International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

# A Study of Message Authentication Protocol with Reduced Computation in Vehicular Ad-hoc Network

**Jaishma Kumari B**

*Assistant Professor, Department of Computer Science and Engineering, Srinivas Institute of Technology, Merlapadavu, Valachil, Mangalore -574 143, Karnataka, India*

---

**Abstract -** *The Vehicular ad-hoc network is an important component of Intelligent Transportation Systems, which has a future potential in terms of different application that it can provide. It presents a very complex cyber-physical system where vehicles need to frequently broadcast their geographic information. Efficient working of the complete system requires proper processing of large data traffic rate that may be caused due to safety message broadcasting in an area with a high density of vehicles. This paper aims at study and analysis of protocol for reducing computation caused by the safety message authentication. Main focus of the study is a cooperative message authentication protocol (CMAP) which enables sharing of verification results between vehicles in a cooperative way and thereby significantly reduces the number of safety messages that each vehicle needs to verify. This reduces vehicles' computation burden. The study also includes the verifier selection algorithms for detecting invalid messages at high rate. Further the study covers analytical model for CMAP and the existing probabilistic verification protocol [8], considering the hidden terminal impact*

***Key Words***: **vehicular ad-hoc network, security, safety application, cooperative authentication, missed detection ratio.**

## 1. INTRODUCTION

The intelligent transportation system (ITS) constitutes advanced communications technologies integrated into transportation infrastructure and vehicles. The vehicular ad-hoc networks (VANET) being at the heart of ITS, have found a wide range of applications such as safety and eliminating excessive cost of traffic collisions, providing information and entertainment services, extending reach of infrastructure networks, mobile advertising, security and privacy provisioning, and energy consumption control for hybrid electric vehicles (HEVs) [3], [7], [28] etc..

The VANET presents a very complex cyber-physical system (CPS) with intricate interplay between the physical domain and the cyber domain. On one side, the complicated physical domain of VANET incurs many challenging issues to the cyber domain. For example, different transportation infrastructures, e.g., those in urban and country areas, require different road side unit (RSU) deployment strategy for optimal VNS performance. Frequent broadcast of safety messages from vehicle along the road may leak the travelling route of a vehicle, which could be a privacy issues. On the other side, the design of control algorithms and networking protocols in the cyber domain significantly impact the performance in the physical domain. For example, the network congestion conditions determine whether certain safety messages could be timely delivered to other vehicles. The lack of a good security solution or a stimulation scheme will discourage vehicles to collaborate with each other for safety related or entertainment-related applications.

This paper focuses on the security aspect of the vehicular cyber-physical system. Security and privacy are crucial for VANETs [3]. In a VANET safety application, each vehicle periodically broadcasts its geographic information (which can be obtained from a global positioning system (GPS) receiver) say, every 300 ms, including its current position, direction and velocity, as well as road information [2]. In order to provide secure functionality of authentication, integrity, and non-repudiation, every message sent by Vehicles needs to have a digital signature [4]. Verifying the signatures of the received messages will incur a significant computation overhead. Furthermore, vehicles have to change their signing keys periodically [2] or employ computational expensive techniques, such as short group signature [5], for the sake of privacy provisioning. Both methods will further increase vehicles' computation load for message verification. When the density of vehicles is high [6], [7], the computation overhead may become intolerable for the on board unit (OBU) installed on a vehicle. Cooperative message authentication is a promising technique to alleviate vehicles' computation overhead for message verification. In [8], vehicles verify messages in a cooperative manner, employing a probabilistic verification protocol (PVP). However, in order to guarantee cooperation efficiency, vehicles have to verify at least 25 messages within 300 ms, which is still a heavy computation burden. Our work in [7] studies how to properly select verifiers to further reduce the computation overhead in cooperative authentication, considering the hidden-terminal impact. However, both [7] and [8] focus only on one-dimensional (1-D) high way scenario.

