2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications

Threshold-based Secure and Privacy-Preserving Message Verification in VANETs

Wei Gao*, Mingzhong Wang*, Liehuang Zhu*, and Xiaoping Zhang†
* Beijing Engineering Research Center of Massive Language Information Processing and Cloud Computing Application
School of Computer Science
Beijing Institute of Technology
{gaowei5623080, wangmz, liehuangz}@bit.edu.cn

† National Key Lab of Vehicular Transmission
China North Vehicle Research Institute
zxp_cnvri@163.com

***Abstract*—Messages spreading inside vehicular ad hoc networks (VANETs) generally need to achieve the property of verifiability and content integrity, while preserving user privacy. Otherwise, VANETs will either fall into chaos, or prevent users from embracing it. To achieve this goal, we propose a protocol, which contains a priori and posteriori countermeasures, to guarantee these features. The a priori process firstly verifies that each message is sent by a vehicle only once. Then it collects and checks whether the count of the message exceeds the threshold value to improve the trustworthiness of the message. The posteriori process verifies the integrity of the message, ensuring it is unchanged during transmission between the vehicle and the road side unit. The privacy is preserved by applying group signature. In case of disruptive events, the proposed solution can trace back to the source vehicle which generates the message.**

***Index Terms*—Group Signature, Threshold Verification, Privacy, Vehicular Communication**

I. Introduction

With the development and growth of wireless communication technologies, vehicular ad hoc networks (VANETs) are proposed as an enabling technology with potential revolutionary impact on the lifestyles of our society. The exchange of information between vehicles can make drivers familiar with the surrounding environment so as to improve the driving experience, as well as to reduce the probability of traffic accidents [1]. With the benefit of information sharing among vehicles, VANETs provide new opportunities for road safety and traffic management. Therefore, governments, academia, and the automobile industry have carried out extensive research effort in recent years. For instance, TracNet [2], an automotive-vehicle Internet-access system, was introduced by Microsoft's MSN TV [3]. KVH [4] can turn the whole vehicle into an IEEE 802.11-based Wi-Fi coverage so that passengers can use their wireless-enabled devices to get useful information or what they are interested in [11].

A general architecture for VANETs is shown in Fig. 1. It consist of two-layer. The bottom layer is composed by vehicle nodes and stationary roadside units (RSUs). The communication happens between vehicles, or vehicles and RSUs. Since RSUs are usually built up by authorities and have better computing power, they play as the coordinators for vehicles. Each vehicle has its own public keys which are known by others and private keys which are only known by itself, messages communicated by them will firstly be signed and then sent to its neighbouring RSU. Each RSU receiving the signed message has the responsibility to verify the digital signatures of the message [34].

The top layer is comprised of application servers and a trust authority (TA). RSUs communicate with an application server and TA using a secure transmission protocol so that the transmission is safe. RSUs forward valid messages received from vehicles to the application server. After receiving messages transmitted by vehicles, application server makes further analysis and gives feedbacks to RSUs after collecting traffic-related information, such as location, traffic distribution, and weather. We assume that TA is trustworthy which will not be compromised.

Vehicular ad hoc networks have made great contributions to traffic management and road safety, but they have to achieve several challenges, particularly security and privacy threats, before their prevalence. Since vehicles are closely attached to our daily life, the information sharing between vehicles in VANETs may lead to privacy disclosure, or even worse that malicious manipulating of messages may cause hazardous road conditions. For example, attackers may trace the route of a vehicle, as well as the identity of the driver, by analysing related messages. Moreover, attackers can transmit false messages to fool other vehicles, resulting in traffic accidents. Hence, efforts should be devoted to guaranteeing the correctness and privacy of exchanged messages.

