GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications

Xiaodong Lin, *Student Member, IEEE*, Xiaoting Sun, Pin-Han Ho, *Member, IEEE*, and Xuemin Shen, *Senior Member, IEEE*

***Abstract*—In this paper, we first identify some unique design requirements in the aspects of security and privacy preservation for communications between different communication devices in vehicular *ad hoc* networks. We then propose a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques. We demonstrate that the proposed protocol cannot only guarantee the requirements of security and privacy but can also provide the desired traceability of each vehicle in the case where the ID of the message sender has to be revealed by the authority for any dispute event. Extensive simulation is conducted to verify the efficiency, effectiveness, and applicability of the proposed protocol in various application scenarios under different road systems.**

***Index Terms*—Conditional privacy, group signature, identity (ID)-based signature, security, vehicular communications.**

I. Introduction

The advance and wide deployment of wireless-communication technologies have revolutionized our lifestyles by providing the best ever convenience and flexibility in accessing Internet services and various types of personal-communication applications. Recently, car manufactories and telecommunication industries have geared up to equip every car with the technology that allows drivers and passengers from different cars to communicate with each other in order to improve the driving experience. For example, KVH [1] and Microsoft's MSN TV [2] introduced an automotive-vehicle Internet-access system called TracNet, which can bring the Internet services to in-car video screens and turn the entire vehicle into an IEEE 802.11-based Wi-Fi hotspot. The passengers can then use their wireless-enabled laptops to go online. Furthermore, by using those communication devices equipped in vehicles [also known as onboard units (OBUs)], the vehicles can communicate with each other, as well as with roadside units (RSUs) located at the critical points on the road, such as a traffic light at a road intersection. With the OBUs and the RSUs, a self-organized network can be formed, which is called a vehicular *ad hoc* network (VANET). Due to low cost and easy deployment of wireless technology, it is expected that the roadside will be densely covered with a variety of RSUs, like traffic lights, traffic signs, and wireless routers, which will provide wireless access to vehicles on the road. In addition, the RSUs could be connected to the Internet backbone to support diversified services, such as transmission control protocol and real-time multimedia streaming applications. Thus, increasing interest has been raised by both industry and academia on the applications of roadside-to-vehicle communication and inter-vehicle communication (IVC), aiming to improve the driving safety and traffic management while providing drivers and passengers with Internet access at the same time.

The creation of a VANET is significant to traffic management and roadside safety. Unfortunately, a VANET also comes with its own set of challenges, particularly security and privacy. As a special implementation of mobile *ad hoc* networks, a VANET could be subject to many security threats, which will lead to increasing malicious attacks and service abuses. It is obvious that any malicious behavior of users, such as a modification and replay attack on the disseminated messages, could be fatal to other users. Furthermore, conditional privacy preservation must be achieved in the sense that user-related private information, including the driver's name, license plate, speed, position, maker, model, and vehicle identification number (VIN) of the vehicle, and traveling routes, as well as their relationships, has to be protected, while the authorities should be able to reveal the identities of message senders in case of a traffic event dispute, such as a crime/car accident scene investigation, which can be used to look for witnesses. Therefore, it is critical to develop a suite of elaborate and carefully designed security mechanisms to achieve security and conditional privacy preservation in VANETs before they can practically be launched. However, only a very limited number of previously reported studies have tackled the security and privacy issues of VANETs, in spite of its ultimate importance.

In this paper, we are committed to tackling the problem of security assurance and conditional privacy preservation in vehicular communication applications. To the best of our knowledge, this is the first study that deals with the issues of both security and conditional privacy in VANETs through a cryptographic approach. We introduce a secure and privacy-preserving protocol for VANETs by integrating the techniques of **G**roup **S**ignature [7] and **I**dentity (ID)-based **S**ignature [8], called (GSIS). Security problems are divided into the following two aspects: security and privacy preservation between OBUs and OBUs, as well as that between the OBUs and the RSUs, in light of their different design requirements. In the first aspect, group signature is used to secure the

Manuscript received February 15, 2007; revised June 4, 2007 and July 16, 2007. The review of this paper was coordinated by Dr. L. Cai.

X. Lin, 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: xdlin@bbcr.uwaterloo.ca; pinhan@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Sun is with the David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: x7sun@cs.uwaterloo.ca).

Digital Object Identifier 10.1109/TVT.2007.906878

communication between OBUs and OBUs, where messages can securely and anonymously be signed by the senders, while the identities of the senders can be recovered by the authorities. In the second aspect, a signature scheme using ID-based cryptography (IBC) is adopted in the RSUs to digitally sign each message launched by the RSUs to ensure its authenticity, where the signature overhead can greatly be reduced. OBUs that are installed in emergency vehicles will be treated in the same way as the RSUs, since it is unnecessary to protect the privacy of both the RSUs and the OBUs installed in emergency vehicles. Note that, with IBC, any string can serve as a valid public key for an RSU or an emergency vehicle, such as the location of the RSU, the unique number and the code of the RSU, or the emergency vehicle's license plate number [9]. By adopting any publicly known ID of an RSU or an emergency vehicle, such as the location of the RSU or the emergency vehicle's license plate number, as the public key, the certificate management in the VANETs can greatly be simplified as compared with that in the traditional public key infrastructure.

The remainder of this paper is organized as follows. A survey on the related work is conducted in Section II. Preliminaries and background of the proposed security protocol are presented in Section III. In Section IV, the proposed security protocol is presented along with the enabling signaling initiations and transactions in detail. Section V evaluates the performance of the proposed protocol through extensive simulation. Finally, we conclude this paper in Section VI.

II. Related Work

The IEEE 802.11p task group is working on the Dedicated Short Range Communications (DSRC) Standard, which aims to enhance the 802.11 protocol to support wireless data communications for vehicles and roadside infrastructure [4]. Extensive studies have been reported on the IVC; however, most of them have focused on either the feasibility of a specific application scenario or the medium access control (MAC) layer performance analysis or various routing solutions [11]–[15]. Very limited efforts have been made on the issues of security and privacy preservation [3], [4], [16], [17].

The studies in [16] and [17] discussed the general security issues, such as the attack models, security requirements, and properties of the IVC systems, instead of providing any solution to ensure the identified security and privacy preservation requirements. In [3], a security protocol was introduced by way of creating a large number of anonymous certificates in vehicles. With a pool of around 43 800 certificates, each vehicle randomly chooses one of the available certificates for signing the message at one time in order to meet the driver's privacy requirement. To achieve traceability, a unique electronic ID is assigned to each vehicle by which the police and authorities can verify the ID of the owner in case of any dispute. Although this scheme can effectively meet the conditional privacy requirement, it is far from efficient and can hardly become a scalable and reliable approach, because the ID management authority has to keep all the anonymous certificates for each vehicle in the administrative region, which could be a province or a country. Once a malicious message is detected, the authority has to exhaustedly search in a very huge database (probably 43 800 certificates * millions of cars) to find the ID related to the compromised anonymous public key.

The Vehicle Safety Communications Project was to evaluate the feasibility of using the DSRC Standard to support the roadside safety related applications [4]. In [4], a solution was proposed to take advantage of a list of short-lived anonymous certificates to keep the privacy of the drivers, where the short-lived certificates are discarded right after being used. The scheme can provide a higher security assurance than that in [3], because the certificates are blindly signed by the certificate authority (CA) in order to deal with the "insider" attack. A linkage marker is used for the escrow authorities to connect together the blindly signed anonymous certificates with a single vehicle. All compromised but not expired vehicles have to be revoked so as for all the certificates belonging to those vehicles, which is done simply by updating the certificate revocation list (CRL). The disadvantage of this scheme is that the CRL may grow quickly, which may not only have a large CRL size but also take a long time to look through the whole CRL to see if a certificate is still valid or not. The CRL size, which is referred to as the memory space, means the amount of memory required by a CRL.

Different from the above reported schemes, we propose a secure and privacy-preserving protocol, which cannot only guarantee the requirements of security and privacy but can also provide the desired traceability of each vehicle in the case where the ID of the message sender has to be revealed by the authority for any dispute event. Furthermore, the size of the CRL is considerably reduced. Thus, the proposed protocol can practically be launched for enabling the application scenario of VANETs.

III. Preliminaries and Background

A. Threat Model

There are several possible attacks in VANETs, which are listed as follows.

1) *Bogus information attack:* The adversary may send fake messages to meet a specific purpose. For example, one may send a fake traffic jam message to the others such that it can manipulate to get a better traffic condition.
2) *Unauthorized preemption attack:* In many places, an RSU, particularly a traffic light, can be controlled to provide special traffic priority for emergency vehicles, such as ambulance, police, and fire vehicles. Similar to a bogus information attack, the adversary may illegally interrupt traffic lights by manipulating the traffic light preemptive system in order to get a better traffic condition [5].
3) *Message replay attack:* The adversary replays the valid messages sent some time before in order to disturb the traffic.
4) *Message modification attack:* The message is altered during or after transmission. The adversary may wish to change the source or content of the message in terms of the position or time information that had been sent and saved in its device to escape from the consequence of a criminal/car accident event.

5) *Impersonation attack:* The adversary may pretend to be another vehicle or even an RSU to fool the others.
6) *RSU replication attack:* Due to the fact that there exist a large number of RSUs, cost considerations prevent the RSUs from having sufficient protection from malicious attacks, which results in an RSU compromise. Afterward, an adversary can relocate the captured RSU to launch any malicious attack, such as broadcasting fake traffic information.
7) *Denial-of-service (DoS) attack:* The adversary sends irrelevant bulk messages to take up the channel and consume the computational resources of the other nodes, such as RF interference or jamming or layer-two-packet flooding [6].
8) *Movement tracking:* Since wireless communication is on an openly shared medium, an adversary can easily eavesdrop on any traffic. After the adversary intercepts a significant amount of messages in a certain region, the adversary may trace a vehicle in terms of its physical position and moving patterns simply through information analysis.

Since DoS attack in wireless communication networks has extensively been investigated in the past [6], [22]–[25], in this paper, we will focus on the security and privacy issues which are not related to the DoS attack.

