IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 2 April 2013; revised 30 May 2013; accepted 29 June 2013. Date of publication 12 July 2013;
date of current version 20 September 2013.

Digital Object Identifier 10.1109/TETC.2013.2273221

Cooperative Message Authentication in Vehicular Cyber-Physical Systems

WENLONG SHEN, LU LIU, XIANGHUI CAO (Member, IEEE), YONG HAO, AND YU CHENG (Senior Member, IEEE)

Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616, USA
CORRESPONDING AUTHOR: Y. CHENG (cheng@iit.edu)

This work was supported in part by NSF grant CNS-1117687.

ABSTRACT The vehicular ad hoc network presents a very complex cyber-physical system with intricate interplay between the physical and cyber domains. In the physical domain, vehicles need to frequently broadcast their geographic information. The safety message broadcasting in an area with a high density of vehicles tends to incur a large data traffic rate that should be properly processed in the cyber domain. In this paper, we address the issue of large computation overhead caused by the safety message authentication. Especially, a cooperative message authentication protocol (CMAP) is developed to alleviate vehicles' computation burden. With CMAP, all the vehicles share their verification results with each other in a cooperative way, so that the number of safety messages that each vehicle needs to verify reduces significantly. Furthermore, we study the verifier selection algorithms for a high detection rate of invalid messages in a practical 2-D road scenario. Another important contribution in this paper is that we develop an analytical model for CMAP and the existing probabilistic verification protocol [8], considering the hidden terminal impact. Simulation results over a practical map are presented to demonstrate the performance of the proposed CMAP with comparison to the existing method.

INDEX TERMS Vehicular ad hoc network, security, safety applications, cooperative authentication, missed detection ratio.

I. INTRODUCTION

The recent research efforts on transportation management have pointed to a paradigm shift in intelligent transportation systems (ITS), where advanced communications technologies are integrated into transportation infrastructure and vehicles. At the heart of ITS, the vehicular ad hoc networks (VANET) have found a wide range of applications including safety and mobility enhancement, data downloading for entertainment, mobile advertising, security and privacy provisioning, and energy consumption control for hybrid electric vehicles (HEVs) [3], [7], [28].

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 a vehicle along the road may leak the travelling route of a vehicle, which could be a privacy issue. 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.

II. 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 linkability 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 1-dimension 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 underdeveloped areas. The IEEE 802.11 based network can support both base station to vehicle communication and vehicle to vehicle ad hoc 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.

III. 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.

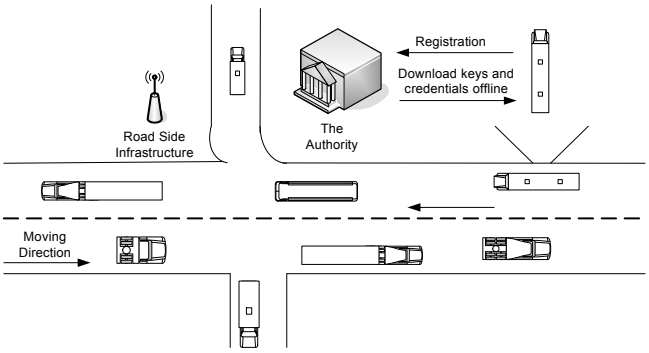


FIGURE 1. Vehicular ad hoc networks.

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.

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 signer of an invalid message. So, we must filter all the invalid messages.

IV. 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.

A. THE WORK FLOW 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.

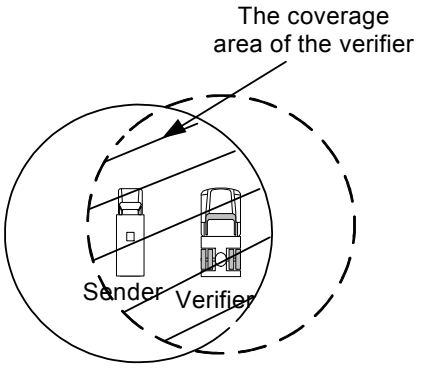


FIGURE 2. The coverage area.

B. 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 vehicles' location information. Meanwhile, it maintains the neighbor vehicle list and the process queue. The cooperative authentication process controls message authentication and cooperation among vehicles. 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.

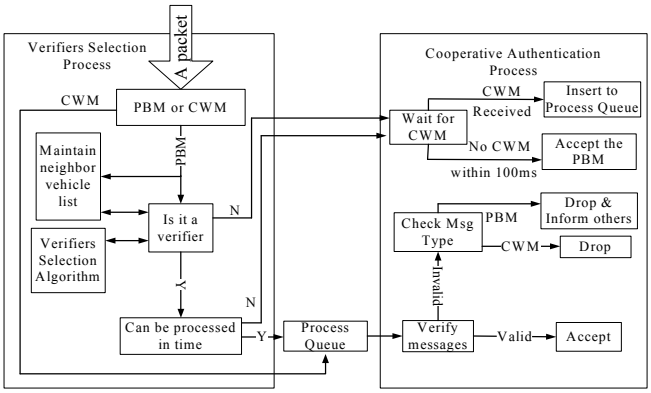


FIGURE 3. The process procedure.

As shown in Fig. 3, upon receiving a PBM, a vehicle extracts the geographic information from the message and updates its neighbor vehicle list accordingly. It then decides whether it should be a verifier according to the verifier selection algorithm based on the location of its own, the locations of its neighbors 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 once it reaches the queue front. Being a verifier, if the vehicle finds that the PBM is an invalid message (i.e., the sender is a malicious vehicle), it will inform its neighbors by broadcasting a cooperative warning message (CWM). Otherwise, the message is valid; hence it will be accepted by the verifier and no CWM will be generated. If the vehicle is not a verifier for the received PBM or cannot process the PBM in time, it will hold the PBM in its message storage buffer for one verification period. If there is no CWM related to this PBM received during the verification period, the vehicle will accept the PBM 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.[1] If this PBM is valid, it will be accepted; otherwise, the vehicle will discard the message without sending any CWM.