Although users' privacy need to be protected, some user-related information, including the driver's identity, license plate, position, speed, and travelling routes, should be preserved for authorized investigation [5], [7]. For example, the police may need to reveal the identities of drivers or message senders who violate traffic regulations or make cheating. Furthermore, anonymity will greatly reduce the trustworthiness

978-1-4799-6513-7/14 $31.00 © 2014 IEEE
DOI 10.1109/TrustCom.2014.105

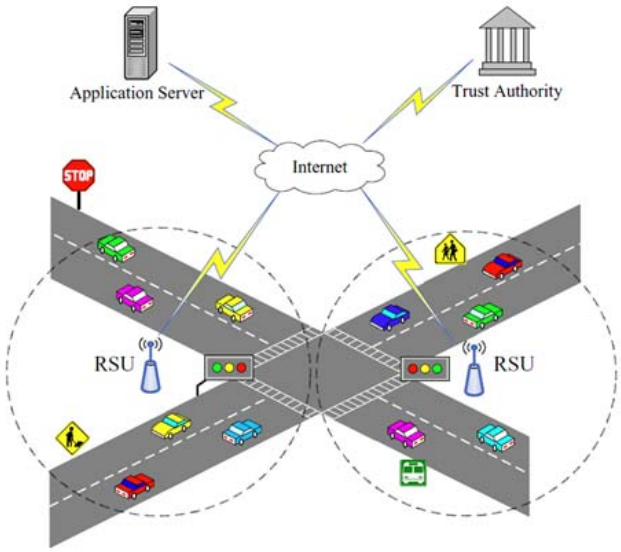

Fig. 1. Vehicular Ad Hoc Network Structure

of communications between vehicles because the generators of messages are indistinguishable and cannot be identified for liability [12]. Therefore, it is crucial to find a trade-off between message traceability and privacy protection.

Attackers in VANETs can be generally categorized as external attackers and internal attackers according to whether they are member of VANETs. Cryptographic authentication can be applied to prevent external attackers. However, internal attackers are hard to resist because they are legitimate system users who have the right to access the secret key. Therefore, they have the ability to fabricate fake messages which will lead to unpredictable outcomes.

The method against internal attackers can be roughly divided into a priori and posteriori category. A priori countermeasures attempt to prevent the fraudulent messages by checking if the number of messages received reaches a threshold. If the number is less than the threshold, these messages are not trusted, and are discarded directly. Otherwise, these messages enter the next round of judgement. That is, a message is trusted only if it was endorsed by a number of vehicles in the vicinity. The underlying assumption for this approach is that most users are honest and will not endorse any message containing false data. Another implicit assumption is the common sense that the more people that endorse a message, the more trustworthy it is [8], [9], [12].

In contrast, posteriori countermeasures enable punitive actions against vehicles that have been considered illegal. In anonymous authentication systems, it requires trustworthy institutions to locate and revoke malicious users. The implementation involves the mechanisms of cryptographic authentication and digital signature. For example, PKI (Public Key Infrastructure) is suggested in VANETs [6], in which a large number of pseudonyms certificate are pre-loaded in vehicles [10], [13].

Neither a priori nor a posteriori countermeasures alone can ensure the security of VANETs [12], [16]. Therefore, combined solutions were proposed to achieve privacy-preserving authentication [12], [14], [15]. In order to ensure the privacy of vehicles, the proposed protocols should satisfy unlinkability, which means that given two signatures on messages, a verifier can't distinguish whether they come from the same vehicle. Thus, all messages disseminated in VANETs must be anonymous so that no one can know their real identities. For a vehicle which receives n messages, how it can find out these messages come from n different legitimate vehicles without discovering their identities is a challenging issue.

Addressing this issue, in this paper, we propose a novel privacy-preserving authentication protocol with a priori and posteriori countermeasures by using group signature. By recording a message's count filed within a certain period of time , we can recognize how many times the same message is signed by the same vehicle, thus we can judge whether the message should be discarded or should be accepted. We apply RSU verification instead of vehicle verification to increase system efficiency.

The remainder of this paper is organized as follows. Section 2 provides a survey on the related work. Section 3 introduces and explains the proposed scheme. Section 4 provides an analyse to the security of the scheme. Section 5 evaluates the system and Section 6 concludes.

II. Related Work

Only when the messages disseminated are correct and trustworthy, VANETs can improve traffic safety. However, the avoidance of fraudulent messages in VANETs is extremely difficult because of the fast changing participants and topology. The complexity boosts when vehicles want to retain their privacy. In this case, message senders are anonymous, and can not be identified when violating the rules or exercising criminal behaviour. A number of schemes have been proposed to reduce fraudulent messages while maintaining the privacy requirement.