B. Desired Requirements

To countermeasure and mitigate the potential threats in the aforementioned security threats/attack models, a well-developed security protocol should meet the following requirements.

1) *Data origin authentication and integrity:* All the messages should be unaltered in the delivery and can be authenticated by the receiver no matter how the messages are sent by an RSU or an OBU.
2) *Anonymous user authentication:* Anonymous user authentication is the process of attempting to verify that a user is authentic and legitimate but does not reveal the real ID of the user.
3) *Vehicle anonymity:* The ID of a vehicle should be transparent to any normal message receiver to support the sender anonymity while providing their position information.
4) *RSU ID exposure:* The RSUs or any other roadside infrastructure are not subject to any privacy issue; instead, they should evidently present their identities, including the physical locations and the services that can be provided.
5) *Prevention of RSU replication:* It is very likely to happen that an RSU is compromised and/or relocated to any other place by an adversary, by which the adversary can launch various attacks through the compromised/relocated RSU, possibly causing the whole VANET into disruption. Effective countermeasures to the RSU replication attack must be provided to maintain the security of VANETs.
6) *Vehicle ID traceability:* The authorities should be able to reveal the real identities of the message senders in order to guard the truth when there is any dispute.
7) *Efficiency:* The communication overhead of each packet and processing latency at each vehicle must be as small as possible.

C. Bilinear Pairing

Bilinear pairing has brought tremendous interests and attentions from the security community, since the technique has been identified to be able to solve some problems that were previously well recognized as unsolvable, such as IBC [9]. Another advantage in considering pairing-based schemes is that they can save communication bandwidth as compared with the traditional schemes, such as RSA and ElGamal, due to a smaller signature overhead.

As a fundamental enabling technique of the proposed protocol, the bilinear pairing and the underlying problems are briefly introduced as follows.

Definition 1 (Admissible Bilinear Map [9]): Let $(\mathbb{G}_1, \times)$, $(\mathbb{G}_2, \times)$, and $(\mathbb{G}_T, \times)$ be three groups of the same prime order q and P_1 and P_2 be two generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. An admissible bilinear map is a map $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ satisfying the following properties.

1) *Bilinearity:* $\forall (U, V) \in \mathbb{G}_1 \times \mathbb{G}_2$, and $\forall\ a,\ b \in \mathbb{Z}_q^*$; $\hat{e}(U^a, V^b) = \hat{e}(U, V)^{ab}$.
2) *Nondegeneracy:* $\hat{e}(P_1, P_2) \neq 1_{\mathbb{G}_T}$.
3) *Computability:* There exists an efficient algorithm to compute $\hat{e}(U, V)$, for all $(U, V) \in \mathbb{G}_1 \times \mathbb{G}_2$.

Definition 2 (Bilinear Parameter Generator [9]): A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input and outputs a heptuple $(q, P_1, \mathbb{G}_1, P_2, \mathbb{G}_2, \mathbb{G}_T, \hat{e})$, satisfying the following conditions: q is a prime with $2^k < q < 2^{k+1}$; the groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are all of order q; P_1 and P_2 generates $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively; and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an admissible bilinear map.

For most cryptographic applications, an efficiently computable isomorphism $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ is essentially required. When $\mathbb{G}_1 = \mathbb{G}_2$ and $P_1 = P_2$, ψ can be the identity map. Therefore, for simplicity, we consider $\mathbb{G}_1 = \mathbb{G}_2$. Then, with k as the input security parameter, the bilinear parameter generator $\mathcal{G}en(k)$ generates a quintuple $(q, P_1, \mathbb{G}_1, \mathbb{G}_T, \hat{e})$, where $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Next, we state the following three underlying problems, which serve as a basis of our proposed protocol.

1) *Computational Diffie–Hellman (CDH) problem:* For unknown $a,\ b \in \mathbb{Z}_q^*$, given P_1^a, $P_1^b \in \mathbb{G}_1$, compute for $P_1^{ab} \in \mathbb{G}_1$.
2) *Decisional Diffie–Hellman (DDH) problem:* For unknown $a,\ b,\ c \in \mathbb{Z}_q^*$, given P_1^a, P_1^b, $P_1^c \in \mathbb{G}_1$, decide whether $ab = c \bmod q$. It is known that DDH in $\mathbb{G}_1$ is easy and can be solved in polynomial time by checking $\hat{e}(P_1^a, P_1^b) \overset{?}{=} \hat{e}(P_1^c, P_1)$.
3) *Bilinear Diffie–Hellman (BDH) problem:* For unknown $a,\ b,\ c \in \mathbb{Z}_q^*$, given P_1^a, P_1^b, $P_1^c \in \mathbb{G}_1$, compute for $\hat{e}(P_1, P_1)^{abc} \in \mathbb{G}_T$.

IV. Proposed Secure and Privacy-Preserving Protocol

A. Problem Formulation

Each vehicle is equipped with a reliable positioning device (e.g., a Global Positioning System) and can get accurate time information. To explore the highest security level, we assume a very critical scenario where the adversaries can intercept any message that they desire in the VANET. Furthermore, based on the fact that keeping the confidentiality of each message in IVC applications is not necessary (since everybody has the right to know the content of the message), we choose to use the digital signature technique to sign every message sent by the OBUs and the RSUs. Therefore, any receiver can verify the received messages and make sure of the integrity and authenticity of the messages with the nonrepudiation property. The security design is divided into the following two categories: the security mechanisms between two OBUs, as well as those between an RSU and an OBU. With this, the security solutions are considered separately in these two categories due to the different design requirements, which are discussed as follows.

1) Communications Between OBUs[1]*:* The main challenge of the communications between OBUs lies in the contradiction between the design requirements for vehicle anonymity from regular users and for traceability by the authorities.[2] Because of this, the traditional public key encryption scheme is not suitable in signing the safety messages, because the ID information is included in the public key certificates. One solution is to use a list of anonymous certificates for message authentication, where the relationships of these anonymous certificates with their owners are kept in the Transportation Regulation Center (TRC), such that the real ID of a message sender can be traced. This method can achieve the conditional privacy in a straightforward manner at the expense of possibly huge efforts paid to maintain and manage a global certificate list by the authorities. It could also be a time-consuming task in tracing back to the real ID of a vehicle when there is any dispute. Thus, we propose a security protocol by using the group signature scheme [7] to sign the messages sent by the vehicles. The main feature of the group signature scheme is that it provides anonymity of the signers. A verifier can judge whether the signer belongs to a group without knowing who the signer is in the group. However, in an exceptional situation, the CA, which serves as a group manager, can reveal the unique ID of the signature's originator. Therefore, the group signature technique brings up a better way to meet the anonymity and traceability requirements rather than storing all the certificates in the terminal devices. The group signature technique also reduces the workload of the public key and certificate path verification operations. Besides, the group signature scheme can satisfy other basic security requirements, such as message integrity and data origin authentication.

A secure group signature must be correct, anonymous, and unlinkable while also being traceable under some circumstances (more details of these properties can be found in [28] and [38]). In addition to the aforementioned properties, some other features are also preferred in the IVC application, which are listed as follows.

1) *Role separation:* In the real world, it is preferred if the role of the group manager can be divided into a membership manager (MM) and a tracing manager (TM). The TRC can serve as the MM for assigning private keys and group public keys to the vehicles, whereas the law authorities could serve as a TM for possibly revealing the real IDs of the message senders if necessary.
2) *Group membership revocation:* It is indispensable in the IVC system to have the ability to selectively revoke the group membership of a compromised vehicle either by updating keys or releasing revocation lists (RLs).
3) *High efficiency:* The computational cost and the length of the signatures should be small in order to meet the stringent communication requirement in the IVC system.

Dozens of group signature schemes have been proposed since 1991. However, some proposed group signature schemes are questionable in the security and anonymity assurance. For instance, many ID-based group signature schemes, such as in [28]–[31], failed to meet the unlinkability requirement. In addition, some schemes, such as [28] and [32], were proven to be forgeable and traceable. In addition, most of the reported group signature schemes take very long and are nonrevocable signatures, and/or the role of the group manager is indivisible, which fails to meet the requirements in the application scenario of interest. Thus, after a thorough evaluation, we choose the short group signature scheme that was introduced by Boneh *et al.* [34], which is secure and considered to be best suited to the IVC application.

2) Communications Between RSU and OBU[3]*:* The main feature with respect to the security requirements between RSUs and OBUs is that the messages sent by RSUs are not subject to the privacy requirement. Therefore, we propose to use the identifier string of each RSU as the public key to sign the messages launched from the RSUs. For OBUs installed in emergency vehicles, the license plate numbers are used as their public keys. With the ID-based signature scheme, the workload of certificate management can significantly be reduced, and the public key update and revocation operations can largely be simplified. Among all the known ID-based signature schemes, the provably secure ID-based signature scheme given in [27] is adopted in this paper, since the length of the signature is significantly reduced due to the use of bilinear pairing. The scheme is also among the most efficient ones in terms of the complexity of verification operation, which takes only one-pairing computation.

For ease of presentation, the notations throughout this paper in describing our security protocol are listed in Table I.

[1] It refers to communications launched from the OBUs.

[2] In this paper, we term the coexisted privacy and identity traceability as conditional privacy.

[3] It refers to communications launched from the RSUs.