In this paper, we present a cooperative message authentication protocol (CMAP) for a general two-dimensional (2-D) city road scenario with an assumption

that each safety message carries the location information of the sending vehicle. Verifiers of each message are defined according to their locations relative to the sender. Only the selected verifiers check the validity of the message, while those non-verifier vehicles rely on verification results from those verifiers. A brand new research issue with CMAP is how to select verifiers in the city road scenario. Our previous work [7] studies CMAP for the 1-D highway scenario. However, the CMAP in the 1-D scenario cannot be directly implemented to the 2-D city road scenario [9]. For example, on the highway, if we ignore collisions and packet loss in the wireless channel, two verifiers (one verifier in front of the sending vehicle and one verifier behind the sending vehicle) are enough to inform all the non-verifiers when invalid messages are identified. Obviously, this is not true in the city road case. In this paper, we propose three verifier selection algorithms, i.e., n-nearest method, most-even distributed method, and the compound method for the CMAP. We present both theoretical and simulation studies to examine the performance of the CMAP, in comparison to the PVP [8]. Specifically, this paper has three main contributions as follows.

- We develop an efficient cooperative message authentication protocol and associated verifier selection methods for a general 2-D city road scenario. With our CMAP protocol, the computation overhead of each vehicle can be reduced significantly compared to the pure probabilistic cooperative protocol [8].
- We develop an analytical model to quantitatively evaluate the performance of our CMAP protocol as well as the existing PVP protocol [8]. The accuracy of our protocol is verified through simulations.

We conduct NS2 simulations of an IEEE 802.11 based VANET over a practical road map to examine the missed detection ratio of invalid messages, when malicious vehicles are present. Simulation results confirm the efficiency improvement of CMAP compared to the existing method.

The remainder of this paper is organized as follows. Section II reviews more related work. Section III describes the system model. Section IV presents the detailed protocol design and discusses the verifier selection algorithms. Simulation results are presented in Section VI. Section VII gives the concluding remarks.

## 2. RELATED WORK

There have been many studies on how to protect the location privacy of a vehicle in a VANET, where each vehicle needs to periodically broadcast safety messages. A natural idea is using pseudonyms [32], where a vehicle can update its pseudonym after each transmission to break the link ability between its locations. The pseudonym scheme can be further enhanced with the techniques of mix zone [16] and silent period [17] to fully break the linkage between previous and current pseudonyms. The AMOEBA scheme [3] protects the location privacy of vehicles with a group-based technique. The messages of all group members are forwarded by the group leader. However, the group leader has to sacrifice its location privacy. Even worse, when a malicious vehicle is selected as the group leader, privacy of the whole group is under threat.

An anonymous signing protocol is proposed in [2] to provision security functions of authentication, integrity and nonrepudiation, in addition to the location privacy in VANET. In this protocol, each vehicle keeps a large number of certificated anonymous public and private key pairs. A key pair is assigned to only one user and will be discarded after a short period of time. One disadvantage of this scheme is that each vehicle has to store a large number of pseudonyms and certifications, so that a revocation for abrogating malicious vehicles is very difficult

The group signature [18] is a promising technique to provision both privacy and authentication. The group signature has the magic property that the signatures from different group members can be verified with the same group public key, so that the exact identities within the group are protected. A vehicular communication framework based on group signature is proposed in [19]. The work in [20] systematically discusses the implementation of group signature protocol in VANETs. The group signature is integrated with the pseudonym scheme in [21] to avoid storing pseudonyms and certifications in vehicles. While most of the existing studies on group signature rely on a centralized key management scheme, our previous study in [7] develops a distributed key management framework based on group signature to provision privacy in VANET. The framework is equipped with techniques to detect compromised road side units and their colluding malicious vehicles.

In a VANET safety application, it is critically important to design protocols with small computation overhead for timely and reliable message processing. The work in [10] shows that the TESLA technique, which is a hash function based protocol, can be applied in VANET for an authentication protocol with small computation overhead. However, TESLA does not have the property of non-repudiation. An aggregate signature and certificates verification scheme is proposed in [11], which is particularly efficient when the density of vehicles is high. Zhang *et. al.* developed an infrastructure aided message authentication protocol which requires infrastructures to cover all the area because they have to be involved in the authentication [12].

A promising thread of techniques to reduce the computation overhead in authentication is cooperative authentication.