[1]The reason for such double-check is to prevent a valid PBM from being discarded in the case that malicious vehicles send fake CWMs.

In conventional non-cooperative message authentication protocols, each vehicle verifies all its received PBMs sent from its neighbors. 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.

C. VERIFIER SELECTION ALGORITHMS

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 be 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.

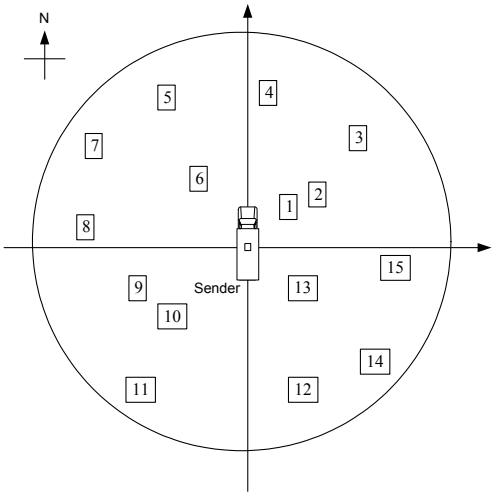


FIGURE 4. Verifier selection.

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. 4, 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.

The N-nearest method has two advantages. First, it is easy to implement. Vehicles only need to calculate their distances from the sending vehicle. Second, the closer a verifier is to the sender, the larger coverage area it has. Therefore, with n closest verifiers selected, the expected overall coverage area is large, meaning that most of the non-verifiers can receive n CWM for a certain invalid message. In this method, since each vehicle only knows the locations of its neighbors, the number of verifiers may be more than expected due to the vehicles' limited scope. For instance, in Fig. 4, from the view of vehicle 14, it may consider vehicle 12, 13, 14 and 15 as four nearest vehicles to the sender. Fortunately, this phenomenon will be mitigated when the vehicle density is high. If there is a vehicle 16 between vehicle 12 and 13, vehicle 14 will not consider itself as a verifier. Although the N-nearest method always chooses vehicles with large coverage areas as verifiers, it has its own weakness. As illustrated in Fig. 4, non-verifier vehicles close to the sender could receive several CWMs. Whereas, if all verifiers are located at one side (e.g. left side) of the sender, some non-verifiers at the other side (e.g. right side) of the sending vehicle will not be informed.

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. 4, 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 4 rays (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. 4, 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.

3) THE COMPOUND METHOD

In 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. 4, 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 $n \geq 6$, 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.

4) DISCUSSIONS

In the following, when we claim that there are n verifiers for a certain message, we mean that, on average, n vehicles will verify the message. Since the vehicles decide whether to be verifiers in a fully distributed manner where each vehicle has only limited scope, the number of verifiers for one PBM may fluctuate along time. The fluctuation could be mitigated if the vehicle density is high. In a low density scenario, message-by-message verification is always preferred for a higher level of security. The CMAP can be triggered by either RSU or vehicles themselves. When a vehicle activates the CMAP, all its neighbors should switch to the CMAP mode. However, vehicles with a small number of neighbors can still verify all the messages on the condition that they share CWM to others. For a certain vehicle, if the number of its neighbors is low enough, it will try to change back to the message-by-message verification. One bit called "self-verification" will be added in the PBM. If all the neighbors of a certain vehicle are willing to change back to the self-verification mode, the vehicle can switch back.

Fairness is an important issue for large scale networks. For a single broadcasting vehicle, the verifier selection method (e.g., the N-nearest method) may incur unfairness to its neighbors. However, if we consider that many vehicles are uniformly distributed in an area, every vehicle can be a regular broadcasting vehicle and can also be a verifier for a received message according to the CMAP. Hence, each vehicle on average fairly achieves the similar performance.

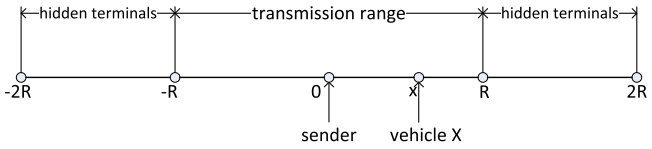


FIGURE 5. One-dimensional VANET model.

V. ANALYTICAL MODEL DEVELOPMENT

In this section, we develop analytical models for the proposed CMAP and the existing PVP. For mathematical tractability, we here focus on the one-dimensional VANET as shown in Fig. 5. We will resort to practical simulations to evaluate CMAP and PVP in Section VII. We consider IEEE 802.11 protocol, where the broadcasting of each vehicle is coordinated by a distributed coordination function (DCF). For simplicity, we make the following assumptions:

1) The vehicles are randomly distributed along the road such that the number of vehicles within a certain length of road follows a Poisson distribution. Let ρ be the vehicle density and hence the expected number of vehicles in length l is ρl. Thus, the probability of having i vehicles within a road of length l is

$$P(i, l) = \frac{(\rho l)^i e^{-\rho l}}{i!}. \quad (1)$$

2) There is no acknowledgment and retransmission for the broadcast messages and verification messages. The backoff window size of IEEE 802.11 DCF is fixed at W_0;
3) All the vehicles have the same transmission, carrier sensing and receiving range which is denoted as R. We do not consider the channel fading effect in our analysis for simplicity.

We adopt the missed detection ratio (the probability that an invalid PBM is considered valid by a receiver) as the performance metric. To evaluate this ratio, an arbitrary pair of sender and receiver vehicles are picked for analysis. In the following, we use P^s and P^m to indicate probabilities of successful packet delivery and missed detection ratios, respectively.

A. IEEE 802.11 BACKOFF PROCESS

With the IEEE 802.11 protocol, each vehicle senses the channel before transmitting its broadcast message. If the channel is busy, a backoff procedure is launched. In each backoff period, the backoff counter starts from a randomly selected value between 0 and W_0. It counts down when the channel is sensed idle and freezes when the channel is sensed busy. Once the backoff counter reaches zero, a transmission of the broadcast message is attempted.