TABLE I
NOTATIONS AND DESCRIPTIONS

Notations	Descriptions
TRC	**T**ransportation **R**egulation **C**enter.
MM	**M**embership **M**anager.
TM	**T**racing **M**anager.
$gpk = (g_1, g_2, g, w)$	Group public key.
$gmsk_t = (\xi_1, \xi_2)$	The TM's private key.
$gmsk_m = \gamma$	The MM's private key.
$gsk[i]$	Vehicle i's private key.
$\gamma \overset{R}{\leftarrow} \mathbb{Z}$	randomly select a number γ from set $\mathbb{Z}$
RL	**R**evocation **L**ist
$1_{\mathbb{G}_1}$, $1_{\mathbb{G}_2}$ and $1_{\mathbb{G}_T}$	The identity element of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$, respectively

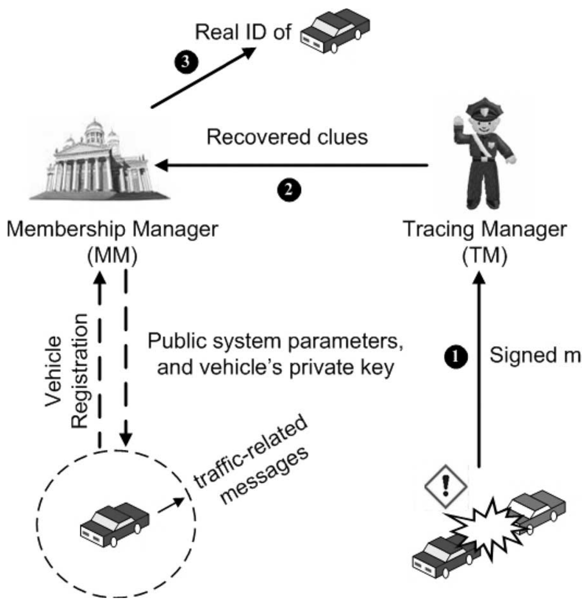


Fig. 1. Secure communication system between OBUs.

B. System Setup

For the considered system, there are three types of network entities: the TM, the MM, and the mobile OBUs equipped on the moving vehicles,[4] and their relationship is shown in Fig. 1. All vehicles need to be registered with the MM and preloaded with public system parameters and their own private key before the vehicles can join the VANET. When the vehicles are on the road, they regularly broadcast routine traffic-related messages, such as position, current time, direction, speed, brake status, steering angle, acceleration/deceleration, traffic conditions, traffic events, etc., to help drivers get a better awareness of what is going on in their driving environment and take early actions to respond to an abnormal situation [4]. Whenever there is a situation where the involved vehicles' IDs need to be revealed, for example, police officers looking for someone who may be able to provide valuable information about an accident, the evidence, such as signed traffic messages, can be submitted to the TM, who is responsible for the authorization for revealing the real IDs of the wanted vehicles. The TM then forwards recovered clues and evidences to the MM, who finally finds the real IDs from its membership database.

TABLE II
MESSAGE FORMAT FOR OBU

Group ID	Message ID	Payload	Timestamp	Signature	TTL
2 bytes	2 bytes	100 bytes	4 bytes	192 bytes	1 byte

First, the law authority, which serves as a TM, generates the required bilinear groups as the system parameters [9], which are described as follows.

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ denote two multiplicative cyclic groups with a generator g_1 and g_2 of the same prime order p, respectively. Let ψ be a computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$, and $\hat{e}$ be a computable map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ with the following properties. 1) Bilinearity: For all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$, and $a, b \in \mathbb{Z}_p^*$, $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$. 2) Nondegeneracy: $\hat{e}(g_1, g_2) = g \neq 1_{\mathbb{G}_T}$.

Furthermore, we assume that the strong Diffie–Hellman (SDH) assumption holds on $(\mathbb{G}_1, \mathbb{G}_2)$ and that the linear Diffie–Hellman assumption holds on $\mathbb{G}_1$ [33].

Then, the TM randomly selects two elements $h \overset{R}{\leftarrow} \mathbb{G}_1 \setminus \{1_{\mathbb{G}_1}\}$ and $h_0 \overset{R}{\leftarrow} \mathbb{G}_2 \setminus \{1_{\mathbb{G}_2}\}$, along with two random numbers ξ_1 and $\xi_2 \overset{R}{\leftarrow} \mathbb{Z}_p^*$, and sets $u, v \in \mathbb{G}_1$ such that $u^{\xi_1} = v^{\xi_2} = h$ and $h_1, h_2 \in \mathbb{G}_2$ such that $h_1 = h_0^{\xi_1}$, $h_2 = h_0^{\xi_2}$. In the end, the TM keeps the TM's private key $\text{gmsk}_t = (\xi_1, \xi_2)$ secretly and sends the system parameters

$$(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, g, p, \psi, \hat{e}, u, v, h, h_0, h_1, h_2)$$

to the TRC, which works as the MM.

Finally, the TRC randomly selects $\gamma \overset{R}{\leftarrow} \mathbb{Z}_p^*$ as the MM's private key gmsk_m and sets $w = P_{\text{pub}} = g_2^{\gamma}$ as a system parameter. The TRC also chooses two secure cryptographic hash functions $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ and $H_1 : \{0,1\}^* \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$. In the end, the TRC publishes the system parameters param and group public key gpk, as follows:

$$\begin{cases} \text{param} = \begin{pmatrix} \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, g, p, \psi, \hat{e} \\ H, H_1, P_{\text{pub}}, u, v, h, h_0, h_1, h_2 \end{pmatrix} \\ \text{gpk} = (g_1, g_2, g, w). \end{cases}$$

In such a way, the security system is initialized.

C. Security Protocol Between OBUs

1) Message Format: The format of the safety messages sent by the OBU is defined in Table II, where Group ID is used to identify to which group the vehicle belongs. The message payload may include the information on the vehicle's position, message sending time, direction, speed, acceleration/deceleration, traffic events, etc. According to [4], the payload of a message is 100 B. A timestamp is used to prevent the message replay attack. The last second field is the

[4] For simplicity, we assume that a vehicle is equipped with an OBU. Without loss of generality, we use the terms "vehicle" and "OBU" interchangeably in this paper.

OBU's signature of the first four parts of the message. The last field is time to live (TTL), which records a timer that controls how long the message is allowed to remain in the VANETs. In this case, the situation in which a VANET becomes swamped by messages can be avoided.

2) Security Protocol for OBU and OBU Communication: The proposed security protocol is an elaboration of short group signature scheme [34] in order to support the proposed hybrid membership revocation scheme, which will be detailed in the following. Specifically, the proposed security protocol contains five phases, which are described in the following paragraphs.

1) *Membership registration:* During the vehicle's registration process, the MM generates a tuple (A_i, x_i) for each vehicle i with identity ID_i, which is the vehicle's private key $\mathrm{gsk}[i]$, which is shown as follows. By using γ, the MM first computes

$$x_i \leftarrow H(\gamma, \mathrm{ID}_i) \in \mathbb{Z}_p^*$$

and then sets $A_i \leftarrow g_1^{1/(\gamma+x_i)} \in \mathbb{G}_1$. In the end, the MM stores the pair (A_i, ID_i) in its record, which completes the membership registration.

Note that, since the value x_i can be computed by γ and ID_i, the MM does not need to store x_i in order to save storage space.

2) *Signing:* Given message M, vehicle i signs on M before sending it out. With the group public key gpk and the private key pair (A_i, x_i), the signing procedure is composed of the following computations.

a) Select the exponents $\alpha, \beta \xleftarrow{R} \mathbb{Z}_p^*$.

b) Compute an encryption of A_i and (T_1, T_2, T_3), where

$$T_1 \leftarrow u^\alpha, \quad T_2 \leftarrow v^\beta, \quad T_3 \leftarrow A_i h^{\alpha+\beta}. \qquad (1)$$

c) Compute $\delta_1 \leftarrow x_i\alpha$ and $\delta_2 \leftarrow x_i\beta$.

d) Randomly pickup blinding values $r_\alpha, r_\beta, r_{x_i}, r_{\delta_1}$, and r_{δ_2} from $\mathbb{Z}_p^*$.

e) Compute R_1, R_2, R_3, R_4, and R_5 as follows:

$$\begin{cases} R_1 \leftarrow u^{r_\alpha} \\ R_2 \leftarrow v^{r_\beta} \\ R_3 \leftarrow \hat{e}(T_3, g_2)^{r_{x_i}} \cdot \hat{e}(h, w)^{-r_\alpha - r_\beta} \cdot \hat{e}(h, g_2)^{-r_{\delta_1} - r_{\delta_2}} \\ R_4 \leftarrow T_1^{r_{x_i}} \cdot u^{-r_{\delta_1}} \\ R_5 \leftarrow T_2^{r_{x_i}} \cdot v^{-r_{\delta_2}}. \end{cases}$$

f) Obtain the challenger c using the above values and M

$$c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in \mathbb{Z}_p^*.$$

g) Compute s_α, s_β, s_{x_i}, s_{δ_1}, and s_{δ_2}, where

$$\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_{x_i} = r_{x_i} + cx_i \\ s_{\delta_1} = r_{\delta_1} + c\delta_1 \\ s_{\delta_2} = r_{\delta_2} + c\delta_2. \end{cases} \qquad (2)$$

h) Finally, combine the values of (1) and (2) to form the message signature σ

$$\sigma \leftarrow (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2}).$$

i) Formulate the message according to Table II and send it out.

3) *Verification:* Once a message is received, the receiver first checks if the time information in the message payload is in the allowable time window. If so, the receiving vehicle will perform signature verification by first recomputing the challenger $\tilde{c}$, followed by reconstructing ($\tilde{R}_1$, $\tilde{R}_2$, $\tilde{R}_3$, $\tilde{R}_4$, and $\tilde{R}_5$), according to the following formula:

$$\begin{cases} \tilde{R}_1 \leftarrow u^{s_\alpha}/T_1^c \\ \tilde{R}_2 \leftarrow v^{s_\beta}/T_2^c \\ \tilde{R}_3 \leftarrow \hat{e}(T_3, g_2)^{s_{x_i}} \cdot \hat{e}(h, w)^{-s_\alpha - s_\beta} \\ \qquad \cdot \hat{e}(h, g_2)^{-s_{\delta_1} - s_{\delta_2}} \cdot \left(\hat{e}(T_3, w)/\hat{e}(g_1, g_2)\right)^c \\ \tilde{R}_4 \leftarrow T_1^{s_{x_i}} \cdot u^{-s_{\delta_1}} \\ \tilde{R}_5 \leftarrow T_2^{s_{x_i}} \cdot v^{-s_{\delta_2}}. \end{cases}$$

Then, $\tilde{c}$ is recomputed from

$$\tilde{c} = H(M, T_1, T_2, T_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5).$$

The receiver finally checks if this value is the same as c in signature σ. If so, the receiver considers the message to be valid and unaltered from a trusted group member. If not, the receiver neglects the message.