Through cooperative verification, the number of messages to be authenticated by each vehicle will be reduced considerably. Our cooperative message authentication protocol (CMAP) in [7] indicates that purely random selection of verifiers cannot lead to the best performance of cooperative authentication, due to the impact of hidden terminals, and proposes a verifier selection approach to improve performance. However, the work in [7] only considers the 1dimension highway scenario. In [29], we extend the CMAP to a practical two-dimensional city road scenario. An important open issue with the existing cooperative authentication is the lack of analytical model. Although there are a few analytical studies on message broadcasting in VANET [27], [30], [31] , none of them can be directly applied to analyze the cooperative authentication protocols. In this paper, we develop analytical models for the proposed CMAP and the existing PVP protocols, taking into account the hidden terminal problem.

VANETs can be established based on different networking protocols such as cellular networks, IEEE 802.16 (WiMAX), and IEEE 802.11 [22], [23]. Cellular and WiMAX networks relies on the availability of base station, which is expensive and might not be available in under developed areas. The IEEE 802.11 based network can support both base station to vehicle communication and vehicle to vehicle adhoc communication, so it is considered as the mainstream protocol for VANETs [8], [12], [24]–[27]. In this paper, we also focus on the IEEE 802.11 based VANETs.

## 3. SYSTEM MODEL

As shown in Fig-1, the entities in VANETs can be classified into three categories: the authority, road side infrastructures and vehicles.

**The authority** generates all the keys and is responsible for the system maintenance.

**Road side infrastructures (RSI)** are wireless infrastructures that are deployed at the road sides. Traffic lights or road signs can serve as RSI after renovation. Note that, in the VANETs, especially at the early stage, RSI may not be available in some areas.

**Vehicles** are equipped with on board units which are in charge of all communication and computation tasks and GPS receivers [13] utilizing DGPS technology [14] with an accuracy on the order of one meter. As shown in Fig. 1, before vehicles join the VANETs, they have to register to the authority and then preload signing keys and credentials off-line from the authority. In our protocol, we employ the short group signature [7], [20] as the signing protocol for vehicles. In the real application, vehicles may choose the anonymous signing protocol [2] or other protocols instead of the group signature protocol. But the essence is the same. The verification time for short group signature is 11 ms with a 3 GHz Pentium IV system [7] and all the safety messages must be verified within 100 ms after they are sent out.

Vehicles communicate with each other through radio over the IEEE 802.11p on 5.9 GHz [15]. Among all seven communication channels in the IEEE 802.11p, there is one accident avoidance channel for safety message broadcasting. All vehicles broadcast their geographic information periodically in the accident avoidance channel with the same communication range, e.g. 300 meters. Moreover, warning messages induced by the cooperation are also transmitted in this channel.

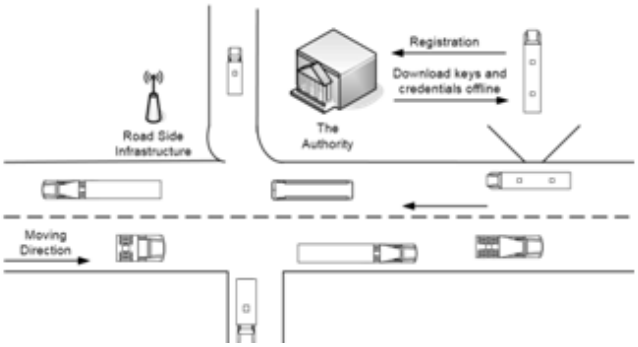


**Fig -1**: Vehicular Ad-hoc Network

We assume that the overwhelming majority of vehicles are honest which is reasonable in the civilian use system. Moreover, "good" vehicles are willing to cooperate with each other. In our protocol, there are also some malicious vehicles who always broadcast invalid messages. Meanwhile, they never share their verification results with others.

Before discussing the details of the protocol, we would like to demonstrate two concepts. If a vehicle would like to cheat others, it will send false messages. The false message means that the content of the message is wrong, but the sender's signature may be valid. For example, a vehicle may claim a traffic jam somewhere; however in fact no traffic jam happens there. With a valid signature attached in the message, the authority can track the cheating vehicle. The other phrase we will use in the cooperative message authentication is invalid message. An invalid message is a message that cannot pass the signature verification. In such a case, even the authority cannot find the sender of an invalid message. So, we must filter all the invalid messages.

