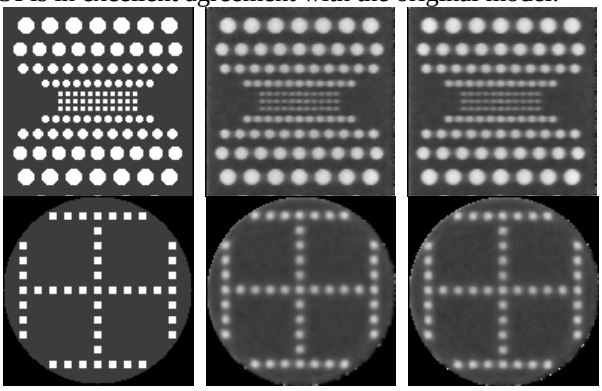


Figure 7. Slice of image at x=64 and z=86
Left: original model; middle: reconstruction by TV-OS-SART
Right: reconstruction by TV-OS-SART-FOI

From Table Ⅲ, after the 4th iteration ,we can see that the TV-OS-SART-FOI performs better than TV-OS-SART in the aspects of PSNR.

TABLE Ⅲ.
PEAK SIGNAL TO NOISE RATIO

Number of Iterations	1	2	3	4
TV-OS-SART	18.3031	19.0062	19.4554	19.8095
TV- OS-SART-FOI	18.3031	19.0062	19.4554	18.2894
Number of Iterations	5	6	7	8
TV-OS-SART	20.0907	20.2795	20.4719	20.5705
TV- OS-SART-FOI	20.5227	20.7569	20.8017	20.8174

5.3 The Number of Subsets is 8 for TV-OSEM-FOI

At the 4th iteration, in which the reconstruction images were shown in Fig.8,we adopt weight coefficient $a_x = a_y = 2$, $a = 0.9$,it can be seen in Fig.8 that TV-OSEM-FOI can still improve the brightness of the background and spherical area, while MSE becomes greater, just as shown in Fig.9.

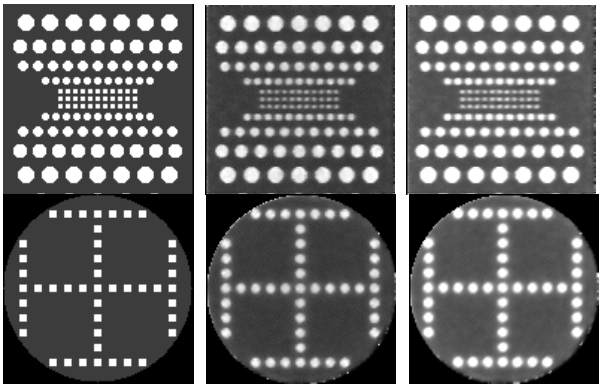


Figure 8. Slice of image at x=64 and z=86
Left: original model; middle: reconstruction by TV-OSEM
Right: reconstruction by TV-OSEM-FOI

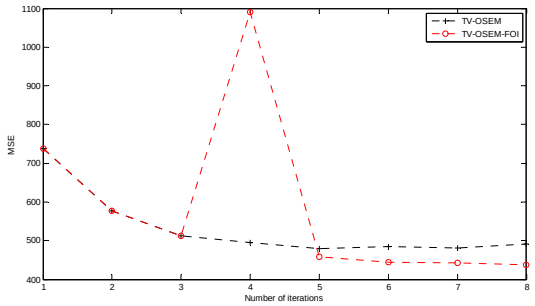


Figure 9 . Mean Squared Error

After the 4th iteration, TV-OSEM-FOI has faster convergence speed than TV-OSEM is shown in Fig.9.

At the 8th iteration, we adopt weight coefficients $a_x = a_y = 0.9$ $a = 2$ .The reconstruction images were shown in Fig.10,It can be seen in Fig.10 that the reconstructed image using our proposed TV-OSEM-FOI is in excellent agreement with the original model.

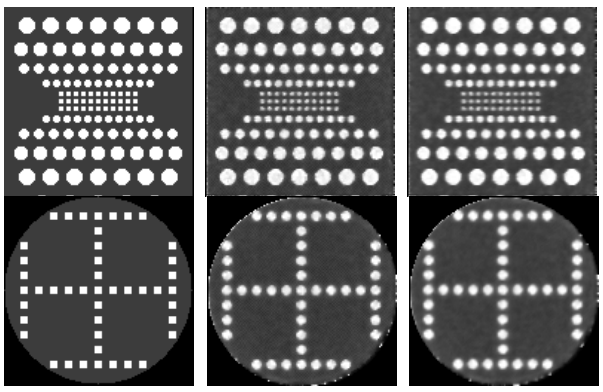


Figure 10 . Slice of image at x=64 and z=86
Left: original model; middle: reconstruction by TV-OSEM
Right: reconstruction by TV-OSEM-FOI

TABLE Ⅳ.
PEAK SIGNAL TO NOISE RATIO

Number of Iterations	1	2	3	4
TV-OSEM	19.4523	20.5147	21.0368	21.1885
TV- OSEM-FOI	19.4523	20.5147	21.0368	17.7510
Number of Iterations	5	6	7	8
TV-OSEM	21.3255	21.2702	21.3001	21.2057
TV- OSEM-FOI	21.5137	21.6533	21.6691	21.7073

From Table Ⅳ, we can see that the TV-OS-EM-FOI performs better than TV-OS-EM in the aspects of PSNR after 4th iteration .

5.4 The Number of Subsets is 4 for TV-OSEM-FOI

At the 4th iteration, we adopt weight coefficients $a_x = a_y = 1.8$, $a = 0.9$ .The reconstruction images were shown in Fig.11,it can be seen in Fig. 11 that TV-OSEM-FOI can improve the brightness of the background and spherical area, while MSE becomes greater, just as shown in Fig.12.

After 4th iteration , TV-OSEM- FIO has faster Convergence speed than TV-OSEM is shown in Fig.12.

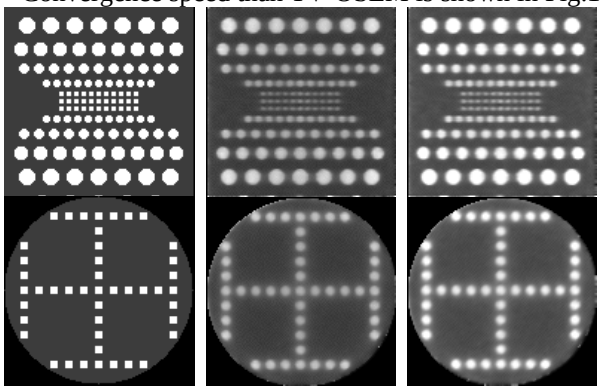


Figure 11.Slice of image at x=64 and z=86
Left: original model; middle: reconstruction by TV-OSEM
Right: reconstruction by TV-OSEM-FOI

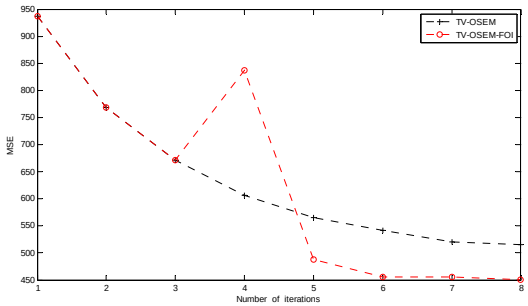


Figure 12 . Mean Squared Error

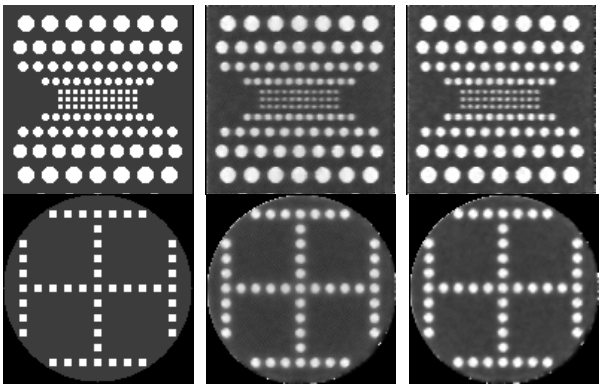


Figure 13. Slice of image at x=64 and z=86
Left: original model; middle: reconstruction by TV-OSEM
Right: reconstruction by TV-OSEM-FOI

At 8th iteration, we adopt weight coefficients $a_x = a_y = 0.7$, $a = 2.4$ .The reconstruction images were shown in Fig.13,it can be seen in Fig.13 that the reconstructed image using our proposed TV-OSEM-FOI is in excellent agreement with the original model.

TABLE Ⅴ.
PEAK SIGNAL TO NOISE RATIO

Number of Iterations	1	2	3	4
TV-OSEM	18.4119	19.2767	19.8612	20.2951
TV- OSEM-FOI	18.4119	19.2767	19.8612	18.8997
Number of Iterations	5	6	7	8
TV-OSEM	20.6070	20.7878	20.9571	20.0097
TV- OSEM-FOI	21.2412	21.5361	21.5387	21.5883

From Table Ⅴ, after 4th iteration, we can see that the TV-OSEM-FOI performs better than TV-OSEM in the aspects of PSNR.

VI. CONCLUSION

This paper introduces a fractional order integral approach for reconstructing image from noisy data. This method is addressed as TV-OS-IR-FOI. Experimental results show that TV-OS-IR-FOI has faster convergence speed and achieves higher PSNR than TV-OS-IR.

This TV-OS-IR–FOI is evaluated in numerical simulations, in the future, we shall research this approach from theory.

ACKNOWLEDGMENTS

The idea of iterative algorithm via fractional order integral was presented at the International Conference on Computational Intelligence and Security (CIS)2012,in this paper, the further computer simulations prove this idea is effective;

This project is supported by Tianjin Natural Science Foundation (12JCYBJC10600) and Scientific development Fund of Tianjin University of Technology and Education (KJ11-19, KJYB11-5)

REFERENCES

[1] B.D.Liu, L.Zeng, L.S.Li,“Iterative reconstruction algorithm of projection data truncation problem caused by the long chords of pipe wall ,”Chinese Journal of Scientific Instrument。32(1),2011,pp:52-56

[2] X.Li., J.Ni, G.Wang, “Parallel iterative cone beam CT image reconstruction on a PC cluster,”Journal of X-Ray Science and Technology, Number 13, 2005, pp:1-10

[3] X.B.Zou, “Improved Scanning and Approximate Reconstruction Algorithm of Cone-Beam Industrial CT,” Chongqing University,2007

[4] Z. Z. Zhang, Z. P. Guo, P.Zhang, X.G.Wang, “Technology and principle of industrial CT,”Beijing: Science Press:2009

[5] C.R. Vogel,“Computational Methods For Inverse Problems ,”SIAM, 2002

[6] D.J. Ji,, W.ZH.He. and X.B.Zou, “TV OS-SART with fractional order integral filtering,”2012 Eighth International Conference on Computational Intelligence and Security,Guangzhou, Guangdong,China,2012,pp:132-135.

[7] E.Y.Sidky, C.M.Kao and X.C.Pan., “Accurate image reconstruction from few-views and limited-angle data in

divergent-beam CT," Journal of X-Ray Science and Technology,14,2006,pp:119-139
[8] G.Wang and M.Jiang, "Ordered-subset simultaneous algebraic reconstruction techniques (OS-SART) ,"Journal of X-Ray Science and Technology, Number 12,2004, pp:169–177
[9] H. M. Hudson and R.S. Larkin, "Accelerated image reconstruction using ordered subsets of projection data," IEEE Trans on medical imaging, 13(4),1994,pp: 601-609
[10] H.Y.Yu and G.Wang,"A soft-threshold filtering approach for reconstruction from a limited number of projections,"Medical Physics, 55(13),2010,pp:3905-3916
[11] K. S.Miller and B.Ross, " An introduction to the fractional calculus and fractional differential equations," New York: John Wiley & Sons Inc,1993
[12] Y. F. Pu., "Research on Application of Fractional Calculus to Latest Signal Analysis and Processing ," Sichuan University,2006
[13] Y. F.Pu and W.X.Wang. "Fractional Differential Masks of Digital Image and Their Numerical Implementation Algorithms ," Acta Automatica Sinica, 33(11),2007,pp:1128-1135
[14] X. D.Zhang, G. D. Lu and J. Feng, "Fundamentals of Image Coding and Wavelet Compressing–Principles, Algorithm and Standards,"Beijing: Tsinghua University Press, 2004

Dongjiang Ji, male, 1979.3.lecturer.master
Research Direction: Computer Tomography and Image Processing

Wenzhang He, male, 1961.12. Professor, doctor,
Research Direction: Image Processing and Wavelet analysis.