4) *Membership traceability:* A membership tracing operation is performed when solving a dispute, where the real ID of the signature generator is desired. The TM first checks the validity of the signature and then computes A_i by using the following equation:

$$A_i \leftarrow T_3 / \left(T_1^{\xi_1} \cdot T_2^{\xi_2}\right).$$

Once the MM gets element A_i from the TM, it can lookup the record (A_i, ID_i) to find the corresponding identity ID_i.

5) *Membership revocation:* Once a vehicle is found compromised, the vehicle will be excluded from the system. Currently, there are two approaches of revoking a compromised vehicle. One is through updating the group public key and private key at all unrevoked vehicles. Given the released private key pairs of the revoked vehicles in an RL, unrevoked vehicles can locally update their private key pair $\mathrm{gsk}[i]$ and the group public key gpk, whereas those revoked vehicles cannot update their keying materials [34]. Obviously, this scheme may introduce a significant amount of overhead since it is needed to change the group public and private keys of each vehicle from time to time. The other revoking mechanism is similar to the traditional CRL-based revocation scheme, called verifier-local revocation (VLR) [35]–[37], by which only verifiers are involved in the revocation check-up operation. The VLR scheme is efficient when there are only a few revoked vehicles. However, since the signature verification time grows linearly

with the number of revoked vehicles, the vehicle revocation verification procedure becomes very time-consuming and inefficient when a large number of revoked vehicles exist in the RL. Therefore, to initiate a graceful tradeoff, we propose a hybrid membership revocation mechanism. The basic idea of the proposed mechanism is that, when the number of revoked vehicles in the RL (denoted as $|\mathrm{RL}|$) is less than some predefined threshold T_τ, the VLR mechanism is adopted; otherwise, the first approach through updating the corresponding public keys and private key pairs is employed. The proposed mechanism is further described as follows:

Case 1) When $|\mathrm{RL}| < T_\tau$, the MM publishes the revocation list $\mathrm{RL} = \{A_1, \ldots, A_b\}$, where $b < T_\tau$. For a given group signature σ, any verifier first executes the signature verification operation and then executes the revocation check, which is shown in Algorithm 1 as follows:

```
**Algorithm 1 (Revocation Verification Algorithm)**
**Data**: **Input** (param, RL, $\sigma$)
**Result**: **Output** valid or invalid
**for** $i \leftarrow 1$ **to** $|\mathrm{RL}|$ **do**
    get one $A_i$ from RL;
    **if** $\hat{e}(T_3/A_i, h_0) = \hat{e}(T_1, h_1)\hat{e}(T_2, h_2)$ **then**
        **return** invalid;
    **end**
**end**
**return** valid;
```

where param is ($\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, g_1, g_2, g, p, ψ, $\hat{e}$, H, H_1, P_{pub}, u, v, h, h_0, h_1, h_2). If the returned value is valid and no element of RL is encoded in (T_1, T_2, T_3) of σ, the signer of the group signature σ has not been revoked. However, if the returned value is invalid, then there exists some A_i being encoded in (T_1, T_2, T_3), which can be checked by $\hat{e}(T_3/A_i, h_0) = \hat{e}(T_1, h_1)\hat{e}(T_2, h_2)$, since

$$\begin{aligned}\hat{e}(T_3/A_i, h_0) &= \hat{e}\left(A_i h^{\alpha+\beta}/A_i, h_0\right)\\ &= \hat{e}\left(h^{\alpha+\beta}, h_0\right)\\ &= \hat{e}\left(h^{\alpha}, h_0\right)\hat{e}\left(h^{\beta}, h_0\right)\\ &= \hat{e}\left(u^{\alpha\xi_1}, h_0\right)\hat{e}\left(v^{\beta\xi_2}, h_0\right)\\ &= \hat{e}\left(u^{\alpha}, h_0^{\xi_1}\right)\hat{e}\left(v^{\beta}, h_0^{\xi_2}\right)\\ &= \hat{e}\left(T_1, h_1\right)\hat{e}\left(T_2, h_2\right).\end{aligned}$$

Case 2) When $|\mathrm{RL}| \geq T_\tau$, the MM sends all signers and verifiers in the system the revocation list $\mathrm{RL} = \{(A_1^*, x_1), \ldots, (A_b^*, x_b)\}$, where $b \geq T_\tau$. For each private key (A_i^*, x_i), $x_i \leftarrow H(\gamma, \mathrm{ID}_i) \in \mathbb{Z}_p^*$, and $A_i^* \leftarrow g_2^{1/(\gamma+x_i)} \in \mathbb{G}_2$. It is worth noting that $A_i = \psi(A_i^*)$.

After receiving the revocation list RL, group public key gpk can easily be updated. The following lemma demonstrates how to use a given group public key and all the revoked private keys to construct a new group public key.

Lemma 1: Given group key $\mathrm{gpk} = (g_1, g_2, g, w)$ and all revoked private keys $\{(A_1^*, x_1), \ldots, (A_b^*, x_b)\} \in \mathrm{RL}$, the new group public key can be constructed as

$$\mathrm{gpk}_{\mathrm{new}} = (\hat{g}_1, \hat{g}_2, \hat{g}, \hat{w})$$

where $\hat{g}_1 = g_1^{1/y}$, $\hat{g}_2 = g_2^{1/y}$, $\hat{g} = \hat{e}(\hat{g}_1, \hat{g}_2)$, and $\hat{w} = \hat{g}_2^{\gamma}$, with $y = \prod_{i=1}^{b}(\gamma + x_i) \in \mathbb{Z}_p^*$.

Proof: See Appendix A. ■

Next, we show how an unrevoked vehicle updates its private key, $(A = g_1^{1/(\gamma+x_0)}, x_0)$, for a new one denoted as $(\hat{A}, x_0)$, where $\hat{A} = A^{1/y} \in \mathbb{G}_1$.

Lemma 2: Given all revoked private keys $\{(A_1^*, x_1), \ldots, (A_b^*, x_b)\} \in \mathrm{RL}$, the new private key for an unrevoked vehicle $i = 0$ can be constructed as

$$(\hat{A}, x_0)$$

where $x_0 = H(\gamma, \mathrm{ID}_0) \in \mathbb{Z}_p^*$, $\hat{A} = A^{1/y} \in \mathbb{G}_1$, with $y = \prod_{i=1}^{b}(\gamma + x_i) \in \mathbb{Z}_p^*$.

Proof: See Appendix B. ■

3) Message Length: The length of the OBU message can be expressed as

$$\begin{aligned}L_{\mathrm{msg\_OBU}} = L_{\mathrm{groupID}} + L_{\mathrm{msgID}} + L_{\mathrm{payload}}\\ + L_{\mathrm{timestamp}} + L_{\mathrm{sig}} + L_{\mathrm{TTL}}.\end{aligned}$$

We have p as a prime that is 170 b long [34]. Each element in $\mathbb{G}_1$ is 171 b long, and $L_{\mathrm{sig}} = 192$ B long. Thus, $L_{\mathrm{msg\_OBU}} = 2 + 2 + 100 + 4 + 192 + 1 = 301$ B.

4) Security Analysis: Using group signatures allows any member in the group to anonymously sign an arbitrary number of messages on behalf of the group. The security requirements of a group signature scheme include correctness, unforgeability, anonymity, unlinkability, traceability, and revocation [38], which will be discussed as follows.

1) *Correctness:* With the proposed security protocol, a group signature σ generated by a valid group member can surely be identified by the aforementioned verification procedure.
2) *Unforgeability:* Only a valid group member can sign a message on behalf of the group. A valid group signature cannot be forged; otherwise, the SDH assumption will be in contradiction.
3) *Anonymity:* Given a valid group signature σ of some messages, it is computationally difficult to identify the actual signer by every one but the group manager. Due to the linear Diffie–Hellman assumption, the interactive protocol underlying the group signature scheme is zero-knowledge, such that no information is revealed by σ.
4) *Unlinkability:* According to the verification procedure, it is computationally hard to decide whether two valid signatures of different groups are computed by the same group member.

TABLE III
MESSAGE FORMAT FOR RSU

Type ID	Message ID	Payload	Timestamp	Signature	ID	TTL
2 bytes	2 bytes	100 bytes	4 bytes	43 bytes	40 bytes	1 byte

TABLE IV
FORMAT OF RSU'S ID

Serial No	Physical Location Information	Type ID

5) *Traceability:* The group manager can always create a valid signature and identify the actual signer by the membership recovery procedure. Let the group signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2})$ be valid. The group manager can thus first derive

$$A_i \leftarrow T_3 / \left(T_1^{\xi_1} \cdot T_2^{\xi_2}\right)$$

by which the signer's ID can be traced.

6) *Revocation:* Membership revocation can be fulfilled by the aforementioned two revocation schemes.

We refer to [34] for a more comprehensive description of security analysis.

D. Security Protocol Between RSUs and OBUs

1) Message Format: We define the format of safety messages between RSUs and OBUs, as shown in Table III.

The first four fields are signed by the RSU, by which the "signature" field can be derived. The "ID" is 40 B long and serves as the public key of the sender. Note that the ID may also include the name of the RSU, the authorized geographical region to operate, and the authorized message type. As aforementioned, OBUs installed in emergency vehicles are treated the same way as RSUs. Thus, the ID can also be the emergency vehicle's license plate number; the types of emergency vehicles, for example, such as police, fire, or emergency medical services; and the name of municipality where emergency services are provided. The last field is TTL, which records a timer that controls how long the message is allowed to remain in VANETs. In this case, the situation in which a VANET becomes swamped by messages can be avoided. Without loss of generality, we use RSU as an example to illustrate the proposed protocol. The length of the signature will be discussed later.

2) Security Protocol for RSU and OBU Communication: The proposed security protocol between RSU and OBU contains the following three phases.

