REVIEW OF DIFFERENT APPROACHES FOR PRIVACY SCHEME IN VANETS

Sapna S. Kaushik
Department of Computer Engineering, DBNCOET, Yavatmal, Maharashtra, India

ABSTRACT

Mobile nodes that are connected in a self-organized way without an underlying hierarchical infrastructure form mobile ad hoc network (MANET)[7]. The MANET is called a vehicular ad hoc network (VANET) in the special case where the mobile nodes are embedded in vehicles. VANET communications, employing a combination of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [4,6] wireless communication are expected to integrate the driving experience into a ubiquitous and pervasive network that will enable novel traffic monitoring and incident detection paradigms[4]. Exchanged messages can take part in road safety applications therefore, it is fundamental to take security into account when designing protocols and mechanisms for VANETs. In particular, security requirements include authentication, data consistency and integrity, availability, non-repudiation and privacy [26]. Among these requirements, privacy is key to the VANET, because a lack of privacy could rise concern about the adoption of this new technology, delaying its widespread diffusion. A review about various implementation techniques to achieve privacy has been done.

KEYWORDS: *Vanet, authentication, data consistency and integrity, availability, non-reputiation, privacy*

I. INTRODUCTION

Recently, Vehicular ad hoc network (VANET) [1] can offer various services and benefits to VANET users and thus deserves deployment effort. In recent years, the number of motorists has been increasing drastically due to rapid urbanization. The number of automobiles has been increased on the road in the past few years. Due to high density of vehicles, the potential threats and road accident is increasing. Wireless technology is aiming to equip technology in vehicles to reduce these factors by sending messages to each other. Critical traffic problems such as accidents and traffic congestion require the development of new transportation systems [2]. Intelligent Transportation Systems (ITS) [3, 4] are aimed at addressing critical issues like passenger safety and traffic congestion, by integrating information and communication technologies into transportation infrastructure and vehicles. They are built on top of self-organizing networks, known as a Vehicular Ad hoc Networks (VANET), Vehicular communication systems facilitate communication devices for exchange of information among vehicles and between vehicles and roadside equipment. Working in tandem with the fielded Intelligent Transportation Systems (ITS) infrastructure, VANET is expected to enhance the awareness of the traveling public by aggregating, propagating and disseminating up - to - the minute information about existing or impending traffic-related events. The nodes of a VANET [1,8] are commonly divided in two categories: On-Board Units (OBU), that are radio devices installed on vehicles, and Road Side Units (RSU)[18], that constitute the network infrastructure. RSUs are placed along the roadside and are controlled by a network operator [2]. VANETs are expected to allow for transmission of information between vehicles or between vehicles and the roadside units (RSUs) [17] and, thus, to enhance the safety of both vehicle drivers and passengers [1]. Even though vehicles are organized mostly in an ad hoc manner in the network topology, directly applying the existing communication approaches designed for traditional mobile ad hoc networks to large -scale VANETs with fast-moving vehicles can be ineffective and inefficient. To achieve success in a vehicular environment, VANET-specific communication solutions are imperative. Via inter - vehicle communications, drivers can be informed of crucial traffic information such as treacherous road conditions and accident sites by communicating with each other and/or with the roadside infrastructure. With better knowledge of traffic conditions, it is plausible that the problem of accidents can be alleviated. Traffic monitoring and management can also be facilitated by vehicular communications. Value added services can enhance drivers' traveling experience by providing convenient Internet access, navigation, toll payment services, etc. [21], [23], [24], [25]. The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. Some of the popular architectures of VANETs (Vehicular Ad hoc NETworks) are WAVE by IEEE, CALIM by ISO, C2CNet by C2C consortium / GeoNet. The safety related application protocols in VANETs are WSMP by WAVE, CALM FAST by ISO and C2CNet by C2C consortium.

II. TECHNICAL DETAILS OF VANET PROTOCK STACK

This section discusses the VANETs protocol stack in detail. The discussion focuses on Network, MAC and PHY layers for WAVE .The approved frequency band is 5.9 GHz (in Europe 5 GHz). It was initially approved by U.S Federal Communications Commission (FCC) under Dynamic Short Range Communication (DSRC) concept. The spectrum is divided into six service channels (SCH) and one control channel (CCH) with equal bandwidth of 10 MHz each. For emergency messages (originated by safety related applications) and control messages, CCH is used. SCH is used for other applications' packets. The entire spectrum is divided into time slots of 50 ms. If the CCH channel is active, all nodes are bound to stop their communication during CCH time frame to receive and transmit emergency messages on CCH channel.

