This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks

Chenxi Zhang, Xiaodong Lin, Rongxing Lu, and Pin-Han Ho
Electrical and Computer Engineering, University of Waterloo, Canada
c14zhang@engmail.uwaterloo.ca, {xdlin, rxlu, pinhan}@bbcr.uwaterloo.ca

***Abstract*—Addressing security and privacy issues is a prerequisite for a market-ready vehicular communication network. Although recent related studies have already addressed most of these issues, few of them have taken scalability issues into consideration. When the traffic density becomes larger, a vehicle cannot verify all signatures of the messages sent by its neighbors in a timely manner, which results in message loss. Communication overhead as another issue has also not been well addressed in previously reported studies. To deal with these issues, this paper introduces a novel RSU-aided messages authentication scheme, called RAISE. With RAISE, roadside units (RSUs) are responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. In addition, our scheme adopts the k-anonymity approach to protect user identity privacy, where an adversary cannot associate a message with a particular vehicle. Extensive simulations are conducted to verify the proposed scheme, which demonstrates that RAISE yields much better performance than any of the previously reported counterparts in terms of message loss ratio and delay.**

***Keywords*—Vehicular ad hoc networks, security, privacy, scalablity.**

I. Introduction

As a promising Internet and wireless application scenario, vehicular ad hoc networks (VANETs) have been attracting more and more attentions from both industry and academia. In VANETs, vehicles are equipped with wireless on-broad units (OBUs), which communicate with each other or with roadside units (RSUs) with a dedicated short range communications (DSRC) [1] protocol. According to DSRC, each vehicle periodically broadcast its routine traffic-related information [2] containing its current speed, location, deceleration/acceleration, etc. With the received information, other drivers can make an early response in case of exceptional situations such as accidents, emergent braking, and traffic jams. In addition to safety and traffic-related applications, VANETs can also provide some entertainment related applications such as electronic advertisements [3], downloading/uploading data information through the Internet, and local information acquisition (e.g., road maps and restaurant/hotel/gas-bar information).

In spite of the numerous advantages by launching a VANET, security issues have to be well addressed before we put these application scenarios into practice. First of all, message integrity must be guaranteed. Secondly, message senders should be authenticated in order to prevent impersonation attacks. In addition, user privacy concerns must also be well mitigated, where the identity, the position, and the movement track of a specific vehicle should not be obtained by the third party.

Many related studies have been reported on security and privacy preservation in VANETs [4]–[8]. To achieve both message authentication and anonymity, Raya *et al*. in [5] proposed that each vehicle should be pre-loaded with a large number of anonymous public and private key pairs and the corresponding public key certificates. There is a pseudo identity in each public key certificate. Traffic messages are signed with a public key based scheme, and each public and private key pair has a short life time to achieve privacy preserving. To avoid pre-loading a large number of anonymous key materials in each vehicle, Lin *et al*. in [6] introduced a group signature scheme to sign each message. In this scheme, each vehicle has only one public and private key pair. The public key is the same for all vehicles, and the private key of each vehicle is different. For a message signature, a vehicle only knows the authenticity of the signature, and the vehicle has no information on the identity of the message sender. Lu *et al*. in [7] proposed a conditional privacy preservation scheme called ECPP, which divides privacy into three levels. In ECPP, RSUs are responsible for issuing temporary public key certificates to vehicles. Zhang *et al*. in [8] developed an identity-based batch verification scheme called IBV, which employs a tamper-proof device to protect privacy. Freudiger *et al*. in [9] and Sampigethava et al. in [10] respectively proposed location persevering schemes.

Although the above-mentioned studies respectively solved the security and privacy threats to different extents, they have all failed in taking the scalability issue and resultant communication overhead into consideration. First of all, they have not addressed the stringent time requirement for a vehicle to verify all message signatures sent by its neighboring vehicles especially when the traffic density becomes larger. Moreover, the packet length is dramatically increased due to the signatures and public key certificates attached with each message. Therefore, these cryptographic operations have incurred very high computation and communication overhead when securing VANETs, which could be intolerable and make those schemes unsuitable to meet the current standard specifications. This becomes a particularly serious problem when inter-vehicle communication (IVC) is performed in a metropolitan area with many vehicles in each other's communication range.