1) *Private key generation:* A unique identifier string is obtained for each RSU as its ID according to its property, whose format is shown in Table IV, where the first field records a unique serial number, the second field records its physical location information, and the third field indicates the attribute of the message, such as a traffic-sign-related message and a warning message. The TRC computes the private key for each RSU by

$$S_{\mathrm{ID}_i} \leftarrow g_1^{1/(\gamma + H(\mathrm{ID}_i))}$$

and sends it to each RSU through a secure channel.

2) *Signing:* Before sending each safety message M, RSU signs the message M by first picking up a random value $x \xleftarrow{R} \mathbb{Z}_p^*$ and computing

$$r \leftarrow g^x \in \mathbb{G}_T.$$

With r, we can set

$$h_\sigma \leftarrow H_1(M, r) \in \mathbb{Z}_p^*$$

and compute

$$S_\sigma \leftarrow S_{\mathrm{ID}_i}^{x + h_\sigma} \in \mathbb{G}_1.$$

The signature σ is nothing but the pair $(h_\sigma, S_\sigma) \in \mathbb{Z}_p^* \times \mathbb{G}_1$. Finally, the message can be formatted according to Table III and can then be sent.

3) *Verification:* Any vehicle receiving a message from an RSU will first guarantee that the sender is working under the authorized domain. The vehicle compares the physical location of the message sender with the location information in the RSU's identifier string in order to prevent any attacker from taking the device down from one RSU and putting it elsewhere. Then, the receiver compares the type ID in the received message with the property stated in the identifier string. If the type ID cannot match with the property, the message will be ignored. For example, the messages with a property of curve speed warning will not be acceptable in case the content of the message is about "road under construction ahead." The receiver should also check the time information in the payload to make sure the message is in the allowable time window. Finally, the receiver checks the validity of the message signature by computing

$$\tilde{h}_\sigma \leftarrow H_1\left(M, e\left(S_\sigma, g_2^{H(\mathrm{ID}_i)} \cdot P_{\mathrm{pub}}\right) g^{-h_\sigma}\right).$$

This check is to see whether $\tilde{h}_\sigma = h_\sigma$, where h_σ is from σ. If the equation holds, the vehicle accepts the message; otherwise, the message is dropped.

3) Message Length: The length of an RSU message can be evaluated in the following expression:

$$L_{\mathrm{msg\_RSU}} = L_{\mathrm{typeID}} + L_{\mathrm{msgID}} + L_{\mathrm{payload}} + L_{\mathrm{timestamp}} + L_{\mathrm{sig}} + L_{\mathrm{ID}} + L_{\mathrm{TTL}}.$$

Similarly, since p is a prime that is 170 b long and each element in $\mathbb{G}_1$ is 171 b long, we get the size of the signature σ as 43 B. Therefore, $L_{\mathrm{msg\_RSU}} = 2 + 2 + 100 + 4 + 43 + 40 + 1 = 192$ B.

4) Security Analysis: Using the provably secure ID-based signature scheme in [27] allows RSU to sign an arbitrary number of messages by guaranteeing unforgeability, authentication, data integrity, and nonrepudiation. We refer to [27] for a more comprehensive description of security analysis. In this section, we analyze the proposed protocol, particularly in these aspects: 1) RSU replication attack prevention and 2) replay attack prevention, which will be discussed as follows.

1) *Prevention of RSU replication attack:* The message from an RSU has an "ID" field, keeping the RSU's original physical location, as well as its type, indicating the type of traffic management offered by the RSU. Upon receipt of the message, the OBU compares the physical location of the OBU with the location information in the RSU's ID string. If the distance is farther than RSU's transmission range, the OBU ignores the message. Therefore, the RSU replication attack can be defeated. Furthermore, the OBU compares the type ID in the received message with the property specified in the ID string of the RSU. If the type ID cannot match with the property, the message will be ignored. For example, the messages with a property of curve speed warning will not be acceptable in case the content of the message is about "road under construction ahead."
2) *Prevention of replay attack:* With a replay attack, an adversary replays the intercepted message from an RSU in order to impersonate as a legitimate RSU. Obviously, it cannot work in the proposed protocol because of the time interval check in verification procedure. Upon receiving the message, the OBU checks the time information in the timestamp to make sure the message is in the allowable time window. If the time information included in the timestamp of the message is not reasonable, the OBU will simply drop the message.

V. Performance Evaluation

In this section, simulation is conducted to verify the efficiency of the proposed secure protocol for IVC applications with ns-2 [39]. In order to properly estimate the real-world road environment and vehicular traffic, two different types of road system are considered. The first real-world environment is by way of the mobility model generation tool introduced in [40], which is specialized to generate realistic city-traffic-scenario files for vehicles under ns-2. This tool makes use of the publicly available Topologically Integrated Geographic Encoding and Referencing (TIGER) database from the U.S. Census Bureau, where detailed street maps of each city/town in the United States are given. The map adopted in this paper is a real-world city-traffic environment, as shown in Fig. 2, which corresponds to the Afton Oaks area of Houston, TX. Each vehicle is first randomly scattered on one intersection of the roads and repeatedly moved toward another randomly selected intersection along the paths in the map. Each vehicle is driving with a randomly fluctuated speed in a range of ±5 mi/h centered at the road-speed limit that ranges from 35 to 75 mi/h along different streets. The second type of road system considered in this paper is the traffic scenario on a straight bidirectional six-lane highway, where the vehicles' speed is within the range of 100 ± 10 mi/h. In both cases, an RSU is allocated every 500 m along each road, which sends messages every 300 ms. Other simulation parameters are listed in Table V.

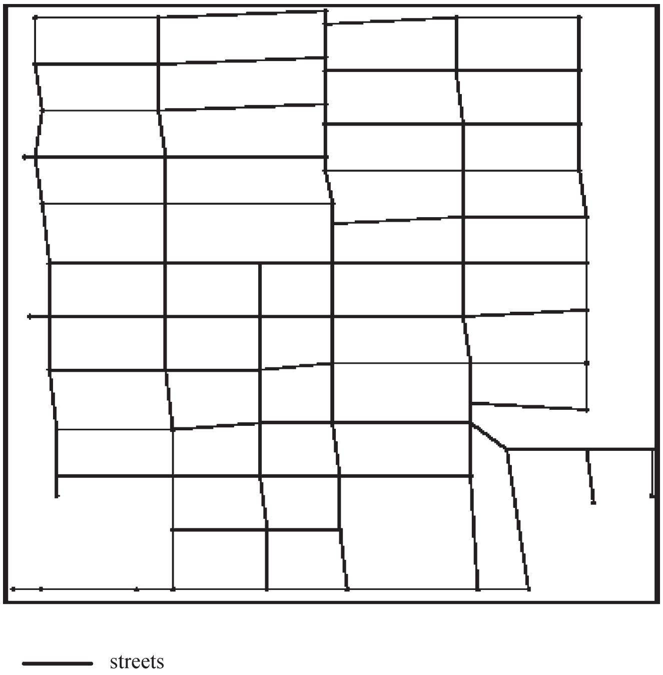


Fig. 2. City-street scenario corresponding to a square area of size $1000 \times 1000\ m^2$.

TABLE V
SIMULATION CONFIGURATION

Simulation scenario	City environment
City simulation area	$1000m \times 1000m$
Communication range	300 m
Simulation time	100 s
Channel bandwidth	6 Mbs
Pause time	0 s
Packet size for OBU message	301 bytes
Packet size for RSU message	200 bytes
Highway simulation area	$2500m \times 30m$

The performance metrics considered are the average message delay and average message loss ratio, which are denoted as $\mathrm{avg}D_{\mathrm{Msg}}$ and avgLR, respectively, and are expressed as follows:

$$\mathrm{avg}D_{\mathrm{Msg}} = \frac{1}{N_D \cdot M_{\mathrm{sent}\_n} \cdot K_n} \sum_{n \in D} \sum_{m=1}^{M_{\mathrm{sent}\_n}} \sum_{k=1}^{K_n} \times \left(T_{\mathrm{sign}}^{n\_m} + T_{\mathrm{transmission}}^{n\_m\_k} + T_{\mathrm{verify}}^{n\_m\_k} \cdot \left(L_{n\_m\_k} + 1\right)\right)$$

where D is the sample district in the simulation, N_D is the number of vehicles in D, M_{sent_n} is the number of messages sent by vehicle n, K_n is the number of vehicles within the one-hop communication range of vehicle n, $T_{\mathrm{sign}}^{n\_m}$ is the time taken by vehicle n for signing message m, n_m_k represents the message m sent by vehicle n and received by vehicle k, and

$L_{n\_m\_k}$ is the length of the queue in vehicle k when message m sent by vehicle n is received

$$\text{avgLR} = \frac{1}{N_D} \sum_{n=1}^{N_D} \frac{M^n_{\text{consumed}}}{\sum_{k=1}^{K_n} M^n_{\text{arrived}}}$$

where M^n_{consumed} represents the number of messages consumed by vehicle n in the application layer, and M^n_{arrived} represents the number of messages that are received by vehicle n in the MAC layer. Here, we only consider the message loss caused by the security protocol rather than the wireless transmission channel. Note that the message will be lost if the queue is full when the message arrival rate is higher than the message verification rate. In the following, two sets of experiments are conducted to analyze the impacts of having different traffic loads and cryptographic algorithm processing speeds.

A. Impact of Traffic Load

The density of the vehicles on the road is the main factor that has a major impact on the system performance, since it is related to the total number of messages received by each vehicle. Previous studies considered the effect brought by the actual vehicle density on the road, such as vehicles per kilometer or vehicles per square kilometer, which failed to capture the varying relationship between the communication range and the actual vehicle density. The study in [4] explored that the denser the traffic is, the shorter the communication range (or a smaller radiation power) should be adopted in order to achieve a satisfied packet loss ratio. Therefore, the number of messages received by a certain vehicle within a dissemination period should be considered as a factor for evaluating system performance instead of taking only the actual traffic density into consideration. Thus, this paper takes the average number of neighboring vehicles within the communication range of each vehicle as the traffic load, which serves as the upper bound on the number of packets a vehicle could receive within a dissemination cycle. Furthermore, the delay induced by any cryptographic operation is considered in the ns-2 simulation through the measurement of cryptographic library MIRACL [41]. In this paper, the group signature signing delay and verification delay are 3.6 and 7.2 ms,[5] respectively, while the delay by an ID-based signature verification is 3.6 ms.