IEEE introduced a complete protocol stack of 1609 protocol family and named it as WAVE (Wireless Access in Vehicular Environment). There are six sub-standards under 1609 family named as IEEE 1609.1,2,3,4,5,6. Each one handles different issues at different layers.

Fig. 1 provides an insight into the six sub-standards and their relationship with respect to the tasks at the various OSI layers [50]

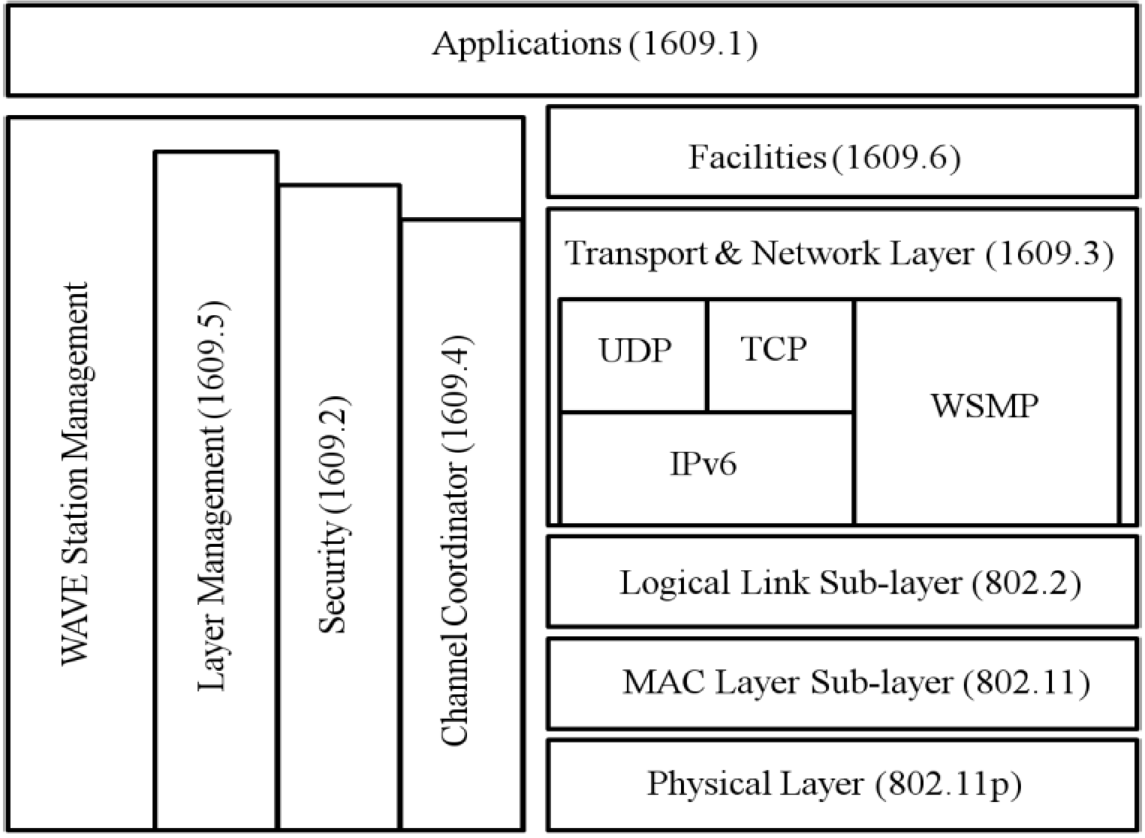
Applications (1609.1)
WAVE Station Management
Layer Management (1609.5)
Security (1609.2)
Channel Coordinator (1609.4)
Facilities (1609.6)
Transport & Network Layer (1609.3)
UDP
TCP
WSMP
IPv6
Logical Link Sub-layer (802.2)
MAC Layer Sub-layer (802.11)
Physical Layer (802.11p)