978-1-4244-2075-9/08/$25.00 ©2008 IEEE

To address the above issues, this paper proposes an RSU-aided message authentication scheme, called RAISE, aiming to yield a significant improvement in authentication efficiency and scalability for metropolitan-area IVC. Compared with previous message authentication schemes [5] and [6], which only considered IVC, RAISE explores the unique features of VANETs by employing RSUs to assist vehicles in authenticating messages. By taking advantage of the fact that a metropolitan area could most likely be covered by RSUs, a vehicle that receives a message does not need to verify the message through a conventional public key infrastructure (PKI) based scheme that could lead to significant overhead. Instead, each IVC message will be attached with a short keyed-hash message authentication (HMAC) code generated by the vehicle, and the corresponding RSU in the range will verify these HMACs and disseminate the notice of authenticity to each vehicle. The notice message is the aggregation of hash values of IVC messages. With the short HMAC code attached to each IVC message, the verification of message authenticity can be performed in an extremely fast and efficient way because HMAC is performed using fast symmetric decryption.

We will describe in detail how RAISE works and how it ensures security and privacy preservation without incurring much overhead and scalability problems in presence of the high density of vehicles in metropolitan areas. The rest of the paper is organized as follows: Section II briefly introduces the system model and the preliminaries including adopted assumptions, problem statements, and security objectives. Section III presents the proposed RAISE in detail. Section IV analyzes the performance of RAISE through extensive simulations. We draw the conclusions in Section V.

II. System Model and Preliminaries

A. System Model

A VANET is hierarchically composed of two layers. The upper layer is composed of application servers (ASs) and road side units (RSUs), as shown in Figure 1. The ASs can connect with RSUs through secure channels, such as a 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. The lower layer is composed of RSUs and vehicles. Notice that in this paper we aim to address the security and privacy issues in the lower layer.

B. Assumption

According to the above system model, this paper is based on the following assumptions: 1) RSUs are trusted, and is hard to be compromised. 2) RSUs have higher computation capability than vehicles; 3) The proposed scheme only considers IVC message authentication when any RSU is available. We assume that the locations where the density of vehicles is high will be allocated with an RSU, such as an intersection and any possible traffic bottleneck. Such locations will be where our scheme works most effectively. For those areas with a sparse vehicle distribution, we do not consider whether there is an RSU or not.

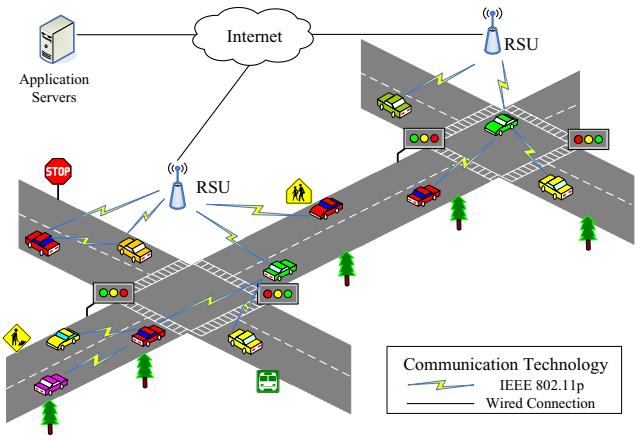

Fig. 1. The network model

The reason is that the scalability issue will not be a problem, and that a conventional PKI-based authentication scheme can sufficiently work well. 4) The communication range of an RSU can be larger than that of the vehicles, so that some vehicles can hear from the RSU while the RSU cannot hear from the vehicles.

C. Problem Statement

The current IEEE Trial-Use standard [11] for VANETs security provides us a detailed documentation including the choice of crytosystems. To authenticate a message sender and guarantee the message integrity, OBUs and RSUs should sign messages with their private keys before the messages are sent. Figure 2 shows the format of a signed message according to [11]. We can observe that a 125-byte certificate and a 56-byte ECDSA signature have to be attached for each 69-byte IVC message. Obviously, the cryptographic overhead (the certificate and the signature) takes up a significant portion of the total packet size.