Simulation results are shown in Figs. 3 and 4. It can be seen that, with the increase of traffic load (i.e., the number of vehicles within the communication range), the message end-to-end delay does not vary a lot (around 22 ms), which is smaller than the maximum allowable message end-to-end transmission latency of 100 ms, as defined in [4]. However, the message loss ratio increases when the traffic load is increased. It is notable that the loss ratio reaches as high as 68% when the traffic load is up to 150. However, such a traffic load can only be experienced when there is a severe traffic jam according to the relationship between the communication range and the intervehicle distance [4]. In this situation, it is acceptable if a large number of messages are lost because most of the messages are repeatedly sent by each vehicle. Normal traffic load happens when the traffic load is below 50, where 20% loss ratio is achieved.

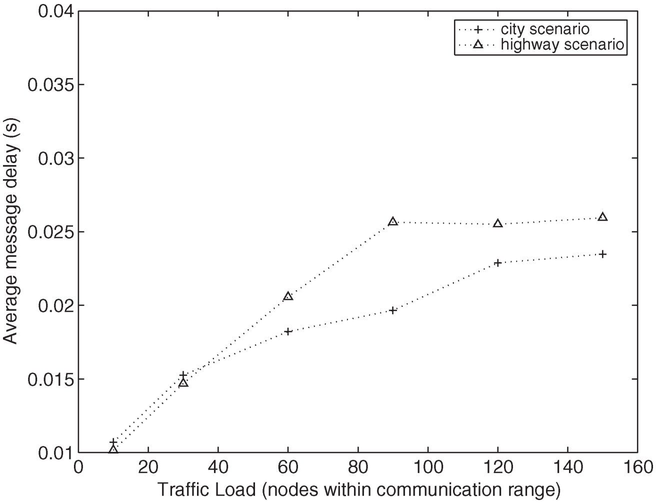


Fig. 3. Impact of traffic load on the message end-to-end delay.

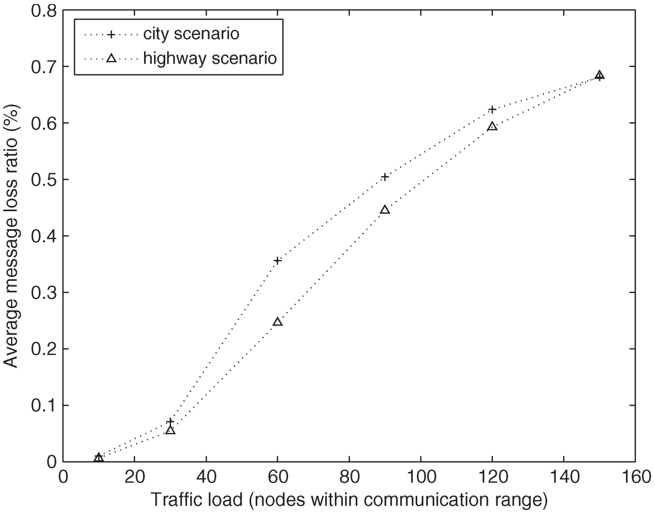


Fig. 4. Impact of traffic load on the message loss ratio.

B. Impact of Cryptographic Signature Verification Delay

Another important factor that determines the performance of a security protocol is the latency taken by the cryptographic operations in the protocol. However, the speed of implementing a cryptographic algorithm is highly determined by the adopted hardware facility. In this paper, we assume that a powerful processor is installed in each vehicle, which can achieve a very high processing speed. By referring to the parameter in [27], where one pairing operation takes 3.6 ms and that in MIRACL lib takes 8.5 ms, it is a reasonable assumption that the group signature verification latency ranges from 1 to 8.5 ms. In the simulation, a normal traffic load in a city is assumed, wherein

[5] The computation bottleneck for the signing process of the group signature is the one-pairing operation and the two-pairing operations for verification. Based on the measurement, the time to do one pairing is 3.6 ms, so we use 7.2 ms as the verification delay. Similarly, the bottleneck for identity-based signatures is the one-pairing operation during verification, so we use 3.6 ms as the verification delay.

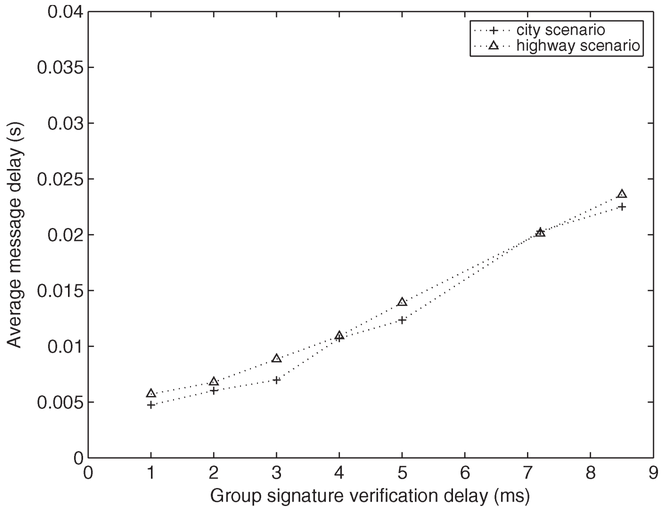


Fig. 5. Impact due to signature verification delay on the message end-to-end delay.

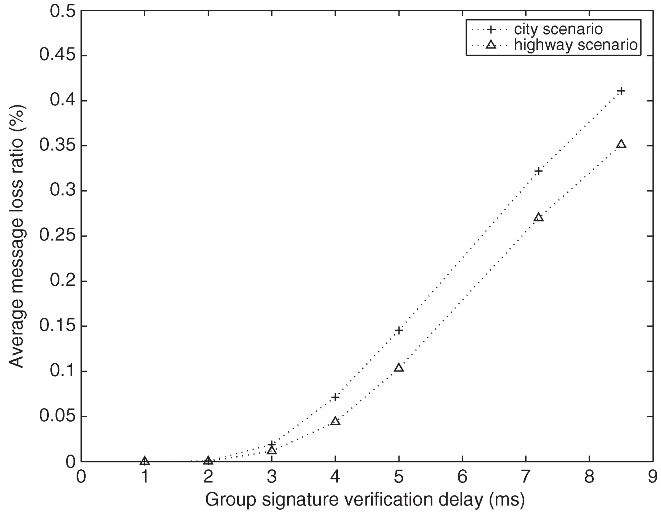


Fig. 6. Impact of signature verification delay on the average message loss ratio.

an average of 60 vehicles are within the communication range of a vehicle (simulation results are shown in Figs. 5 and 6).

It is shown that the message end-to-end delay and loss ratio increase when the cryptographic operation cost becomes larger. In addition, the message loss ratio is significantly increased after the signature verification latency reaches a certain value. Furthermore, the performances under various road systems are very close. This demonstrates the stability and insensitivity of the proposed security protocol to different road systems and traffic loads.

C. Membership Revocation and Tracing Efficiency

Next, we evaluate the efficiency of membership revocation and tracing schemes in the proposed protocol. We give an efficiency comparison against the schemes in [3]. The efficiency of the membership revocation and tracing schemes is a key requirement to the success of any vehicular application since a user is exposed to a serious risk if a malicious user conducts any dangerous activity or an adversary impersonates a compromised legitimate group member, which has been shown to be very popular in our daily life. Thus, we need to improve the performance of membership revocation and tracing schemes as much as possible.

When a vehicle is compromised, the certificates that the vehicle have need to be revoked in order to prevent potential threats due to vehicle compromise. In [3], the total of 43 800 anonymous certificates have to be put on the CRL. The storage cost of the CRL is 43 800 kB.[6] For the proposed membership revocation scheme, only an A_i needs to be put on the CRL, where i represents vehicle i. The storage cost of the CRL is only 171 b. It can easily be seen that the size of the CRL is considerably reduced. The larger the number of revoked vehicle in the CRL, the more saving the proposed membership revocation scheme can have. This is extremely important since the CRL can be distributed to any individual OBU and RSU in order to avoid contacting a centralized CRL whenever membership revocation verification is performed.

Furthermore, in the case of a traffic event dispute, such as a crime/car accident scene investigation, which can be used to look for witnesses, it is desired that the authorities should be able to trace the message senders by revealing their IDs. In [3], the authority has to keep all the anonymous certificates for each vehicle in the administrative region, which results in a very huge database with the storage cost as 43 800 kB $* n$, where n is the total number of vehicles (probably millions of cars). Similarly, the proposed membership tracing scheme also needs to maintain a table containing an A_i and its corresponding real ID of the vehicle for each vehicle, which is only 307 b if the ID of the vehicle is 136 b (the VIN of a vehicle is a 17-character number made-up of both alpha and numeric characters). Thus, the storage cost for the proposed scheme is only 307 b $* n$, and this is very significant for storage saving.

VI. Conclusion

A novel security protocol has been proposed for the IVC applications based on group signature and ID-based signature schemes. With group signature, security, privacy, and efficient traceability can be achieved without inducing the overhead of managing a huge number of stored certificates at the MM and TM's sides. With the ID-based signature, the management complexity on the public key and the certificate can be further reduced. Extensive simulation has been conducted on both a city road and highway systems to demonstrate that the message delay and loss ratio can be kept quite low, even in the presence of a large computational latency due to the cryptographic operations. For future research, we will further enhance the performance and reduce the communication overhead by using a more efficient broadcast authentication protocol, such as TESLA [45], which uses a one-way hash chain, where the chain elements are the secret keys to computing message authentication code.

[6] The size of an X.509 public key certificate is about 1 kB [44].