Group-signature-based schemes [16], [17] and pseudonymous authentication schemes [18], [19] were proposed to achieve identity privacy and data integrity. They address the security requirements of non-repudiation, conditional anonymity, identity revocation, and authentication. In group signature, vehicles first join a group in an authentication way, and then use the group's public key to do sign operation on behalf of the group without revealing its identity. Therefore, recipients only know which group the message comes from and do not know the specific identity of the vehicle. When a vehicle is found to be illegal or have sent unlawful messages, the group manager can trace the signer's true identity. However, the overhead of signing and verifying messages is far higher than traditional PKI.

Pseudonymous authentication [21], [22] was proposed to solve the high overhead problem. Each vehicle is supported with a large number of pseudonymous certificates generated by

the trust mechanism. When a message needs to be signed, the vehicle randomly selects one of the available pseudonymous certificates to sign it. The drawback is the storage usage.

In VANETs, both schemes have been applied to design privacy-preserving authentication schemes that combined a priori and posteriori measures. TAA [14] achieved reliability, privacy, and auditability without the intervention of any third party. It maintains a list of history events L to detect repeated messages. BTSP [12] used an additional signature to indicate whether the message is signed by the same vehicle. It is not efficient because the computational overhead of signature verifying process is generally high. PPAP [15] used group signature and supported message linkability. It satisfies the privacy and security requirements, but it is not suitable to large-scale messages verification because of random oracle model.

Our scheme applies group signature to guarantee the security and privacy of vehicles. Signature validation process is implemented in RSUs rather than vehicles receiving messages, thus improving verification speed and preventing Dos attacks.

III. Threshold-based Verification Scheme

This section provides a detailed explanation to the proposed scheme. Part A and B introduce system settings and assumptions. Part C to G explains the operational steps of the scheme. That is, Setup, Registration, Message Signature, Verification, and Threshold Authentication.

A. Computation Assumptions

Our scheme is based on bilinear pairing groups.

A bilinear pairing instance is generated by an probabilistic polynomial-time algorithm which on the input of a security parameter outputs a tuple $\gamma = (p, G_1, G_2, G_T, g_1, g_2, e)$.$p$ is the prime order of the finite cyclic groups G_1=$< g_1 >$ and G_2=$< g_2 >$. we write G_1,G_2 additively and G_T multiplicatively. e is an efficient non-degenerate bilinear map $G_1 \times G_2 \rightarrow G_T$ satisfying the following properties.

1) Bilinearity: for all $h_1 \in G_1, h_2 \in G_2$, and $u, v \in \mathbb{Z}, e(h_1^u, h_2^v) = e(h_1, h_2)^{uv}$.

2) Nondegeneracy: $e(g_1, g_2) \neq 1$.

3) Computability: There exits an efficient algorithm to compute $e(g_1, g_2)$, for all $(g_1, g_2) \in G_1 \times G_2$.

For most of the encryption program, $\Psi : G_2 \rightarrow G_1$ is essentially needed which played the role of an effective computable isomorphism. If there is $G_2 = G_1$ and $g_1 = g_2$, we call Ψ the identity map. Therefore, for generally, we consider $G_2 = G_1$. Then, if we enter a security parameter k, the bilinear parameter generator $gen(k)$ will generate a tuple that contains five elements (p, g_1, G_1, G_T, e), where $e : G_1 \times G_2 \rightarrow G_T$. The following three problems, which server as a basis of our proposed protocol, are believed to be hard.

1) Computational Diffie-Hellman (CDH) problem: Given an element g and the values of g^a and g^b which meet the conditions that $a, b \in \mathbb{Z}_p^*$ and g^a,$g^b \in G_1$. Then compute what is the value of g^{ab}.

2) Decisional Diffie-Hellman (DDH) problem: For the three unknown parameters such as $a, b, c \in \mathbb{Z}_p^*$, and g_1^a,g_1^b,$g_1^c \in G_1$ is given and known. Now the DDH is to decide whether $ab = c$ mod p. As we also known that DDH in G_1 is easy and can be solved by checking $e(g_1^a, g_1^b) = e(g_1^c, g_1)$ within polynomial time.

3) Bilinear Diffie-Hellman (BDH)problem: For the three unknown parameters such as $a, b, c \in \mathbb{Z}_p^*$, and g_1^a,g_1^b,$g_1^c \in G_1$ is given and known. The task of BDH is to compute $e(g_1, g_1)^{abc} \in G_T$.