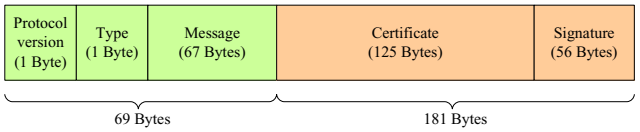

Fig. 2. The format of a signed message

Cryptographic operations also lead to high computation burden for receivers who wish to verify these messages. According to DSRC [1], a vehicle sends a message within the time interval of 100-300 ms. Generating a signature every 100 ms is not a problem for current pubic key based signature schemes. However, in the case that 50-200 vehicles are within the communication range, the receiver needs to verify around 200-2000 messages per second. Public key certificates have to be verified as well sometimes. Signing and verifying each message are certainly able to achieve secure communication; however, these cryptographic operations make the security

protocol 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 public key infrastructure or group signature schemes are far from satisfactory to this stringent time requirement.

D. Security Objectives

The proposed scheme, RAISE, aims to achieve the following security objectives:

Message integrity and source authentication: All messages should be delivered unaltered, and the origin of the messages should be authenticated to guard against an impersonation attack.

Low communication overhead and fast verification: The security scheme should be efficient with small communication overhead and acceptable processing latency. A large number of message signatures should be verified in a short interval.

Conditional privacy preservation: The identities of vehicles should be hidden from a normal message receiver during the authentication process in order 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.

Prevention of an internal attack: A vehicle holding its own keying material cannot know key materials of other vehicles.

III. The Proposed Scheme

In this section, we propose an RSU-aided message authentication scheme, called RAISE. With RAISE, when an RSU is detected nearby, vehicles start to associate with the RSU. Then, the RSU assigns an unique shared symmetric secret key and a pseudo ID that is shared with other vehicles. With the symmetric key, each vehicle generates a symmetric keyed-hash message authentication (HMAC) code, and then broadcasts a message by signing the message with the symmetric HMAC code instead of a PKI-based message signature. Other vehicles receiving the messages signed with the HMAC code are able to verify the message by using the notice about the authenticity of the message disseminated by the RSU. The reason why the RSU knows the authenticity of the messages is that the RSU has the HMAC encryption keys shared with vehicles. Note, in any circumstance that a vehicle cannot recognize a received message, it will simply go back to use the traditional PKI-based scheme to verify the message.

The detailed implementation of RAISE will be presented in the following subsections. For ease of presentation, the notations throughout this paper are listed in Table I.

TABLE I
Notations

Notation	Descriptions
R_i:	the i-th RSU
V_i:	the i-th vehicle
M_i:	the message sent by V_i
K_i:	the key shared between V_i and R_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
T:	the current time
PK_U:	the public key of U
SK_U:	the private key of U
C_U:	U's certificate
$\{M\}_{SK_U}$:	U's digital signature on M
$H(.)$:	a one-way hash function such that SHA-1
$HMAC(.)$:	a keyed-hash message authentication code
$\|\|$:	message concatenation operation, which appends several messages together in a special format

A. Symmetric Key Establishment

Once a vehicle V_i detects that there is an RSU R_i nearby (e.g., through a Hello message of R_i), V_i initiates a mutual authentication process and establishes a shared secret key with R_i. This process can be achieved by adopting the Diffie-Hellman key agreement [12] protocol secured with public key based signature scheme. The mutual authentication and key agreement processes are shown as follows:

$$\begin{aligned} V_i &\longrightarrow R: \quad g^a, \{g^a\}_{SK_{V_i}}, C_{V_i}. \\ R &\longrightarrow V_i: \quad ID_i||g^b, \{ID_i||g^a||g^b\}_{SK_R}, C_R. \\ V_i &\longrightarrow R: \quad \{g^b\}_{SK_{V_i}}. \end{aligned}$$

where g^a and g^b are elements of the Diffie-Hellman key agreement protocol[1], and the shared key between R_i and V_i is $K_i \leftarrow g^{ab}$. When receiving the first message from V_i, R_i can verify V_i's public key PK_{V_i}, and then uses PK_{V_i} to verify the signature $\{g^a\}_{SK_{V_i}}$ on g^a. In a similar manner, V_i authenticates R_i. If the above three flows succeeds, the mutual authentication process is done. At the same time, in the second flow, R_i assigns a pseudo identity ID_i to the vehicle V_i. The pseudo ID is uniquely linked with K_i[2]. With ID_i, R_i can know which vehicle sends the message, and can further verify the authenticity of the message with their shared symmetric key. Therefore, R_i maintains an ID-Key table in its local database, as shown in Figure 3. Vehicles update their anonymous certificates once they get out of the communication range of an RSU. In Figure 3, T_i denotes the time when R_i 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_i and T_i exceeds a pre-defined threshold, the record corresponding to T_i will be deleted from the table.