Fig. 1. WAVE Architecture

The types of applications are divided into two main categories as defined by IEEE 802.11p [51]
i. Safety
ii. Infotainment.
IEEE 1609.1 details the management activities required for the proper operation of the applications. 1609.2 describes the considerations to be taken into account for communication security. For Transport and Network Layer handling of traffic safety related applications, 1609.3 provides a dedicated single protocol, named as WSMP (Wave Short Messages Protocol). 1609.4 defines the coordination between the multiple channels of the spectrum. 1609.5 deals with Layer Management while 1609.6 offers an additional middle layer between transport and application layer, for handling of additional facilities at the Applications Layer. IEEE 802.11p details the MAC Layer operation of the WAVE architecture [52].
Vehicular nodes in VANETs can move very fast, leading to fast topological changes. WAVE uses two available services sets [53] for network topology handling. WAVE Basic Service Set (WBSS) is defined for communication between RSUs and OBUs and closely resembles the 802.11a specifications for communication of nodes with the 98 M.S. Akbar, A. Rasheed, and A. Qayyum Access Points (AP). After listening to a beacon message, any new user can join WBSS without authentication process. The second service set is called WAVE independent basic service set (WIBSS). This service set supports the communication between two nodes in a mesh network i.e. V2V communication without the involvement of an RSU. IEEE WAVE allows only one option at the MAC layer, i.e. 802.11p. Though this restricts the degree of freedom of research activities, open source simulators, like NCTUns, often provide extended protocol stack support, which assist researchers to use other options at the MAC layer as well. However, here it must be noted that 802.11p is based on a time tested standard (802.11a) which has proven its suitability for short range communications.

III. ATTRIBUTES OF SECURE NETWORK

In general, a secure network should have the following Attributes: authentication, non-repudiation, confidentiality, data integrity, Access Control and availability, Privacy [49].
2.1 Authentication is the verification of a user identity prior to granting access to the network. It can be considered as the first line of defense against intruders.
2.2 Non-repudiation is the verification that the data was sent with a user credentials so that without denial or repute the data can be associated to the sender.
2.3 Confidentiality is the assurance that the data could not have been accessed by any other user than the designated recipient for whom it was meant; thus insuring that the data was untouched until reception.
2.4 Data integrity and consistency is the assurance that the content of the data was not modified while in transit.
2.5 Availability is the proportion of time that a system is in a functioning state. Each of these attributes brings its network requirements whose balance and compromises make network security challenging.
2.6 Privacy is the assurance of the sender that his identity is not revealed to the receiver.

IV. PRIVACY IN VANETS

Attacks on privacy [14,19] over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle´s circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:
Identity revealing. Getting the owner´s identity of a given vehicle could put its privacy at risk. Usually, a vehicle´s owner is also its driver, so it would simplify getting personal data about that person.
Location tracking. The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle´s profile and, therefore, that of its driver [16].

V. REVIEW OF METHODOLOGIES TO IMPLEMENT PRIVACY IN VANETS

While the pure pseudonym schemes do not support the secure functionality of authentication, integrity, and nonrepudiation, an anonymous signing protocol [39] is proposed to provide such functions as well as privacy. In the protocol, each vehicle preloads a large number of certificated anonymous public/private key pairs. A key pair will be used for a short period of time and then be discarded. Each key pair is assigned to only one user, and authorities maintain the key distribution records which can be used to trace possible malicious vehicles. The shortcoming of this protocol is that it requires vehicles to store a large number of pseudonyms and certifications, where a revocation scheme for abrogating malicious vehicles is difficult to implement. It is preferable to preserve the location privacy of a vehicle by breaking the linkability between two locations, for which the vehicle can update its pseudonym after each transmission. Considering that a powerful adversary may still link the new and old pseudonyms by monitoring the temporal and spatial relations between new and old locations, the techniques of mix zone [10] and silent period [27] have been proposed to enhance the pseudonym scheme. Each vehicle in a mix zone will keep silent in transmission, and randomly update its pseudonym when it travels out of the mix zone and becomes reactivated. Given a reasonable large mix zone, the location privacy can be well protected due to the un-traceability of location and pseudonym updating in the silent period.

