An Efficient Message Authentication Scheme for Vehicular Communications

Chenxi Zhang, *Student Member, IEEE*, Xiaodong Lin, Rongxing Lu,
Pin-Han Ho, *Member, IEEE*, and Xuemin (Sherman) Shen, *Senior Member, IEEE*

***Abstract*—In this paper, we introduce a novel roadside unit (RSU)-aided message authentication scheme named RAISE, which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. In addition, RAISE adopts the *k-anonymity* property for preserving user privacy, where a message cannot be associated with a common vehicle. In the case of the absence of an RSU, we further propose a supplementary scheme, where vehicles would cooperatively work to probabilistically verify only a small percentage of these message signatures based on their own computing capacity. Extensive simulations are conducted to validate the proposed scheme. It is demonstrated that RAISE yields a much better performance than previously reported counterparts in terms of message loss ratio (LR) and delay.**

***Index Terms*—Cooperation, privacy, security, vehicular communications.**

I. Introduction

A VEHICULAR ad hoc network (VANET) is a promising network scenario for facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. By being equipped with communication devices, vehicles can communicate with each other as well as with the roadside units (RSUs) located at critical points of the road, such as intersections or construction sites. In VANETs, onboard units (OBUs) frequently broadcast routine traffic-related messages [1] with information about position, current time, direction, speed, acceleration/deceleration, traffic events, etc. By frequently broadcasting and receiving traffic-related messages, drivers can get a better awareness of their driving environment. They can take early action to respond to an abnormal situation to avoid any possible damage or to follow a better route by circumventing a traffic bottleneck. In addition, with a VANET connected with the backbone Internet, passengers sitting in vehicles can go online to enjoy various entertainment-related Internet services with their laptops. These services include downloading/uploading data information from the Internet, local information acquisition (e.g., road maps and hotel information), and electronic advertisements [2].

Before putting the above attractive applications into practice in VANETs, we must resolve security and privacy issues. Particularly, we must guarantee message authenticity and integrity. Moreover, we have to protect user-related privacy information, such as the driver's name, license plate, model, and traveling route. Although previous studies have addressed the aforementioned issues, they have not taken the scalability and communication overhead into consideration. The main idea of the previous security schemes for VANETs is to sign each message before sending it and verify each message when receiving it. According to the Dedicated Short-Range Communication (DSRC) protocol [3], a vehicle sends each message within a time interval of 100–300 ms. Generating a signature every 100 ms is not an issue for any current signature technique. However, in a high-density traffic scenario, e.g., if 50–200 vehicles are within the communication range, the receiver needs to verify around 500–2000 messages/s, which will lead to a high computation burden to the receivers. Furthermore, traditional public key infrastructure (PKI)-based security schemes require the public key of the sender and the corresponding certificate to be included in the messages. The security overhead is usually bigger than the useful message contents. This issue has to be well addressed due to the limited wireless channel bandwidth available in VANETs. Conventional PKI-based schemes also do not consider the issue.

To address the above issues and provide a significant improvement in authentication efficiency and scalability for the intervehicle communications (IVC) of VANETs, in this paper, we propose an RSU-aided message authentication scheme named RAISE. Compared with previous message-authentication schemes [4]–[10], RAISE explores an important feature of VANETs by employing RSUs to assist vehicles in authenticating messages. The main idea of RAISE is illustrated as follows. A metropolitan area could likely be covered under a communication range of RSUs in the near future. When vehicles enter an area covered by an RSU, vehicles first perform mutual authentication and key agreement with the RSU. Vehicles that received safety messages do not need to verify the message through a conventional PKI-based scheme. Instead, each safety message will be attached to a short message authentication code (MAC) generated by the sender under the secret key shared between the sender and an RSU. The RSU helps to verify MACs and disseminate the results of the authenticity of the safety messages for vehicles in its

Manuscript received December 29, 2007; revised June 5, 2008 and June 12, 2008. First published July 15, 2008; current version published November 12, 2008. This work was supported by research grants from the Provincial Centre of Excellence Communications and Information Technology Ontario (CITO), Canada. The review of this paper was coordinated by Dr. T. Zhang.

C. Zhang, R. Lu, P.-H. Ho, and X. Shen are with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: c14zhang@uwaterloo.ca; rxlu@bbcr.uwaterloo.ca; pinhan@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada (e-mail: Xiaodong.Lin@uoit.ca).

Digital Object Identifier 10.1109/TVT.2008.928581

communication range. The verification of the message can be performed in an extremely fast manner due to the nature of the MAC authentication, which is just a fast symmetric decryption operation. RAISE improves the authentication efficiency and reduces the communication overhead in the mean time. Nevertheless, in a case where the presence of RSUs is not pervasive at the beginning of the VANET deployment stage, we propose a supplementary scheme, i.e., cooperative message-authentication scheme (named COMET), which works in the absence of RSUs. With COMET, vehicles do not need to verify all the message signatures that they receive from their neighboring vehicles; instead, they cooperatively work and verify a small percentage of these message signatures with some probability based on their own computing capacity. As such, the authentication efficiency can be improved, and a low message loss ratio (LR) can also be guaranteed in COMET.

The remainder of this paper is organized as follows. Section II surveys the related work. Section III briefly introduces our system model and the preliminaries, including problem statements and design objectives. Section IV presents the proposed RAISE scheme in detail and explains how RAISE can ensure security and privacy without incurring high overhead and scalability concerns. The proposed COMET scheme is described in Section V. Section VI analyzes the performance of the proposed schemes through extensive simulations. Section VII analyzes the security of the proposed schemes. We draw conclusions and outline future work in Section VIII.

II. Related Work

Many related studies have been reported on the security and privacy-preservation issues for VANETs [4]–[11]. To achieve both message authentication and anonymity, Raya and Hubaux [4] proposed that each vehicle should be preloaded with a large number of anonymous public and private key pairs together with the corresponding public key certificates. Traffic messages are signed with a public-key-based scheme. To achieve privacy, each public and private key pair has a short life time, and a pseudo ID is used in each public key certificate. However, this scheme requires a large storage capacity to store this security information. Recently, Lin *et al.* [5] introduced a group-signature-based scheme to sign each message. Since there is no identity information included in messages, this approach can also achieve identity privacy preservation. Furthermore, the group-signature-based scheme reduces the storage cost of the public and private key pairs and reduces the bandwidth consumption used to transmit the certificate revocation list (CRL) over the Internet. To reduce the overhead of the group-signature-based scheme, Calandriello *et al.* [6] developed a similar scheme in which a vehicle can generate public and private key pairs by itself by using a group key. This scheme can achieve a tradeoff between the group-signature-based scheme and the traditional PKI-based scheme. Xi *et al.* [7] introduced a random key-set-based authentication protocol to preserve the vehicles' privacy. Lu *et al.* [8] proposed a conditional privacy-preservation scheme. The scheme divides privacy into three levels. First, an RSU is responsible for issuing temporarily anonymous certificate to vehicles, and thus, the RSU can know which vehicle uses the anonymous certificate it issued. Second, however, for IVC, a vehicle's identity is absolutely anonymous to other vehicles. Third, the proposed scheme can make a trust authority (TA) know a vehicle's real identity. The TA has the highest priority, which can trace a vehicle in the case where a malicious attack and resource abuse has occured. In addition, since the expiration date in the certificate indicates the validity period of the certificate, this scheme inherently addresses certificate revocation issues as well. Although these schemes have well-addressed privacy issues in VANETs, however, they all do not take scalability issues into consideration.