ID_1	K_1	C_1	T_1
ID_2	K_2	C_2	T_2
...	...	...	...
ID_i	K_i	C_i	T_i

Fig. 3. The ID-Key table

[1]Let p be a large prime, g be a generator of $\mathbb{Z}_p^*$, and $a, b \in \mathbb{Z}_p^*$. Here, to facilitate presentation, we let g^a (or g^b, g^{ab}) denote g^a (or g^b, g^{ab}) mod p.

[2]In order to protect the identity privacy, it is necessary that vehicles do not have unique pseudo IDs. This case will be discussed in Section III.D. For ease of representation, we explain the protocol with the assumption that vehicles are allocated with unique pseudo ID in this subsection

B. Hash Aggregation

Once the vehicle V_i obtains the symmetric key K_i from the RSU R_i, V_i uses K_i to compute the message authentication code $HMAC(ID_i||M_i)$ on $ID_i||M_i$, where ID_i is V_i's pseudo identity assigned by R_i and M_i is the message to be sent. Then, V_i one-hop broadcasts $ID_i||M_i||HMAC(ID_i||M_i)$. Since K_i is only known by R_i in addition to V_i itself, only R_i can verify M_i. Thus, to make other vehicles be able to verify the authenticity of M_i, and at the same time to reduce communication overhead, the RSU R_i is responsible to aggregate multiple authenticated messages in a single packet and to send it out. The detailed process is shown as follows:

1) R_i checks if the time interval between the current time and the time when R_i sent the last message authenticity notification packet is less than a predefined threshold. If so, go to Step 2. Otherwise, go to Step 4.
2) When R_i receives a message, $ID_i||M_i||HMAC(ID_i||M_i)$, sent by the vehicle V_i, R_i first checks whether ID_i is in R_i's ID-Key table. If yes, go to Step 3. Otherwise, go to Step 4.
3) R_i uses ID_i's K_i to verify $HMAC(ID_i||M_i)$. If it is valid, R_i computes $H(ID_i||M_i)$ and then go to Step 1. Otherwise, drop the packet.
4) R_i aggregates all hashes generated at Step 3, i.e., $HAggt = H(ID_1||M_1)||H(ID_2||M_2)||...||H(ID_n||M_n)$, and signs it with its private key SK_{R_i}. Then, R_i one-hop broadcasts $HAggt||\{HAggt\}_{SK_{R_i}}$ to vehicles within its communication range.

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_i in the ID-Key table, the RSU can distinguish the unique sender of a message. Thus, in case that 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 the other vehicles, it only buffers the received messages in its local database without verifying them immediately. The buffered record has the following format: M_i, ID_i, $H(ID_i||M_i)$ (note that $H(ID_i||M_i)$ is computed by the receiver). Once vehicles obtain the signed packet $HAggt||\{HAggt\}_{SK_{R_i}}$ 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_i} to verify the signature $\{HAggt\}_{SK_{R_i}}$. 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 de-aggregate message. For example, V_i checks to see if $H(ID_i||M_i)$ 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 exist in the next $HAggt$ packet. If $H(ID_i||M_i)$ does not appear in two successive aggregate $HAggt$ packets, M_i is regarded as invalid. Here, the reason why $H(ID_i||M_i)$ is double checked is because the RSU might have not aggregated the message M_i yet when V_i receive the first $HAggt$ packet from the RSU.