An Ad Hoc Network Load Balancing Energy-Efficient Multipath Routing Protocol

De-jin Kong
Shanxi Finance and Taxation College, Taiyuan, China
Email: dejinkong@163.com

Xiao-ling Yao
Shanxi Finance and Taxation College, Taiyuan, China

***Abstract*—Multipath routing protocol establishes multiple transmission paths between source node and destination node, which can not only transmit data in parallel, but also one as main path and others as backup paths. The paper proposed a multipath routing protocol PL_AOMDV with power controlling and load balancing based on AOMDV. In order to implement load balancing and prolong network lifetime, it allocates traffic bandwidth based on node remaining power and load status along the path. Appropriate power is used to transmit data packets. As Ad hoc network is complicated and changeable, the proposed protocol conducts periodical routing maintenance to adjust bandwidth allocation of traffic in time. Simulation experiment results show that the improved PL_AOMDV protocol achieves better performance in the aspects of load balancing and average node lifetime.**

***Index Terms*—multipath routing, Ad hoc, power controlling, load balancing**

I. Introduction

Ad hoc has not wireless infrastructure, but runs in the manner of wireless multi-hop relay. For its high flexibility, mobility, self-organizations as well as access anytime and anywhere, Ad hoc has been widely used in various military and civilian fields of emergency relief, smart communications, environmental monitoring and etc. Ad hoc routing protocol has several classification methods. According to transmission path number between source node and destination node, it can be divided into single-path routing protocol and multi-path routing protocol. Single-path routing protocol means there is only one path between source and sink. Common single-path routing protocols include AODV [1], DSR [2], OLSR [3] and etc. The multi-path routing protocol establishes multiple transmission paths from source to destination, which can not only be sued for data transmission, but also one as main path and others as backup. The paper addressed to former situation. Typical multi-path routing protocols include AOMDV [4], SMR [5], MP-DSR [6], TBP [7] and etc. Among them, AOMDV is a kind of on-demand multi-path routing protocol expanded from AODV, the main idea of which is to build multiple independent paths between source node and destination node to implement parallel transmission of data.

The paper brings out a multi-path routing protocol with power controlling and load balancing PL_AOMDV. Similar as AOMDV, PL_AOMDV protocol should firstly establish multiple independent paths. Secondly, in order to balance node load and power as possible, it should allocate traffic among paths to achieve optimal traffic transmission mode. Finally, PL_AODMV protocol needs to control single hop transmission power to save precious energy. Among them, independence of multi-path is the first problem to be solved, which is also the premise to execute other traffic allocation algorithms or QoS resource reservation algorithms [8]. The paper is organized as follows. Section 2 gives establish method of PL_AOMDV independent path. Section 3 introduces implement strategy of protocol. Section 4 designs routing process of PL_AOMDV in detail. Section 5 performs simulation experiments and result analysis. Section 6 concludes our work.

Ⅱ. Establishment of PL_AOMDV Independent Paths

The independence of path is very important to multi-path routing. Stronger is independence of path, the network resource utilization can be more adequate and the node congestion probability is lower.

In the multi-path routing, independent paths can be divided into node disjoint paths and link disjoint paths [6]. Node disjoint path means there is not two same nodes in these paths. Link disjoint path refers to there is not same link along two paths. The paths not belong to these above two are un-disjoint. Generally, the number of node disjoint paths is less than that of link disjoint. However, the independence of node disjoint is better than that of link disjoint. Therefore, we try to establish node disjoint path. Various disjoint paths are shown from Fig. 1 to Fig. 3. Where, *S* is source node and *D* as the destination. The path *SACD* and *SEFG* in Fig. 1 are node disjoint paths. The *SABCD* and *SEBFD* in Fig. 2 are link disjoint paths. The SABD and SCBD in Fig. 3 are un-disjoint paths. In the Ad hoc, if un-disjoint multipath are used for data transmission, the nodes or links been commonly used by

doi:10.4304/jsw.9.1.246-250

paths can easily become a bottleneck, thus effect of traffic division cannot be achieved. If the common nodes failed, multiple paths will simultaneously breaking.

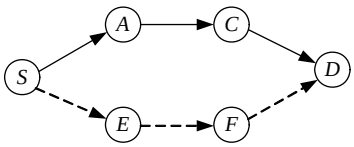


Figure 1. Node disjoint path

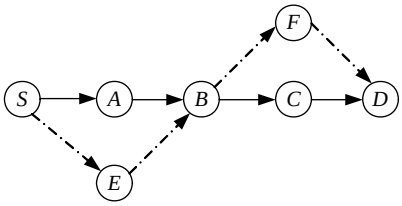


Figure 2. Link disjoint path

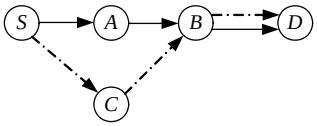


Figure 3. Un-disjoint path

In order to effectively establish multiple node disjoint paths and avoid consuming too much network resources, PL_AOMDV introduce the following theorem [9, 10].

Theorem 1: The path from source node S to destination D along all different adjacent nodes of S is node disjoint.

III. Implementation Strategies

A. PL_AOMDV Flow Distribution Manner

To implement traffic balancing, routing protocol should perform traffic allocation on built multiple paths. The traffic strategy in the paper is as following. In the routing searching, save bandwidth along the path and remaining power to routing reply packet. Source node computes traffic allocation of each path based on these two parameters. Here we will introduce computation method of bandwidth and power as well as traffic allocation strategy below.

The idle time of node in the channel is an important factor to measure effective bandwidth, which is comprehensively determined by traffic of node and its neighbors. Therefore, the effective bandwidth can be computed as follows:

$$B_{available}(i) = B_{\max} \times T_{idle} / T_{\text{int}erval} \tag{1}$$

Where, $B_{available}(i)$ is available bandwidth of node i; B_{max} is maximum transmission bandwidth of node; $T_{interval}$ is statistics interval; T_{idle} is idle time in channel statistics. We also use linear decreasing model to smoothen changes of bandwidth parameters:

$$B_{real}(i) = (1-\alpha) \times B_{real}(i-1) + \alpha \times B_{available}(i) \tag{2}$$

Where, $B_{real}(i)$ is real effective bandwidth at time i; $B_{real}(i\text{-}1)$ is the real bandwidth at time i-1; $B_{available}(i)$ is effective bandwidth at time i according to (1); α is the adjustable weight in the interval (0,1).

Remaining power of nodes along the path has important effect on path lifelong. The computation of energy bottleneck of path nodes should firstly obtain residual energy of each node, which can be directly obtained by checking battery of nodes.

As numerical level of available bandwidth and energy is magnitude, the paper unifies metric of residual bandwidth and energy before path reliability computation. Available bandwidth and energy were divided into eight different levels. The higher the level, the available resources are more abundant. The level of available bandwidth and energy are computed as follows:

$$L_B = floor(\max\_L \times B_{real}(i) / B_{\max}) \tag{3}$$

$$L_E = floor(\max\_L \times E_{real}(i) / E_{\max}) \tag{4}$$

Where, L_B and L_E are level of node bandwidth and residual energy; $E_{real}(i)$ is residual energy of node at time i; E_{max} is initial node energy; max_L is set 8; floor means floor function been used.

Assume the path from S to D is $(S, S_1, S_2, \cdots, S_i, \cdots, S_j, D)$. The L_B^i and L_E^i are used to represent available and residual energy of node S_i. The bandwidth L_{B_min} and energy bottleneck L_{E_min} can be obtained:

$$L_{B\_\min} = \min(L_B^i, i = 1, 2, \cdots, j) \tag{5}$$

$$L_{E\_\min} = \min(L_E^i, i = 1, 2, \cdots, j) \tag{6}$$

Assume source node S established k paths to destination node, reliability of the i-th path is

$$R_i = (L_{B\_\min} \times L_{E\_\min}) / hopCount\ . \tag{7}$$

Where, *hopCount* is hop number of the path. Allocate traffic on these k paths according to reliability, bandwidth of the i-th path is:

$$B_i = R_i / \sum_{j=1}^{k} Rj \tag{8}$$

It is worth noting disorder of packets of multi-path in TCP flow transmission [8]. We use different method to process different traffic. If some node needs to transmit UDP, it will be divided to be transmitted along different paths, others being backup.

B. PL_AOMDV Transmit Power Control

Ad hoc is a restricted network. Once power energy of node is exhausted, it will directly affect implementation of network functions.

In the case of no power-aware, packet is transmitted with maximum power. If power control is added in MAC and each hop be transited with appropriate power, node energy consumption can be inevitably reduced. Meanwhile, as data packet transmission range being smaller, interference among nodes also inevitable reduces. The messages in MAC can be broadly divided into broadcast massage and unicast message. PL_AOMDV

protocol transmits broadcast message with maximum power and unicast message with appropriate power.

For example, if node *A* and *B* are neighbor nodes and *A* needs to transmit to *B*, *A* sends RTS with maximum power P_{max}. After *B* received RTS from *A*, it will send CTS with P_{max}. When node *A* received CTS, it computes data transmission power P_{data_send} according to receiving power $P_{receive}$ and transmitting power P_{max}.

$$P_{data\_send} = \frac{P_{\max}}{P_{receive}} \times P_{threshold} \times c \quad (9)$$

Where, $P_{threshold}$ is the necessary power for correctly receiving; c is a constant to prevent too small power to receive data, which is generally set $c>1$. As P_{data_send} is smaller than P_{max}, it can save data transmitting power by power controlling.

IV. PL_AOMDV Routing Process

A. Routing Discovery

In order to implement node disjoint path and traffic controlling, we should firstly expand format of routing control packet and routing table package of AODV protocol. Firstly, expand format of RREQ. Add next hop node address SN field of source node in RREQ to record first neighbor node address of source node. At the same time, add bandwidth BW field and residual energy LE filed to record bottleneck of forward routing. Secondly, expand routing table. Add source address SA, bandwidth BW, residual energy LE items in routing table. Thirdly, destination node maintain node neighbor list list(sn) to record source node address SA and neighbor node address SN in RREQ. Add fields of BW and LE in RREP to record reverse routing bottleneck.

- RREQ packet processing

When node s needs to communicate but there is not available routing, it initiate routing discovery process to broadcast routing request RREQ to all neighbors. The fields of BW and LE in RREQ packet are initialed values of source node.

After intermediate node i received RREQ packets, it determines whether received repeated packet with same source address, destination address and request ID in source neighbor address field SN in time of path_traversal_time.

After all intermediate nodes received RREQ for first time, compare bandwidth and residual energy of this node with BW and LE in RREQ. If current value is smaller than that in packet, the node may become bottleneck. Update value of current node to RREQ packet. When intermediate node received request packet with same destination address from different source nodes, establish different routing items for different source nodes. Other routing update mechanism and forward mechanism of intermediate node are same as that of AODV.

When destination node received RREQ, it will extract source address SA and neighbor address SN and determine whether SA and SN from packet in list(sn). If so, directly discard the packet. Otherwise, add (SA, SN) into list(sn) and establish reverse path with source node. Send routing reply packet RREP to source node. As to same source node, PL_AOMDV protocol at most establishes three paths.

- RREP packet processing

The BW and LE fields in RREP are used to record bottlenecks from current node to destination node, which is different from bottleneck to destination node. Therefore, the BW and LE fields in RREP are initialized as value of destination node.

The processing method of intermediate node after received RREP packet is substantially same as that of RREQ, namely compare bandwidth and residual energy of this node with BW and LE in RREP. If value of this node is smaller than that in packet, update node value into packet. Otherwise, do not update. All nodes received RREP should establish forward path for source node and record bandwidth and energy bottleneck to destination node. Then, it forwards RREP.

After source node received multiple RREP, it extracts BW and LE fields in order to establish routing items to destination node.

B. Routing Maintenance Process

Ad hoc network has complex characteristics. After source node traffic transmission, nodes along transmission paths may access new traffic or shift to region with poor bandwidth resources. Bandwidth and energy bottleneck of each path will inevitable change as time. If the source node still allocate traffic according to situation in routing establishment, it is obviously very unreasonable. Therefore, PL_AOMDV protocol added periodic routing maintenance on paths to find network congestion or node energy change in time, so as to achieve bandwidth allocation of traffic adjustment.

PL_AOMDV adds periodic routing maintenance process. In the routing discovery phase, destination node builds a timer once receiving first RREQ of source node. The timer is responsible for periodic routing maintenance to this source node. We call it as routing maintenance timer. When the timer expires, if this path still active recently, destination node firstly add ID of this node and then send RREP along multiple paths to source nodes. After source node received RREP, it updates BW and LE information of this packet to routing table. In case of source node sending packets to destination node in next time, if allocates traffic in accordance with new parameters.

We uses destination node to maintain paths. The benefit is that overhead of destination node sending path maintenance information to source node directly is less than source node send to destination and then return. However, it should ensure the path from source to destination is same as that from destination to source. Otherwise, the obtained bandwidth and bottleneck is not real value along transmission path. The references [11-13] have proved that the established path with theorem 1 can meet above conditions.

The processing on path failure of PL_AOMDV is similar to that of AODV. After intermediate node find path failure to destination node, it firstly send path failure message to source node and delete reverse paths to source

node. If upper hop of some intermediate node to destination node, it send path failure message to source node and delete reverse paths to destination node. After source node and destination node along this path received message, delete path in routing table respectively. Different from AODV, if there is available path to destination node in the routing table of source node, PL_AOMDV does not perform route recovery operation till there is no available path from source to destination node.