## 4. COOPERATIVE MESSAGE AUTHENTICATION

In this section, we will discuss cooperative message authentication protocol for the city road scenario in details. The work flow of CMAP will be presented followed by three verifier selection algorithms that are tailored for the city road scenario,

### 4.1 The Workflow Overview

In the CMAP, each vehicle sends periodically broadcasted messages (PBM) which include its current geographic information every 300 ms. when its neighboring vehicles receive the PBM, they will decide whether they are verifiers of this message in a distributed manner according to the verifier selection protocol. If a vehicle is the verifier of the message, it will start to verify the message by itself. Non-verifiers will wait for cooperative warning messages (CWM) from verifiers. Once an invalid message is identified, verifiers will broadcast a one hop warning message to others. Otherwise, verifiers will keep silent. When a non-verifier receives a CWM from other vehicles, it will double check the corresponding PBM. The reason for such double-check is to prevent a valid PBM from being discarded in case bad vehicles can send malicious CWMs. Non-verifiers will consume the message if it does not receive any CWM from others within 100 ms. In Fig-2, the solid circle is the communication range of the sender and the dotted circle is the communication range of a verifier. We define the shaded area as the coverage area of the verifier. All non-verifiers in the coverage area of the verifier can be informed by it when the sender broadcasts invalid messages.

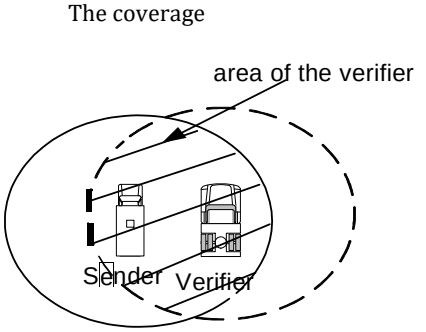


**Fig -2**: The coverage area

### 4.2 The Process Procedure

Vehicles cooperate with each other according to the process flow chart illustrated in Fig. 3. The procedure has been discussed in our previous work [7]. However, for the purpose of completeness, we still give a brief introduction in this paper.

Basically, the cooperative authentication mechanism is composed of several components including a verifier selection process, a cooperative authentication process, a neighbor vehicle list, a process queue and a message storage buffer. The verifier selection process determines whether the vehicle is a verifier of a received PBM according to the verifier selection algorithm and vehicle location information. Meanwhile it maintains the neighbor vehicle list and the process queue. The cooperative authentication process controls message authentication and cooperation among vehicle. In other words, the verifier selection process inserts the selected PBM into the process queue while the cooperative authentication process clears it up. The neighborhood list contains neighbor vehicles geographic information. Messages that are not processed will be stored in the message storage buffer.

As shown in Fig-3 upon receiving a PBM, a vehicle extracts the geographic information from the message and updates the neighbour vehicle list accordingly. It than decides whether it should be a verifier according to verifier selection algorithm based on the location of its own, the locations of its neighbours and the sender of the received PBM. If the vehicle decides to be a verifier and the PBM can be processed in time (within the verification period (e.g., 100 ms) which is shorter than the broadcast period), it will insert the message to the process queue and verify this message onc4 it reaches the queue front. Being a verifier, if the vehicle finds that PBM is an invalid message (i.e., the sender is a malicious vehicle), it will inform its neighbours by broadcasting a cooperative warning message (CWM).