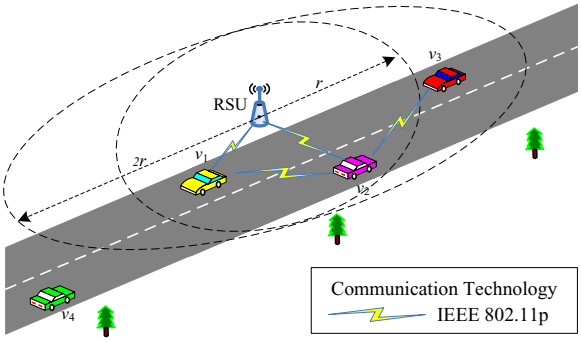

Fig. 4. The communication range of an RSU

In addition, we have to make sure that a vehicle can verify 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 communications between the RSU and a vehicle (or termed RSU to Vehicle Communications (RVC)) has the same distance limit as that of IVC, a vehicle will loss the messages sent by the vehicles that have not been in the eligible distance with the RSU. Figure 4 demonstrates an example. Let the distance limit of RVC be r, and obviously the RSU can communicate with vehicles V_1 and V_2. Since V_3 has 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 can simply require the distance limit for RVC is two times longer than that for IVC. This requirement can be fulfilled since the power taken by RSUs and OBUs is dynamically configurable according to IEEE 802.11p standard.

Note that the power on IVC should not be too large in order not to cover too many vehicles at a time, where the packet collision probability under the CSMA-CD protocol [13] will be exponentially increased with the number of contending vehicles. However, the RVC is not subject to such a problem since the amount of traffic could be an order less than that in IVC for a single vehicle. Thus, we justify here that the power taken by RSUs and OBUs for RVC could be much larger than that by IVC.

D. Enhancement of 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 identity privacy, we employ the concept of *k-anonymity* [14] 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

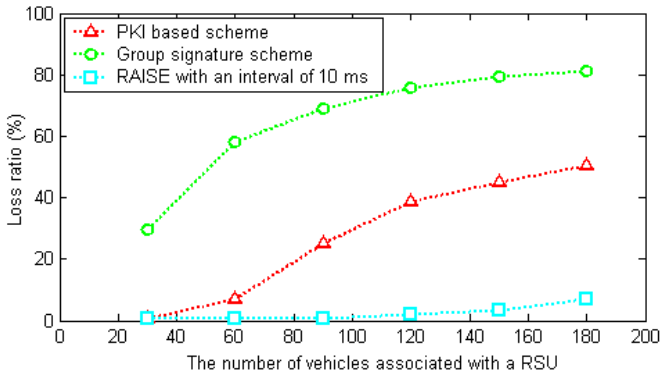

Fig. 5. Average loss ratio vs. Traffic load

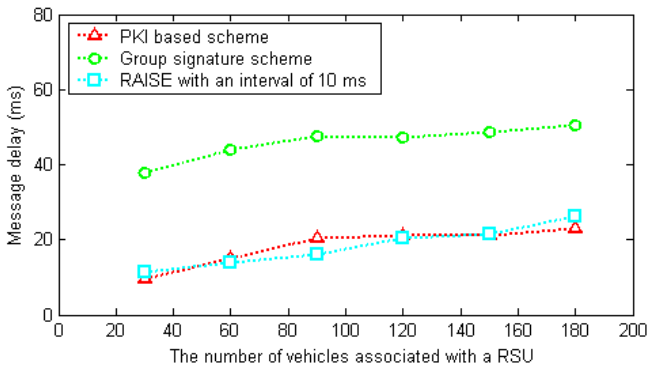

Fig. 6. Average message delay vs. Traffic load

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 the messages of all vehicles are mixed and cannot be distinguished. Note that such a scenario is equivalent to the fact that 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. Each pseudo ID corresponds to k unique symmetric keys. Suppose a vehicle V_i sends $ID_i||M_i||HMAC(M_i)$ to RSU R_i. R_i first finds out k possible keys corresponding to the pseudo identity *ID*. Then, R_i sequently checks whether $HMAC(M_i)$ is equal to $HMAC(M_i)'$ 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 equal 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 local ID-Key table. Being able to find out the anonymous 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 *HMAC* values after R_i has tried all possible k keys, the message is considered as invalid and will be dropped. After this process, R_i can continue the message aggregation process as presented in Section III.C.

With the adoption of *k-anonymity*, the verification process remains the same as before. Vehicles compare whether there is a match between the de-aggregate $H(ID_i||M_i)$ from *HAggt* and the buffered $H(ID_i||M_i)$ value in any record. Here, the cost of comparison computation can be neglected compared with message verification of the PKI-based scheme in [5].