V. Simulation Experiment and Result Analysis

A. Simulation Scenario

We designed simulation experiment on PL_AOMDV protocol with NS-2.33 platform under Linux operation system. In the simulation, the terrain was set plane network of 800m × 800m; node number 20; MAC protocol as IEEE 802.11DCF; signal propagation manner as dual-diameter ground reflection model; node maximum communication range as 250m; channel bandwidth 2Mbps. The initial energy of all nodes was set same value. Data packet length is 512Byte and simulation time as 800s. The constant UDP bit stream was used to simulate real-time traffic and 8 connections were initiated randomly. We select the following performance parameters to evaluate algorithm.

(1) Node number of energy exhausted.

(2) Average lifespan of first half dead nodes.

(3) Control overhead.

In order to validate PL_AOMDV performance, the paper simulated AODV protocol and AOMDV protocol with same moving speed under same conditions. The AOMDV protocol in experiment is transmitted in parallel with multiple paths and at most three decile paths been established. Compared with PL_AOMDV, the simulated AOMDV protocol has not power controlling and traffic allocation.

B. Result Analysis

The relation between dead node number and elapsed time reflects uniformity of the energy consumption of each node. If the image is steeper, it indicates that life cycle of each node in the network has greater difference and energy consumption more uneven. On the contrary, if the image is gentler, each node survival smaller the difference between the consumption of energy is more uniform, network because the node energy is exhausted and the probability of splitting the smaller. At the same time, since the node of the energy consumption and the node load substantially proportional, the node energy consumption also reflects the degree of load balancing in the network, the node energy consumption is more uniform, and the network load is more balanced.

Fig. 4, Fig. 5 and Fig. 6 show relations between dead node number and elapsed time at moving speed of 0m/s, 2m/s and 5m/s. After comparison, we can know that the curves of AODV are relatively steep. The curve of AOMDV is slightly better than that of AODV, they are also very steep. It suggests that node energy consumption of AODV and AOMDV has large difference. The curve of PL_AOMDV protocol is also on the top of that of AOMDV and AODV. Meanwhile, the PL_AOMDV is relatively smooth, which indicates node energy consumption of PL_AOMDV is more uniform than AOMDV and AODV. We can also know from these three images that PL_AOMDV protocol can reach energy and load evenly at different moving speed.

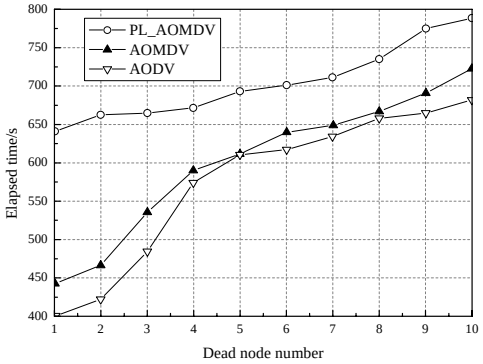


Figure 4. Relationship between dead node and elapsed time at 0m/s

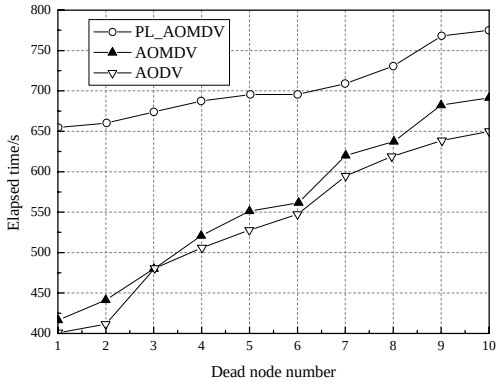


Figure 5. Relationship between dead node and elapsed time at 2m/s

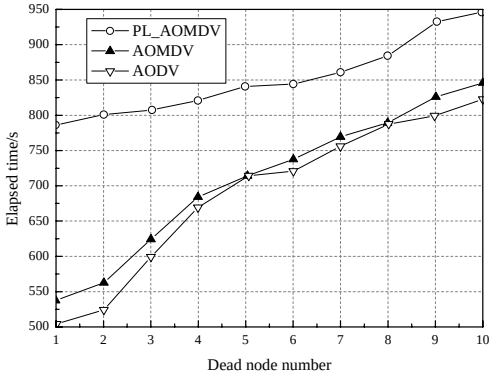


Figure 6. Relationship between dead node and elapsed time at 5m/s

Fig. 7 shows average life of first 10 dead nodes from experiment in Fig. 4 to Fig. 6. Under different moving speeds, average life of first half dead nodes in PL_AOMDV protocol delay 2%-5% than that of AOMDV and AODV, while PL_AOMDV prolongs 12%-18% than AODV, which means PL_AOMDV can also achieves energy saving with power controlling.

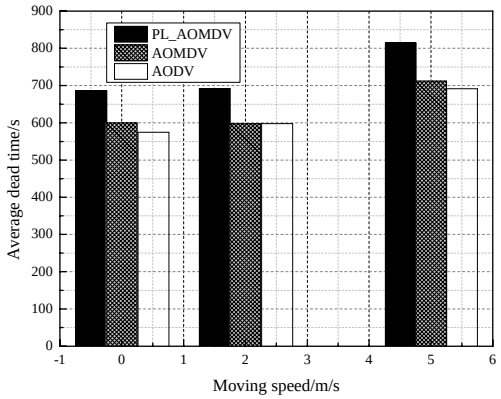


Figure 7. Average life of first 10 dead nodes

Fig. 8 shows comparison of network overhead. As PL_AOMDV adds bandwidth and energy parameters in routing packet as well as periodic network maintenance mechanism, the overhead of PL_AOMDV is slightly increased than AOMDV, but still less than that of AODV. Seen from performance of energy and load balancing, the increased overhead is worthy.

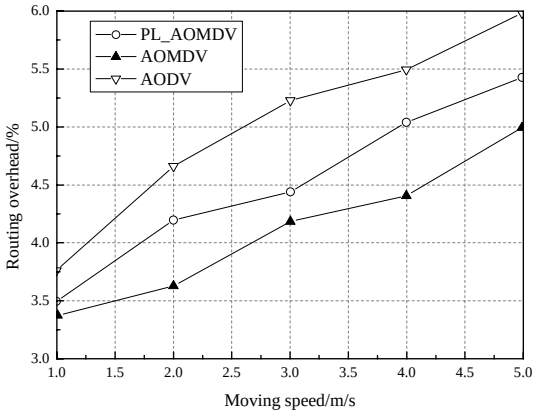


Figure 8. Network overhead comparison

VI. CONCLUSION

The paper improved on AOMDV protocol to bring out a multi-path routing protocol PL_AOMDV with power controlling and load balancing. It established multiple node disjoint paths between source node and destination node to implement parallel data transmission. The protocol allocates bandwidth according to residual energy and load bottleneck so that path load and residual energy balanced roughly, so as to reduce probability of failure caused by node energy exhausted and prolong overall connectivity. As Ad hoc is complex and volatile, the established path may shift to region with poor bandwidth resources and node bottleneck may change, PL_AOMDV adds periodic routing maintenance to adjust bandwidth allocation in real-time. In addition, PL_AOMDV protocol transmits data packets with appropriate energy in case of data transmission to avoid using maximum power and save node energy. Simulation experiment with NS-2 shows that the improved PL_AOMDV protocol better network performance in aspects of load balancing and average node lifespan. In the next working, we will further analyze various traffic allocation algorithms to provide theoretical basis for further improvement.

REFERENCES

[1] Perkins C. E., Royer E. M., "Ad-hoc on-demand distance vector routing", *Proceedings of 1999 Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 99)*, Feb 25-26, pp. 90-100, 1999.

[2] Lei Wang, Lian-fang Zhang, Yan-tai Shu, Miao Dong, "Multipath source routing in wireless ad hoc networks", *Proceedings of 2000 Canadian Conference on Electrical and Computer Engineering*, pp. 479-483, 2000.

[3] Jacquet P., Muhlethaler P., Clausen T., Laouiti A., Qayyum A., Viennot L., "Optimized link state routing protocol for ad hoc networks", *Proceedings of 2001 IEEE Multi Topic Conference on Technology for the 2st Century (INMIC)*, pp.62-68, 2001.

[4] Mateen W., Raza S., Uzmi Z. A., Baqai S., "Adaptive multi-path on-demand routing in mobile ad hoc networks", *Proceedings of Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*, pp.237-244, 2005.

[5] Lee S. J., Gerla M., "Split multipath routing with maximally disjoint paths in ad hoc networks", *Proceedings of IEEE International Conference on Communications (ICC 2001)*, pp.3201-3205, 2001.

[6] Rashida Hashim, Qassim Nasir, Saad Harous, "Adaptive Multi-path QoS Aware Dynamic Source Routing Protocol for Mobile Ad-Hoc Network", *Proceedings of 2006 Innovations in Information Technology*, pp. 1-5, 2006.

[7] Leung R., Ji-lei Liu, Poon E., Chan A.L.C., Bao-chun Li, "MP-DSR: a QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks", *Proceedings of 26th Annual IEEE Conference on Local Computer Networks*, pp.132-141, 2001.

[8] Shigang Chen, Nahrstedt K., "Distributed quality-of-service routing in ad hoc networks", *IEEE Journal on Selected Areas in Communications*, vol.17, no.8, pp. 1488-1505, 1999.

[9] Cheng-yong Liu, La-yuan Li, Yang Xiang, "Research of Multi-Path Routing Protocol Based on Parallel Ant Colony Algorithm Optimization in Mobile Ad Hoc Networks", *Proceedings of Fifth International Conference on Information Technology: New Generations (ITNG 2008)*, pp.1006-1010, 2008.

[10] Ramesh V., Subbaiah P., "Preemptive AOMDV routing for mobile Ad-hoc networks", *Proceedings of International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2011)*, pp. 622-625, 2011.

[11] Yang Qin, Wen Y.Y., Ang H.Y., Choon Lim Gwee, "A routing protocol with energy and traffic balance awareness in wireless ad hoc networks", *Proceedings of 2007 6th International Conference on Information, Communications & Signal Processing*, pp.1-5, 2007.

[12] Yao-guo Wang, Jin Liu, "Improving TCP Performance of Mobile Ad hoc Networks by Back-up Multi-path Routing", *Journal of Convergence Information Technology*, vol. 7, no. 23, pp. 18-24, 2012.

[13] Rui Yang, Ying Song, Gui Chao, Bao-lin Sun, "Energy Entropy-Aware Multipath Routing Algorithm in MANET", *International Journal of Advancements in Computing Technology*, vol. 4, no. 15, pp. 287-294, 2012.

A Model-Based Fault Detection Framework for Vacuum Circuit Breaker by Trip Coil Analysis

Yuhuang Zheng[1,2,3]
1.Department of Physics, Guangdong University of Education,Guangzhou, 510303, China
2. School of Mechanical and Automotive Engineering, South China University of Technology,Guangzhou, 510640, China
3. Guangdong Zhujiang Switchgear Co. ,Ltd. Foshan, 528200, China
Email: zhyhaa@126.com

***Abstract*—Vacuum circuit breaker becomes more and more complicated, integrated, high-speed and intellectualized. To insure vacuum circuit breaker in its good conditions, the function of fault diagnosis gets more important than before in the process of repairing. This paper is addressed a model-based fault detection framework for vacuum circuit breaker by trip coil analysis. At first, the electromagnetic model of the trip coil is built. Secondly, algorithm of abrupt changes detection and dynamic time warping algorithm is introduced. At last, value comparison between the similarity and the threshold concludes whether a fault has occurred or the trip coil has potentially hazardous effects. The experimental results show that this method is effective.**

***Index Terms*—Vacuum Circuit Breaker (VCB), Fault Diagnosis, Dynamic Time Warping (DTW)**

I. INTRODUCTION

Circuit breakers must be fully operational and available at all times. Now circuit breakers are the important system protection assets which should be in condition assessment and performance monitoring. Therefore, any risk of dangerous situations could be surely reduced. In such complex system of vacuum circuit breaker, fault diagnosis plays a vital role. A fault in a system will lead to economic losses. Therefore, fault diagnosis must be done correctly and efficiently. Fault diagnosis is performed when a vacuum circuit breaker is malfunctioning and is to determine the cause responsible for a set of observed symptom [1-3]. One practical predictive maintenance approach is based on the trip coil current.