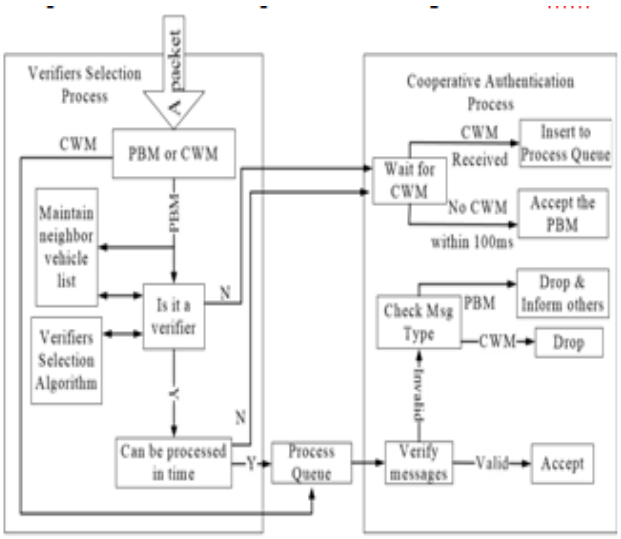


**Fig -3**: The Process Procedure

Otherwise, the message is valid; hence it will be accepted by the verifier and no CWN will be generated. If the vehicle is not a verifier for the received PBM in its message storage buffer for one verification period. If there is no CWM related to this PBM received and delete it from the storage buffer. When a CWM is received and the corresponding PBM is found in the buffer, the vehicle will delete the PBM from the buffer and insert the PBM to the front of the process queue and verify it. If this PBM is valid, it will be accepted; otherwise, the vehicle will discard the message without sending any CWM. In conventional non-cooperative message authentication protocols, each vehicle verifies all its received PBMs sent from its neighbours. In our CMAP, with the help of verifiers,

each vehicle only needs to verify a very small amount of PBMs. In the CMAP, the shorter the CWM is, the smaller the communication overhead resulted from cooperation among vehicles will be. The payload of CWM can be the hash value of the invalid PBM or the timestamp included in the PBM.

### 4.3 Verifier Selection Algorithm

Different from the 1-D highway scenario, when vehicles travel on the 2-D city road, it is more difficult for verifiers to inform all the non-verifiers of a certain message. Without an elegant design, the missed detection ratio of invalid messages may very high. In this section, three verifier selection algorithms, i.e., n-nearest method, most-even distributed method and the compound method are proposed.

As illustrated in Fig-4, the vehicle at the center of the circle is the sender. The circle represents the communication range of the sender. In the figure, there are totally 15 vehicles located in the communication range of the sending vehicle. When the sender broadcasts a message, each vehicle decides whether to be a verifier of the message in a fully distributed manner and verifies the message in a cooperative way to save computation resources. We need to emphasize that the CMAP will be activated only when the density of vehicles reaches a threshold. Otherwise the message-by-message verification is preferred. Details about the authentication mode switch mechanism will be discussed later. We draw 15 neighboring vehicles in Fig-4 just to illustrate verifier selection methods. In the real application, more neighboring vehicles may be needed to trigger the CMAP.

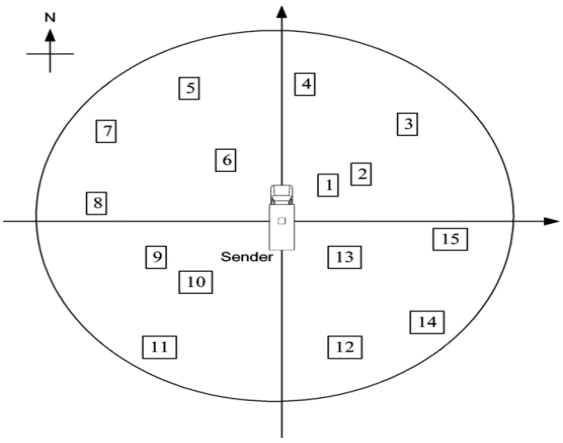


**Fig -4**: Verifier Selection

#### 1) N-Nearest Method

Selecting *n nearest vehicles* is the simplest way to define verifiers. Consider an arbitrary vehicle within the sender's communication range. As shown in Fig-5, when the vehicle receives the sender's message, it calculates the distance between itself and the sender and the distances between the sender and all the neighbors of the vehicle and then compare. If the vehicle finds itself is one of the *n* nearest vehicles to the sender, it needs to be a verifier of this message. For example, if *n* = 4, vehicles 1, 2, 6 and 13 will serve as verifiers.