IV. Performance Evaluation

In this section, we use the ns-2 simulator to evaluate the performance of RAISE in terms of the message loss ratio, the message end-to-end delay, and the communication overhead, respectively, compared with the group signature scheme in [6] and the standard PKI-based signature scheme in [11]. We simulated a traffic scenario with a high vehicle density. An RSU is located at an intersection, and 30-200 vehicles can associate with the RSU. The inter-vehicular distance varied from 7.5 m to 15 m to simulate the scenarios with different traffic densities. The distance limit for IVC and RVC is 300 m and 600 m, respectively. Inter-vehicle Messages are sent every 300 ms at each vehicle. IEEE 802.11a is used to simulate the medium access control layer transmission protocol as was done by [5]. The bandwidth of the channel is 6 Mb/s. The group signature verification delay is taken as 11 ms[3] The ECDSA signature verification delay is taken as 3.87 ms[4]. All possible cryptographic time intervals are represented as equal time delays in the simulation.

A. Message Loss Ratio

Average message loss ratio (LR) is defined in Eq. (1), where N represents the total number of vehicles in the simulation. For the group signature and PKI signature schemes, M^i_{mac} represents the total number of messages received by the vehicle i in the medium access control layer, and M^i_{app} represents the total number of messages consumed by the vehicle i in the application layer. For RAISE, M^i_{mac} represents the total number of messages received directly from other vehicles in the medium access control layer; M^i_{app} represents the total number of $H(ID_i||M_i)$s that are sent by the RSU, and are consumed by the application layer. Here, for group signature and PKI signature scheme, we only consider the message loss incurred by delays due to the security protocol rather than the wireless transmission channel. Since RAISE needs two hops communication, we considered the loss caused by wireless

[3]For considerations of efficiency, the curve we used to estimate the short group signature scheme is the MNT curve [16] with embedding degree k=6 and 163-bit prime order p. As in [15], the verification process of the group signature includes 1 non-preprocessable pairing plus 4 non-preprocessable multi-exponentiations in G_1, plus 1 preprocessable multi-exponentiation in G_2, and 1 non-preprocessable multi-exponentiation in G_T. The timings to do these operations are estimated based on the numbers provided by [17] with a 3 GHz Pentium IV system.

[4]The 224 bits ECDSA cryptographic delays are quoted from MIRACL cryptographic lib [18] with the 3GHz Pentium IV system.

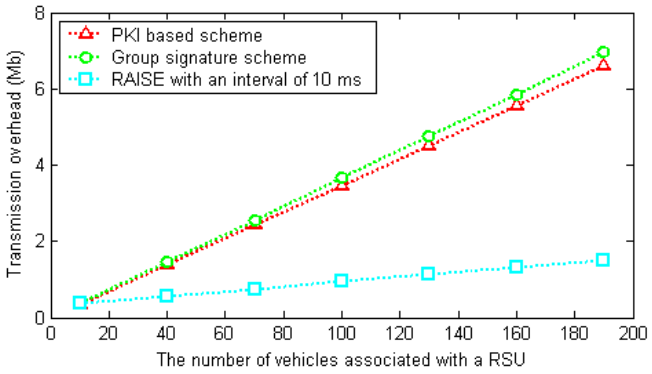

Fig. 7. Communication overhead vs. Traffic load

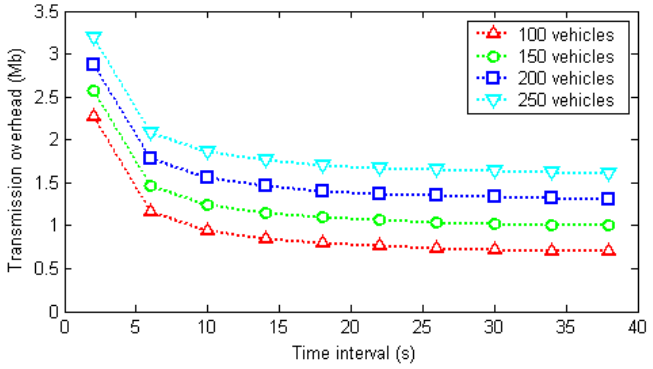

Fig. 8. Communication overhead vs. Time interval

communications between the RSU and vehicles.