To cope with the aforementioned scalability issues, Lin *et al.* [9] developed a time-efficient and secure vehicular communications (TSVC) scheme, which employs the TESLA [12] approach to address the scalability issue. With TSVC, a vehicle first broadcasts a commitment of hash chain to its neighbors and then uses the elements of the hash chain to generate a MAC with which other neighbors can authenticate this vehicle's following messages. Because of the fast speed of MAC verification, TSVC can reduce the message LR. However, TSVC is not robust when the dynamics of traffic becomes large because a vehicle should broadcast its key chain commitment much more frequently. Under this situation, the LR of TSVC could increase. Zhang *et al.* [10] proposed an identity-based batch verification (IBV) scheme for vehicular sensor networks. IBV not only achieves conditional privacy but also reduces the overall verification delay of a batch of message signatures. IBV is a PKI-based signature scheme, and it uses a pairing-based cryptographic [13], [14] approach. It is clear that the computation speed of a paring is slower than that of a multiplication operation. Thus, when verifying a single signature, IBV is slower than other common PKI-based signature schemes. However, when verifying a batch of message signatures, the verification speed of IBV is much faster than that of other PKI-based schemes. Nevertheless, IBV is still a PKI-based scheme, and thus, it is still difficult to solve the scalability issue, particularly for IVC.

III. System Model and Preliminaries

A. System Model

A vehicular communication network hierarchically consists of two layers. The upper layer is composed of application servers (ASs) and RSUs, as shown in Fig. 1. The ASs can be connected with RSUs through secure channels, such as the transport layer security (TLS) protocol, with either wired or wireless connections. The ASs provide application data for RSUs, and RSUs work as gateways to deliver data to the lower layer, which is composed of vehicles. All vehicles and RSUs keep time synchronization. Vehicles can communicate with each other and with RSUs. In this paper, we aim at addressing the security issues in the lower layer.

In general, RSUs have a higher computation capability than vehicles and are trusted since it is not easy for RSUs to be compromised. According to DSRC, the communication range of an RSU is adjustable, and thus, it can be larger than that

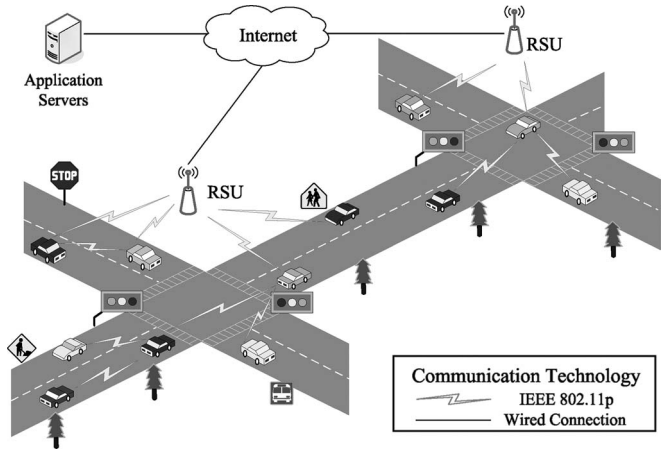

Fig. 1. Network model.

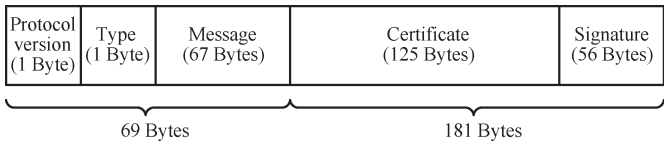

Fig. 2. Format of the signed message.

of the vehicles, such that some vehicles can hear from the RSU while the RSU may not hear from the vehicles. The locations where the density of vehicles is high will be allocated with an RSU, such as an intersection and any possible traffic bottleneck. Notice that only the IVC message authentication is considered when any RSU is available. For those areas with sparse vehicle distribution, the scalability issue will not be a problem, and a conventional PKI-based authentication scheme can work sufficiently well.

B. Problem Statement

The current IEEE Trial-Use standard [15] for VANET security provides detailed documentation, including the choice of cryptosystems. To authenticate a message's sender and guarantee the message's integrity, OBUs or RSUs should sign messages with their private keys before the messages are sent. Fig. 2 shows the format of a signed message [15], where a 125-B certificate and a 56-B Elliptic Curve Digital Signature Algorithm (ECDSA) signature have to be attached for each 69-B IVC message. Obviously, the cryptographic overhead (the certificate and the signature) takes up a significant portion of the total packet size.

Cryptographic operations also lead to high computation cost for receivers to verify these messages. According to DSRC [3], a vehicle sends each message within a time interval of 100–300 ms. Generating a signature every 100 ms is not an issue for current public-key-based signature schemes. However, in the case where 50–200 vehicles are within the communication range, the receiver needs to verify around 500–2000 messages/s. Public key certificates have to be verified as well. Signing and verifying each message can certainly achieve secure communication; however, these cryptographic operations make the security scheme not scalable to the traffic density. Therefore, the verification algorithms are required to be very fast such that the incoming messages can be processed. Unfortunately, all currently available signature schemes for VANETs based on PKI-based or group-signature-based schemes are not suitable for this stringent time requirement.

C. Design Objectives

In this paper, we aim at achieving the following security objectives.

1) *Message integrity and source authentication:* All accepted messages should be delivered unaltered, and the origin of the messages should be authenticated to guard against impersonation attack.
2) *Low communication overhead and fast verification:* The security scheme should be efficient in terms of small communication overhead and acceptable processing latency. A large number of message signatures should be verified in a short interval.
3) *Conditional privacy preservation:* The identities of vehicles should be hidden from a normal message receiver during the authentication process to protect the senders' private information, such as the driver's identity and any personal information. On the other hand, the authorities should be able to trace the sender of a message by revealing its identity in case of any exceptional case, such as liability investigation.
4) *Prevention of internal attack:* Different from the study in [16], a normal vehicle holding its own keying material cannot obtain the other vehicles' keying materials. Furthermore, even if a vehicle is compromised, an adversary cannot use the compromised vehicle to obtain the other vehicles' important information.

IV. RSU-Aided Message Authentication Scheme

In this section, we propose an RSU-aided message-authentication scheme named RAISE. With RAISE, when an RSU is detected nearby, the vehicle tries to associate with the RSU, and the RSU assigns a unique shared symmetric secret key and a pseudo ID that could be shared with other vehicles. With the symmetric key, the vehicle generates a symmetric MAC code and then broadcasts each message by signing the message with the symmetric MAC code instead of a PKI-based message signature. Upon receiving the messages signed with the MAC code, the receiving vehicles cannot immediately verify the message because the MAC code is not known to the receiving vehicle. Instead, the RSU knows the key of generating the MAC code; thus, the RSU can be responsible for verifying the message and then notifying the authenticity of the message to other receiving vehicles.

The detailed implementation of RAISE will be presented in the following sections. For clarity of presentation, the notations throughout this section are listed in Table I.

A. Symmetric Key Establishment

Once a vehicle V_i detects the existence of an RSU R (e.g., through a Hello message from the R), V_i initiates anonymous