APPENDIX A

Proof of Lemma 1:

1) Since $\hat{g}_2 = g_2^{1/y}$ should be derived from $(A_1^*, x_1), \ldots, (A_b^*, x_b)$, we first construct the following equation:

$$\begin{aligned} g_2^{1/y} &= \prod_{i=1}^{b} (A_i^*)^{y_i} \\ &= (A_1^*)^{y_1} \cdot (A_2^*)^{y_2} \ldots (A_b^*)^{y_b} \\ &= g_2^{y_1/(\gamma+x_1)} \cdot g_2^{y_2/(\gamma+x_2)} \ldots g_2^{y_b/(\gamma+x_b)} \\ &= g_2^{\sum_{i=1}^{b} y_i/(\gamma+x_i)} \end{aligned} \tag{A.1}$$

with b unknown values $y_1, y_2, \ldots, y_b$.
We raise (A.1) to an exponential equation as

$$\frac{1}{y} = \sum_{i=1}^{b} \frac{y_i}{\gamma + x_i} = \frac{y_1}{\gamma + x_1} + \cdots + \frac{y_b}{\gamma + x_b}.$$

Then, we have

$$\begin{aligned} 1 &= y \left(\frac{y_1}{\gamma + x_1} + \cdots + \frac{y_b}{\gamma + x_b} \right) \\ &= \prod_{i=1}^{b} (\gamma + x_i) \cdot \left(\frac{y_1}{\gamma + x_1} + \cdots + \frac{y_b}{\gamma + x_b} \right) \\ &= \prod_{i=2}^{b} (\gamma + x_i) \cdot y_1 + \prod_{i=1, i\neq 2}^{b} (\gamma + x_i) \cdot y_2 \\ &\quad + \cdots + \prod_{i=1, i\neq b}^{b} (\gamma + x_i) \cdot y_b. \end{aligned} \tag{A.2}$$

Without loss of generality, assume that $b = 2$, which leads to

$$\begin{aligned} 1 &= y_1(\gamma + x_2) + y_2(\gamma + x_1) \\ &= (y_1 + y_2)\gamma + y_1 x_2 + y_2 x_1. \end{aligned} \tag{A.3}$$

Then, we have the following two equations:

$$\begin{cases} y_1 + y_2 = 0 \\ y_1 x_2 + y_2 x_1 = 1. \end{cases} \tag{A.4}$$

Solving (A.4), we obtain

$$\begin{cases} y_1 = \frac{1}{x_2 - x_1} \\ y_2 = \frac{1}{x_1 - x_2}. \end{cases} \tag{A.5}$$

Substituting (A.5) in (A.1) gives

$$\begin{aligned} \hat{g}_2 &= (A_1^*)^{y_1} \cdot (A_2^*)^{y_2} \\ &= g_2^{1/(\gamma+x_1)(x_2-x_1)} \cdot g_2^{1/(\gamma+x_2)(x_1-x_2)} \\ &= g_2^{1/(\gamma+x_1)(\gamma+x_2)} \\ \hat{g}_1 &= \psi(g_2) = g_1^{1/(\gamma+x_1)(\gamma+x_2)} \end{aligned}$$

and

$$\hat{g} = \hat{e}(\hat{g}_1, \hat{g}_2).$$

2) To compute $\hat{w} = \hat{g}_2^{\gamma} = g_2^{\gamma/y}$, we construct the following equation:

$$\begin{aligned} g_2^{\gamma/y} &= g_2^{y_0} \cdot \prod_{i=1}^{b} (A_i^*)^{y_i} \\ &= g_2^{y_0} \cdot (A_1^*)^{y_1} \cdots (A_b^*)^{y_b} \\ &= g_2^{y_0} \cdot g_2^{y_1/(\gamma+x_1)} \cdots g_2^{y_b/(\gamma+x_b)} \\ &= g_2^{y_0 + \sum_{i=1}^{b} y_i/(\gamma+x_i)} \end{aligned} \tag{A.6}$$

with $b + 1$ unknown values $y_0, y_1, y_2, \ldots, y_b$.
We raise (A.6) to an exponential equation as

$$\frac{\gamma}{y} = y_0 + \sum_{i=1}^{b} \frac{y_i}{\gamma + x_i} = y_0 + \frac{y_1}{\gamma + x_1} + \cdots + \frac{y_b}{\gamma + x_b}.$$

Then, we have

$$\begin{aligned} \gamma &= y \left(y_0 + \frac{y_1}{\gamma + x_1} + \cdots + \frac{y_b}{\gamma + x_b} \right) \\ &= \prod_{i=1}^{b} (\gamma + x_i) \cdot \left(y_0 + \frac{y_1}{\gamma + x_1} + \cdots + \frac{y_b}{\gamma + x_b} \right) \\ &= \prod_{i=1}^{b} (\gamma + x_i) \cdot y_0 + \prod_{i=2}^{b} (\gamma + x_i) \cdot y_1 \\ &\quad + \cdots + \prod_{i=1, i\neq b}^{b} (\gamma + x_i) \cdot y_b. \end{aligned}$$

Similarly, assuming that $b = 2$, we have

$$\begin{aligned} \gamma &= y_0(\gamma + x_1)(\gamma + x_2) + y_1(\gamma + x_2) + y_2(\gamma + x_1) \\ &= y_0 \gamma^2 + (y_0(x_1 + x_2) + y_1 + y_2)\gamma + y_0 x_1 x_2 \\ &\quad + y_1 x_2 + y_2 x_1 \end{aligned}$$

which leads to the following three equations:

$$\begin{cases} y_0 = 0 \\ y_0(x_1 + x_2) + y_1 + y_2 = 1 \\ y_0 x_1 x_2 + y_1 x_2 + y_2 x_1 = 0. \end{cases} \tag{A.7}$$

Solving (A.7), we obtain

$$\begin{cases} y_0 = 0 \\ y_1 = \frac{x_1}{x_1 - x_2} \\ y_2 = \frac{x_2}{x_2 - x_1}. \end{cases} \tag{A.8}$$

Substituting (A.8) in $\hat{w} = g_2^{\gamma/y}$ gives

$$\begin{aligned} \hat{w} &= \hat{g}_2^{\gamma} = g_2^{\gamma/y} \\ &= g_2^{y_0} \cdot (A_1^*)^{y_1} \cdot (A_2^*)^{y_2} \\ &= (A_1^*)^{x_1/x_1 - x_2} \cdot (A_2^*)^{x_2/x_2 - x_1} \\ &= g_2^{x_1/(\gamma+x_1)(x_1-x_2)} g_2^{x_2/(\gamma+x_2)(x_2-x_1)} \\ &= g_2^{\gamma/(\gamma+x_1)(\gamma+x_2)}. \end{aligned}$$

As a result, we proved that the group public key can be constructed as follows: $\mathrm{gpk}_{\mathrm{new}} = (\hat{g}_1, \hat{g}_2, \hat{g}, \hat{w})$. ■

APPENDIX B

Proof of Lemma 2:

1) Since $\hat{A} = A^{1/y}$ should be derived from (A, x_0) and $(A_1^*, x_1), \ldots, (A_b^*, x_b)$, we first construct the following equation:

$$\begin{aligned} A^{1/y} &= A^{y_0} \cdot \prod_{i=1}^{b} \left(\psi\left(A_i^*\right)\right)^{y_i} \\ &= A^{y_0} \cdot \left(\psi\left(A_1^*\right)\right)^{y_1} \cdots \left(\psi\left(A_b^*\right)\right)^{y_b} \\ &= g_1^{y_0/(\gamma+x_0)} \cdot g_1^{y_1/(\gamma+x_1)} \cdots g_b^{y_b/(\gamma+x_b)} \\ &= g_1^{\sum_{i=0}^{b} y_i/(\gamma+x_i)} \qquad \text{(B.1)} \end{aligned}$$

with $b+1$ unknown values $y_0, y_1, \ldots, y_b$. We raise (B.1) to an exponential equation as

$$\begin{aligned} \frac{1}{y(\gamma+x_0)} &= \sum_{i=0}^{b} \frac{y_i}{\gamma+x_i} \\ &= \frac{y_0}{\gamma+x_0} + \frac{y_1}{\gamma+x_1} + \cdots + \frac{y_b}{\gamma+x_b}. \end{aligned}$$

Then, we have

$$\begin{aligned} 1 &= y(\gamma+x_0)\left(\frac{y_0}{\gamma+x_0} + \cdots + \frac{y_b}{\gamma+x_b}\right) \\ &= \prod_{i=0}^{b}(\gamma+x_i) \cdot \left(\frac{y_0}{\gamma+x_0} + \cdots + \frac{y_b}{\gamma+x_b}\right) \\ &= \prod_{i=1}^{b}(\gamma+x_i) \cdot y_0 + \prod_{i=0, i\neq 1}^{b}(\gamma+x_i) \cdot y_1 \\ &\quad + \cdots + \prod_{i=0, i\neq b}^{b}(\gamma+x_i) \cdot y_b. \end{aligned}$$

Without loss of generality, assume that $b = 2$. Thus, we have

$$\begin{aligned} 1 &= y_0(\gamma+x_1)(\gamma+x_2) + y_1(\gamma+x_0)(\gamma+x_2) \\ &\quad + y_2(\gamma+x_0)(\gamma+x_1) \\ &= (y_0+y_1+y_2)\gamma^2 \\ &\quad + \left[y_0(x_1+x_2) + y_1(x_0+x_2) + y_2(x_0+x_1)\right]\gamma \\ &\quad + y_0x_1x_2 + y_1x_0x_2 + y_2x_0x_1 \end{aligned}$$

which leads to the following three equations:

$$\begin{cases} y_0 + y_1 + y_2 = 0 \\ y_0(x_1+x_2) + y_1(x_0+x_2) + y_2(x_0+x_1) = 0 \\ y_0x_1x_2 + y_1x_0x_2 + y_2x_0x_1 = 1. \end{cases} \qquad \text{(B.2)}$$

Solving (B.2), we obtain

$$\begin{cases} y_0 = \frac{1}{(x_1-x_0)(x_2-x_0)} \\ y_1 = \frac{1}{(x_0-x_1)(x_2-x_1)} \\ y_2 = \frac{1}{(x_0-x_2)(x_1-x_2)}. \end{cases} \qquad \text{(B.3)}$$

Substituting (B.3) in (B.1) gives

$$\begin{aligned} \hat{A} &= A^{1/y} \\ &= A^{y_0} \cdot \left(\psi\left(A_1^*\right)\right)^{y_1} \cdot \left(\psi\left(A_2^*\right)\right)^{y_2} \\ &= g_1^{1/(\gamma+x_0)(x_1-x_0)(x_2-x_0)} \cdot g_1^{1/(\gamma+x_1)(x_0-x_1)(x_2-x_1)} \\ &\quad \cdot g_1^{1/(\gamma+x_2)(x_0-x_2)(x_1-x_2)} \\ &= g_1^{1/(\gamma+x_0)(\gamma+x_1)(\gamma+x_2)}. \end{aligned}$$

Thus, $(\hat{A}, x)$ is a valid private key with respect to the group public key $\mathrm{gpk}_{\mathrm{new}} = (\hat{g}_1, \hat{g}_2, \hat{g}, \hat{w})$. ■

REFERENCES

[1] KVH Industries, Inc. [Online]. Available: http://www.kvh.com/

[2] MSN TV. [Online]. Available: http://www.msntv.com/

[3] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Security Ad Hoc Sensor Netw.*, Alexandria, VA, Nov. 2005, pp. 11–21.