The group signature [26] is a promising security scheme to provide privacy in VANETs. In the group signature, one group public key is associated with multiple group private keys. Under the group signature scheme, although an eavesdropper can know that a message is sent by the group, it cannot identify the sender of the message. A general vehicular communication framework based on group signature is given in [27]. Lin et. al. systematically discuss how to implement group signature protocol in VANETs [28]. In the AMOEBA [40], vehicles form groups. The messages of all group members are forwarded by the group leader, which implies that the privacy of group members is protected by sacrificing the privacy of group leader. Moreover, if a malicious vehicle is selected as a group leader, all group members' privacy may be leaked by the malicious leader.

The work in [29] combines pseudonym schemes with the group signature to avoid storing pseudonyms and certifications in vehicles.

Gollan and Meinel [30] propose the use of digital signatures along with Global Positioning System technology to securely identify cars, improve the fleet management, and provide new applications for the private and public sectors.

Cryptographic digital signatures are applied to messages or hashes over messages to provide authenticity, integrity protection and non- repudiation. Digital message signatures are commonly using public-private key cryptography. Messages or hashes over the respective messages are signed with the message originators private keys. By using private key, it is guaranteed that the messages originate from nodes holding the required cryptographic key material and the messages have not been altered by intermediate forwarding nodes. The message receiver verifies the integrity and authenticity of the messages, by using the corresponding public keys. The node cannot be impersonated because the node only knows private key. In VANETs, any message sent by a vehicle should be digitally signed specially safety messages or warning messages. Furthermore, messages that serve as input or triggers to the safety system could also be signed. The main advantage is the requirements for digitally signature are very small i.e. the nodes need a possibility to receive or create and store cryptographic key pairs. They need the processing power for creating and verifying message signatures.

Main disadvantage is Message forging and denial of service (DoS) attacks are possible.

A foundational proposal is given by Raya and Hubaux [42]. The authors use anonymous certificates to hide the real identities of users. Although anonymous certificates do not contain any publicly known relationship to the true identities of the key holders, privacy can still be invaded by logging the messages containing a given key and tracking the sender until her identity is discovered (e.g., by associating her with her residence).

Lin *et al.* [31] presented Grey Systems and Intelligent Services (GSIS), which is a conditional privacy-preserving vehicular communications protocol based on group signatures and ID-based signatures [32]. The main advantage of using group signature schemes is that they guarantee the unlinkability of the messages because group members can anonymously sign on behalf of the group.

In the GSIS protocol, a single membership manager who issues secret member keys for vehicles is used. Unfortunately, this approach cannot effectively cope with the exclusion of compromised vehicles from the system.

The Secure Group Communications (SeGCom) scheme proposed in [33] is a lightweight solution that addresses some of these challenges for the V2V scenario by exploiting only one encryption method when creating and disseminating emergency messages.

Several proposals suggest the use of a public key infrastructure (PKI) and digital signatures to secure VANETs. To evict misbehaving vehicles, Raya et al. further proposed protocols focusing on revoking certifications of malicious vehicles [47]. A big challenge arising from the PKI-based schemes in VANETs is the heavy burden of certificate generation, storage, delivery, verification, and revocation.

Blum and Eskandarian [41] propose a secure communications architecture based on a PKI and a virtual network controlled by cluster heads intended to counter the so-called “intelligent collisions,” which are collisions that are intentionally caused by malicious vehicles. This approach produces a remarkable overhead, and the use of cluster heads can create bottlenecks.

The authors in [34] proposed an ID-based cryptosystem (for safety-related applications) that implements strong repudiation and privacy while eliminating the overheads associated with certificate management prevalent in Public Key Infrastructure (PKI) systems.

In [43], the method of mix zones is used to enhance the anonymity of vehicles. However, this scheme still relies on preloading a large set of anonymous certificates in each vehicle.

Wasef et al. [35] propose an Efficient Certificate Management Scheme for Vehicular Ad Hoc Networks (ECMV) based on a Public Key Infrastructure (PKI). In ECMV, each node has a short-lifetime certificate, which can be updated from any RSU. The scheme depends on frequent update of the certificates to provide privacy-preserving authentication.