TABLE I
NOTATIONS

Notation	Descriptions
R:	an RSU
V_i:	the i-th vehicle
M_i:	the message sent by V_i
K_i:	a key shared between V_i and an RSU
TS_i:	a timestamp that records the current time when V_i sends M_i
ID_i:	a pseudo identity of V_i assigned by R
U:	an entity, which could be an RSU R or a vehicle V_i
PK_U:	the public key of U
SK_U:	the private key of U
C_U:	U's anonymous certificate
$\{M\}_{PK_U}$:	encrypt the message M with a public key encryption algorithm, where PK_U is the public key of U
$\{M\}_{SK_U}$:	U's digital signature on M, where SK_U is the private key of U
$H(.)$:	a one-way hash function such as SHA-1
G, g, q:	G is a finite cyclic group generated by a generator g with a large prime order q
$MAC_k(.)$:	a message authentication code, which is generated with a symmetric key k
$\|\|$:	message concatenation operation, which appends several messages together in a special format

mutual authentication and establishes a shared secret key with R. This can be achieved by adopting the Diffie–Hellman key-establishment protocol secured with the signature scheme [17]. The mutual authentication and key-establishment processes are shown as follows:

$$V_i \longrightarrow R : \{g^a \| C_{V_i}\}_{PK_R}$$
$$R \longrightarrow V_i : ID_i \| g^b \| \{ID_i \| g^a \| g^b\}_{SK_R}$$
$$V_i \longrightarrow R : \{ID_R \| g^a \| g^b\}_{SK_{V_i}}$$

where g^a and g^b are random elements of the Diffie–Hellman key-establishment protocol and $a, b \in Z_q^*$, and the shared session key between R and V_i is $K_i \leftarrow g^{ab}$. When receiving the first message from V_i, R decrypts $\{g^a \| C_{V_i}\}_{PK_R}$ ($\|$ as a concatenation operation is described in Table I) with its private key SK_R and then verifies V_i's public key PK_{V_i} in the anonymous certificate C_{V_i}. Then, R sends $ID_i \| g^b \| \{ID_i \| g^a \| g^b\}_{SK_R}$ to V_i. V_i verifies the signature $\{ID_i \| g^a \| g^b\}_{SK_R}$ on $ID_i \| g^a \| g^b$. At last, V_i sends back the signature $\{ID_R \| g^a \| g^b\}_{SK_{V_i}}$, where ID_R is the identity of R, and R verifies the signature. If the above three steps are correctly completed, the mutual authentication succeeds. Note that the mutual authentication in the protocol is probably secure (see [17] for more details). The pseudo identity ID_i that R sends to the vehicle V_i in the second flow is uniquely linked with K_i.[1] With ID_i, R can know which vehicle sends the message and can further verify

[1]To protect the privacy, it is necessary that vehicles do not have unique pseudo IDs. This case will be discussed in Section IV-D. For ease of representation, we explain the scheme with the assumption that vehicles are allocated with a unique pseudo ID in this section.

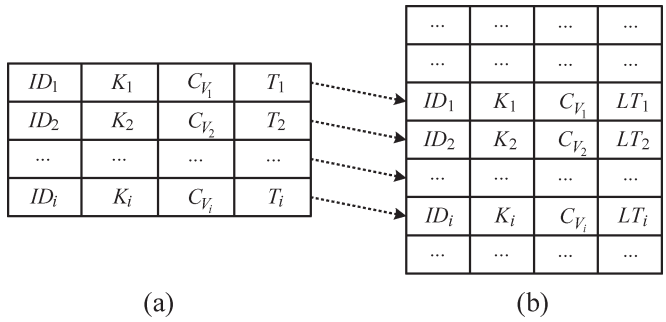

Fig. 3. (a) ID-Key table. (b) Trace evidence table.

the authenticity of the message with their shared symmetric key. Therefore, R maintains an ID-Key table in its local database, as shown in Fig. 3(a). Vehicles update their anonymous certificates once they get out of the radio range of an RSU. For instance, vehicles choose a new public/private key pair [4] to sign messages. In Fig. 3(a), T_i denotes the time when R receives the latest message from V_i. T_i is used to determine the freshness of a record. If the interval between the current time of R and T_i exceeds a predefined threshold, the record corresponding to T_i will be removed from the ID-Key table and stored in the trace evidence table, as shown in Fig. 3(b), which will be used for the purpose of traceability. The LT_i in Fig. 3(b) is used to control how long trace evidence is kept. In reality, it is decided by the authority and is much larger than the T_i in Fig. 3(a). The details of the trace process will be discussed in the following section.

B. Hash Aggregation

Once the vehicle V_i establishes the symmetric key K_i with an RSU R, V_i can use K_i to compute the MAC $MAC_{K_i}(ID_i \| M_i \| TS_i)$ on $ID_i \| M_i \| TS_i$, where ID_i is V_i's pseudo identity assigned by R, M_i is the message to be sent, and TS_i is a timestamp that records the current time when sending the message M_i. TS_i is used to thwart the replay attack. Then, V_i one-hop broadcasts $\langle ID_i \| M_i \| TS_i \| MAC_{K_i}(ID_i \| M_i \| TS_i) \rangle$. Because K_i is only known by R in addition to V_i itself, only R can verify M_i. Thus, to give the other vehicles the ability to verify the authenticity of M_i and, at the same time, reduce the communication overhead, the RSU R is responsible for aggregating multiple authenticated messages in a single packet and send it out. The detailed process is given as follows.

1) R checks if the time interval between the current time and the time when R sent the last message-authenticity notification packet is less than a predefined threshold Δt. If so, go to Step 2. Otherwise, go to Step 4.
2) When R receives a message $\langle ID_i \| M_i \| TS_i \| MAC_{K_i}(ID_i \| M_i \| TS_i) \rangle$ sent by the vehicle V_i, R first checks whether ID_i is in R's ID-Key table. If yes, go to Step 3. Otherwise, go to Step 4.
3) R uses ID_i's K_i to verify $MAC_{K_i}(ID_i \| M_i \| TS_i)$. If it is valid, R computes $H(ID_i \| M_i \| TS_i)$, and then, go to Step 1. Otherwise, drop the packet.

4) R aggregates all the hashes generated at Step 3, i.e., $HAggt = H(ID_1\|M_1\|TS_1)\|H(ID_2\|M_2\|TS_2)\|, \ldots, \|H(ID_n\|M_n\|TS_n)$, and signs it with its private key SK_R. Then, R one-hop broadcasts $\langle HAggt\|\{HAggt\}_{SK_R}\rangle$ to vehicles within its communication range.

The predefined threshold Δt in the above algorithm can affect the message authentication delay (MAD), which will be further discussed in Section VI-B. In addition, the above algorithm supports the identity traceability property. Since there is a one-to-one mapping between the key K_i and the certificate C_{V_i} in the trace evidence table, the RSU can distinguish the unique sender of a message. Thus, in the case where a malicious vehicle sends a bogus message (e.g., the context of the message is found to be fake after a while), the RSU can trace back to the message sender by finding out its certificate. The RSU could also report the certificate to a trusted authority for further investigation.

C. Verification

When a vehicle receives messages sent by other vehicles, it only buffers the received messages in its local database without immediately verifying them. The buffered record has the following format: M_i, ID_i, TS_i, and $H(ID_i\|M_i\|TS_i)$ (notice that $H(ID_i\|M_i\|TS_i)$ is computed by the receiver). Once vehicles obtain the signed packet $\langle HAggt\|\{HAggt\}_{SK_R}\rangle$ from the RSU, they are able to verify the buffered messages one by one. First of all, vehicles use the RSU's public key PK_R to verify the signature $\{HAggt\}_{SK_R}$. If it is valid, vehicles will check the validity of the previously received messages buffered in the record in the local database. This is done by comparing whether there is a match between the buffered record with the deaggregated message. For example, V_i checks if $H(ID_i\|M_i\|TS_i)$ coming in $HAggt$ has been buffered in any record before. If so, M_i is consumed. Otherwise, V_i waits to see if M_i will be in the next $HAggt$ packet. If $H(ID_i\|M_i\|TS_i)$ does not appear in two[2] successive aggregated $HAggt$ packets, M_i is regarded as invalid. The reason that $H(ID_i\|M_i\|TS_i)$ is double checked is because the RSU may have not aggregated the message M_i yet when V_i receives the first $HAggt$ packet from the RSU. In addition, a vehicle has to be capable of verifying all incoming messages sent by neighboring vehicles, which means all messages received by the vehicle can be received by its corresponding RSU as well. However, if the communication between the RSU and a vehicle [or RSU to vehicle communications (RVC)] has the same distance limit as that of IVC, a vehicle will lose the messages sent by the vehicles that have not been in the eligible distance with the RSU. Fig. 4 shows the illustration. Let the distance limit of RVC be r. The RSU can communicate with vehicles V_1 and V_2. Since V_3 is not associated with the RSU, V_2 cannot verify messages from V_3, although the two vehicles are supposed to be communicable. To overcome this problem, we require the distance limit for RVC to be two times longer than that for IVC. The distance between vehicles and vehicles, and between vehicles and RSUs, can be derived from GPS coordinates, because the GPS coordinates can be contained in the messages of vehicles.