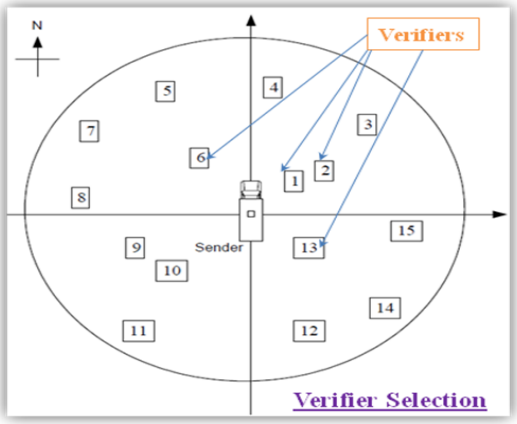


**Fig -5**: Verifier Selection for N-Nearest Method

#### 2) Most-Even Distributed Method

In order to tackle the problem above, we propose a most-even distributed method. In this method, the selected verifiers of a message are distributed evenly in the communication range of the sender, and most the non-verifiers can be informed of any invalid PBM by the verifiers. In this method, the angles between receivers and the sender are utilized to select verifiers. Zero degree angle can be defined according to either geographic orientations (e.g., the east) or the direction of the road on which the sender travels. As shown in Fig-6, the area indicating the communication range of the sender is evenly divided by *n* rays. For ease of exposition, take *n* = 4 for example. The most-even distributed verifier selection algorithm for each vehicle works as follows:

- Step 1: Upon receiving a PBM, the vehicle extracts the sender's location information from the message and determines the 4rays (e.g., towards the north, south, west and east) started at the sender.
- Step 2: It compares its own location with those of all its neighbors and decides if it is the closest to any of these 4 rays.
- Step 3: If Step 2 returns true, the vehicle becomes a verifier to this PBM.

In Fig-6, vehicle 4, 8, 12 and 15 will be verifiers. Similar to the N-nearest method, due to limited scope of each vehicle, more than *n* verifiers may be selected sometime. Moreover, if a vehicle is the closest one to two rays, it is also possible that

less than *n* verifiers are selected. In an extreme case, if a vehicle is very close to the sender, possibly only this vehicle will be the verifier.

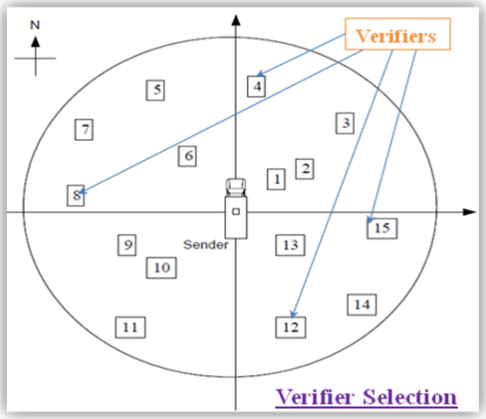


**Fig -6**: Verifier Selection for Most-Distributed Method

### 3) The Compound Method

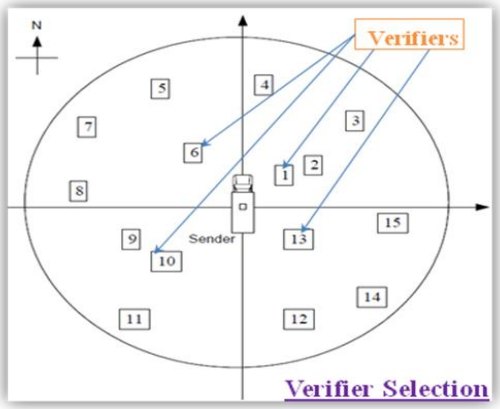


**Fig -7**: Verifier Selection for Compound Method

The 2-dimension verifier selection algorithm, verifiers are expected to be evenly distributed and close to the sender. As aforementioned, even distribution has the advantage that most non-verifiers can be informed of any invalid PBM by the verifiers, while verifiers in the N-nearest method are closer to the sender and can bring a larger coverage area. Therefore, combining the merits of the above two methods together, we propose the compound method. In this method, the area will be divided into *n* parts. The nearest vehicle to the sender in each part will be selected as a verifier. For instance, when *n* = 4, the algorithm that a vehicle decides whether to verify a received PBM works as follows:

- Step 1: Upon receiving a PBM, the vehicle extracts the sender's location information from the message and determines the 4 rays to equally divide the area into four sectors centered at the sender. It then decides which sector it belongs to.
- Step 2: It compares its own location with those of all its neighbors within the same sector, and then decides if it is the closest to the sender.
- Step 3: If Step 2 returns true, the vehicle becomes a verifier to this PBM.