For an arbitrary vehicle on the road, its backoff process can be described by a discrete-time Markov chain. Let τ denote the channel access probability in a generic slot. Under saturated traffic conditions, $\tau = \frac{2}{W_0+1}$ according to [37]. For unsaturated traffic cases,

$$\tau = \frac{2(1-P_0)}{W_0+1} \tag{2}$$

where P_0 is the probability that no packet in this vehicle's buffer is ready for transmission. In order to calculate P_0, we need to know the channel busy probability P_b and the average packet transmission time T.

This vehicle will sense a busy channel if at least one another vehicle in its sensing range is transmitting. Therefore,

$$\begin{aligned} P_b &= 1 - Pr(\text{no vehicle in the sensing range of the tagged node transmit}) \\ &= 1 - \sum_{i=0}^{\infty}(1-\tau)^i P(i, 2R) = 1 - e^{-2\rho R\tau}. \end{aligned} \tag{3}$$

Upon detecting a busy channel, the backoff counter will be suspended for a time period equal to the transmission time of a packet. Let L_H and L_P denote the packet header size and the average payload size, respectively, C denote the wireless channel capacity, *DIFS* denote the DCF inter-frame space, and δ denote the propagation delay. Then the average transmission time of a packet can be expressed as

$$T = \frac{L_H + L_P}{C} + DIFS + \delta. \tag{4}$$

Based on (2)–(4), P_0 and τ can be obtained using the algorithm proposed in [27].

B. ONE HOP PACKET DELIVERY RATIO

Without loss of generality, suppose the coordinate of the sender is 0. As shown in Fig. 5, our analysis model is perfectly symmetric with respect to the sender. Therefore, we focus on the part to the right side of the sender in the following. We are interested in the packet delivery ratio from the sender to an arbitrary vehicle (say vehicle X) located to the right of the sender. The distance between vehicle X and the sender is $x \in [0, R]$. There are two reasons that may cause collision to the packet from the sender to vehicle X: the concurrent transmission from any vehicles within the sensing range of the sender and the hidden terminal problem. They are analyzed as follows.

1) IMPACT OF CONCURRENT TRANSMISSION

Consider that the sender broadcasts a message at the time slot when its backoff counter reaches zero. If any other vehicle within the sensing range of the sender (i.e. vehicles in $[-R, R]$) transmits at the same time slot, collision may happen. For vehicle X, any concurrent transmissions from vehicles within the overlapping region of its receiving range and the transmission range of the sender (i.e. $[x-R, R]$) will cause collision to the packet from the sender. In other words, if vehicle X can successfully receive the packet from the sender, it is necessary that no vehicles in $[x-R, R]$ transmit at the same time slot in which the sender transmits. Therefore, the probability that the packet from sender to vehicle X is free from collision caused by concurrent transmission can be calculated as:

$$\begin{aligned} P_1^s &= Pr(\text{none of the vehicles in } [x-R, R] \text{ transmits in a slot}) \\ &= \sum_{i=0}^{\infty}(1-\tau)^i P(i, 2R-x) \\ &= e^{-\rho(2R-x)\tau}. \end{aligned} \tag{5}$$

2) IMPACT OF HIDDEN TERMINAL PROBLEM

The hidden terminal terminal problem relates to the situation that two nodes are outside of each other's sensing range but share a same set of nodes that are within their transmission ranges. Consider the scenario shown in Fig. 5, the potential hidden terminals of the sender are the vehicles located in $[-2R, -R]$ and $[R, 2R]$. Since the sender and its potential hidden terminals cannot sense the transmissions of each other, collisions may happen if any potential hidden terminal transmits during the vulnerable period (with length T_{vul} in number of slots) of the sender. For a transmission of period T (in number of slots), the vulnerable period is the interval within which any other transmission will collide with the sender. Therefore, $T_{\text{vul}} = 2T$.

The hidden terminals that have impact on the packet delivery ratio at vehicle X are the vehicles located in $[R, R+x]$. Thus the probability that the packet is free from collision caused by hidden terminal problem can be evaluated as:

$$\begin{aligned} P_2^s &= Pr(\text{none of the vehicles in } [R, R+x] \text{ transmits in } T_{\text{vul}}) \\ &= \left[\sum_{i=0}^{\infty}(1-\tau)^i P(i, x)\right]^{T_{\text{vul}}} \\ &= e^{-\rho x\tau T_{\text{vul}}} = e^{-ax} \end{aligned} \tag{6}$$

where $a \triangleq 2T\rho\tau$.

Since the impact of concurrent transmission and the impact of hidden terminal problem are mutually independent, the packet delivery ratio from the sender to vehicle X is

$$\begin{aligned} P^s(x) &= P_1^s P_2^s = e^{-\rho(2R-x)\tau} e^{-ax} \\ &= e^{-2\rho R\tau} e^{-(a-\rho\tau)x}. \end{aligned} \tag{7}$$

C. MISSED DETECTION RATIO FOR CMAP

A missed detection happens when an invalid PBM from the sender is considered valid by the receiver for the following two reasons:

1) the PBM packet from the sender to the verifiers or the CWM packet from the verifiers to the receiver gets lost due to collisions in wireless channel;
2) the coverage area of the verifiers cannot cover all the receivers within the sender's transmission range, thus the vehicles out that coverage area cannot get verification results for the invalid PBM.

In the following, we focus on the 2-verifier case. In the CMAP, we focus on the proposed compound verifier selection method such that the two nearest vehicles to the left and right of the sender are chosen as verifiers. Denote them as verifier Y and verifier Z, respectively, as shown in Fig. 6.

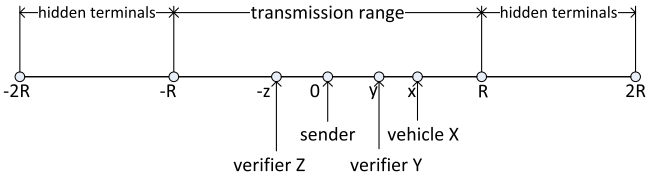


FIGURE 6. One-dimensional VANET model with two verifiers.