$$LR = \frac{1}{N}\sum_{i=1}^{N}(M_{app}^{i}/M_{mac}^{i}) \quad (1)$$

Figure 5 shows the relationship between the message loss ratio and the traffic load. Here the traffic load is represented by the number of vehicles associated with the RSU. The RSU periodically broadcasts an aggregation of $H(ID_i||M_i)$s every 10 ms. Clearly, we can observe that the message loss ratio of the three schemes increases as the traffic load increases. The group signature scheme has the highest loss ratio, and the PKI-based scheme ranks in the middle. Our RAISE scheme, on the other hand, has yielded the lowest loss ratio. Also, from the simulation, we observed that most of the message losses come from the two-hop wireless transmission.

B. Message delay

Average message delay (MD) is defined in Eq. (2), where N represents the total number of vehicles in the simulation, M is the number of messages sent by the vehicle i, and K is the number of adjacent vehicles within the communication range of vehicle i. $T_{recv}^{i,k,m}$ represents the moment that the vehicle k in the application layer receives the mth message from the vehicle i. $T_{send}^{i,k,m}$ represents the moment that the vehicle i in the application layer sends the mth message to the vehicle k.

$$MD = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{MK}\sum_{m=1}^{M}\sum_{k=1}^{K}(T_{recv}^{i,k,m} - T_{send}^{i,k,m}) \quad (2)$$

Figure 6 shows the relationship between the message delay and the traffic load. Again, the group signature scheme has the highest message delay. The reason is due to the high delay used to verify a message signature. The PKI-based scheme and RAISE yield nearly the same message delay. 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 is 10 ms in our simulation, which serves as the main contribution of the message delay. To reduce the message delay, we can decrease this time interval at the expense of increasing the communication overhead and bringing more conflicts to the medium access control layer wireless communications, which will be further discussed in the next subsection.

C. Communication Overhead

First of all, the communication overhead is listed for ECDSA in [11], the group signature scheme in [6], and *HMAC* in RAISE, respectively. With ECDSA, each massage yields 181 bytes as the additional overhead due to cryptographic operations, which includes a certificate and an ECDSA signature, as shown in Figure 2. With the group signature scheme, the additional communication overhead is 184 bytes[5]. With RAISE, the additional communication overhead is 128 bits + 128 bits + (56+2)/n bytes, where the first 128 represents the length of a *HMAC* that is sent by a vehicle, the second 128 represents the length of a $H(ID_i||M_i)$ packet that is sent by an RSU, 56 is the length of an ECDSA signature [11] signed by the RSU, and 2 is the length of a message header as shown in Figure 2. Here, 56+2 is 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.

Figure 7 shows the relationship between the overall communication overhead in 1 minute and the traffic load within an RSU. Clearly, we can observe that RAISE with the time interval of 10 ms has much lower communication overhead than that by the PKI-based signature scheme and the group signature scheme. By further observing Figure 7, we can compute the communication overhead caused by RAISE, which is 24.94% of that of the PKI-based signature scheme and 23.64% of the group signature scheme.

To further illustrate the effect of the time interval on RAISE, Figure 8 shows the relationship between the time interval and the overall communication overhead, caused by 100, 150, 200, and 250 vehicles, respectively in 1 minute. Clearly, as the time interval increases, particularly from 2 ms to 10 ms, the communication overhead decreases sharply. However, when the time interval is up to 10 ms or larger, the time interval has very little effect on the communication overhead. From

[5]As discussed in footnote 2, since p is a 163-bit prime and the elements of G_1 are 164 bits long,the length of a group signature is therefore 184 bytes. The computations can be referred from [15].

Figure 8, we can also observe that the communication overhead increases approximately 0.3 megabytes every time the number of vehicles increases by 50.

V. System analysis

The proposed RAISE scheme meets all the security requirements presented in Section II.D.

Message integrity and source authentication: With RAISE, a vehicle generates a *HMAC* for each launched message. The *HMAC* can only be generated by the vehicle who has the key assigned by the RSU. If an adversary tempers a message, the RSU cannot find a responding validation key that can compute a matching *HMAC* for the message, and therefore the tempered message will be ignored. In addition, for each vehicle, there is an unique key stored in the ID-Key table in the RSU side. If an RSU finds out a key that can verify the *HMAC*, the RSU knows the identity of the message sender, and therefore the source is authenticated.