In Fig-7, vehicle 1, 6, 10 and 13 will be selected when the compound method is employed. When *n* = 4, consider a vehicle close to one of the outmost corners of the sector to which it belongs. If it has no other neighbor within this sector, with limited scope, it is possible for the existence of a blind area that may deviate its decision. However, such a situation is possible when the vehicle density is very low. Moreover, when *n* ≥ 6, one can easily see that the communication range of each vehicle will cover its own sector. In this case, the distributed decisions are accurate. Therefore, compared with the above two methods, the compound method is more convenient for distributed implementation.

## 5. CONCLUSIONS

In this paper, we have studied message verification and verifier selection methods in vehicular cyber-physical systems. We propose a cooperative message authentication protocol (CMAP) and three verifier selection methods, i.e., the n-nearest method, the most-even distributed method and the compound method. For one-dimensional roads, we have developed an analytical model for the proposed protocol and the existing probabilistic verification protocol. Moreover, we also show that the missed detection ratio of the compound method can be reduced if we use more verifiers, reduce the transmission range or increase the broadcast periods

## REFERENCES

[1] Y. Hao, J. Tang, Y. Cheng, and C. Zhou, "Secure data downloading with privacy preservation in vehicular ad hoc networks," in Proc. IEEE ICC, May 2010, pp. 1–5.

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

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

[4] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in Proc. IEEE Globecom, Nov. 2008, pp. 1–5.

[5] D. Boneh, X. Boyen, and H. Shacham, ‘‘Short group signatures,’’ in Proc. CRYPTO 2004, vol. 3152. pp. 41–55.

[6] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, ‘‘Routing in sparse vehicular Ad Hoc wireless networks,’’ IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1538–1556, Oct. 2007.

[7] Y. Hao, Y. Cheng, C. Zhou, and W. Song, ‘‘A distributed key management framework with cooperative message authentication in VANETs,’’ IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.

[8] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, ‘‘An efficient message authentication scheme for vehicular communications,’’ IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[9] M. Pan, P. Li, and Y. Fang, ‘‘Cooperative communication aware link scheduling for cognitive vehicular ad-hoc networks,’’ IEEE J. Sel. Areas Commun., vol. 30, no. 4, pp. 760–768, May 2012.

[10] X. Lin, C. Zhang, X. Sun, P.-H. Ho, and X. Shen, ‘‘Performance enhancement for secure vehicular communications,’’ in Proc. IEEE Global Telecommun. Conf., Nov. 2007, pp. 480–485.

[11] A. Wasef and X. Shen, ‘‘ASIC: Aggregate signatures and certificates verification scheme for vehicular networks,’’ in Proc. IEEE Globecom, Dec. 2009, pp. 1 – 6.

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

[13] J. Jeong, S. Guo, T. He, and D. Du, ‘‘Trajectory-based data forwarding for light-traffic vehicular Ad Hoc networks,’’ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 743–757, May 2010.

[14] P. Enge, ‘‘Retooling the global positioning system,’’ Sci. Amer., vol. 290, no. 5, pp. 90–97, May 2004.

[15] D. Niyato, E. Hossain, and P. Wang, ‘‘Optimal channel access management with QoS support for cognitive vehicular networks,’’ IEEE Trans. Mobile Comput., vol. 10, no. 4, pp. 573–591, Feb. 2011.

[16] J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos, and J. P. Hubaux, ‘‘Mix zones for location privacy in vehicular networks,’’ in Proc. Int. Workshop Wireless Netw. Intell. Trans. Syst., Aug. 2007, pp. 1–7.

[17] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, ‘‘Enhancing wireless location privacy using silent period,’’ in Proc. IEEE WCNC, Mar. 2005 , pp. 1187–1192.

[18] D. Chaum and E. van Heyst, ‘‘Group signatures,’’ in Proc. Adv. Cryptol. Eur., vol. 547. 1991, pp. 257–265.