Consider an arbitrary vehicle X with coordinate $x \in [0, R]$. We are interested in the missed detection ratio for an invalid PBM from the sender at vehicle X's perspective. To this end, we consider the following two cases:

1) Vehicle X is a verifier. That is: vehicle X is the nearest vehicle on the right side to the sender. Since the number of vehicles follows a Poisson distribution with density ρ, the distance between the sender and the nearest vehicle to the right of it follows an exponential distribution with parameter ρ. Thus the probability that vehicle X itself is a verifier is:

$$\begin{aligned} P_{\text{vrf}} &= Pr(\text{number of vehicles within } [0, x] \text{ is } 0) \\ &= e^{-\rho x}. \end{aligned} \tag{8}$$

In this case, vehicle X will verify the PBM by itself. Then at vehicle X's perspective, the probability that the invalid PBM from the sender gets detected is the probability that vehicle X can receive the invalid PBM without collision. Similar to our analysis above, the impact of hidden terminal problem can be evaluated as (6).

When we consider the impact of concurrent transmission, since there are no vehicles located within $[0, x]$, the probability that the PBM is successful becomes:

$$\begin{aligned} P^s_{1,\text{vrf}} &= Pr(\text{none of the vehicles in } [x-R, 0] \cup [x, R] \\ &\qquad \text{transmits in a time slot}) \\ &= e^{-2\rho(R-x)\tau}. \end{aligned} \tag{9}$$

Therefore, the probability that the invalid PBM from the sender gets detected is

$$\begin{aligned} P^s_{\text{vrf}} &= P^s_2 P^s_{1,\text{vrf}} = e^{-ax} e^{-2\rho(R-x)\tau} \\ &= e^{-2\rho R\tau} e^{-(a-2\rho\tau)x}. \end{aligned} \tag{10}$$

2) Vehicle X is not a verifier. That is: another vehicle serves as a verifier that locates between vehicle X and the sender. Such a verifier exists with probability $1 - P_{\text{vrf}}$. We denote this verifier as verifier Y, whose coordinate is y $(0 < y < x)$. The probability density function (PDF) of y conditioned on that there is at least one verifier in $(0, x)$ is:

$$p(y) = \frac{\rho e^{-\rho y}}{1 - P_{\text{vrf}}} = \frac{\rho e^{-\rho y}}{1 - e^{-\rho x}}, \qquad y \in (0, x). \tag{11}$$

Vehicle X can only receive the CWM of the invalid PBM from verifier Y when verifier Y receives the PBM without collision and successfully delivers a CWM to vehicle X. According to (10), the probability that verifier Y receives the invalid PBM is

$$P^s_Y = e^{-2\rho R\tau} e^{-(a-2\rho\tau)y}. \tag{12}$$

Then we consider the packet delivery ratio from verifier Y to vehicle X. The distance between them is $(x - y)$. Similar to (6), the packet collision ratio caused by hidden terminal problem will be

$$P^s_{2,Y\to X} = e^{-a(x-y)}. \tag{13}$$

When considering the concurrent transmission, the vehicles which can cause collision to the CWM from verifier Y to vehicle X is the vehicles located in $[x-R, R+y]$. Since there is no vehicles within $[0, y]$, the probability that the CWM is free from collision caused by concurrent transmission is

$$P^s_{1,Y\to X} = e^{-\rho\tau(2R-x)}. \tag{14}$$

Combining (13) and (14), the probability that vehicle X can receive the CWM from verifier Y is

$$\begin{aligned} P^s_{Y\to X} &= P^s_{1,Y\to X} P^s_{2,Y\to X} \\ &= e^{-\rho\tau(2R-x)} e^{-a(x-y)}. \end{aligned} \tag{15}$$

Based on (11), (12) and (15), the probability that vehicle X successfully receives the CWM from the verifier to the right side of the sender is

$$P^s_{X,\text{right}} = \int_0^x p(y) P^s_Y P^s_{Y\to X} \mathrm{d}y. \tag{16}$$

There is also a verifier on the left side of the sender. Suppose the nearest vehicle to the left of the sender is verifier Z, with coordinate $-z$ where $z \in [0, R]$. The PDF of z is

$$p(z) = \rho e^{-\rho z}. \tag{17}$$

Similar to (12), the probability that vehicle Z receives the invalid PBM is

$$P^s_Z = e^{-2\rho R\tau} e^{-(a-2\rho\tau)z}. \tag{18}$$

Verifier Z can only deliver its CWM to vehicle X when vehicle X is located within its transmission range, i.e. $0 < z < x - R$. So the probability that verifier Z delivers the CWM to vehicle X is

$$P^s_{Z\to X} = \begin{cases} e^{-a(z+x)-\rho(2R-2z-x)\tau} & 0 < z < R - x \\ 0 & z > R - x. \end{cases} \quad (19)$$

Based on (17), (18) and (19), we have the probability that vehicle X receives the CWM from the verifier on the left side of the sender is:

$$P^s_{X,\text{left}} = \int_0^R p(z) P^s_Z P^s_{Z\to X} \mathrm{d}z. \quad (20)$$

The invalid PBM will miss the detection when vehicle X neither receives the CWM from the verifier on the left nor from the verifier on the right, and the probability is

$$P^c_X = (1 - P^s_{X,\text{right}})(1 - P^s_{X,\text{left}}). \quad (21)$$

Then, base on P_{vrf}, P^s_{vrf} and P^s_X, we can calculate the missed detection ratio for the invalid PBM at vehicle X as

$$P^m_{\text{CMAP}}(x) = P_{\text{vrf}}(1 - P^s_{\text{vrf}}) + (1 - P_{\text{vrf}})P^c_X. \quad (22)$$

Vehicle X is randomly chosen on $[0, R]$, so we can derive the missed detection ratio for CMAP by doing the integration on x over $[0, R]$:

$$P^m_{\text{CMAP}} = \frac{1}{R}\int_0^R P^m_{\text{CMAP}}(x)\mathrm{d}x. \quad (23)$$