The trip coil is an electromagnetic actuator which when energized causes an armature to strike and release the trip latch. It can be seen therefore, that while current flowing through the coil affects a force upon the armature, the movement of the armature through the coil generates an electromagnetic field in the coil, which in turn has an effect upon the current flowing through it [4]. The method identifies the critical time instants in the trip coil current, to be used for diagnostic analysis [6-7]. The shape of the coil current characterizes the operating health of the breaker to a greater extent. The shape is influenced by both the electrical parameters of the control circuit and the mechanical movement of the armature. The characteristic behavior of the trip coil in a circuit breaker must be analyzed and modeled before the trip coil can be predictive maintenance. [8-10]

We address a model-based fault detection framework for vacuum circuit breaker by trip coil analysis in this paper. At first, we build the electromagnetic model of the trip coil. Secondly, we introduce the algorithm of abrupt changes detection to get the key points and the DTW algorithm to compute the similarity value of the trip coil current between the test data and the theoretical results. At last, if the similarity value is larger than the threshold value, comparison concludes that a fault has occurred or the trip coil has some potentially hazardous effects. The results of experiment show the diagnosis methodology is accurate and reliable. Such a model-based fault detection framework helps to increase the reliability and availability of the vacuum circuit breaker by reducing the number of shutdowns that are necessary for systematic maintenance.

II. THE DYNAMIC MODEL OF TRIP COIL

The electrical schematic of the ideal trip coil is given in Fig.1. The trip coil has an inductance $L(x)$ and a resistance R. The voltage u applied to the coil results in a current i governed by the differential equation [3-4]. The trip coil has an inductance $L(x)$ and a resistance R in series. The voltage u is applied to the coil results in a current i governed by the equations (1)-(4). The dynamic model of the trip coil in a vacuum circuit breaker is presented by means of solving these functions. Table 1 is these variables in representation.

Manuscript received May 10, 2013; revised June 15, 2013; accepted July 20, 2013.

doi:10.4304/jsw.9.1.251-257

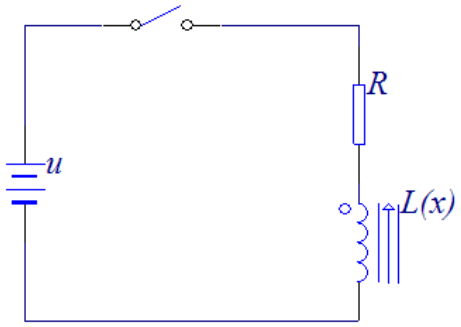


Figure.1 An electrical schematic of the ideal trip coil.

TABLE I.
VARIABLES REPRESENTATION IN THE DYNAMIC MODEL OF TRIP COIL

Variables	Variables Representation
x	an effective displacement of the armature
$L(x)$	inductance of the trip coil with the armature displacement x
R	resistance of the trip coil
i	the trip coil current
u	supply voltage of the trip coil current
m	mass of the armature
k	coefficient of the spring rigidity
F_e	electrodynamic force of the trip coil
v	the armature velocity
a	the armature acceleration
f_0	the friction force of the armature movement
t_0	the time when supply voltage u being applied
t_1	the time when the coil current starts rising
t_2	The time that end of armature movement

$$u = Ri + L(x)\frac{di}{dt} + vi\frac{dL(x)}{dx} \tag{1}$$

The balance equation of forces acting on the armature of a mass m is as follows:

$$F_e - kx - f_0 = m\frac{dv}{dt} \tag{2}$$

$$F_e = \frac{1}{2}i^2\frac{dL(x)}{dx} \tag{3}$$

$$\frac{dx}{dt} = v \tag{4}$$

The simulation of the close coil is performed by means of the Matlab 2012 with Simulink(Fig. 2). A simulation model is made in Simulink basing on Equ.1-Equ.4. This model is used to simulate the mathematical model of the close coil. The simulation results in obtaining time curves of the coil current i. The course of current i changes over time displays the way in which the electromagnetic force of the coil is controlled. The simulation curve is shown in Fig.3.

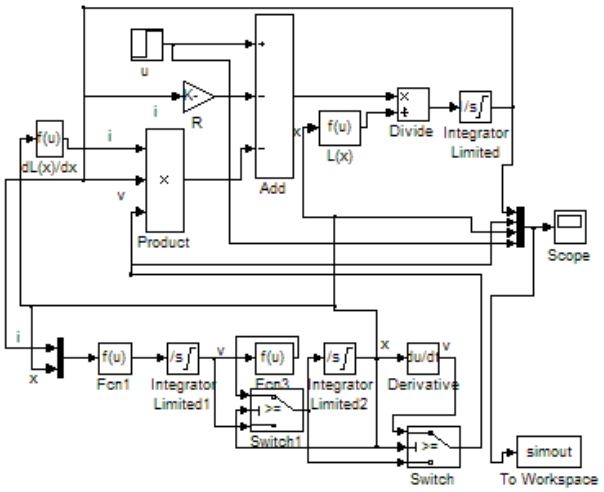


Figure.2 Simulation model

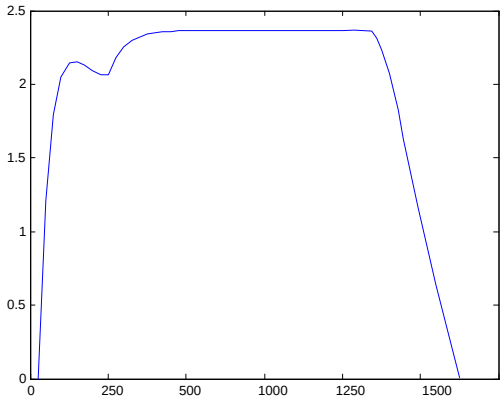


Figure.3 Result of simulation

III. A MODEL-BASED FAULT DETECTION FRAMEWORK

The problem of fault detection for a trip coil in VCB involves two aspects. Firstly, the detection of failures should be achieved. Secondly, the detection of smaller faults, which affect a trip coil without causing it to stop. And this is also required to prevent the subsequent faults. Both faults and failures in a trip coil can be approached in the abrupt change detection [11-12]. Algorithm of abrupt changes detection is the core of the fault detection framework.

Algorithm of abrupt changes detection is a powerful new tool for determining whether a change has taken place. It is capable of detecting subtle changes by three steps, which are data smoothing, change-point detection, and potential hazards detection. Data smoothing is used to eliminate "noise" and extract real trends and patterns of the trip coil current. Change-point detection is to discover time points at which properties of the trip coil current change. Finally, potential hazards detection is to scan for potential hazards of the trip coil and accidents in a vacuum circuit breaker can be avoided.

A. Data Smoothing

An input sampling sequence of the trip coil current with a fixed sampling rate is $i = \{i_1, i_2, \ldots, i_t\}$. Data smoothing produces a "smooth" set of values from the

trip coil current which has been contaminated with noise. The LOWESS smoothing is introduced in this abrupt changes detection. LOWESS smoothing is an improvement over least squares smoothing when the data are not equally spaced. The following is a brief sketch of the LOWESS algorithm [13-15].

- **Step1:** Choose a fraction *f* of the data points which is to be used for computation of each fitted value. Let *b* be the nearest integer to *f.t*/2 where *t* is the size of the data *i*. In other words, 2.*b* is the number of points around each element of *i*, to be used for fitting. We choose *f*=0.01.
- **Step2:** Let d_i be the distance from i_x to its b_{th} nearest neighbor along the *i* axis and *T* be the weight function. Then the weight w_k given to the point (k, i_k) when computing a smoothed value at i_x, is as follows:

$$w_k = T\left(\frac{x_i - x_k}{d_i}\right), T(u) = \begin{cases} (1-|u|^3)^3, |u| < 1 \\ 0 \quad , |u| \geq 1 \end{cases} \tag{5}$$

- **Step3:** To compute the fitted value at i_x weighted least squares fit is obtained.

$$b_{estimate} = \frac{\sum w_x^2 (2x - t - 1)(k - \bar{i})}{2\sum w_x^2 (k - \bar{i})^2} \tag{6}$$

$$a_{estimate} = \bar{i} - \frac{1}{2} b_{estimate}(t+1) \tag{7}$$

$$i_x^s = a_{estimate} + b_{estimate} i_x \tag{8}$$

And the smoothing set is $i^s = \{i_1^s, i_2^s, \ldots, i_t^s\}$.

B. Change Points Detection (CPD)

We now describe the Change Points Detection (CPD) process that guarantees that the required change points are got. In the proposed method, we have selected extrema information as the feature vector. To reduce the detection time, the extrema are extracted from the smoothed data. This procedure consists of three components, one accounting for the finding extrema process, one accounting for computing Euclidean distances among all extrema and the other accounting for the clustering problem of the Euclidean distances.

In the first component, we want to determine all extrema of given trip coil current data. To do this, we use Golden Section Search, which is an elegant and robust method of locating all extrema in trip coil current data. The book [16] is shown that this method is available for use. We can get the set of extrema

$i^e = \{\cdots, i_j^s, i_k^s, \cdots, i_p^s, i_q^s, \cdots\}$.

In the second component, we compute Euclidean distances between two of closet extrema. For example, in time *p*, the Euclidean distance between i_p^s and i_q^s is d_p.

$d_p = \sqrt{(p-q)^2 + (i_p^s - i_q^s)^2}$.

And we can get the set of Euclidean distances

$d = \{\cdots, d_j, \cdots, d_p, \cdots\}$.

In the third component, in order to detect the key change points, the set of Euclidean distances *d* is processed using clustering method. Euclidean distances d are grouped into two clusters: "change points" and "normal points". K-Means is a rather simple but well known algorithm for grouping objects, clustering. Using the kernel K-Means clustering algorithm, the elements in *d* are clustered into "change points" cluster i_{cp} and "normal points" cluster i_{np}.

$i_{cp} = \{\cdots, d_p, \cdots\} \xrightarrow{p} \{\cdots, i_p, \cdots\}$

$i_{np} = \{\cdots, d_j, \cdots\} \xrightarrow{j} \{\cdots, i_j, \cdots\}$

The Change Points Detection algorithm is illustrated in Table 2.

C. Dynamic Time Warping Fault Detection

Dynamic time warping (DTW) is an algorithm for measuring similarity between two sequences which may vary in time or speed. DTW has been applied for the data which can be turned into a linear representation. And DTW can be used in partial shape matching application. For details of DTW algorithm, please see [17-18].

Suppose we have two current series, an input sequence *Q* of length *n*, and a temple sequence *C* of length *m*, where

$Q = q_1, q_2, \ldots, q_i, \ldots, q_n$

$C = c_1, c_2, \ldots, c_j, \ldots, c_m$

To align these two sequences using DTW, we first construct an *n*-by-*m* matrix where the (i_{th} , j_{th}) element of the matrix corresponds to the squared distance,

$$d(q_i , c_j) = (q_i + c_j)^2 \tag{9}$$

which is the alignment between points q_i and c_j. To find the best match between these two sequences, we retrieve a path through the matrix that minimizes the cumulative total distance between them. In particular, the optimal path is the path that minimizes the warping cost

$$Path(Q,C) = \min\left\{\sqrt{\sum_{k=1}^{K} w_k}\right. \tag{10}$$

Where w_k is the matrix element $(i,j)_k$ that also belongs to k_{th} element of a warping path, a contiguous set of matrix elements that represent a mapping between *Q* and *C*.

This warping path can be found using dynamic programming to evaluate the following recurrence

$r(i, j) = d(i, j) + \min\{r(i-1, j-1), r(i-1, j), r(i, j-1)\}$

where $d(i,j)$ is the distance found in the current cell, and $r(i,j)$ is the cumulative distance of $d(i,j)$ and the minimum cumulative distances[19-21].

In this type of fault detection technique, the theoretical data is converted to templates. The diagnosis process consists of matching the test data with stored templates. A fault is detected if the distance is larger than the threshold value. The distance is based upon dynamic programming. This is called the DTW fault detection.

The implementing processes of the fault detection method are illustrated in Fig 4.

TABLE II.
CHANGE POINTS DETECTION ALGORITHM

Step	ALGORITHM : Change Points Detection
1:	**Input:**
2:	trip coil current *i;*
3:	**Output:**
4:	change points i_{cp};
5:	**Functions:**
6:	LOWESS smoothing function: LOWESS()
7:	Locating all extrema function: extrema ()
8:	Computing Euclidean distances function: Euclidean ()
9:	K-Means clustering function: K-Means ()
10:	**Algorithm:**
11:	Smoothed Data i^s= LOWESS(i);
12:	Smoothed Data extrema i^e= extrema (i^s);
13:	Euclidean distances d= Euclidean(i^e);
14:	change points i_{cp} = K-Means (d);

IV. EXPERIMENT

The experimental system includes hardware composition and software system used for trip coil current signal acquisition and fault detection software. The system offers PC-Based oscilloscope that have the performance and features necessary to monitor trip coil current waveform data.