In [46] RSU based signature key establishment is proposed. Vehicles negotiate with RSU using their group signature keys to obtain safety message signing key which has a very short period of lifetime. When message signing key expires, vehicles need to renegotiate for new signing key with RSU. Introducing communication overhead, changing signature key implies changing all identifiers Offering great potential for privacy protection for VANET, group signature schemes introduce scalability problem. Forming groups containing large number of vehicles and allowing mobility between regions administrated by different group managers are the problems to be addressed.

In [45], by exploiting a keyed hash message authentication code, a scheme with low communication overhead is proposed for secure vehicle communication. This scheme requires a vehicle to obtain a symmetric key from an RSU using a key agreement protocol. To protect its privacy, the vehicle should use different public keys to communicate with the RSUs. Hence, the vehicle still needs to preload a certain number of anonymous certificates. As to robustness, the schemes in [44] and [45] fully rely on RSUs. If an RSU collapses, then these schemes will no longer work.

We have proposed achieving location privacy by using random encryption periods (REPs) where a vehicle changing its certificate surrounds itself with an encrypted communication zone using group communications until it ensures that all the conditions to be tracked are violated. How to protect the location privacy of vehicles against legitimate insiders in traditional certificate-based PKI is still an open research issue. [36]

Elliptic curve cryptography is adopted to reduce the verification delay and transmission overhead. The security of ABAKA is based on the elliptic curve discrete logarithm problem, which is an unsolved NP complete problem. To deal with the invalid request problem, which may cause the batch verification fail, a detection algorithm has been proposed.[37]

We deployed a hierarchical identity-based cryptography to the location-based signature verification for providing location assurance, and a pseudonym-based privacy-preserving authentication. ID-based authenticated key agreement for mutual authentication between a vehicle and an RSU, and the hierarchical ID-based signature for location-based signature generation and verification for location assurance. [38]

This scheme provides unconditional privacy and removes the need of group manager. A signer can create a signature on behalf of an ad hoc group without taking their consent by using public keys of the ring members. This scheme has limited usefulness in VANETs as it provides unconditional privacy without non repudiation [48]

VI. CONCLUSION

A review of the various approaches to achieve privacy in VANETs have been made in the recent years. However each of the methods has advantages as well as disadvantages. A totally acceptable method which overcomes all the drawbacks is yet to be achieved and research in this direction has been done at present. The security aspects have to be achieved as it of paramount importance else implementation of VANETs will not be a success.

ACKNOWLEDGEMENTS

I acknowledge my guide who has been a constant source of motivation by guiding me all the way.

REFERENCES

[1] Ho Ting Cheng, Hangguan Shan, Weihua Zhuang, Infotainment and road safety service support in vehicular networking: From a communication perspective, Mechanical Systems and Signal Processing 25 (2011) 2020–2038, journal homepage: www.elsevier.com/locate/jnlabr/ymssp

[2] Josiane Nzouonta, Neeraj Rajgure, Guiling (Grace) Wang, "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009

[3] Razvan Stanica , Emmanuel Chaput, André-Luc Beylot, ―Simulation of vehicular ad-hoc networks: Challenges, review of tools and recommendations Computer Networks, journal homepage: www.elsevier.com/ locate/comnet2011.

[4] C. Sommer, Z. Yao, R. German, and F. Dressler, "Simulating the Influence of IVC on Road Traffic Using Bidirectionally Coupled Simulators," Proc. IEEE INFOCOM: Mobile Networking for Vehicular Environments (MOVE '08), Apr. 2008.

[5] M. Bakhouya , J.Gaber , P.Lorenz, "An adaptive approach for information dissemination in Vehicular Ad hoc Networks" Journal of Network and Computer Applications, journal homepage: www.elsevier.com/locate/jnca

[6] M.E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," Proc. EuropeanWireless Conf. '02, Feb. 2002.

[7] A. Shastri, R. Dadhich, Ramesh C. Poonia, "Performance Analysis Of On-Demand Routing Protocols For Vehicular Ad-Hoc Networks" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011 DOI : 10.5121/ijwmn.2011.3407

[8] Yasser Toor And Paul Mühlethaler, Inria "Vehicle Ad Hoc Networks: Applications And Related Technical Issues" IEEE Communications Survey**,** 3rd Quarter 2008, Volume 10, No. 3 www.comsoc.org/pubs/surveys

[9] Hannes Hartenstein, University of Karlsruhe Kenneth P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks" Toyota Technical Center.