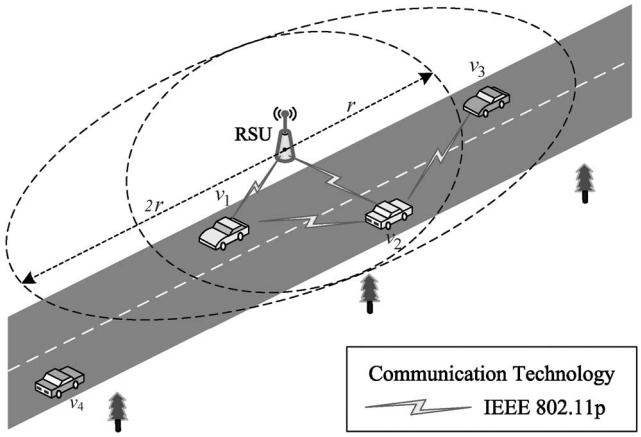

Fig. 4. Radio range of an RSU.

D. Enhancement of User Privacy

With RAISE, if a vehicle does not change its pseudo ID all the time during the association period, an adversary can trace the vehicle movement trajectory according to the vehicle's unchanged ID. Therefore, the vehicle's trace privacy is violated during the small time duration.

To preserve the trace privacy, we employ the concept of *k-anonymity* (k entities are not distinguishable) [19] in the proposed RAISE scheme to mix k vehicles. With RAISE, RSUs assign a common pseudo ID to k vehicles, where the k vehicles (as a group) will take the same pseudo ID when communicating with the RSU. When an adversary intends to trace a specific vehicle through the pseudo ID, he/she will easily get lost after the group of vehicles passes through an intersection (where an RSU is allocated). In other words, the route of a specific vehicle cannot be identified. The biggest value of k would be the total number of vehicles within the coverage range of an RSU, in which all the vehicles' messages are mixed and cannot be distinguished. Notice that such a scenario is equivalent to the case in which vehicles have no identity at all.

In the *k-anonymity* RAISE, RSUs can still identify a vehicle by finding the symmetric key shared with the vehicle, and each pseudo ID corresponds to k unique symmetric keys. Suppose a vehicle V_i sends $\langle ID\|M_i\|TS_i\|MAC_{K_i}(ID\|M_i\|TS_i)\rangle$ to RSU R. R first finds out k possible keys corresponding to the pseudo identity ID. Then, R subsequently checks whether $MAC_{K_i}(ID\|M_i\|TS_i)$ is equal to the $MAC_K(ID\|M_i\|TS_i)'$ that is generated by one of the k symmetric keys. If there is a match, the message is considered valid. Since a vehicle holds a distinct key shared with the RSU, the key that makes the above comparison can be used to find the message sender's anonymous certificate that was used during the first mutual authentication process. This can be done by looking up the RSU's local ID-Key table. Being able to find out the anonymous

[2]Suppose a vehicle V_i receives a message M_j sent by V_j and then immediately receives an aggregate $HAggt$ sent by an RSU R. Since R could not receive M_j at all before R sends $HAggt$, $H(M_j)$ will appear at the following $HAggt$.

certificate used during the mutual authentication process is to support the future ID traceability property.

However, if there is still no match with the two MAC values after R has tried all possible k keys, the message is considered as invalid and will be dropped. After this process, R can continue the message-aggregation process as presented in Section IV-C.

With the adoption of *k-anonymity*, the verification process remains the same as before. Vehicles compare whether there is a match between the deaggregated $H(ID_i \| M_i \| TS_i)$ from $HAggt$ and the buffered $H(ID_i \| M_i \| TS_i)$ value in any record. Here, the cost of comparison computation can be neglected compared with the message verification of the PKI-based scheme in [4].

V. Cooperative Message Authentication

In general, RSUs may not cover all the busy streets in a city or a highway, for example, at the beginning of VANETs' deployment period, or due to the physical damage of some RSUs, or simply for economic considerations. How to address the scalability issues under the aforementioned circumstances is the focus of this section. In this section, we introduce a cooperative message authentication scheme named COMET. By making the neighboring vehicles cooperatively work, COMET can ensure that a vehicle knows the authenticity of all received messages without verifying all the message signatures it receives. Notice that COMET is a supplementary approach of RAISE solving the message LR issue. The details of COMET are presented as follows.

A. Probabilistic Verification

First of all, we present the basic idea behind COMET, which is enlightened in [20] and [21] in different application scenarios. Suppose a vehicle sends a message using a PKI-based signature scheme to its n neighbors. To make sure the message is valid, all the neighbors (e.g., n neighbors) should verify the same signature. In other words, n neighbors do the duplicated work. Clearly, much redundant work is done, particularly when n is large. On the contrary, in COMET, we make n neighbors cooperate such that only a small number of them verify the same signature. Once a neighbor who verified the signature discovers an invalid signature, it will one-hop broadcast the result to other neighbors.

The details of COMET are shown in Algorithm 1. In Algorithm 1, V_i, V_j, and V_k are three vehicles that can one-hop communicate with each other, where $i, j, k = 1, \ldots, n$, and $i \neq j \neq k$. When V_i receives a message $\langle M_j \| \sigma_j \rangle$ sent by V_j, V_i determines whether to verify the signature σ_j with probability p (we name p the *verification probability*). If V_i determines the verification of σ_j, and σ_j is proved to be valid, V_i keeps silent and consumes M_j. On the other hand, if V_i verifies σ_j and discovers that σ_j is invalid, V_i informs the other neighbors that $\langle M_j \| \sigma_j \rangle$ is an invalid message by one-hop broadcasting $\langle ID_{M_j} \| \sigma_i \rangle$, where ID_{M_j} is used to uniquely identify the message $\langle M_j \| \sigma_j \rangle$, and σ_i is the signature signed by V_i on ID_{M_j}. Otherwise, if V_i determines not to verify σ_j, V_i waits

Data: V_i received a message M_j and its corresponding signature σ_j from V_j
Result: *True* if σ_j is valid; *False* if σ_j is invalid

```
for each vehicle V_i that received ⟨M_j||σ_j⟩ do
    V_i chooses either 1 with probability p or 0 with probability 1 − p;
    if V_i chooses 1 then
        V_i verifies σ_j;
        if σ_j is valid then
            V_i keeps silence;
            return True;
        else
            V_i one-hop broadcasts ⟨ID_{M_j}||σ_i⟩;
            return False;
        end
    else
        V_i waits Δt ms for other vehicles' reports, which tell whether σ_j is valid or not;
        if there no such report then
            return True;
        else
            V_i received such a report from V_k;
            V_i verifies σ_j;
            if σ_j is indeed invalid then
                return False;
            end
        end
    end
end
```

Algorithm 1: Probabilistic Verification Algorithm

Δt milliseconds for the other neighbors' reports. If V_i receives an invalidity report $\langle ID_{M_j} \| \sigma_k \rangle$ from V_k in Δt, V_i knows that $\langle M_j \| \sigma_j \rangle$ may be invalid. To ensure $\langle M_j \| \sigma_j \rangle$'s invalidity, V_i verifies $\langle M_j \| \sigma_j \rangle$ by itself. If V_i receives no report from other neighbors within Δt, V_i treats $\langle M_j \| \sigma_j \rangle$ as a valid message by default. Here, Δt should be greater than the total time to verify two signatures and the transmission delay between two vehicles, which is further discussed in Section VI-B.