ACS712 is a linear current sensor. The device consists of a precise, low-offset, linear Hall sensor circuit. Applied current flowing through this copper conduction path generates a magnetic field which is sensed by the integrated Hall IC and converted into a proportional voltage. Device accuracy is optimized through the close proximity of the magnetic signal to the Hall transducer. A precise, proportional voltage is provided by the low-offset, chopper-stabilized BiCMOS Hall IC, which is programmed for accuracy after packaging. The output of the device has a positive slope when an increasing current flows through the primary copper conduction path, which is the path used for current sensing.[22]

The data acquisition platform uses DSO3064 digital oscilloscope which has 4 Channels Oscilloscope,60MHz Bandwidth, 200MS/s sampling rate and 10k--16M memory depth. The software environment consists of Matlab and a newly developed fault diagnosis library. (Fig.5)

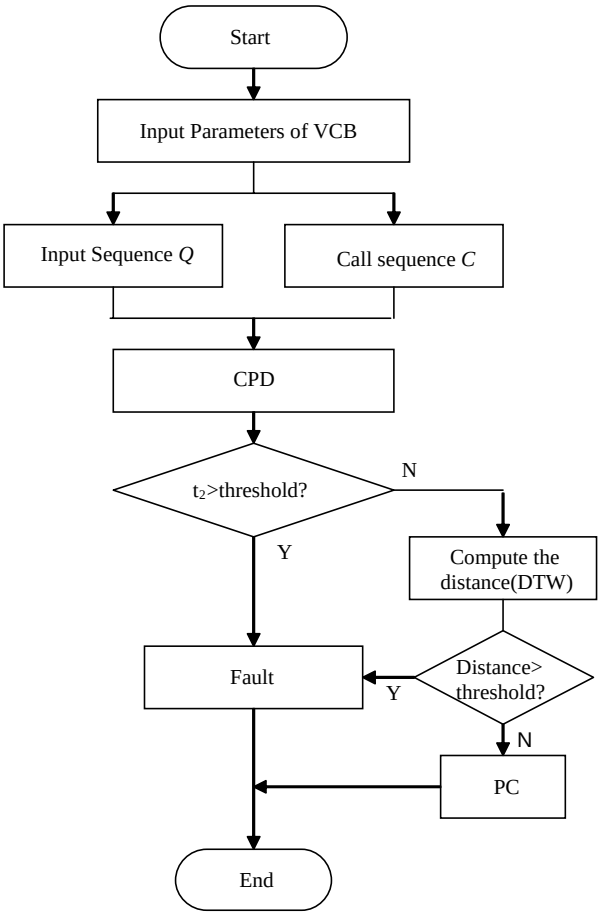


Figure.4 the implementing processes of the fault detection method

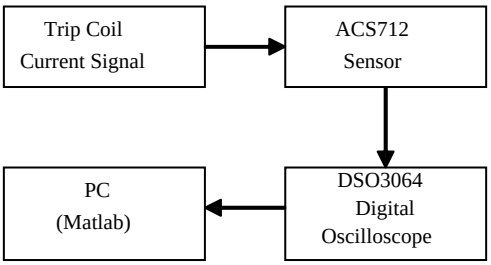


Figure.5 Experimental system

A. Change Points Detection Experiment

We sample the sequence of the trip coil current with a fixed sampling rate 50 kHz. The sequence is shown in Fig. 6(a). In this sequence, the true signal amplitudes changes rather smoothly as a function of the time values, whereas many kinds of noise are seen as rapid, random changes in amplitude from point to point within the signal. We attempt to reduce the noise by LOWESS smoothing. In this smoothing, the sequence of the trip coil current is modified so that individual points that are higher than the immediately adjacent points are reduced, and points that are lower than the adjacent points are increased. This leads to a smoother sequence and it is shown in Fig. 6(b).

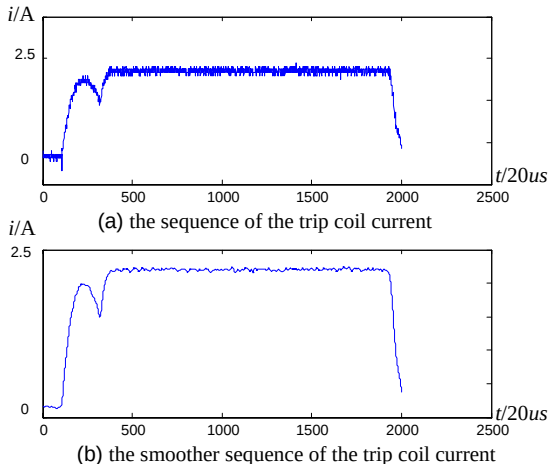


Figure.6 LOWESS smoothing

The CPD algorithm requires the identification of all local extrema in the smoother sequence. Fig.7 shows performance results of the algorithm for identification of extrema.

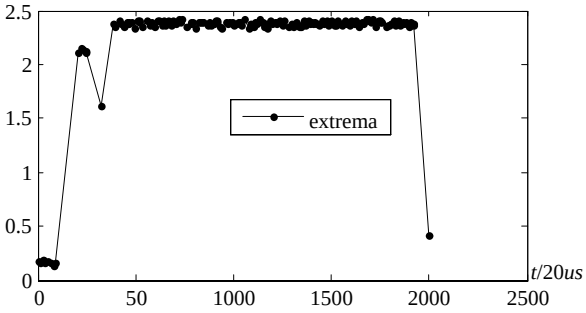


Figure.7 Identification of extrema

By computing the Euclidean distances between these extrema, we obtain the distance sequence shown in Fig.8.

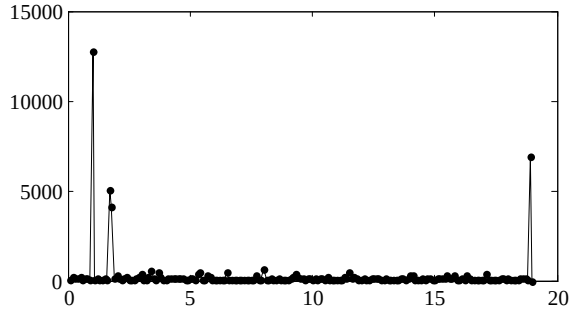


Figure.8 Distance sequence

Cluster distance sequence into two disjoint subsets which are shown in Fig.9.We get the key points in the sequence of the trip coil current by the change point's subset in Fig.10.

B. DTW Fault Detection Experiment

This experiment presents the analysis of current signals to identify and quantify common faults from a trip coil based on DTW algorithm. Experimental data sets of normal signal and abnormal signal have been studied using DTW algorithm. We can obtain better fault detection and diagnosis results, as depicted in Fig. 11 and 12. Results show that the method is effective.

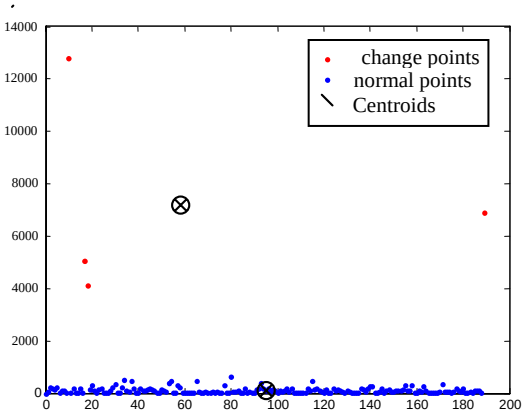


Figure.9 K-Means Clustering

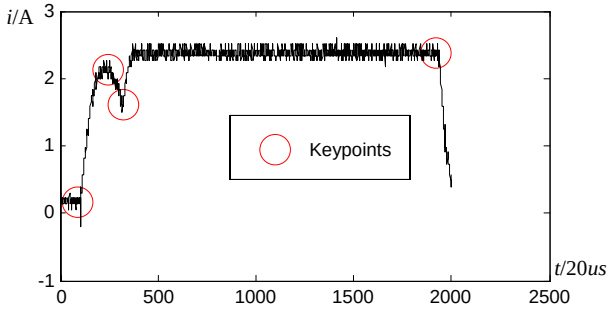


Figure.10 the key points in the sequence of the trip coil current

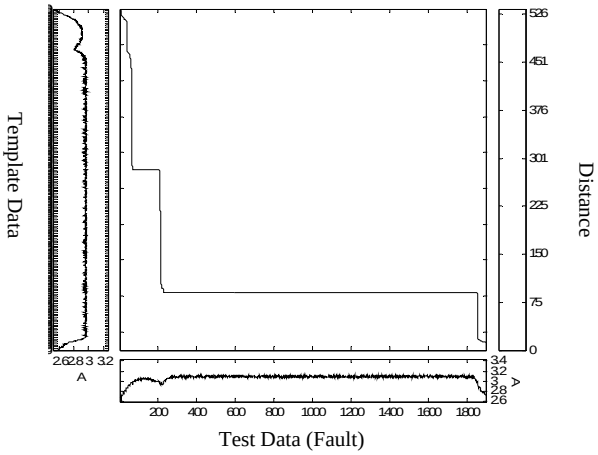


Figure. 11 Abnormal signal

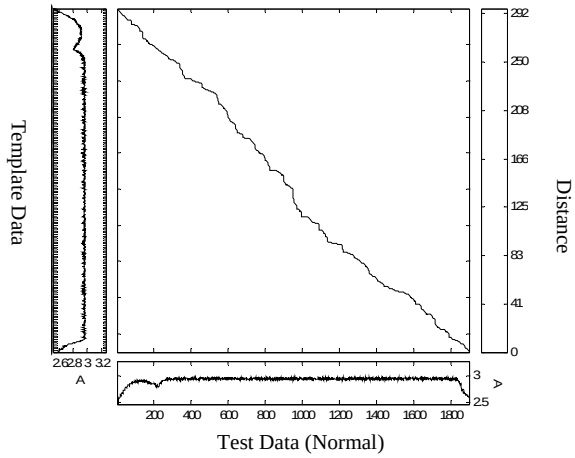


Figure. 12 Normal signal

V. CONCLUSIONS

This paper summarizes the key features of the model-based fault detection framework for vacuum circuit breaker and the methodology scheme is proposed. At first, the mathematical model has been developed for the dynamic characteristics of the close coil. The results of simulation show that the accuracy of the dynamic-state model equations is satisfactory. Secondly, the algorithm of change points detection for applications in fault detection for a trip coil is presented. The algorithm includes three parts which are data smoothing, extrema search and K-Means clustering. Fault analysis processing is based on dynamic time warping technology. Thirdly, fault analysis processing is based on dynamic time warping technology and the change points detection algorithm. Experimental results prove the effectiveness of the methodology in the vacuum circuit breaker fault detection.

ACKNOWLEDGMENT

This project is funding by Appropriative Researching Fund for Professors and Doctors, Guangdong University of Education (No. 11ARF04). This project is funding by ministry of education of China (MCM20121051), higher school science and technology innovation project of Guangdong Province (No. 2012KJCX0079), Economic and Information Technology Commission Project of Guangdong Province (No. GDEID2011IS064) and Dongguan City (No.DG201101).

REFERENCES

[1] B.V.Klimenko, “The control of polarized bistable electromagnetic actuators of medium voltage vacuum circuit breakers“, *Russian Electrical Engineering*, Vol.83, pp.243-248, May 2012.

[2] Y. Luo, X. Duan and Z. Tian, “Status Monitoring and Digital Communication of the Intelligent Vacuum Circuit Breaker in Smart Grid”, *Journal of Computational Information Systems*, Vol. 21, pp.8707-8715, August 2012.

[3] S. M. Strachan, S. D. J. McArthur, B. Stephen, J. R. McDonald and A. Campbell, “Providing Decision Support for the Condition-Based Maintenance of Circuit Breakers Through Data Mining of Trip Coil Current Signatures”, *IEEE Trans. on Power Delivery*, Vol.22, pp.178-186, January 2007.

[4] S. Beattie, "Circuit breaker condition assessment by vibration and trip coil analysis ",*IEE Colloquium on Monitors and Condition Assessment Equipment*, pp.1-5, December 1996.

[5] B. Falahati, Z. Darabi, Mirrasoul J. Mousavi and Y. Fu, “Stochastic Latency Assessment in Substation Automation Systems,” *2012 IEEE PES General Meeting*, pp.36-40, July 2012.

[6] A.V. Schneider, S.A. Popov, A.V. Batrakov, G. Sandolache and S.W. Rowe, “Diagnostics of the Cathode Sheath Expansion After Current Zero in a Vacuum Circuit Breaker”, *IEEE Trans. on Plasma Science*, Vol.39, pp. 1349 – 1353, June 2011.

[7] N. Du, Y. Guan, J. Zhang, J. Niu, S. Yao and G. Xu, “Phenomena and Mechanism Analysis on Overvoltages Caused by 40.5-kV Vacuum Circuit Breakers Switching Off Shunt Reactors”, *IEEE Trans. on Power Delivery*, Vol.26, pp.2102 – 2110, April 2011.

[8] P. Rao, J. Huang and X. Hu,”Testing of circuit breakers using coil current characteristics analysis”, *IEEE International Conference on Control and Automation*, pp. 185-189, August 2009.

[9] Z. Li, G. Tan, Y. Li,” Fault diagnosis based on improved kernel Fisher discriminant analysis”, *Journal of Software*, Vol.7, pp.2657-2662, December 2012.

[10] Y. Xu, S. Xiu, “A new and effective method of bearing fault diagnosis using wavelet packet transform combined with support vector machine”, *Journal of Computers*, Vol.6,pp.2502-2509, November 2011.