B. System Architecture

The system contains four parties. Following notations are used to represent them.

RM: Registration Manager. It is responsible for the registration of a vehicle as it joins VANETs. When dispute event happens, it is responsible to find the real identity of vehicles.

TM: Tracing Manager. When an accident occurs, *TM* is responsible for recording the pseudonym of related vehicles and transmitting them to *RM*.

R: Road Side Unit (RSU). It is responsible for providing services for vehicles. It is responsible to verify the signatures from vehicles within its coverage.

V: Vehicles. A Vehicle or On Board Unit (OBU) has a valid pseudonym and a valid certificate. It can collect messages from its neighbouring vehicles and send them to the RSUs that it belongs to.

All vehicles should firstly register with a *RM* to become a legal group member. During the registration, some tracing information is securely sent to *TM*, so that *TM* can trace the vehicle if it later maliciously behaves. *RM* should be implemented by a trusted authority, for example, transportation companies for commercial vehicles or by vehicle management agencies for private cars. *TM* can be implemented by police that is a law authority actually performs traffic management. Fig. 2 illustrates the general structure of the proposed scheme. The implementation of the transmission of messages is explained as follows.

Firstly, vehicle V_i generate message m_i and then sign it use its own private key sk_{v_i} before send it out. Next,V_i send message m_i and its signature $sign_{sk_{v_i}}(m_i)$ to RSU. After receiving the transmitted information RSU verify the message m_i by computing $verify_{PK}(sign_{sk_{v_i(m_i)}})$,if message is not changed when it is transmitted the RSU would sign the message m_i using the RSU's own private key $\mu H(R_i)$ and generate $sign_{\mu H(R_i)}(m_i)$, with the verification transmitted to the application server. After verification by application server,the information generated by vehicle V_i would communicated to other neighbour vehicles.

C. System Setup

During the system initialization, we should first select public parameters for all the protocols and algorithms within our scheme as well as other parameters for each vehicles and RSUs. In the generation process of the system parameters, private input is not required.

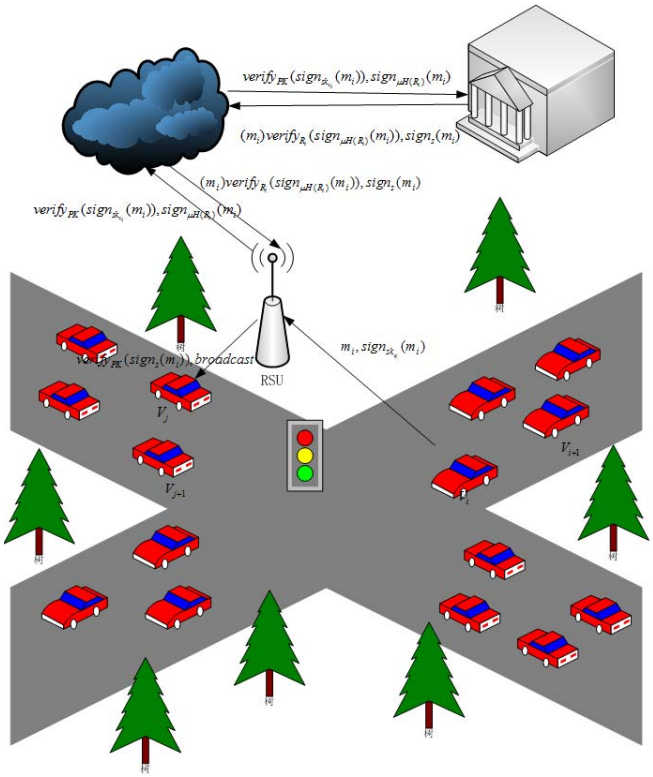

Fig. 2. Scheme Structure

Let $\gamma = (p, G_1, G_2, G_T, g_1, g_2, e) \leftarrow gen(1^\lambda)$ be generated as aforementioned. Furthermore, we assume that the strong Diffie-Hellman assumption holds on (G_1, G_2) and that the linear Diffie-Hellman assumption holds on G_1. Let Ψ be a computable isomorphism from G_2 to G_1 such that $\Psi(g_2) = g_1$.