B. Reliability Analysis

This section discusses how to guarantee that the validity result of a specific message (M_i) will always be received by all neighboring vehicles. Intuitively, at least one vehicle should work as the candidate to verify the message M_i, namely, the probability that there exists at least one vehicle, which will verify M_i, is as close to 1 as possible. However, from the communication range's point of view, only one vehicle that verifies a message is not enough. For example, in Fig. 4, suppose that V_1 and V_3 are V_2's neighbors. V_2 sends a bogus message, and V_3 determines to verify it, while V_1 does not. Since V_1 is not in the communication range of V_3, it cannot receive the report from V_3. Therefore, without loss of generality, there should exist at least two vehicles verifying a message sent by a vehicle, for example, V. One vehicle should physically be in front of V, whereas the other should be behind V.

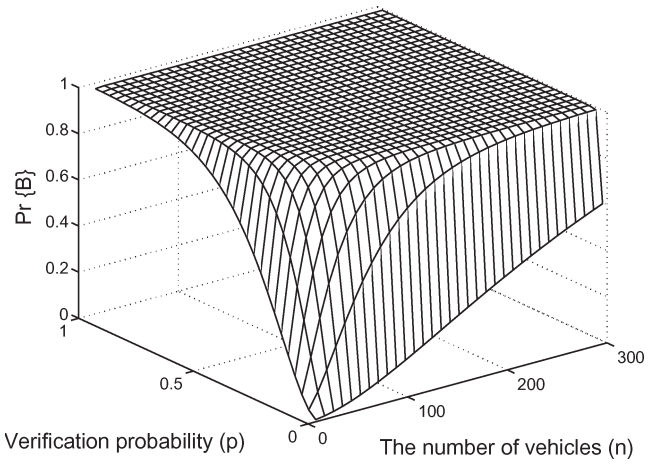

Fig. 5. $\Pr\{\mathrm{B}\}$ versus traffic load (n) and verification probability (p).

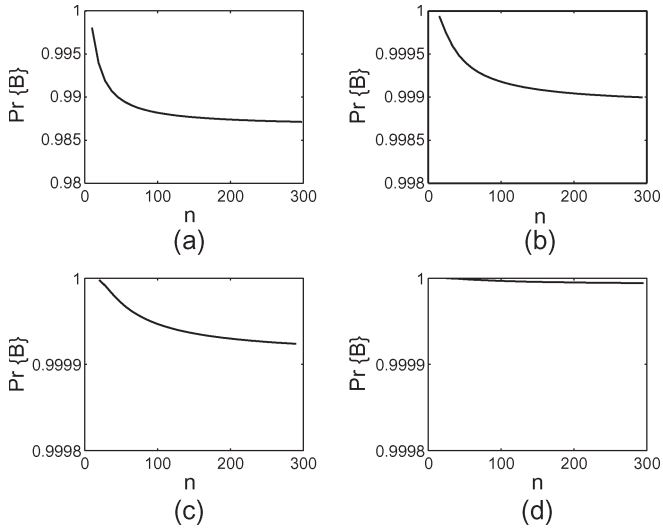

Fig. 6. $\Pr\{\mathrm{B}\}$ versus traffic load (n). (a) $k = 10$. (b) $k = 15$. (c) $k = 20$. (d) $k = 25$.

Let n be the total number of neighboring vehicles of V, i be the number of neighbors in front of V, and $n - i$ be the number of neighbors behind V. Notice that the value of n can be known by each vehicle because each vehicle periodically broadcasts its traffic-related information (e.g., a pseudo identity and a position) every 300 ms. Suppose that V's neighbors are uniformly distributed around V and that each vehicle's position is independent. Let A_i be the event that there are i vehicles in front of V and $n - i$ vehicles behind V. Let B be the event that there are at least two vehicles that will verify a message sent by V, one of which is in front of V and where the other is behind V. Then, $\Pr\{B\}$ can be represented as a function of n and p as

$$\begin{aligned}\Pr\{B\} &= \sum_{i=0}^{n} \Pr\{B|A_i\} \cdot \Pr\{A_i\} \\ &= 1 + (1-p)^n - 2 \cdot \left(1 - \frac{p}{2}\right)^n \end{aligned} \tag{1}$$

where $\Pr\{B|A_i\} = (1-(1-p)^i) \cdot (1-(1-p)^{n-i})$, and $(1-p)^i$ is the probability that none of the i vehicles in front of V will verify a message sent by V, $1-(1-p)^i$ is the probability that there is at least one vehicle that will verify the message, and $1-(1-p)^{n-i}$ is the probability that there is at least one vehicle behind V that will verify the message, respectively; $\Pr\{A_i\} = \binom{n}{i} \cdot (1/2)^i \cdot (1-1/2)^{n-i}$ because each vehicle's position is independent, and the number of vehicles in front of (or behind) V follows the binomial distribution with parameters n and 1/2. Our objective is to make $\Pr\{B\}$ as close to 1 as possible.

Fig. 5 shows the relationship among $\Pr\{B\}$, p, and n. It can be seen that $\Pr\{B\}$ increases as either p or n increases. The increasing gradient is rather sharp. $\Pr\{B\}$ quickly approaches 1 when p is a small value (e.g., $\Pr\{B\} = 99.98\%$ when $p = 15\%$ and $n = 120$). Moreover, we can conclude from Fig. 5 that when $\Pr\{B\}$ is fixed, p is inversely proportional to n. In particular, when n is large, p should be small, and *vice versa*. Our objective is to change p to make $\Pr\{B\}$ approach 1 as much as possible. On the other hand, under the condition that $\Pr\{B\}$ has sufficiently approached 1, we try to make p as small as possible because a small value of p implies that a vehicle can potentially save processor (e.g., CPU) resources and can further verify more messages when the traffic load becomes larger.

For each vehicle to choose an appropriate p under different values of n, we use the parameter $k = n \cdot p$ to leverage the inversely proportional relationship between p and n. Notice that k presents the average number of signatures that a vehicle verifies every 300 ms because n is the total number of neighbors (each of which sends a message every 300 ms), and p is the verification probability. If we can find a suitable k, then the corresponding p can be determined. Based on (1), we can obtain the relationship between $\Pr\{B\}$ and n in terms of different k, as shown in Fig. 6. From Fig. 6(a) and (b), we can see that $\Pr\{B\}$ with $k = 10$ and $\Pr\{B\}$ with $k = 20$ are not very close to 1. However, from Fig. 6(d), we can see that $\Pr\{B\}$ with $k = 25$ is sufficiently close to 1, no matter how large n is. Therefore, we conclude that in COMET, we can set k as a constant value, i.e., 25. Since k is fixed, p can be computed as k/n (that is, $25/n$). In other words, we can change p according to n. For example, a vehicle V having 50 neighbors receives a message M_i, and V will verify M_i with the probability of 25/50. Notice that V knows the number of its neighbors. In the case where n is less than 25, let p be equal to 100%. It is worth noting that k cannot be larger than the vehicle V's verification capability, which is the maximum number of verifications that the vehicle V can process.

C. Misbehavior Resilience

Misbehavior or selfish behavior is an inherent attack in cooperative networks. In our scheme, there are two kinds of misbehaviors. 1) Some vehicles do not verify any signature, and instead, they just wait for the other honest nodes' reports. 2) Some vehicles verify signatures, but they do not send any report to other vehicles.[3] Previously related studies have

[3]Notice that if an internal adversary sends a false report to others, its signature will be verified by others. After other vehicles know the report is a false one, they could report the false message to an authority. The authority can trace the internal adversary.