D. MISSED DETECTION RATIO FOR PVP

In PVP, once a vehicle receives a broadcast message, with probability α it will decide to verify the message itself; with probability $(1 - \alpha)$ it will wait for the verification results from other vehicles (i.e., the verifiers). Consider the sender and an arbitrary vehicle X located at 0 and x, respectively. Suppose the sender sends out an invalid broadcast message, with probability $\alpha P^s(x)$ vehicle X will receive the message and verify the message itself; with probability $(1 - \alpha)$, vehicle X will not serve as a verifier but rely on the other vehicles for verification. Assume there is a verifier W whose coordinate is $w \in [-R, R]$ deciding to verify the message. The probability that verifier W receives the invalid broadcast message from the sender is:

$$P^s_W = e^{-2\rho R\tau} e^{-(a-\rho\tau)|w|}. \quad (24)$$

The probability that verifier W successfully delivers its verification result to vehicle X is:

$$P^s_{W\to X} = \begin{cases} e^{-2\rho R\tau} e^{-(a-\rho\tau)|x-w|} & x - R < w < R \\ 0 & -R < w < x - R. \end{cases} \quad (25)$$

With (24) and (25), we can get the probability that vehicle X successfully receives the verification result from one verifier is:

$$\tilde{P}^s_X = \frac{1}{2R}\int_{-R}^R P^s_W P^s_{W\to X}\mathrm{d}w. \quad (26)$$

Consider the range $[x - R, R]$, the probability that there are n vehicles among which i vehicles are verifiers follows binomial distribution. For a specific i, the probability that vehicle X misses the detection of the invalid broadcast message is $(1 - \tilde{P}^s_X)^i$. Considering all possible n and i, we can calculate the missed detection ratio of the invalid message as

$$P^m_X(x) = \sum_{n=0}^{\infty} P(n, 2R) \sum_{i=0}^{n} \binom{n}{i} \alpha^i (1-\alpha)^{n-i} \times (1 - \tilde{P}^s_X)^i. \quad (27)$$

In general, the missed detection ratio at vehicle X is

$$P^m_{\text{PVP}}(x) = \alpha(1 - P^s(x)) + (1 - \alpha)P^m_X(x). \quad (28)$$

Vehicle X is randomly chosen in $[0, R]$, so after calculating the integration on x over $[0, R]$ we get the missed detection ratio for PVP as follows.

$$P^m_{\text{PVP}} = \frac{1}{R}\int_0^R P^m_{\text{PVP}}(x)\mathrm{d}x. \quad (29)$$

Note that P^m_{PVP} is a function of the probability α.

VI. SIMULATION RESULTS

In this section, we develop NS2 simulation programs to validate our analytical models in a 1-D highway road scenario, and to evaluate the performance of the proposed cooperative message authentication protocols in a more complex 2-D city road scenario. In order to properly estimate the real-world road environment and vehicular traffic, we generate vehicles' mobility through the mobility model generation tool called VanetMobiSim [33]. This tool makes use of the publicly available topologically integrated geographic encoding and referencing (TIGER) database [34] from the U.S. Census Bureau.

In both scenarios, each vehicle is equipped with an IEEE 802.11 wireless module that periodically broadcasts messages (PBM that contains the vehicle's geographic information) every 300 ms. The communication ranges are the same as 300 m. Other physical and MAC layer parameters of the IEEE 802.11 broadcast protocol used in our simulations are listed in Table I.

TABLE I. MAC parameters.

Parameter	Value
Preamble length	40 us
Slot time	16 us
DIFS	64 us
Contention window	16
Wireless channel rate	6 Mbps
MAC header size	28 bytes
PLCP header length	6 bytes
RBM payload size	200 bytes
CAM payload size	28 bytes

We consider different total number of vehicles (i.e., different density) travelling on the roads where 6% of them are malicious ones. A malicious vehicle periodically broadcasts invalid PBMs, but never sends CWM to help others for

message verification. We define the *missed detection ratio* as the percentage of invalid PBMs that are considered as valid by receiving vehicles. The missed detection ratio is computed based on well-behaved vehicles in our simulation. For the PVP protocol, each vehicle becomes a verifier with a probability $\frac{8}{M}$, where M is the total number of receiver's neighbors.

A. ANALYTICAL MODEL VALIDATION

We consider a 5 km-long highway scenario in which vehicles enter the highway according to a Poisson distribution and there speeds vary randomly within 56 $\sim$ 80 mph. For PVP, we set the probability $p = \frac{1}{\rho R}$ so that on average the number of verifiers is the same as that of the CMAP compound method. Fig. 7 shows the analytical results as well as the simulation results of our CMAP compound method and the PVP method. The missed detection ratio of both methods increase with traffic density, while the performance of our CMAP compound method is always better than that of PVP. Moreover, the model based calculation results well match the simulation results, which demonstrates the accuracy of our analytical model.

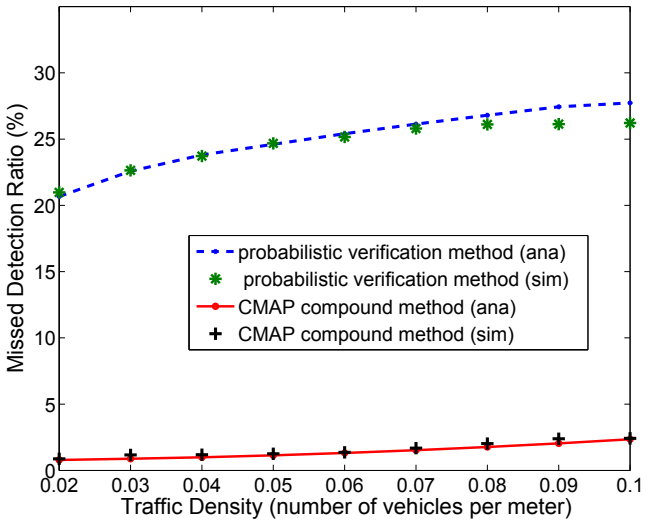


FIGURE 7. Performance comparison in the highway scenario.