[10] J. Freudiger, M. Raya, M. Feleghhazi,P. Papadimitratos and J.- P.Hubaux., "Mix zones for location privacy in vehicular networks," in Proc. International Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia, Aug., 2007.

[11] Lo-Yao Yeh , Yen-Cheng Chen , Jiun-Long Huang, "PAACP: A portable privacy-reserving authentication and access control protocol in vehicular ad hoc networks" Computer Communications 34 (2011) 447–456, Contents lists available at ScienceDirect Computer Communications journal homepage: www.elsevier.com/locate/comcom

[12] Jinyuan Sun, Chi Zhang, Yanchao Zhang, Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 9, SEPTEMBER 2010.

[13] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, Xuemin (Sherman) Shen, "A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs" IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 13, NO. 1, MARCH 2012.

[14] David AntolinoRivas , Jose´ M. Barcelo´ Ordinas, Manel Guerrero Zapata,Julian D.Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation" Journal of Network and Computer Applications 34 (2011) 1942–1955, Contents lists available at ScienceDirect journal homepage: www.elsevier.com/locate/jnca

[15] Bidi Ying , DimitriosMakrakis , HusseinT.Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs" , Contents lists available at SciVerse ScienceDirect journal homepage: www.elsevier.com/locate/jnca

[16] Jinyuan Sun, Xiaoyan Zhu, Chi Zhang, Yuguang Fang, "RescueMe: Location-Based Secure and Dependable VANETs for Disaster Rescue" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011

[17] Ahren Studer, Elaine Shi, Fan Bai§, & Adrian Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs" CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office.

[18] Paolo Cencioni , Roberto Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication" Computer Communications 31 (2008) 2790–2802 , www.elsevier.com/locate/comcom

[19] Levente Butty´an, Tam´as Holczer, and Istv´an Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs" F. Stajano et al. (Eds.): ESAS 2007, LNCS 4572, pp. 129–141, 2007. c_Springer-Verlag Berlin Heidelberg 2007

[20] Dandan Ren and Suguo Du, Haojin Zhu, "A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs", IEEE ICC 2011 proceedings, 978-1-61284-231-8/11/$26.00 ©2011 IEEE.

[21] K. Plo¨ ßl, T. Nowey, and C. Mletzko, "Towards a Security Architecture for Vehicular Ad Hoc Networks," Proc. First Int'l Conf. Availability, Reliability and Security (ARES '06), Apr. 2006.

[22] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," Proc. Fourth Workshop Hot Topics in Networks (HotNets IV), Nov. 2005.

[23] M. Raya and J-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, special issue on security of ad hoc and sensor networks, vol. 15, no. 1, pp. 39-68, 2007.

[24] J.Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing Auditability and Privacy in Vehicular Networks," Proc. First ACM Int'l Workshop QoS and Security for Wireless and Mobile Networks (Q2SWinet '05), pp. 79-87, Oct. 2005.

[25] T. Leinmu¨ ller, C. Maiho¨ fer, E. Schoch, and F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," Proc. Third ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '06), Sept. 2006.

[26] Lo-Yao Yeh , Yen-Cheng Chen , Jiun-Long Huang, "PAACP: A portable privacy-reserving authentication and access control protocol in vehicular ad hoc networks" Computer Communications 34 (2011) 447–456, Contents lists available at Science Direct Computer Communications journal homepage: www.elsevier.com/locate/comcom

[27] L.Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in Proc. IEEE WCNC, pp. 1187- 1192, 2005.

[26] D. Chaum and E. van Heyst, "Group signatures," in Proc. Advances in Cryptology Eurocrypt, vol. 547, pp. 257-265, 1991.

[27] J. Guo, J.-P. Baugh and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. IEEE INFOCOM, Anchorage, Alaska, May 2007.

[28] X. Lin, X. Sun, P.-H. Ho and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442-3456, 2007.

[29] G. Calandriello, P. Papadimitratos, A. Lloy, and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," in Proc. ACM Mobicom, pp. 19-28, QC, Canada, Sept. 2007.