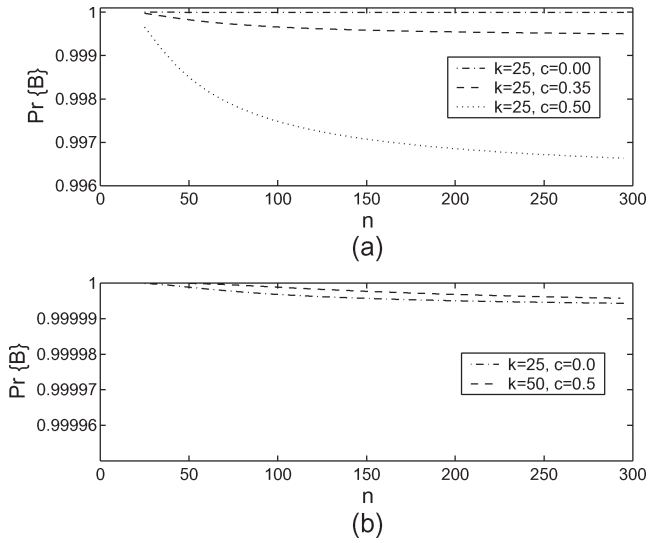

Fig. 7. $\Pr\{\mathrm{B}\}$ versus traffic load (n) given different k and c.

addressed misbehavior issues. Zhang *et al.* [22] introduce a credit-based scheme that encourages nodes forwarding packets in mobile ad hoc networks. Zhang *et al.* [10] employ a tamper-proof device in vehicular sensor networks, and the tamper-proof device can trustworthily generate pseudorandom identities for a vehicle. Although these schemes can prevent misbehavior, the overhead is high (such as credit management in [22]).

Based on COMET, we can increase the value of k (and the corresponding p) to eliminate the effect caused by misbehaving vehicles. Assume that the total percentage of misbehaving vehicles in VANETs is not more than 50%, which is similar to that in [23] and [24]. This assumption is reasonable because, in reality, misbehaving vehicles are expected to make up only a small portion of the total vehicles. Let c represent the percentage of misbehaving vehicles in vehicular networks. In this case, if a vehicle has n neighbors, there would exist $(1-c)\cdot n$ vehicles that apply COMET and $c\cdot n$ misbehaving vehicles. As such, based on (1), $\Pr\{B\}$ equals $1+(1-p)^{(1-c)\cdot n}-2\cdot(1-p/2)^{(1-c)\cdot n}$. Fig. 7(a) shows that $\Pr\{B\}$ decreases as c increases. The ideal result is to keep $\Pr\{B\}$ as the case where $k=25$ and $c=0.0$ [as shown Fig. 6(d)]. Our solution is to increase the parameter k, i.e., let $k=50$. Fig. 7(b) indicates that $\Pr\{B\}$ with $k=50$ and $c=0.5$ approximates $\Pr\{B\}$ with $k=25$ and $c=0.0$. Therefore, COMET with $k=50$ can effectively eliminate the negative effects of misbehaving vehicles. In the next section, through simulation, we will see that $k=50$ is feasible for a PKI-based (e.g., ECDSA [15]) signature scheme, which will not introduce a high message LR.

VI. Performance Evaluation

In this section, we use the ns-2 simulator [25] to evaluate the performance of RAISE and COMET in terms of the message loss radio, the message end-to-end delay, and the communication overhead, respectively, compared with the group-signature-based scheme in [5] and the standard PKI-based ECDSA signature scheme in [15]. In the simulation, COMET is simulated based on the ECDSA signature scheme. We simulate a traffic scenario with high vehicle density. An RSU is located at an intersection, and 30–200 vehicles can associate with the RSU. Notice that an RSU is only used in RAISE, and other schemes do not need an RSU's help. The intervehicular distance varies from 7.5 to 15 m to simulate scenarios with different traffic densities. The distance limits for IVC and RVC are 300 and 600 m, respectively. Intervehicle messages are sent every 300 ms at each vehicle. IEEE 802.11a is used to simulate the transmission protocol in the medium access control layer. The bandwidth of the channel is 6 Mb/s. The group signature verification delay is 11 ms [26]. The ECDSA signature verification delay is 3.87 ms.[4] All possible cryptographic operations in the simulation are considered to have the same simulation delay.

A. Message LR

The average message LR is defined as

$$\mathrm{LR}=\frac{1}{N}\sum_{i=1}^{N}\left(M^i_{\mathrm{app}}/M^i_{\mathrm{mac}}\right) \tag{2}$$

where N represents the total number of vehicles in the simulation. For the group-signature-based and PKI-based signature schemes, M^i_{mac} represents the total number of messages received by the ith vehicle in the medium access control layer, and M^i_{app} represents the total number of messages consumed by the ith vehicle in the application layer. For RAISE, M^i_{mac} represents the total number of messages directly received from other vehicles in the medium access control layer, and M^i_{app} represents the total number of $H(ID_i\|M_i\|TS_i)$s that are sent by the RSU and are consumed by the application layer. For COMET, the group signature, and PKI-based ECDSA signature schemes, we only consider the message loss incurred by delays due to the security scheme rather than the wireless transmission channel. Since RAISE needs two-hop communications, we consider the loss caused by wireless communications between the RSU and vehicles.

Fig. 8 shows the relationship between the message LR and the traffic load. The traffic load is represented by the number of vehicles. For RAISE, the RSU periodically broadcasts an aggregation of $H(ID_i\|M_i\|TS_i)$ every 10 ms. From Fig. 8, we can see that the message LR of RAISE, the group signature, and the PKI-based ECDSA signature schemes increase as the traffic load increases. The group-signature-based scheme has the highest LR, and the PKI-based scheme ranks the second. RAISE, on the other hand, has the lowest LR. From the simulation, most of the message losses of RAISE come from the two-hop wireless transmission. In addition, Fig. 8 shows that COMET with $k=50$ also has a quite low message LR, and the LR does not change with the number of vehicles. Since k is a constant, i.e., 50 in our simulation, each vehicle verifies a constant number of message signatures no matter how many neighbors a vehicle has. In other words, the number of message

[4]The 224-bit ECDSA cryptographic delays are quoted from the MIRACL cryptographic library [27] with the 3-GHz Pentium IV system.

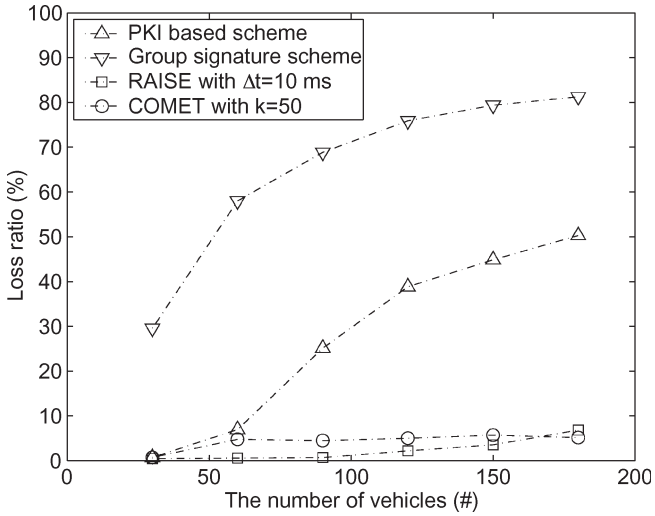

Fig. 8. Average LR versus traffic load.

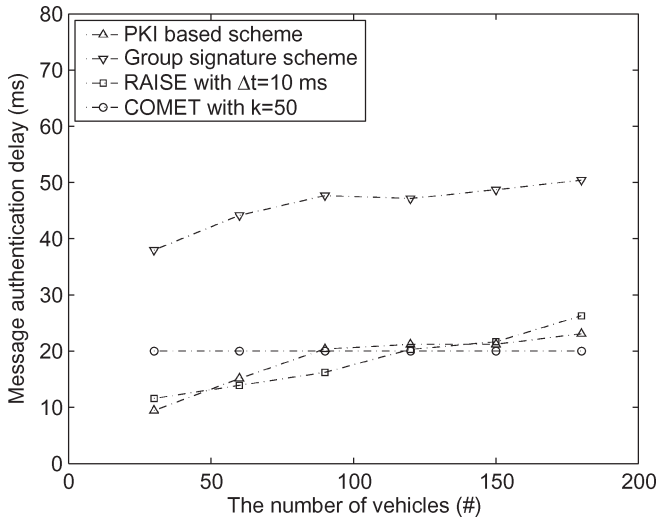

Fig. 9. Average MAD versus traffic load.

signatures that a vehicle may verify is independent of the traffic density, and the message LR is thus independent of the traffic density.