[19] J. Guo, J.-P. Baugh, and S. Wang, ‘‘A group signature based secure and privacy-preserving vehicular communication framework,’’ in Proc. IEEE INFOCOM, May 2007, pp. 1 – 7.

[20] 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, Nov. 2007.

[21] G. Calandriello, P. Papadimitratos, A. Lloy, and J.-P. Hubaux, ‘‘Efficient and robust pseudonymous authentication in VANET,’’ in Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw., Sep. 2007, pp. 19–28.

[22] N. Banerjee, M. D. Corner, D. Towsley, and B. N. Levine, ‘‘Relays, base station and meshes: Enhancing mobile networks with infrastructure,’’ in Proc. 14th ACM Int. Conf. Mobile Comput. Netw., Sep. 2008, pp. 81–91.

[23] A. Studer, E. Shi, F. Bai, and A. Perrig, ‘‘TACKing together efficient authentication revocation, and privacy in VANETs,’’ in Proc. 6th Annu. IEEE VTC, Oct. 2007, pp. 484–492.

[24] X. Sun, ‘‘Anonymous, secure and efficient vehicular communications,’’ M.S. thesis, Dept. Comput. Sci., Univ. Waterloo, ON, Canada, 2007.

[25] D. Jiang and L. Delgrossi, ‘‘IEEE 802.11p: Towards an international standard for wireless access in vehicular environments,’’ in Proc. IEEE VTC, May 2008, pp. 2036–2040.

[26] G. Marha, G. Pau, E. De Sena, E. Giordano, and M. Gerla, ‘‘Evaluating vehicle network strategies for downtown Portland: Opportunistic infrastructure and the importance of realistic mobility models,’’ in Proc. Int. MobiSys Workshop Mobile Opportunistic Netw., 2007, pp. 47–51.

[27] X. Ma, X. Chen, and H. Refai, ‘‘Unsaturated performance of IEEE 802.11 broadcast service in vehicle-to-vehicle networks,’’ in Proc. IEEE VTC, Oct. 2007, pp. 1957–1961.

[28] M. Gerla and L. Kleinrock, ‘‘Vehicular networks and the future of the mobile internet,’’ Comput. Netw., vol. 55, no. 2, pp. 457–469, Feb. 2011.

[29] Y. Hao, T. Han, and Y. Cheng, ‘‘A cooperative message authentication protocol in VANETs,’’ in Proc. IEEE GLOBECOM, Dec. 2012, pp. 5562 – 5566.

[30] X. Ma, X. Chen, and H. Refai, ‘‘on the broadcast packet reception rates in one-dimensional MANETs,’’ in Proc. IEEE GLOBECOM, Dec. 2008, pp. 1 – 5.

[31] X. Ma and H. Refai, ‘‘Analytical model for broadcast packet reception rates in two-dimensional MANETs,’’ in Proc. IEEE ICC, Jun. 2011, pp. 1 – 5.

[32] L. Buttyan, T. Holczer, and I. Vajda, ‘‘on the effectiveness of changing pseudonyms to provide location privacy,’’ in Proc. ESAS, 2007, pp. 129–141.

[33] (2007). VanetMobiSim [Online]. Available: http://vanet.eurecom.fr/

[34] (2002). Topologically Integrated Geographic Encoding and Referencing System (TIGER) [Online]. Available: http://www.census.gov/geo/

www/tiger/

[35] Y. Cheng, X. Ling, and W. Zhuang, ‘‘A protocol-independent approach for analyzing the optimal operation point of CSMA/CA protocols,’’ in Proc. IEEE INFOCOM, Apr. 2009, pp. 1 – 9.

[36] X. Ma, J. Zhang, and T. Wu, ‘‘Reconsider broadcast packet reception rates in one-dimensional MANETs,’’ in Proc. IEEE GLOBECOM, Dec. 2010, pp. 1 – 6.

[37] G. Bianchi, ‘‘Performance analysis of the IEEE 802.11 distributed coordination function,’’ IEEE J. Sel. Areas Commun., vol. 18, no. 3, pp. 535–547 , Mar. 2000.