TM as the law authority randomly selects two elements ε_1 and $\varepsilon_2 \in \mathbb{Z}_p^*$ as *TM*'s private key$(\varepsilon_1, \varepsilon_2)$, along with one random element $h \in G_1 \setminus 1_{G_1}$, and sets $u, v \in G_1$ such that $u^{\varepsilon_1} = v^{\varepsilon_2} = h$. Finally, *TM* keeps $(\varepsilon_1, \varepsilon_2)$ secretly and sends the system parameters $(G_1, G_2, G_T, g_1, g_2, p, \Psi, e, u, v, h)$ to *RM* who works as a credible institution.

RM randomly selects $s \in \mathbb{Z}_p^*$ as the master's private key and then computes the corresponding public keys $PK = g_2^s$. In addition, *RM* also chooses two secure cryptographic hash functions so that they meet the following criteria $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ and $H_1 : \{0,1\}^* \times G_T \rightarrow \mathbb{Z}_p^*$. Finally, *RM* publishes the system parameters $(G_1, G_2, G_T, g_1, g_2, p, \Psi, e, H, H_1, PK, u, v, h)$ to complete system initialization.

D. Vehicle Registration

During the registration stage, a vehicle *V* must contact *RM* by a confidential channel and send its identity ID_i to prove that it is legitimate. It also sends some trapdoor information of its public key so that the tracing manager can trace the vehicle when it has abnormal behaviours. After receiving the vehicle's identity ID_i, the trusted party randomly chooses $r_i \in Z_p$ and generates a tuple (A_i, x_i) as the private key for each vehicle V_i with identity ID_i. The elements of tuple are computed as $x_i \leftarrow H(ID_i, r_i)$, and $A_i \leftarrow g_2^{\frac{1-sx_i}{x_i}}$.

Finally, the trusted party *RM* keeps (ID_i, r_i, A_i) in its database and sends (A_i, r_i) to the vehicle. After receiving (A_i, r_i), the vehicle can ensure the correct completion of initialization by verifying the formula $e(g_1^{H(ID_i, r_i)}, A_i \cdot PK) = e(g_1, g_2)$.

When a RSU R_i wants to join a VANET, *RM* randomly selects a number μ and generates $\mu H(R_i)$ as its private key and its identity R_i is used as the public key. When a vehicle enters the RSU's coverage, it automatically obtains the id of R_i.

TABLE I
FORMAT OF VEHICLE-GENERATED MESSAGE

Group ID	Message ID	Timestamp	Count	Payload	TTL	Signature
2	2	4	4	100	1	128

E. Message Signature

Vehicle-generated messages, M, are designed to contain seven fields: group ID, message ID, timestamp, count, payload, time to live (TTL), and signature.The group ID represents which group the vehicle belongs to, and message ID defines the type of the message. A timestamp is used to record the time of signature, and prevent replay attacks. The count field is newly added to record how times the same message was signature by the same vehicle, and its initial value is 0. There is a list used to store the message which is about to be signed with ΔT. Firstly, the vehicle checks the list to see if there exist the same message, if it holds the value of the count filed add one in the original basis, otherwise, the count field is one and adding the message to the list. The payload field is the main part of the message, it may include the information on the vehicle's position, direction, event time, speed, traffic event and so on. According to[27], the payload of a message is 100B. The TTL field shows the survival time of the message. And the last field is signature on the first six fields. We denote the first six fields by and all of the seven fields by *M*. Because there are two time fields, so the system should require time synchronization. As we know, VANETs is deployed by centralized authorities, it is not difficult to realize time synchronization. Table I shows the format of messages which are disseminated within VANETs.

Group ID represents the group that the vehicle belongs to, and message ID defines the type of the message. A timestamp is used to record the time of signature to prevent replay attacks. The count field is introduced to record the number of times that a message was signed by the same vehicle. The value of count is initialized as 0.