[11] M.Basseville and I.V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*, Prentice-Hall, Inc., Simon & Schuster Company , Englewood Cliffs, NJ, 1993.

[12] D.B. Durocher and L. Walls, S. Becker, “Understanding Circuit Breaker Design and Operation to Improve Safety and Reliability in Underground Mining“, *IEEE Trans. on Industry Applications*, Vol.49,pp.3-9, January 2013.

[13] A.V. Gribok, M.J. Buller, R.W. Hoyt, J. Reifman,"A Real-Time Algorithm for Predicting Core Temperature in Humans", *IEEE Trans. on Information Technology in Biomedicine*, Vol.14,pp.1039 – 1045, April 2010.

[14] Z. Wang, A. Maier, N.K. Logothetis and H. Liang, "Extraction of Bistable-Percept-Related Features From Local Field Potential by Integration of Local Regression and Common Spatial Patterns", *IEEE Trans. on Biomedical Engineering*, Vol.56, pp.2095- 2103,August, 2009.

[15] W. S. Cleveland, “Robust Locally Weighted Regression and Smoothing Scatterplots“, *Journal of the American Statistical Association*, Vol.74,pp.829-836, January 1979.

[16] H. William, *Numerical Recipes 3rd Edition: The Art of Scientific Computing*,Cambridge University Press, 2007.

[17] H.Sakoe and S.Chiba,” Dynamic Programming Algorithm Optimization for Spoken Word Recognition”, *IEEE Trans. on Acoustics, Speech and Signal Processing*, Vol. 26, pp. 43-49, January 1978.

[18] C. A. Ratanamahatana and Keogh. E. “Everything you know about Dynamic Time Warping is Wrong”, *Third Workshop on Mining Temporal and Sequential Data, in conjunction with the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp.78-82, June 2004.

[19] G. Ding, L. Wang, P. Yang, P. Shen, S. Dang,” Diagnosis model based on least squares support vector machine optimized by multi-swarm cooperative chaos particle swarm optimization and its application”, *Journal of Computers*, Vol. 8, pp.975-982, April 2013.

[20] B. Jablonski, "Quaternion Dynamic Time Warping", *IEEE Trans. on Signal Processing*, Vol.60,pp.1174-1183, March 2012.

[21] Y. Chen, K. Chen and M.A. Nascimento, “Effective and Efficient Shape-Based Pattern Detection over Streaming Time Series", *IEEE Trans. on Knowledge and Data Engineering*, Vol.24, pp.265-278, February 2012.

[22] http://allegromicro.com/en/Products/Current-Sensor-ICs/Zero-To-Fifty-Amp-Integrated-Conductor-Sensor-ICs/ACS712.aspx

[23] Z. Xu, J. Wu, S. Qu, “Prediction model based on moving pattern”, *Journal of Computers*, Vol. 7, pp.2695-2701, November 2012

Yuhuang Zheng received his B.S. and M.S. degree from the Faculty of Automation, Guangdong University of Technology, Guangzhou, China in 2002 and 2006 respectively. In 2009, he received his Ph.D. from School of Mechanical & Automotive Engineering, South China University of Technology. His main interests are industrial automation, embedded system design, and pervasive computing. He is a lecturer at the Dept. of Physics, Guangdong University of Education. He also is the postdoctoral researcher in South China University of Technology and Guangdong Zhujiang Switchgear Co., Ltd.

Recent Frequent Item Mining Algorithm in a Data Stream Based on Flexible Counter Windows

Yanyang Guo
School of Information Engineering, Yangzhou Polytechnic College, Yangzhou,China
gyy197966@163.com

Gang Wang[1,a], Fengmei Hou[1,b], Qingling Mei[2,c]
[1]School of Information Engineering, Yangzhou Polytechnic College, Yangzhou,China
[2]Department of Computer Science, Yangzhou University, Yangzhou,China
[a]yzwg001@163.com, [b]yzhfmjs@163.com, [c]mql859@163.com

***Abstract*—In the paper the author introduces FCW_MRFI, which is a streaming data frequent item mining algorithm based on variable window. The FCW_MRFI algorithm can mine frequent item in any window of recent streaming data, whose given length is L. Meanwhile, it divides recent streaming data into several windows of variable length according to m, which is the number of the counter array. This algorithm can achieve smaller query error in recent windows, and can minimize the maximum query error in the whole recent streaming data.**

***Index Terms*—streaming data, counter array, data mining, most recent frequent item**

I. INTRODUCTION

Although there are many algorithms concerning of frequent item mining in streaming data[1,3,5], many of them don't put emphasis on current data. The existing researches of frequent item mining in the most recent streaming data are mainly algorithms based on slide window technology. L. Golab et al. introduced an algorithm based on hopping windows[2], which requires a specified a threshold 1/*m*. Recently, they introduced several algorithms utilizing slide window model. Lee and Ting[7] put forward an algorithm, which can realize space complexity O(ε^{-1}), and processing time of updating and querying O(ε^{-1}). L. Zhang and Y. Guan[6] proposed an Estimate of streaming data frequent value based on slide window, which requires a memory space O(ε^{-1}) , and the processing and querying time of each data item O(ε^{-1}). H.T.Lam,T.Calders[8] presented to mine the first K maximum frequent item in slide windows with dynamic-Change lengths. I.T.Ferry et al. proposed an algorithm which divides the most recent streaming data based on time-inclined method[4]. However, this algorithm demands that the number of counter array must be equal to the number of windows divided, which is not applicable when the number of counter array is already given.

In practical application, it is required that the querying error of recent data be relatively smaller, while errors produced by most existing algorithms are all the same for data at all times[9,10,11]. Aiming at this problem, *FCW_MRFI*, which is a streaming data frequent item mining algorithm based on variable window, is introduced in this paper. The *FCW_MRFI* algorithm can mine frequent item in any window of recent streaming data, whose given length is *L*. Meanwhile, it divides recent streaming data into several windows of variable length according to *m*, which is the number of the counter array. This algorithm can achieve smaller query error in recent windows, and can minimize the maximum query error in the whole recent streaming data. In order to compare its accuracy and recall rate with other existing methods, experiments with real data sets and synthetic data sets are conducted, which shows that *FCW_MRFI* algorithm offers much improved accuracy in data stream recent frequent item mining.

II. DEFINITION

If the maximum length of the most recent streaming data allowed to be queried is *L*, and current time is *t*, then the frequent data item in any window during the period from *t-L* to *t* can be queried. If the particular window to be queried is $w = [w_{\min}, w_{\max}]$ (as illustrated in Figure 1), in which $w_{\min}$ refers to the farthest point, while $w_{\max}$ refers to the nearest one, then it can be seen from Figure 1 that the query window *w* should satisfy: $t - w_{\min} \le L$, to wit, $t - L \le w_{\min} < w_{\max} < t$.

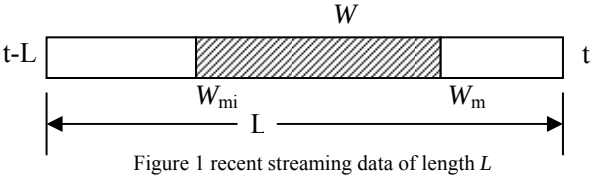


Figure 1 recent streaming data of length *L*

If the particular window to be queried is $w = [w_{\min}, w_{\max}]$, then the length of query window *w* is $|w| = w_{\max} - w_{\min}$. If is a constant defined by the system between [0,1], and if the support of a particular *x* in *w* is equal to or larger than $\phi|w|$ (), then *x* is the frequent item

doi:10.4304/jsw.9.1.258-263

of the window. We are supposed to query the frequent item designated by the user in the most recent streaming data.

If there are *m* counter units available in the system, we are supposed to perform frequent item query against any window in the most recent streaming data of length *L* using only *m* counter units, and at the same time minimize the maximum query error. For data of different time, query errors of those nearer to the current time are relatively smaller. So, the streaming data are divided into several time spans, which are called basic windows. Statistic information of item number in each basic window is stored in an array of counter units. Here Hash function is adopted to get approximate numbers, that is to say, set up a Hash function *H* with *h.count*, and set up H(x) as the counter of each data item x. If the value range of *H*(*x*) is [1, *h*], then there are *h* units. For a particular window *w* to be queried, some window span overlapping with the queried window *w* can be chosen to achieve minimum error between the length of w' which are composed of these spans and the length of *w* which are composed of the queried windows.

A simple way for this problem is to averagely allocate the most recent streaming data *L* into *m* parts, with each part of fixed length *L/m*. With this way, errors between the queried window *w* and the chosen window span w' are less than *L/m*. However, this method sets very high demands for space complexity. Moreover, it treats all data items in recent streaming data equally, which results in much loss of the newer data information. However, the newer data information is often commonly employed and tends to carry more valuable information than historical data.

Another way is to divide recent streaming data with the length of individual window span 1,2,4,…2^{l-1}. The tilted time frame method can estimate the frequency of recent data item more accurately, and decrease the accuracy of the historical data gradually. However, with this method, the error between *w* and w' can reach *L/2*, and it demands the number of counter array be equal to that of divided window span, to wit, $l = \log L = m$, which is not applicable when the value of counter array *m* is give n.

To counter the problems occurred in the two methods, a compromise, *FCW_MRFI*, is proposed in this paper. *FCW_MRFI* tries to preserve as much newer data information as possible, and at the same time minimize maximum and ensemble error.

III. Main Idea of FCW_MRFI Algorithm

3.1 If $m \le \log_2 L$

If the length of slide window is L, the number of counter array defined by the system is m, and the size of basic window is b=$\frac{L}{2^m}$, then the number basic window in current slide window is L'=L/b=2^{l-m}.

The most recent streaming data in slide window is divided into m spans by logarithmic time-inclined of length L, and the length of these spans are respectively b, b, 2b, 4b, …, 2m-2b, 2m-1b. The first window stores b data item from the basic window that comes first, and the length of the following window is twice that of the former clip. Generally, if the size of the first window is represented by w0, then, and the ith window following it is $w_i = 2^{i-1}b, \quad 0 < i < m$. One array of counter is adopted to counter the individual data item in each span, and mark them in turn as C_0, C_1, C_2, C_3, C_4,…. A buffer array, which is marked as C_{-1}, is set up by the system to receive streaming data.

Hcount is adopted to estimate the counting of the individual data item in the most recent basic windows. The counting is added to counter array C_{-1}, and the original value of C_{-1} is transferred to C_0. The counter array correspondent to the window of 2i length is marked as C_i,(i=0,1,2,…m-1), and a counter array C_{-1} is set up to receive the latest data. The counter array C-1 should transfer its data in order to receive the latest data every time when it has received b data item.

Figure 2 is taken as a simple example to illustrate how the counter array conducts *hcount* calculation and transfer operation. In figure 2, *b*=1, *m*=5, the counter arrays correspondent to the individual windows are C_{-1},C_0,C_1,C_2,C_3,C_4: , among which C_{-1} is to counter the latest data item.

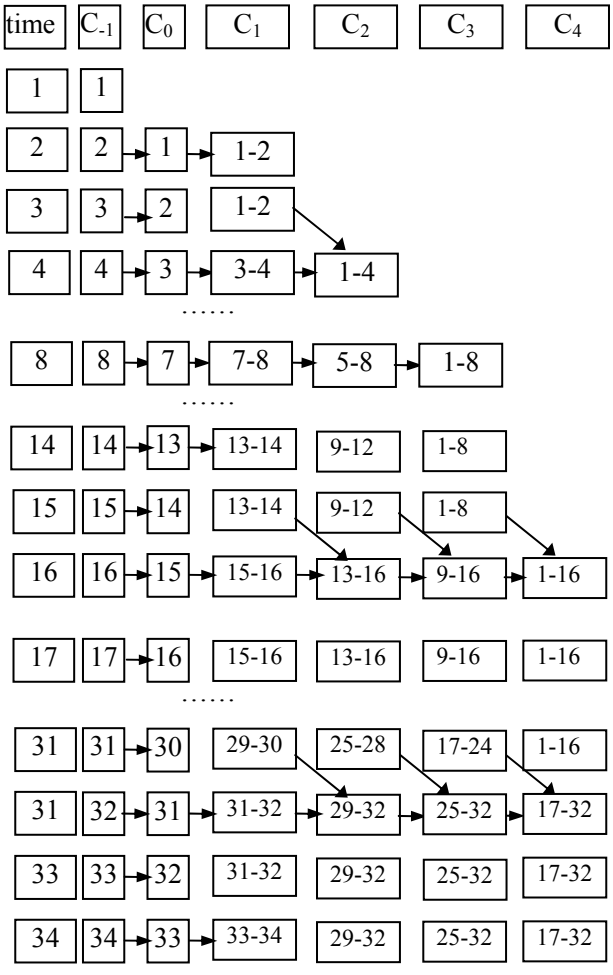


Figure 2 transfer operation f counting windows

Figure 2 shows that counter array C_{-1} always counter the latest data items, and every time when it has received b data item it perform data-transfer. Apart from transferring the values in C_{-1} to C_0, it adds the values of former several counter arrays and transfers them to the following counter arrays. The time of transferring differs in different time t. For example, when t=2, it transfers 2 times to the following counter array, when t=3, it transfers 1 time, and when t=4, it does 3 times. Generally, G(t) is marked as the location of "1" (the low-order bit is bit0), which is the lowest in binary representation of integer t. The times of transferring to be conducted by counter arrays following C_{-1} is identified by G(t). At t, the times of transferring to be conducted is $G(t)$+1. For example: if $2=(00010)_2$, then $G(2)=1$, to wit, when t=2, the times of transferring is 2. Similarly, as $G(3)=0$ $G(4)=2$, when t=3, the times to be transferred should be 1, and when t=4, the times should be 3. After summing and transferring, the correspondent counter arrays should refresh their records.