[30] L. Gollan and C. Meinel, "Digital signatures for automobiles, Institut für Telematik e.V, Trier, Germany, Tech. Rep., 2002. [Online]. Available: http://www.hpi.uni potsdam.de/fileadmin/hpi/FG_ITS/papers/DigitalSignaturesAuto02.pdf

[31] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh.Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[32] A. Shamir, "Identity based cryptosystems and signature schemes," in Advances in Cryptology—CRYPTO, vol. 196, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1984, pp. 47–53.

[33] Verma, M., & Dijiang, H. (2009). SeGCom: secure group communication in VANETs. In Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009, Las Vegas, January 2009.

[34] Choi, J., & Jung, S. (2009). A security framework with strong non-repudiation and privacy in VANETs. In Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009, Las Vegas, January 2009.

[35] Wasef A, Jiang Y, Shen X (2008) ECMV: efficient certificate management scheme for vehicular networks. In: Proceedings of the IEEE GLOBECOM 2008

[36] "Complementing Public Key Infrastructure To Secure Vehicular Ad Hoc Networks" Albert Wasef And Rongxing Lu, University Of Waterpool Xiaodong Lin, University Of Ontario Institute Of Technology Xuemin (Sherman) Shen, University Of Waterloo IEEE Wireless Communications • October 2010

[37] "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks" Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 60, NO. 1, JANUARY 2011

[38] A Privacy-Preserving Location Assurance Protocol for Location-Aware Services in VANETs Youngho Park · Chul Sur · Kyung-Hyune Rhee Published online: 30 October 2011© Springer Science+Business Media, LLC. 2011 Wireless Pers Commun (2011) 61:779–791 DOI 10.1007/s11277-011-0432-2

[39] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[40] K.Sampigethava, L.Huang, M.Li, R.Poovendran, K.Matsuura and K.Sezaki, "AMOEBA: Robust location privacy scheme for VANET," in IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp.1569-1589, 2007.

[41] J. Blum and A. Eskandarian, "The threat of intelligent collisions," IT Prof., vol. 6, no. 1, pp. 24–29, Jan. 2004.

[42] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Secur., vol. 15, no. 1, pp. 39–68, Jan. 2007.

[43] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in Proc. ACM Workshop WiN-ITS, 2007.

[44] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in Proc. ACM Workshop WiN-ITS, 2007.

[45] C. Zhang, X. Lin, R. Lu, and P. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE ICC, May 19–23, 2008, pp. 1451–1457.

[46] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs" in IEEE 6th Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2009, pp. 1–9.

[47] Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.-P.: Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. IEEE Journal Selected Areas in Communication 25(8), 1557–1568 (2007)

[48] Conditional Privacy through Ring Signature in Vehicular Ad-hoc Networks Brijesh Kumar Chaurasia and Shekhar Verma M.L. Gavrilova and C.J.K. Tan (Eds.): Trans. on Comput. Sci. XIII, LNCS 6750, pp. 147–156, 2011 © Springer-Verlag B erlin Heidelberg 2011

[49] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing Vehicular Communications. In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006

[49] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing Vehicular Communications. In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006

[50] Task Group p, IEEE P802.11p: Wireless Access in Vehicular Environments (WAVE). draft standard ed. IEEE Computer Society, Los Alamitos (2006)

[51] Wang, S.Y., Lin, C.C., et al.: On Multi-hop Forwarding over WBSS-based IEEE 802.11(p)/1609 Networks. In: IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo, September 13-16 (2009), E-ISSBN 978-1- 4244-5123-4

[52] Farah, A.E., Bertrand, D.: A Light Architecture for Opportunistic Vehicle-to-Infrastructure Communications. In: Proceedings of the 8th ACM International Workshop on Mobility Management and Wireless Access, MobiWac 2010, Bodrum, Turkey, October 17-18 (2010)

[53] Yi, W., Akram, A., et al.: IEEE 802.11p Performance Evaluation and Protocol Enhancement. In: Proceedings of the IEEE International Conference on Vehicular Electronics and Safety, Columbus, OH, USA, September 22-24 (2008)

AUTHOR BIOGRAPHY

Sapna S. Kaushik completed her M.E. in Computer Science and Engg. from Amravati University. She is working as the Head of Department of Computer Engineering Department in D.B.N.C.O.E.T. Maharashtra State, India. Her current research interests are in the area of Vehicular ad hoc networks