B. Message Authentication Delay (MAD)

The average MAD is defined in (3), where N represents the total number of vehicles in the simulation, M is the number of messages sent by the ith vehicle, and K is the number of adjacent vehicles within the ith vehicle's communication range. $T_{\text{recv}}^{i,k,m}$ represents the moment that the kth vehicle in the application layer receives the mth message from the ith vehicle. $T_{\text{send}}^{i,k,m}$ represents the moment that the ith vehicle in the application layer sends the mth message to the kth vehicle, i.e.,

$$\text{MAD} = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{MK}\sum_{m=1}^{M}\sum_{k=1}^{K}\left(T_{\text{recv}}^{i,k,m} - T_{\text{send}}^{i,k,m}\right). \quad (3)$$

Fig. 9 shows the relationship between the MAD and the traffic load. Again, the group signature scheme has the highest MAD. This is due to the high delay verifying a message signature. The PKI-based ECDSA scheme and RAISE yield nearly the same MAD. Since the comparison computation is very fast, the delay of RAISE is primarily determined by the packet release interval at the RSU. For example, the packet release interval Δt is 10 ms in our simulation, which serves as the main contribution of the MAD. To reduce the MAD, we can decrease this time interval at the expense of increasing the communication overhead, which will further be discussed in the next section. For COMET, as mentioned in Section V-A, the MAD can adjustably be set, but it must be larger than the total time to verify two signatures and the transmission delay between two vehicles. In Fig. 9, we can see that when there are 50 vehicles, the MAD for the PKI-based ECDSA signature scheme is 12 ms. Verifying a single signature with ECDSA needs 3.87 ms. Thus, the MAD of COMET should be larger than 12 + 3.87 ms plus the transmission delay. Since the transmission delay is negligible, the 20-ms delay, which is far larger than 12 + 3.87 ms, is feasible. The reason that we add 3.87 ms is because a vehicle should verify a bogus message signature in person when it receives a report from other vehicles.

C. Communication Overhead

The communication overheads of ECDSA [15], the group-signature-based scheme [5], COMET based on ECDSA, and RAISE, respectively, are listed below. With ECDSA, each message yields 181 B as the additional overhead due to cryptographic operations, which includes a certificate and an ECDSA signature, as shown in Fig. 2. With the group-signature-based scheme, the additional communication overhead is 184 B [26]. With COMET, the communication overhead is the same as the ECDSA when there is no bogus signature. Due to the fact that vehicles sending bogus signatures are rather rare, the additional reports of the bogus signatures are negligible. Therefore, the communication overhead caused by COMET is equal to that of ECDSA. With RAISE, the additional communication overhead is 128 bits + 128 bits + $(56 + 2)/n$ bytes, where the first 128 represents the length of a MAC sent by a vehicle, the second 128 bits represent the length of the $H(ID_i \| M_i \| TS_i)$ packet that is sent by an RSU, 56 B is the length of an ECDSA signature [15] signed by the RSU, and 2 B is the length of a message header, as shown in Fig. 2. Here, 56 + 2 B are shared by n messages, because in RAISE, n messages are batched and signed once. Note that n is determined by the density of vehicles and the packet release interval for the RSU to broadcast a batched packet.

Fig. 10 shows the relationship between the overall communication overhead in 1 min and the traffic load within an RSU. We can see that RAISE with the time interval of 10 ms has a much lower communication overhead than that of the PKI-based ECDSA signature scheme and the group-signature-based scheme. Furthermore, the communication overhead of RAISE is 24.94% of the PKI-based ECDSA signature scheme and 23.64% of the group-signature-based scheme.

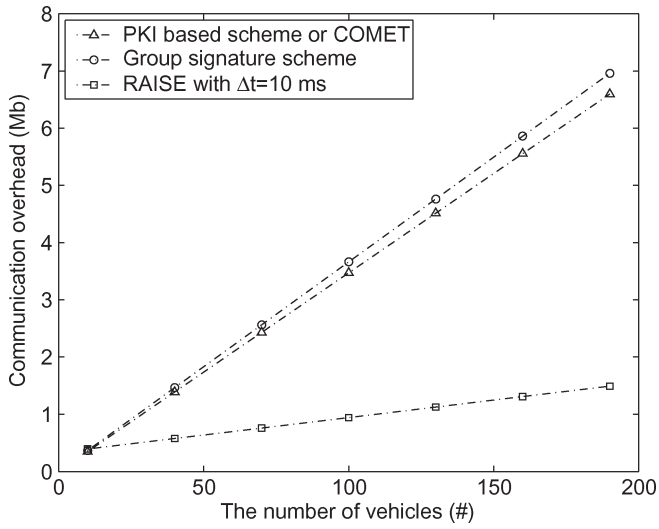

Fig. 10. Communication overhead versus traffic load.

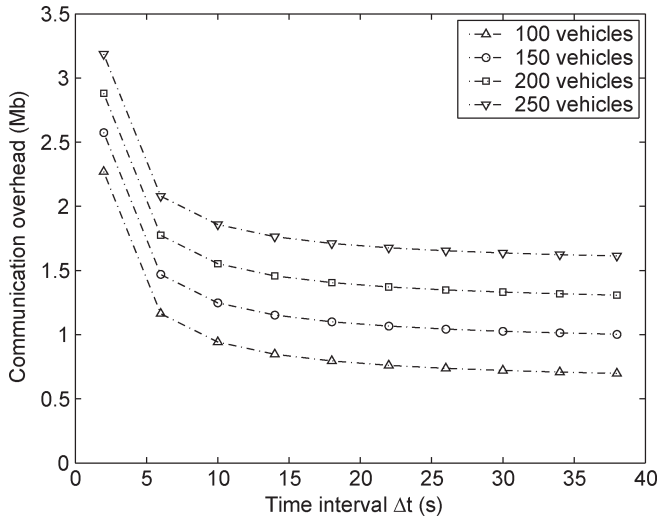

Fig. 11. Communication overhead versus time interval.

To further illustrate the effect of the time interval on RAISE, Fig. 11 shows the relationship between the time interval and the overall communication overhead caused by 100, 150, 200, and 250 vehicles, respectively, in 1 min. Clearly, as the time interval increases, particularly from 2 to 10 ms, the communication overhead sharply decreases. However, when the time interval is up to 10 ms or larger, it has very little effect on the communication overhead. This is because the frequency of sending 56 + 2 B decreases as the time interval increases. From Fig. 11, we can also see that the communication overhead increases by approximately 0.3 MB every time the number of vehicles increases by 50.

VII. Security Analysis

In this section, we analyze the security of the proposed schemes in terms of message integrity and source authentication, prevention of internal attack, replay attack resistance, and conditional privacy preservation.

Message Integrity and Source Authentication: With RAISE, a vehicle generates a MAC for each launched message. The MAC can only be generated by the vehicle that has the key assigned by the RSU. If an adversary tampers with a message, the RSU cannot find a responding validation key that can compute a matching MAC for the message, and therefore, the intercepted message will be ignored. In addition, for each vehicle, there is a unique key stored in the ID-Key table at the RSU side. If an RSU can find out a key to verify a MAC, the RSU can know the identity of the message sender, and therefore, the source is authenticated. On the other hand, with COMET, we can also achieve message integrity and source authentication because COMET works exactly the same way as the other PKI-based schemes such as ECDSA. Due to the nature of message integrity and source authentication, typical attacks, such as bogus attack and impersonation attack [4], can be prevented.