To sum up, FCW_MRFI is given below to illustrate the refresh procedure of individual counter array C_i.

As there are h units in each counter array Ci, $C_i[k]$ is adopted to represent kth unit in Ci, to wit, the counter of data whose Hash value is k. In the following algorithm, $C_i + C_j$ represents the adding up of values of the corresponding units of C_i and C_j. For example, $C_i = C_i + C_j$, represent $C_i[k] = C_i[k] + C_j[k] \quad (k = 1,2,...,h)$

Algorithm 1 *FCW_MRFI*($m \le \log_2 L = l$)

Begin

1. t=2;
2. receive and form *hcount* of the first two windows and save to C_{-1},, C_0, $C_1=C_{-1}+C_0$;
3. While not end condition do
4. $t=t+1$; $C_0=C_{-1}$;
5. form Count for newer group and store to C_{-1}; temp1=C_{-1};
6. q=min(G(t),m) /*m is the number of counter array, $G(t)$ the location of "1", which is the lowest in binary representation of integer t */
7. for j=1 to q do
8. temp2=C_j;
9. $C_j=C_{j-1}$+temp1; temp1=temp2;
10. end for j ;
11. end While ;

End

The counter array produced by the above algorithm can cover all data items in current windows, and for the newer data items, which can offer higher accuracy. If n m=4, L=16, figure 3 shows the range of the individual counter array when t=15, 16, 31, 32. As seen from above, t=15, the range is [1, 15]. As the maximum range of counter array is [1, 8], and the length is 8, the maximum query error is 4, while in range [14, 15], the query error is 0. Generally, at, the query error of range [t-1, t] is 0, and that of [t-2^i+1,t] is 2^{i-1}. One more example, when t=16, the range is [1,16]. As ranges of [1,8] can be achieved by subtracting counting value of [9,16] from that of [1,16], the maximum range is [1,8] or [9,16], and the length of both is 8, the maximum query error is 4. When t=31, the maximum range of counter in the queried windows is [17,24], and the length is 8, the maximum query error is4. When t=32, the maximum range of counter in the queried windows is [17,24] or [25-32], and the length of both is 8, the maximum query error is4. Generally, if t mod 16=g, then the range at t is $[t-16-g+1, t]$, $[t-16-g+1, t]$. The maximum query error of counters within the queried windows is l/2, and minimum query error is 0. Furthermore, for those older data ranges $|w| = (16+g)$, the query errors are greater, while for those newer data ranges, the query errors are smaller.

3.2 *If* $m > \log_2 L$

When $m > \log_2 L$, the recent streaming data L is divided into l windows of length 1, 2, 4, 8, …, 2^{l-1}. Let $m' = m - logL$, mark windows of length 2^i as S_i, and mark the corresponding counter array as C_i. As for those m' unused counter arrays, the length of them is divided according to the following principle: first, from S_{l-1}, delete S_{l-1}, add two S_{l-2}, and subtract 1from the value of m. If m' is not 0, delete one more S_{l-2}, and add two S_{l-3}. And if m' is still not 0, delete one more S_{l-2} , add two S_{l-3} . If all S_{l-2} are deleted, m' is still not 0, delete one S_{l-3}, subtract 1 from m' . The rest follows the same tend till m' is 0.

Mark the number of windows S_i as T_i. According to the method stated above, for given L and m, the maximum number of window k of window S_k which enables $T_k \neq 0$ is defined by the following rule:

Mark: $l = \log_2 L$: first calculate

$$D_i = 2^{l-i+2} - (l - i + 4) \tag{1}$$

Then the maximum number of window k is

$$k = \arg\max_i (D_i \ge m') - 1 \tag{2}$$

T_i, the number of window S_i is defined by

$$T_i = \begin{cases} 0 & i > k \\ D_{i+1} - m' + 1 & i = k \\ 2(2^{l-i-1} - T_{i+1}) - 1 & i = k-1 \\ 1 & k-2 \ge i \ge 1 \end{cases} \tag{3}$$

For example, if L=1024,m=20, l=10, then m′ =10. From (1), by calculation, $D_{10}=0$, $D_9=3$, $D_8=10$, $D_7=25$, $D_6=56$.From (2), by calculation, k=8-1=7. Still, from (3), by calculation:

$T_7=10-10+1=1$,$T_6=2(2^{10-7}-1)-1=13$,

$T_0=T_1=T_2=T_3=T_4=T_5=1$

Thus, the total number of counter array needed is $T_7+T_6+T_5+...+T_1+T_0=1+13+6=20$, which is exactly equal to the given number of counter array m. Therefore, a conclusion can be drawn as follows:

Theorem 1: with the window-arranging method mentioned above, the number of windows arranged is exactly the same as the given number of counter array *m*.

Prove : if Tk≠0 starts at k[th] layer

Total number of windows =Tk+Tk-1+....+T1+T0

$$= T_{k-1} = 2(2^{l-k} - T_k) - 1 \quad +(k-1)$$

$$= 2^{l-k+1} - T_k + k - 2$$

$$= 2^{l-k+1} - \left(C_{k+1} - m' + 1\right) - 2 + k$$

$$= 2^{l-k+1} - 2^{l-k-1+2} + \left(l - k - 1 + 4\right) + m' - 1 - 2 + k$$

$$= l - k + 3 + m' - 3 + k$$

$$= l + m' = m$$

proven

Theorem 2: with the window-arranging method mentioned above, certain given counter array can cover the query of the most recent steaming data of length *L*-1.

Prove : if Tk≠0 starts at k[th] layer

Total coverage length

$$= T_k.2^k + T_{k-1}.2^{k-1} + 2^{k-2} + ... + 2 + 1$$

$$= T_k.2^k + \left[2\left(2^{l-k} - T_k\right) - 1\right]2^{k-1} + 2^{k-1} - 1$$

$$= T_k.2^k + 2^{l-k+1+k-1} - 2^k T_k - 2^{k-1} + 2^{k-1} - 1$$

$$= 2^l - 1 = L - 1$$

proven

If the buffer array C_{-1} is included, it can cover the query of the most recent streaming data with length *L* entirely. As it is within the query range, the maximum coverage range is 2^k. Therefore, it is not difficult to draw a conclusion as follows:

Theorem 3: The window-arranging method mentioned above is a scheme that can employ as many as *m* windows to query the most recent streaming data of coverage length *L*, and can guarantee the error less than 2^{k-1}. Among which:

$$k = \arg\max_i \left[\left(m - \log L\right) \le \left(2^{l-i+2} - \left(l - i + 4\right)\right)\right] - 1$$

Thus it can be seen that the maximum query error of the counter within query windows is 2^{k-1}, and the minimum error is 0. Errors are greater for older data spans, and smaller for newer ones.

According to the window-arranging method mentioned above, m counter array can be employed to counter streaming data of each individual window correspondingly. Each time when a data comes, counter array C-1 counters it, and then transfers it. Apart from transferring the values in C-1 to C0, it adds the values of former several counter arrays and transfers them to the following counter arrays. The time of transferring differs in different time t.

For example, if the length of the most recent streaming data query window *L*=32, then $l = \log_2 L = 5$, and the number of given counter array *m*=7, then $m' = 2$. According to the window-arranging method mentioned above, the number of each individual window should be $T_{-1}=1, T_0=1, T_1=1, T_2=3, T_3=2$.

To sum up, *FCW_MRFI* is given below to illustrate the refresh procedure of individual counter array C_i.

Algorithm 2: *FCW_MRFI*($m > \log_2 L = l$)

```
Begin
 1.  t=2;
 2.  receive and form hcount of the first two windows and save to C-1,, C0, C1=C-1+C0;
 3.  While not end condition do
 4.      t=t+1; C0=C-1;
 5.      form Count for newer group and store to C-1; temp1=C-1;
 6.      q=min(G(t),k)   /*k is the number of counter array, G(t) the location of "1", which is the lowest in binary representation of integer t */
 7.      for j=1 to q do
 8.          temp2=C_j^1 ;  C_j^1=temp1; temp1=temp2;
 9.          for i=2 to T_i do
 9.              temp2= C_j^i ;  C_j^i =temp1; temp1=temp2;
10.          endfor  i
11.          temp1=temp2+C_j^(T_i-1)
10.      end for j ;
11.  end While ;
     End
```

IV. EXPERIMENTAL INVESTIGATION

Experiments with real data sets and synthetic data sets are conducted to measure *FCW_MRFI* algorithm, and compare its performance with *TiTiCount* algorithm which adopts tilted time frame method. All experiments were operated on PCs with 512M memory, 1.7G CPU, WINDOWS XP operating system, and programmed using python2.6. In experiments, parameters are set as: $\phi = 0.05$,*b*=1000.

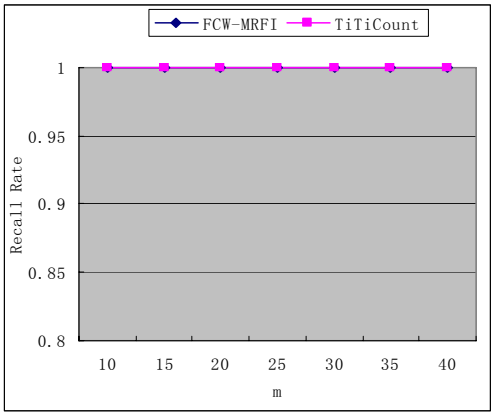
4.1 Synthetic Data

To measure this algorithm, 6 groups of data set satisfying Zipf distribution are created randomly, with parameters of each Zipf Distribution group being 0.5, 0.75, 1, 1.25, 1.5 and 1.75. The size of the data set is 1000k. When different number of counter array is given, recall rate and accuracy of *TiTiCount* and algorithm introduced in this paper are measured by query windows created randomly. Meanwhile, recall rate and accuracy of the two algorithms of different Zipf distributions are compared when *b*=1000, $\phi = 0.05$

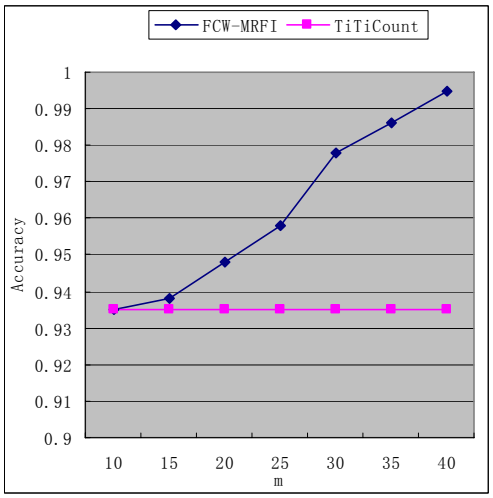
Figure 5(a) illustrates the comparison of recall rate of the two algorithms when ϕ=0.005 and Zipf distribution parameter is 1.5. It can be seen from Figure 5 that recall rate of both algorithms can reach 100% for data sets of relatively stable distribution.

Figure 3(b) illustrates the comparison of accuracy of

the two algorithms when values of *m* vary. For , as the value of *m* increases, the bigger counting window keep subdividing into smaller ones, thus guarantee more accurate frequency counting. However, the number of counting array of *TiTiCount* is stable. Therefore, as the value of *m* increases, *FCW_MRFI* is more accurate than *FCW_MRFI*.



(a) Comparison of Recall Rate

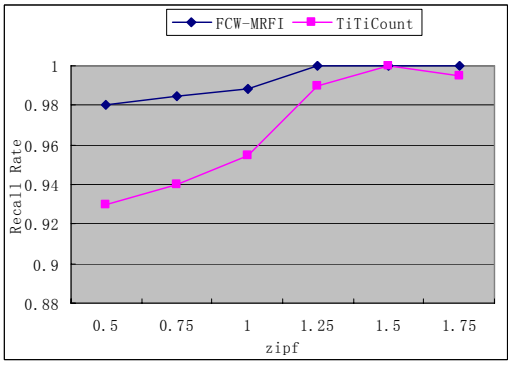


(b) Comparison of Accuracy

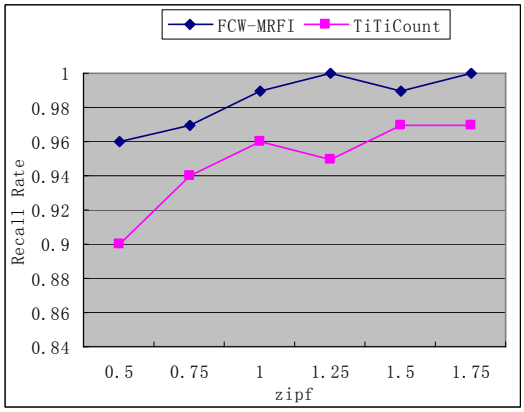
Figure 3 Comparison of Two Algorithm on Recall Rate and Accuracy when the value of *m* varies

When *m*=35, recall rate comparison for data sets of various Zip distribution parameters is illustrated in Figure 4(a). Recall rate of *FCW_MRFI* almost reach 100%, while *TiTiCount* can't reach 100% as its errors are greater in querying and counting windows.