In Fig. 7, the main reason for the increasing error of the proposed analytical model for the PVP is as follows. As in (27), $P_X^m(x)$ is a summation of an infinite series. However, for computation tractability, we consider only the summation of the first 100 elements of the series to approximate the probability. As shown in Fig. 7, with low vehicle densities, the approximated results are accurate. However, as ρ increases, $P(n, 2R)$, i.e., the probability that having n vehicles within the communication range, increases. As a result, the impact of the ignored terms in the summation becomes larger, and hence the model error increases. Nevertheless, the curves in Fig. 7 demonstrates that the performance gap remains quite small, with the beneficial tradeoff of significantly reduced computation overhead in analysis.

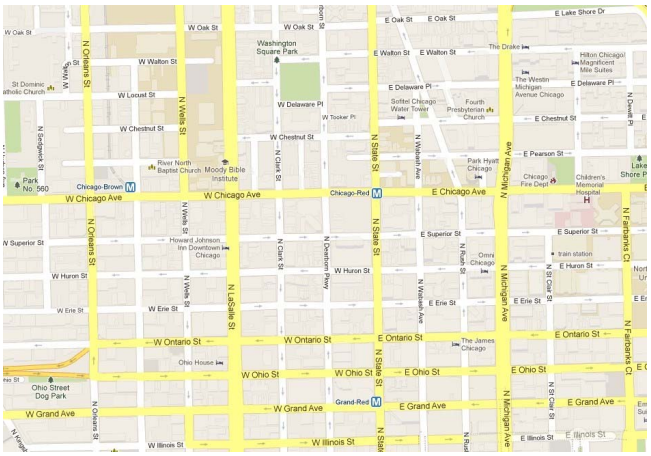


FIGURE 8. City road map.

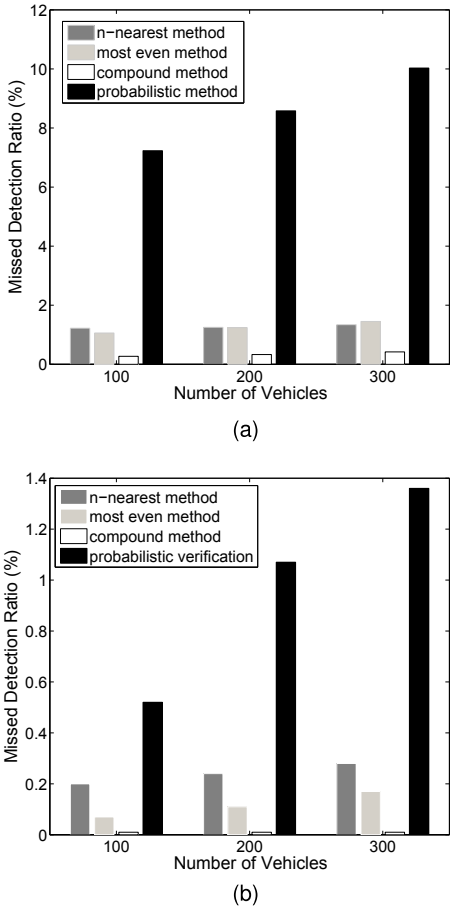


FIGURE 9. Missed detection ratio with different number of verifiers. (a) 4 Verifiers. (b) 8 Verifiers.

B. PERFORMANCE COMPARISON

As shown in Fig. 8, we consider a practical 2 km $\times$ 1 km road map near the water tower in the downtown of Chicago. Vehicles travel on the roads at speeds varying randomly in the range 22.5 $\sim$ 33.5 mph. Fig. 9 shows the simulation results of the missed detection ratios under different number of verifiers. We have the following observations: 1) with the same number of verifiers, the missed detection ratio of PVP is much

higher than that of our proposed protocols, which echo the results in the 1-D scenario. Specifically, with 4 verifiers, the missed detection ratio of the probabilistic method under high vehicle density conditions is about 10%, a value may be able to cause traffic disasters. However, our compound method can achieve a ratio less than 0.5% in this case. 2) The performance under 8 verifiers is obviously better than that under 4 ones. Any more verifiers could not introduces significant performance improvements since, with 8 verifiers, the missed detection ratio of the compound method is already less than 0.02%. Nevertheless, extra verifiers may incur unnecessary communication and computation overheads. 3) The ratio of the n-nearest method is higher than that of the most-even distributed method in most cases, while the compound method always achieves the lowest ratio. This result matches our expectations in the previous section because the compound method is supposed to have a better coverage area. Among the three proposed verifier selection methods, the compound method is obviously preferred over the other two. Therefore, we focus on the compound method in the following.

In the following, we investigate the performances the compound method and PVP from various aspects including the impacts of malicious vehicle ratio, transmission range and broadcast period. The results are shown in Figs. 10–12. The number of verifiers is fixed at 4. From Fig. 10, we can see that the missed detection ratios of both methods increase with the malicious vehicle ratio. The reason lies in that a malicious vehicle does not help verify messages and send CWM to other vehicles if being selected as a verifier.