[4] National highway traffic safety administration, U.S. Department of Transportation, *Vehicle Safety Communications Project—Final Rep.*, Apr. 2006. [Online]. Available: http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFTOC.htm

[5] *Traffic Light*. [Online]. Available: http://en.wikipedia.org/wiki/Traffic_light

[6] C. Liu and J. T. Yu, "An analysis of DoS attacks on wireless LAN," in *Proc. 6th IASTED Int. Multi-Conf. Wireless Opt. Commun.*, Banff, AB, Canada, Jul. 2006, pp. 346–351.

[7] D. Chaum and E. van Heijst, "Group signatures," in *Proc. Adv. Cryptology—Eurocrypt*, ser. *LNCS*, vol. 576. New York: Springer-Verlag, 1991, pp. 257-265.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Adv. Cryptology—Crypto*, ser. *LNCS*, vol. 196. New York: Springer-Verlag, 1984, pp. 47-53.

[9] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing" in *Proc. Adv. Cryptology—Crypto*, ser. *LNCS*, vol. 2139. New York: Springer-Verlag, 2001, pp. 213-229.

[10] *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*, IEEE Std. 802.16e-2005, 2006.

[11] J. Tian and L. Coletti, "Routing approach in cartalk 2000 project," in *Proc. 13th IST Mobile Wireless Commun. Summit*, Aveiro, Portugal, Jun. 2003, pp. 473–477.

[12] J. Luo and J.-P. Hubaux, "A survey of inter-vehicle communication," School Comput. Commun. Sci., EPFL, Lausanne, Switzerland, Tech. Rep. IC/2004/24, 2004.

[13] V. Namboodiri, M. Agarwal, and L. Gao, "A study on the feasibility of mobile gateways for vehicular ad-hoc networks," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, Philadelphia, PA, Oct. 2004, pp. 66–75.

[14] T. Kosch and W. Franz, "Technical concept and prerequisites of car-to-car communication," in *Proc. 5th Eur. Congr. Exhib. Intell. Transp. Syst. Serv.*, Hannover, Germany, Jun. 2005.

[15] R. M. Yadumurthy, C. H. Adithya, M. Sadashivaiah, and R. Makanaboyina, "Reliable MAC broadcast protocol in directional and omni-directional transmissions for vehicular ad hoc networks," in *Proc. 2nd ACM Int. Workshop Veh. Ad Hoc Netw.*, Cologne, Germany, Sep. 2005, pp. 10–19.

[16] K. Plößl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Proc. 1st Int. Conf. Availab., Rel. Security*, Vienna, Austria, Apr. 2006, pp. 374–381.

[17] A. Aijaz, B. Bochow, D. Florian, A. Festag, M. Gerlach, R. Kroh, and L. Tim, "Attacks on inter vehicle communication systems—An analysis," in *Proc. 3rd Int. Workshop Intell. Transp.*, Hamburg, Germany, Mar. 2006.

[18] R. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *Proc. Embedded Security Cars*, Berlin, Germany, Nov. 2005.

[19] H. Zhu, X. Lin, P.-H. Ho, X. Shen, and M. Shi, "TTP based privacy preserving inter-WISP roaming architecture for wireless metropolitan area networks," in *Proc. WCNC*, Hong Kong, China, Mar. 2007, pp. 2957–2962.

[20] 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.

[21] *SeVeCom (Secure Vehicular Communication) Project*. [Online]. Available: http://www.sevecom.org/

[22] I. Aad, J. P. Hubaux, and E. Knightly, "Denial of service resilience in ad hoc networks," in *Proc. ACM MobiCom*, Philadelphia, PA, Sep. 2004, pp. 202–215.

[23] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, "DDoS-resilient scheduling to counter application layer attacks under imperfect detection," in *Proc. IEEE INFOCOM*, Barcelona, Spain, Apr. 2006, pp. 1–13.

[24] J. V. E. Molsa, "Increasing the DoS attack resiliency in military ad hoc networks," in *Proc. IEEE MILCOM*, Atlantic City, NJ, Oct. 2005, pp. 2282–2288.

[25] J. V. E. Molsa, "Cross-layer designs for mitigating range attacks in ad hoc networks," in *Proc. 24th IASTED Int. Conf. Parallel Distrib. Comput. Netw.*, Innsbruck, Austria, Feb. 2006, pp. 64–69.

[26] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2569–2577, Sep. 2006.

[27] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. Adv. Cryptology—Asiacrypt*, ser. *LNCS*, vol. 3788. New York: Springer-Verlag, 2005, pp. 515-532.

[28] G. Wang, *Security Analysis of Several Group Signature Schemes*, Apr. 2004. [Online]. Available: http://eprint.iacr.org/2003/194

[29] S. Han, J. Wang, and W. Liu, "An efficient identity-based group signature scheme over elliptic curves," in *Proc. 3rd Eur. Conf. Univers. Multiservice Netw.*, Porto, Portugal, Oct. 2004, pp. 417–429.

[30] C. Popescu, "An efficient ID-based group signature scheme," *Studia Univ. Babes-Bolyai, Informatica*, vol. XLVII, no. 2, pp. 29–38, 2002.

[31] A. Miyaji and K. Umeda, "A fully-functional group signature scheme over only known-order group," in *Proc. ACNS*, Yellow Mountain, China, Jun. 2004, pp. 164–179.

[32] J. Zhang, Q. Wu, and Y. Wang, "A novel efficient group signature with forward security," in *Proc. 5th Int. Conf. Inf. Commun. Security*, Huhehaote, China, Oct. 2003, pp. 292–300.

[33] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Proc. Adv. Cryptology—Eurocrypt*, ser. *LNCS*, vol. 3027. New York: Springer-Verlag, 2004, pp. 56-73.

[34] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. Adv. Cryptology—Crypto*, ser. *LNCS*, vol. 3152. New York: Springer-Verlag, 2004, pp. 41-45.

[35] G. Atenies, D. Song, and G. Tsudik, "Quasi-efficient revocation of group signatures," in *Proc. Financ. Cryptogr.*, Southampton, Bermuda, Mar. 2002, pp. 183–197.

[36] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. ACM CCS*, Washington DC, Oct. 2004, pp. 166–177.

[37] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable signature," in *Proc. Adv. Cryptology—Eurocrypt*, ser. *LNCS*, vol. 3027. New York: Springer-Verlag, 2004, pp. 571-589.

[38] G. Ateniese, J. Camenisch, M. Joye and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme" in *Proc. Adv. Cryptology—Crypto*, ser. *LNCS*, vol. 1880. New York: Springer-Verlag, 2000, pp. 255-270.

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

[40] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad hoc networks," in *Proc. 1st Int. Workshop Veh. Ad Hoc Netw.*, Philadelphia, PA, Oct. 2004, pp. 91–92.

[41] *Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL)*. [Online]. Available: http://indigo.ie/ mscott/

[42] W. Mao, *Modern Cryptography: Theory and Practice*. Upper Saddle River, NJ: Prentice-Hall PTR, 2003.

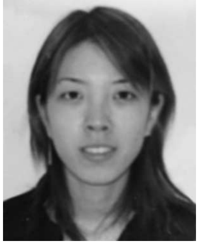
[43] B. Schneier, *Applied Cryptography*, 2nd ed. New York: Wiley, 1996.

[44] X.509. [Online]. Available: http://en.wikipedia.org/wiki/X.509

[45] A. Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast authentication protocol," *RSA Cryptobytes*, vol. 5, no. 2, p. 213, 2002.

Xiaodong Lin (S'07) 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 anomaly-based intrusion detection.



Xiaoting Sun received the B.E. degree from Harbin Institute of Technology, Harbin, China, in 2003. She is currently working toward the Master's degree with the David. R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada.

Her research interests include wireless network security and privacy and security issues in vehicular communication networks.

Pin-Han Ho (M'04) received the B.Sc. and M.Sc. degrees from the Electrical and Computer Engineering Department, National Taiwan University, Taipei, Taiwan, R.O.C., in 1993 and 1995, respectively, and the Ph.D. degree, focusing on optical communications systems, survivable networking, and QoS routing problems, from Queen's University, Kingston, ON, Canada, in 2002.

He joined the Electrical and Computer Engineering (ECE) Department, University of Waterloo, Waterloo, ON, as an Assistant Professor. 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 ECE Department, University of Waterloo, Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award from SPECTS'02, the ICC'05 Optical Networking Symposium, and the ICC'07 Computer and Communications Security Symposium, and the Outstanding Paper Award from HPSR'02.

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

He is a Professor and 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, ultrawideband wireless communication systems, wireless security, and *ad hoc* and sensor networks. He is a coauthor of three books and has published more than 300 papers and book chapters on wireless communications and networks, control, and filtering.

Dr. Shen serves as the Technical Program Committee Chair for IEEE Globecom'07, the General Cochair for Chinacom'07 and QShine'06, and the Founding Chair for the IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; and Editor-in-Chief for *Peer-to-Peer Networking and Application*; an 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 was the recipient of 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 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 the Province of Ontario.