Low computation overhead and fast verification: As shown in Section IV.A, RAISE has the lowest message loss ratio because it does not have to verify all messages signed by vehicles using public key based verification. In addition, unlike traditional PKI-based protocols where a vehicle has to verify public key certificates of all its neighboring vehicles before verifying the message itself, our scheme only verifies the public key certificate of the RSU once during their initial mutual authentication period, which is enough to verify messages coming from other vehicles. Similarly, as shown in Section IV.B, our scheme has almost the same message end-to-end delay with the traditional PKI-based scheme, which is much lower than the maximum allowable message end-to-end latency as was defined in [2].

Low communication overhead: As shown in the analysis part in Section IV.C, the overhead of our scheme is the lowest. The reason is that RAISE uses HMAC code, which dose not require vehicles to transmit public key certificates.

Identity privacy preservation: Since each vehicle uses a pseudo identity and thus, the real identity can be protected. Further more, as presented in Section III.D, the identity privacy can be protected with *k-anonymity* approach, where multiple vehicles using the same pseudo ID are mixed and unable to be distinguished. To maximize the anonymity, all vehicles could use the same ID. Therefore, an adversary cannot map a pseudo identity to a particular vehicle.

Prevention of internal attack: RAISE can defend against not only the external attacks, but also the internal attacks. Even if a vehicle is compromised and its symmetric secret key shared with an RSU is exposed to an adversary, the adversary cannot trace other vehicle's movement because the adversary cannot distinguish the vehicles that use the same pseudo ID with the compromised vehicle.

VI. Conclusions

In this paper, a novel RSU-aided message authentication scheme, called RAISE, was proposed. With RAISE, RSUs are responsible for verifying the authenticity of the messages sent by vehicles and for notifying the authentication results back to all the associated vehicles. The RAISE scheme is much more advantageous than all the previously reported counterparts because of its less computation and communication overhead. RAISE also protects the privacy of vehicles by adopting the *k-anonymity* approach. Extensive simulation was conducted, which showed that RAISE indeed had the lowest message loss ratio and communication overhead than both the PKI-based and the group signature based schemes without losing the desired security and privacy requirements.

Acknowledgment

The research is financially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

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

[2] U.S. Department of Transportation, National Highway Traffic Safety Adimistrtation, Vehicle Safety Communications Project, Final Repot. Apr. 2006.

[3] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Processings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'07)*, Montreal, Canada, 2007.

[4] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy Magazine*, Vol. 2, No. 3, pp. 49-55, 2004.

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

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications" *IEEE Transaction on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456, 2007.

[7] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Processings of the IEEE International Conference on Computer Communications (INFOCOM'08)*, Phoenix, Arizona, 2008.

[8] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Processings of the IEEE International Conference on Computer Communications (INFOCOM'08)*, Phoenix, Arizona, 2008.

[9] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in *Proncessings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS '07)*, Vancouver, Canada, Aug. 2007.

[10] K. Sampigethaya, Mi. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications (JSAC), Special issue on Vehicular Networks*, Vol. 25, No. 8, pp. 1569-1589, Oct. 2007.

[11] IEEE Standard 1609.2 - IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, July 2006.

[12] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. 22, No, 5 pp. 644-654, 1976.

[13] Institute of Electrical and Electronics Engineers, "Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications," ANSI/IEEE Std 802.3-1985, 1985.

[14] L. Sweeney, "K-ANONYMITY: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness, and Knowledge-based Systems*, Vol. 10, No. 5, pp. 557-570, 2002.

[15] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *Advances in Cryptology* , Vol. 3152 of LNCS, pp. 41-55, Springer-Verlag, 2004.

[16] M. Scott and P. S. L. M. Barreto. Generating More MNT Elliptic Curves. Designs, Codes and Cryptography, Vol. 38, No. 2, pp. 209- 217, Feb. 2006.

[17] M. Scott, Implementing Cryptographic pairings. Pairing 2007, LCNS, Vol. 4575, pp. 177-196, Tokyo, Japan, July 2007.

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