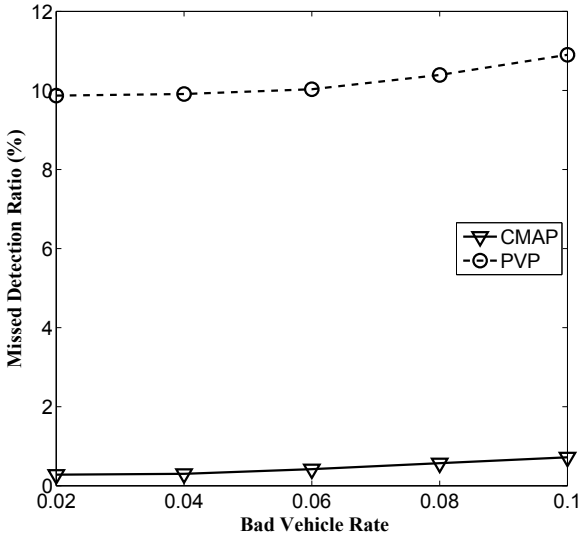


FIGURE 10. **Impact of the ratio of malicious vehicles.**

From Fig. 11 we can see that when the transmission range of vehicles gets larger, both missed detection ratios increase. In fact, with a larger transmission range, the number of neighbors for each vehicle that contend for channel access grows, and thus the packets collision probability becomes higher. The impact of broadcast period on missed detection ratio is

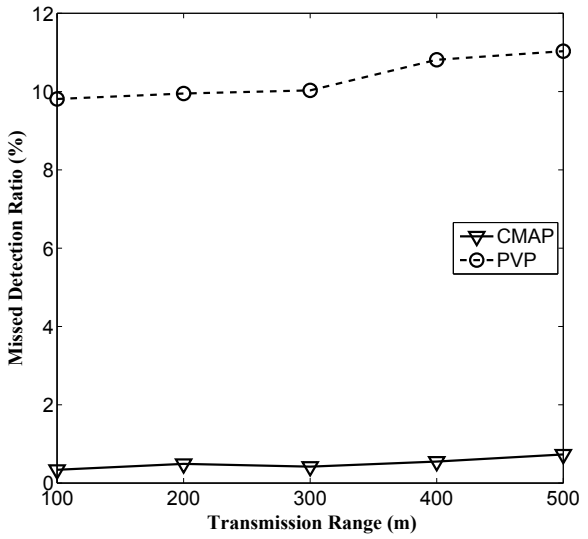


FIGURE 11. **Impact of the transmission range.**

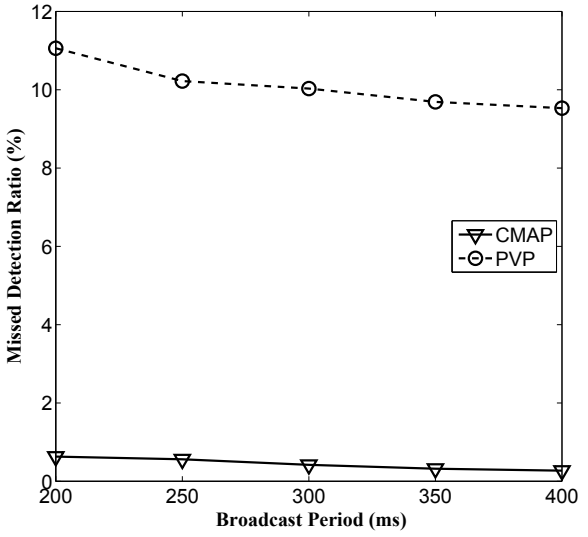


FIGURE 12. **Impact of the broadcast period.**

shown in Fig. 12. A longer broadcast period means a less crowded channel. In this case, the packet successful delivery ratio increases and hence the missed detection ratio decreases.

C. COMPUTATION AND COMMUNICATION OVERHEAD

We conduct simulations to study the computation and communication overhead of both non-cooperative message authentication protocol and the proposed cooperative message authentication protocol (CMAP). Verifying the group signature attached to each broadcast message is the dominating component that consumes computation capacity. In our simulation, we use the average number of verified messages per vehicle per second as the metric for the computation overhead.[2] In this sense, the average computation overheads

[2] As can be seen above, our verifier selection methods are fully distributed and light-weight. The corresponding computation overhead in verifier selection is ignored.

of both CMAP and the PVP are the same providing that the average number of verifiers selected for each broadcast message is the same. It is worth noting that our CMAP method achieves a much lower missed detection ratio than the PVP with the same computation overhead (i.e., with the same number of verifiers), as demonstrated in Figs. 10–12.

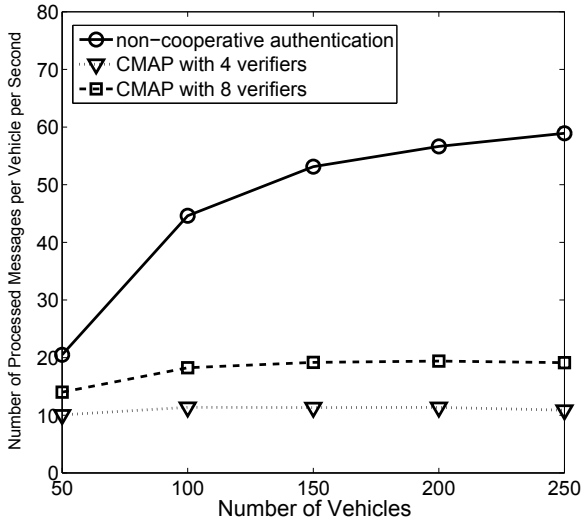


FIGURE 13. Computation overhead comparison.

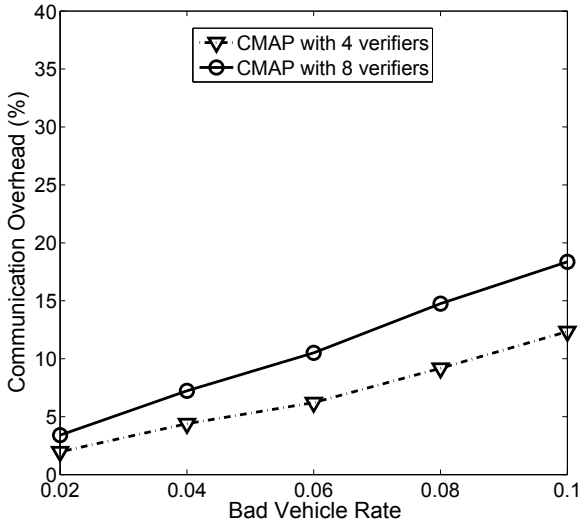


FIGURE 14. Communication overhead.