When *m*=35, mining accuracy comparison for data sets of various Zip distribution parameters is illustrated in Figure 4(b). As can be seen from the figure, for data sets of various Zip distribution parameters, *FCW_MRFI* is more accurate than *TiTiCount*.



(a) Recall Rate Comparison



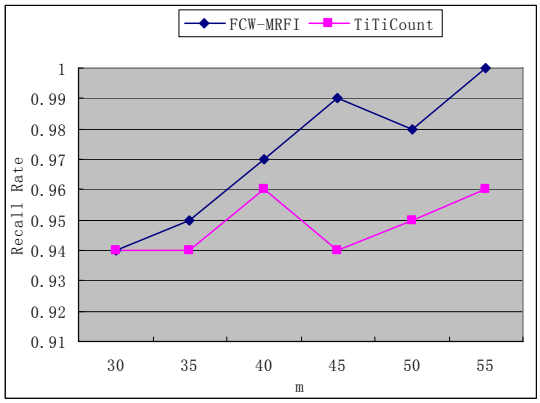
(b) Accuracy Comparison

Figure 4 recall rate and accuracy comparison for data sets of various Zip distribution parameters(ϕ =0.05,*m*=35)

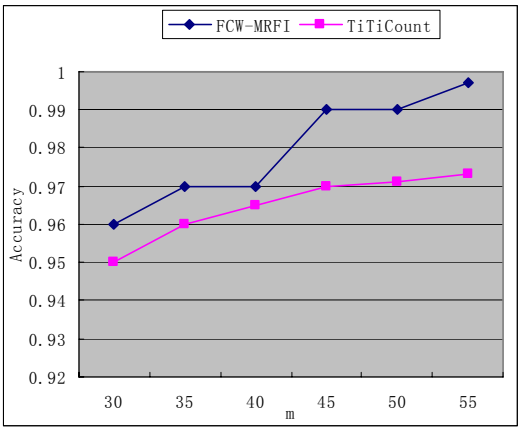
4.2 Real Data

In real data experiments, data set, kosarak[18] ,is adopted (http://fimi.cs.helsinki.fi/data/). The data set is composed of anonymous click stream of a Hungary online news gateway website, which contains about 800 million separate data items. 90 groups of query windows created randomly are adopted to compare their recall rate and accuracy.

Figure 5(a) illustrates the comparison of recall rate when the value of *m* varies. As seen from Figure 5(a), recall rate of *FCW_MRFI* is higher than that of *TiTiCount*. Figure 5(b) illustrates the comparison of accuracy when the value of *m* varies. Obviously, as the value of m increases, *FCW_MRFI* is more accurate than that of *TiTiCount*.



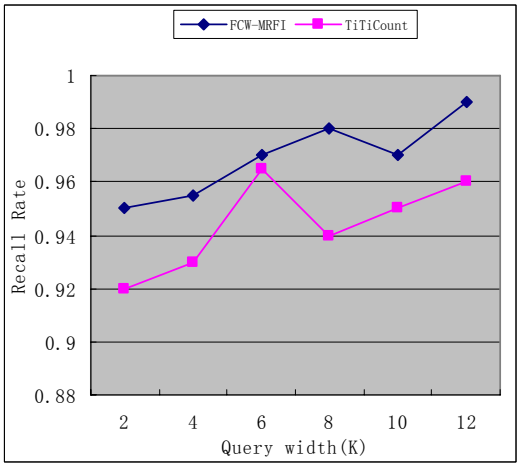
(a) Recall Rate Comparison



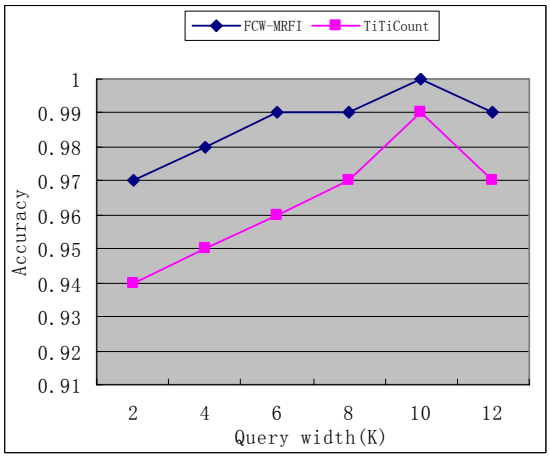
(b) Accuracy Comparison

Figure 5 Recall Rate and Accuracy Comparison when the value of *m* varies (kosarak data set, ϕ=0.05)

Figure 6(a) illustrates the recall rate comparison of two algorithms with different query width. As seen from the figure, recall rate of *FCW_MRFI* is higher than that of *t*. Figure 6(b) illustrate the accuracy comparison of the two algorithms. Results in the figure shows that *FCW_MRFI* is more accurate than *t*. Accuracy rate of *FCW_MRFI* are all over 95%, even 100%, which proves better performance of *FCW_MRFI*.



(a) Recall Rate Comparison



(b) Accuracy comparison

Figure 6 recall rate and accuracy comparison of two algorithms with different query width

V. Conclusion

FCW_MRFI, which is a streaming data frequent item mining algorithm based on variable window, is introduced in this paper. The *FCW_MRFI* algorithm can mine frequent item in any window of recent streaming data, whose given length is *L*. Meanwhile, it divides recent streaming data into several windows of variable length according to *m*, which is the number of the counter array. This algorithm can achieve smaller query error in recent windows, and can minimize the maximum query error in the whole recent streaming data. In order to compare its accuracy and recall rate with other existing methods, experiments with real data sets and synthetic data sets are conducted, which proves that *FCW_MRFI* algorithm offers much improved accuracy in recent frequent item mining in data stream.

Acknowledgements

This research was supported in part by modern education technology research project of Jiangsu province (2013-R-24925).

References

[1] J. Misra, D. Gries. Finding repeated elements[J]. Science of Computer Programming, 1982, pp.143~152.

[2] L. Golab, D. DeHaan, A. L.Ortiz, et al. Finding frequent items in sliding windows with multinomially-distributed item frequencies[C]. In Proceedings of the 16th International Conference on Scientific and Statistical Database Management, 2004, pp.425~426.

[3] G. S. Manku, R. Motwani. Approximate Frequency Counts over Data Streams[C]. In Proc. of VLDB, 2002, pp.346~357.

[4] T. Calders, N. Dexters, B. Goethals. Mining Frequent Itemsets in a Stream[C]. In Proceedings of 7th IEEE International Conference on Data Mining, 2007, pp. 83~92.

[5] Frequent itemset mining dataset repository, university of helsinki (2008), http://fimi.cs.helsinki.fi/data/

[6] L. f. Zhang, Y. Guan, Frequency estimation over sliding windows[C], Proceedings of the 2008 IEEE 24th International Conference on Data Engineering, 2008, pp.1385~1387.

[7] H. F. Li, S. Y. Lee. Mining frequent itemsets over data streams using efficient window sliding techniques[J]. Expert Systems with Applications.2009, pp.1466-1477.

[8] H. T.Lam ,T. Calders, Mining Top-K Frequent Items in a Data Stream with Flexible Sliding Windows,Copyright 2010 ACM 978-1-4503-0055-110/07

[9] C.N. Yang, and Y.Y Yang, and C.Y. Chiu, "Image Library Systems: A Novel Installment Payment for Buying Images on the Web," Journal of Computers, Vol. 20, No.1, 2009,pp. 43-49, Apr.

[10] X. Xu, J. Lin . A novel time advancing mechanism for agent-oriented supply chain simulation. Journal of Computers, Vol.4, No.12, 2009, pp.1301-1308.

[11] Ma cuixia, Meng xiangxu. Research on Object Constraints Model and Inverted Constraints in Parametric Design, Journal of Computers, Vol.23, No.9, 2000, pp.991-995.

Call for Papers and Special Issues

Aims and Scope.

Journal of Software (JSW, ISSN 1796-217X) is a scholarly peer-reviewed international scientific journal focusing on theories, methods, and applications in software. It provide a high profile, leading edge forum for academic researchers, industrial professionals, engineers, consultants, managers, educators and policy makers working in the field to contribute and disseminate innovative new work on software.

We are interested in well-defined theoretical results and empirical studies that have potential impact on the construction, analysis, or management of software. The scope of this Journal ranges from the mechanisms through the development of principles to the application of those principles to specific environments. JSW invites original, previously unpublished, research, survey and tutorial papers, plus case studies and short research notes, on both applied and theoretical aspects of software. Topics of interest include, but are not restricted to:

- Software Requirements Engineering, Architectures and Design, Development and Maintenance, Project Management,
- Software Testing, Diagnosis, and Validation, Software Analysis, Assessment, and Evaluation, Theory and Formal Methods
- Design and Analysis of Algorithms, Human-Computer Interaction, Software Processes and Workflows
- Reverse Engineering and Software Maintenance, Aspect-Orientation and Feature Interaction, Object-Oriented Technology
- Component-Based Software Engineering, Computer-Supported Cooperative Work, Agent-Based Software Systems, Middleware Techniques
- AI and Knowledge Based Software Engineering, Empirical Software Engineering and Metrics
- Software Security, Safety and Reliability, Distribution and Parallelism, Databases
- Software Economics, Policy and Ethics, Tools and Development Environments, Programming Languages and Software Engineering
- Mobile and Ubiquitous Computing, Embedded and Real-time Software, Database, Data Mining, and Data Warehousing
- Internet and Information Systems Development, Web-Based Tools, Systems, and Environments, State-Of-The-Art Survey

Special Issue Guidelines

Special issues feature specifically aimed and targeted topics of interest contributed by authors responding to a particular Call for Papers or by invitation, edited by guest editor(s). We encourage you to submit proposals for creating special issues in areas that are of interest to the Journal. Preference will be given to proposals that cover some unique aspect of the technology and ones that include subjects that are timely and useful to the readers of the Journal. A Special Issue is typically made of 10 to 15 papers, with each paper 8 to 12 pages of length.

The following information should be included as part of the proposal:

- Proposed title for the Special Issue
- Description of the topic area to be focused upon and justification
- Review process for the selection and rejection of papers.
- Name, contact, position, affiliation, and biography of the Guest Editor(s)
- List of potential reviewers
- Potential authors to the issue
- Tentative time-table for the call for papers and reviews

If a proposal is accepted, the guest editor will be responsible for:

- Preparing the “Call for Papers” to be included on the Journal’s Web site.
- Distribution of the Call for Papers broadly to various mailing lists and sites.
- Getting submissions, arranging review process, making decisions, and carrying out all correspondence with the authors. Authors should be informed the Instructions for Authors.
- Providing us the completed and approved final versions of the papers formatted in the Journal’s style, together with all authors’ contact information.
- Writing a one- or two-page introductory editorial to be published in the Special Issue.

Special Issue for a Conference/Workshop

A special issue for a Conference/Workshop is usually released in association with the committee members of the Conference/Workshop like general chairs and/or program chairs who are appointed as the Guest Editors of the Special Issue. Special Issue for a Conference/Workshop is typically made of 10 to 15 papers, with each paper 8 to 12 pages of length.

Guest Editors are involved in the following steps in guest-editing a Special Issue based on a Conference/Workshop:

- Selecting a Title for the Special Issue, e.g. “Special Issue: Selected Best Papers of XYZ Conference”.
- Sending us a formal “Letter of Intent” for the Special Issue.
- Creating a “Call for Papers” for the Special Issue, posting it on the conference web site, and publicizing it to the conference attendees. Information about the Journal and Academy Publisher can be included in the Call for Papers.
- Establishing criteria for paper selection/rejections. The papers can be nominated based on multiple criteria, e.g. rank in review process plus the evaluation from the Session Chairs and the feedback from the Conference attendees.
- Selecting and inviting submissions, arranging review process, making decisions, and carrying out all correspondence with the authors. Authors should be informed the Author Instructions. Usually, the Proceedings manuscripts should be expanded and enhanced.
- Providing us the completed and approved final versions of the papers formatted in the Journal’s style, together with all authors’ contact information.
- Writing a one- or two-page introductory editorial to be published in the Special Issue.

More information is available on the web site at http://www.academypublisher.com/jsw/.

(Contents Continued from Back Cover)