Prevention of Internal Attack: RAISE is robust against not only external attacks but internal attacks as well. Even if a vehicle is compromised, and its symmetric secret session key shared with an RSU is exposed to an adversary, the adversary cannot trace the other vehicle's movement because it cannot distinguish the vehicles that use the same pseudo ID with the compromised vehicle. Therefore, RAISE can resist a key-compromise impersonation attack.

Replay Attack Resistance: With a replay attack, an adversary replays intercepted messages to impersonate a legitimate vehicle. Obviously, this impersonation cannot work with RAISE because a time stamp TS_i is attached with the corresponding M_i, and all vehicles keep time synchronization. Suppose an adversary intercepts a message $\langle ID_i \| M_i \| TS_i \| MAC_{K_i}(ID_i \| M_i \| TS_i) \rangle$ and launches a replay attack at time TS_j. Because the time period $|TS_j - TS_i| > \Delta T$, where ΔT is a mutually agreed to transmission delay, the receiver will reject the message. Therefore, RAISE is robust to resisting the replay attack.

Conditional Privacy Preservation: RAISE makes vehicles use pseudo identities to protect their real identities. Nevertheless, RSUs are able to know the anonymous certificate corresponding to a pseudo identity, and a TA is capable of tracing the real identity of a vehicle from its anonymous certificate. For example, a vehicle V_i sends a bogus message, which contains the pseudo identity ID_i that an RSU allocates. Once the RSU finds out that the content of the message is bogus, the RSU can know the anonymous certificate of the V_i from the trace evidence table in which the ID_i uniquely maps the anonymous certificate C_{V_i}, as shown in Fig. 3(b). Further, the RSU gives the certificate C_{V_i} to a TA, which has the ability to trace the real identity of the V_i from C_{V_i}. Therefore, in RAISE, vehicles cannot tell their real identities to each other, whereas RSUs can distinguish whether two messages are sent by the same vehicle. The TA and RSUs cooperate, which can trace the real identity of a message sender.

VIII. Conclusion and Future Work

In this paper, a novel RSU-aided message authentication scheme named RAISE has been proposed. With RAISE, RSUs

are responsible for verifying the authenticity of messages sent by vehicles and notifying the authentication results back to all the associated vehicles. The RAISE scheme has many advantages because of its lower computation and communication overhead. RAISE also protects the vehicles' privacy by adopting the *k-anonymity* approach. In addition, a cooperative message authentication scheme named COMET has been proposed to work as a supplementary scheme of RAISE in case of the absence of an RSU. COMET not only efficiently reduces the message LR but is also resilient against the misbehavior of vehicles. In our future work, we will explore an efficient revocation scheme to revoke misbehaving or faulty vehicles. In addition, fast disseminating revocation information will also be investigated.

REFERENCES

[1] U.S. Dept. Transp., Nat. Highway Traffic Safety Admin., *Vehicle Safety Communications Project*, 2006. Final Rep.

[2] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. ACM Int. Symp. MobiHoc*, 2007, pp. 150–159.

[3] *Dedicated Short Range Communications (DSRC)*. [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

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

[5] 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.

[6] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," in *Proc. Int. Workshop VANET*, 2007, pp. 19–28.

[7] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proc. ISADS*, 2007, pp. 344–351.

[8] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, Phoenix, AZ, 2008, pp. 1229–1237.

[9] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.,* to be published.

[10] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM*, Phoenix, AZ, 2008, pp. 246–250.

[11] K. Ren, W. Lou, R. H. Deng, and K. Kim, "A novel privacy preserving authentication and access control scheme in pervasive computing environments," *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1373–1384, Jul. 2006.

[12] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA Crypto.*, vol. 5, no. 2, pp. 2–13, 2002.

[13] D. Boneh and M. Franklin, "Identify-based encryption from the Weil pairing," in *Proc. CRYPTO*. New York: Springer-Verlag, 2001, vol. 2139, pp. 213–229.

[14] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, and H.-C. Wong, "Secret handshakes from pairing-based key agreements," in *Proc. IEEE Symp. Security Privacy*, 2003, pp. 180–196.

[15] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages,* IEEE Std. 1609.2-2006, Jul. 2006.

[16] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in *Proc. Int. Workshop WiN-ITS*, Vancouver, BC, Canada, Aug. 2007.

[17] D. R. Stingson, *Cryptography: Theory and Practice*, 3rd ed. Boca Raton, FL: CRC, 2005.

[18] *Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications,* ANSI/IEEE Std. 802.3-1985, 1985.

[19] L. Sweeney, "K-ANONYMITY: A model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[20] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proc. ACM/IEEE Int. Conf. MOBICOM*, 1999, pp. 151–162.

[21] F. Picconi, N. Ravi, M. Gruteser, and L. Iftode, "Probabilistic validation of aggregated data for V2V traffic information systems," in *Proc. Int. Workshop VANET*, 2006, pp. 76–85.

[22] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," *ACM Wireless Netw.*, vol. 13, no. 5, pp. 569–582, Oct. 2007.

[23] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.—Special Issue on Vehicular Networks*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[24] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. Int. Workshop VANET*, 2004, pp. 29–37.

[25] *The Network Simulator—ns-2*. [Online]. Available: http://nsnam.isi.edu/nsnam/index.php

[26] X. Sun, "Anonymous, secure and efficient vehicular communications," M.S. thesis, Univ. Waterloo, Waterloo, ON, Canada, 2007.

[27] *Shamus Software. MIRACL library*. [Online]. Available: http://www.shamus.ie/index.php?page=Elliptic-Curve-point-multiplication

[28] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. Int. Workshop VANET*, 2006, pp. 67–75.

Chenxi Zhang (S'07) received the B.E. and M.E. degrees from Harbin Institute of Technology, Harbin, China, in 2003 and 2005, respectively. He is currently working toward the Ph.D. degree with the Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON, Canada.

His research interests include wireless network security and vehicular network security.

Xiaodong Lin received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in June 2008.

He is currently an Assistant Professor with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON. His research interests include wireless network security, applied cryptography, and anomaly-based intrusion detection.

Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Award of the IEEE International Conference on Communications (ICC'07) - Computer and Communications Security Symposium.

Rongxing Lu is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

He is currently a Research Assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Pin-Han Ho (M'04) received the B.Sc. and M.Sc. degrees from the National Taiwan University, Taipei, Taiwan, R.O.C., in 1993 and 1995, respectively, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2002.

He is currently an Associate Professor with the University of Waterloo. He is the author or coauthor of more than 100 refereed technical papers and book chapters and the coauthor of a book on optical networking and survivability.

Prof. Ho was the recipient of the Distinguished Research Excellent Award from the Electrical and Computer Engineering Department, University of Waterloo, the Early Researcher Award (Premier Research Excellence Award), the Best Paper Award from the 2002 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'02), the IEEE International Conference on Communications (ICC'05 and ICC'07), and the Outstanding Paper Award from the 2002 Workshop on High-Performance Switching and Routing (HPSR'02).

Xuemin (Sherman) Shen (M'97–SM'02) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982 and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, Camden, NJ, in 1987 and 1990, respectively.

He is a Professor and a University Research Chair and the Associate Chair for Graduate Studies with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on mobility and resource management in interconnected wireless/wireline networks, UWB wireless communications systems, wireless security, and ad hoc and sensor networks. He is the coauthor of three books and has published more than 300 papers and book chapters in wireless communications and networks, control, and filtering.

Dr. Shen has served as the Technical Program Committee Chair for IEEE Globecom'07, General Co-Chair for Chinacom'07 and QShine'06, and the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, Editor-in-Chief for *Peer-to-Peer Networking and Application*, Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *KICS/IEEE Journal of Communications and Networks*, *Computer Networks*, *ACM/Wireless Networks*, *Wireless Communications and Mobile Computing (Wiley)*, etc. He has also served as Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, and IEEE COMMUNICATIONS MAGAZINE. He received the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, and the Distinguished Performance Award in 2002 from the Faculty of Engineering, University of Waterloo. He is a registered Professional Engineer in Ontario.