The simulations results are shown in Figs. 13 and 14. From Fig. 13, we have the following observations:

1) Compared with the conventional non-cooperative authentication protocol, our CMAP method achieves significantly lower computation overhead. In fact, with the non-cooperative authentication protocol, each vehicle verifies the broadcast messages from all its neighbors; while with CMAP, depending on whether the vehicle is selected as a verifier, it verifies only a subset of the messages. Particularly, we can see that the CMAP with 4 verifiers can reduce the computation overhead by around 80% when there are 200 vehicles in the simulation map.
2) The computation overhead of CMAP is independent of vehicle density, while that of the non-cooperative protocol increases with the density. In the latter case, each vehicle needs to verify every broadcast message received, so the number of verified messages per vehicle per second grows linearly with the traffic density. Note that the curve for non-cooperative authentication tends to flat when the traffic density is high. The reason is that the severe packet collisions under a high vehicle density constrain the number of broadcast messages successfully received by each vehicle. With the CMAP, each broadcast message from a sending vehicle will be authenticated by the cooperative verifiers around; thus the total number of verified messages is proportional to the traffic density. Therefore, in the normalized sense, the number of verified messages per vehicle per second is irrelevant to the traffic density.

The proposed CMAP introduces some extra communication overhead for dealing with the warning messages generated by the verifiers when an invalid broadcast message is detected. We calculate the average number of bits received by each vehicle per second (i.e., the number of bits per vehicle per second), which counts both the regular broadcast messages and warning messages. We take the percentage of the extra value of bits per vehicle per second in the CMAP case relative to the bits per vehicle per second in the non-cooperative case as the extra communication overhead of CMAP. Fig. 14 shows the simulation results where the number of vehicles is set to 200. We can see that, with 4 verifiers and 6% vehicles being malicious ones that send invalid messages, the CMAP introduces an extra communication overhead of 6.2%. In the simulations, the regular message payload size and the warning massage payload size are according to the setting in Table 1.

From these results, we can see that our CMAP protocol significantly reduces the computation overhead of each vehicle at the cost of a slightly increased communication overhead.

VII. CONCLUSION

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. Simulation results in a highway scenario verify that our models are accurate. Based on a practical 2-dimensional road map, extensive NS2 simulations show that the proposed protocol outperforms the probabilistic one, and that the compound method is the best among all the verifier selection methods. 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. In addition, simulation results demonstrate that the CMAP significantly reduces the computation overhead of each vehicle at the cost of a slightly increased communication overhead.

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-dimentional 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-dimentional 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.

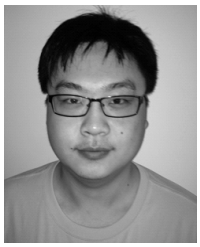
[33] (2007). *VanetMobiSim* [Online]. Available: http://vanet.eurecom.fr/

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

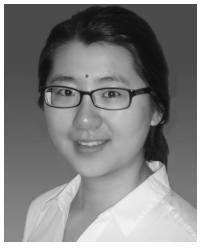
[35] Y. Cheng, X. Ling, and W. Zhuang, "A protocol-independent approach for analyzing the optimal operation point of CSMA/CA protocols," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 1–9.

[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.

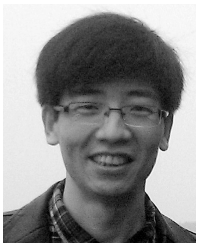
[37] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.



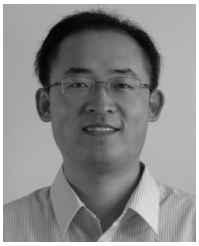
WENLONG SHEN received the B.E. degree in electrical engineering from Beihang University, Beijing, China, in 2010, and the M.S. degree in telecommunication from the University of Maryland, College Park, MD, USA, in 2012. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA. His current research interests include vehicular ad hoc networks, mobile cloud computing, and network security.



LU LIU received the B.S. degree in automation from Tsinghua University, Beijing, China, in 2010, and the M.S. degree in electrical engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2012, where she is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering. Her current research interests include energy efficient networking and communications, performance analysis, and protocol design of wireless networks.



XIANGHUI CAO (S'08–M'11) received the B.S. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2006 and 2011, respectively. From 2008 to 2010, he was a Visiting Scholar in the Department of Computer Science, University of Alabama, Tuscaloosa, AL, USA. Currently, he is a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA. His current research interests include wireless network performance analysis, energy efficiency of wireless networks, networked estimation and control, and network security.



YONG HAO received the B.E. and M.E. degrees in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2003 and 2007, respectively, and the Ph.D. degree in computer engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2012. He is currently with Juniper Networks, Sunnyvale, CA, USA. His current research interests include network security, vehicular ad hoc networks, and wireless networking.

YU CHENG (S'01–M'04–SM'09) received the B.E. and M.E. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1995 and 1998, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2003. From September 2004 to July 2006, he was a Post-Doctoral Research Fellow in the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON. Since August 2006, he has been with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA. He is currently an Associate Professor. His current research interests include next-generation Internet architectures and management, wireless network performance analysis, network security, and wireless/wireline interworking. He received the Postdoctoral Fellowship Award from the Natural Sciences and Engineering Research Council of Canada in 2004 and the Best Paper Award from the conferences QShine in 2007 and ICC in 2011. He received the National Science Foundation CAREER Award in 2011 and IIT Sigma Xi Research Award in the Junior Faculty Division in 2013. He served as a Co-Chair for the Wireless Networking Symposium of the IEEE ICC in 2009, a Co-Chair for the Communications QoS, Reliability, and Modeling Symposium of IEEE GLOBECOM in 2011, a Co-Chair for the Signal Processing for Communications Symposium of IEEE ICC in 2012, a Co-Chair for the Ad Hoc and Sensor Networking Symposium of IEEE GLOBECOM in 2013, and a Technical Program Committee Co-Chair for WASA in 2011. He is an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and *New Books & Multimedia Column Editor for IEEE Network*.