The payload field is the main part of the message. It may include the information of the vehicle's position, direction, speed, traffic event, and time. The size of message payload of is generally set as 100B [27]. The TTL field shows the survival

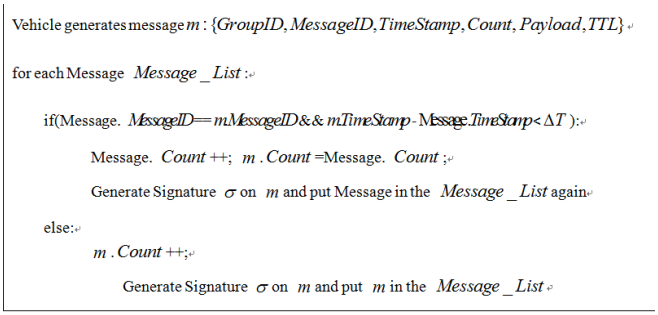

Fig. 3. Message Count Handling in Signature Process

time (in seconds) of a message. The last field is the signature of previous six fields. In this scheme, messages are coordinated by RSU. Therefore, the timestamp used by vehicles will be synchronized by RSUs.

TTL field should be ensured not be changed in the process of the message transmission, so it will also be signed. If the TTL field is not signed, a malicious vehicle can revive an outdated message and mount a corpse attack by merely modifying the TTL field of the message [20], [23]. The count field is signed to prevent modification attacks.

The signing process is based on MLGS [29], which is an interactive protocol between a register manager, a tracing manager, a set of group members, and a set of verifiers. *V* generates an MLGS on the message before sending it out. With the group public parameters and the private key of the vehicle, the signing procedure is composed of the following computation.

a) Randomly choose variables α and $\beta \in \mathbb{Z}_p^*$

b) Compute (T_1, T_2, T_3) where $T_1 \leftarrow u^{\alpha-\beta}, T_2 \leftarrow v^{\beta}$ and $T_3 \leftarrow A_i h^{\alpha}$.

c) Compute $\delta_1 = (A_i)^{\beta}, \delta_2 = PK^{\beta}, \delta_3 = (g_1^{x_i})^{\beta}$ and $X = g_2^{\beta}$.

d) Randomly choose $r_\alpha, r_\beta \in \mathbb{Z}_p^*$ to compute

$$\begin{cases} R_1 = \Psi(X)^{r_\alpha} \cdot r_\beta \\ R_2 = H_1(m)^{r_\beta} \end{cases} \quad \begin{cases} \sigma_1 = g_2^{x_i} \\ \sigma_2 = (hX)^{\beta} \\ \sigma_3 = \sigma_2^{x_i} \\ \sigma_4 = H(m, \sigma_1, \sigma_2, \sigma_3, R_1, R_2) \\ \sigma_5 = r_\beta - \sigma_4 \\ \sigma_6 = r_\alpha - x_i \sigma_2 \end{cases} \tag{1}$$

Finally, the result of the message signature is σ and the value of it is $\sigma = (T_1, T_2, T_3, \delta_1, \delta_2, \delta_3, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, X)$ as the group signature of *m*, and add the message *m* to the message list before sending (m, σ, R_i) to RSU.

One key operation before signing process is the handling of the parameter $count$. The detailed steps are shown in Fig. 3.

Each vehicle maintains a list of messages it has sent out. When a new message m comes, the vehicle firstly compares the message ID of m repeatedly with each record in the message list. Within a certain duration ΔT, if m is a repeat, then the count value of the recorded message is updated by 1, and the count of m is set accordingly. Otherwise, increase the count of m from 0 to 1, and add it to the sent list.

F. Verification

When receiving a message, the RSU will perform signature verification for each message as follows:

1) Check $e(\delta_1 \cdot \delta_2 \cdot \delta_3) = e(\Psi(X), X)$ to validate the group certificate blindly.

2) Check $\sigma_4 = H(m, \sigma_1, \sigma_2, \sigma_3, \Psi(X)^{\sigma_6} \cdot \delta_3^{\sigma_2} \cdot (\sigma_4 + \sigma_5), H_1(m)^{\sigma_4} \cdot H_1(m)^{\sigma_5})$ to validate the signature. This ensures the verifier with the standard arguments that the vehicle *V* knows the secret value x_i satisfying $\sigma_3 = \sigma_2^{x_i}$.

If both checks are correct for the signature, the RSU considers the message to be valid. That is, all message fields are not changed during transmission. If any verification fails, the RSU invalidates and discards the message.

G. Threshold Authentication

Even though the verification is correct, it does not mean that the message will be accepted by the receiver. The RSU checks the content of a message, and discards it if either of following conditions is true:

- $currenttimestamp > m.timestamp + TTL$
- $m.count > 1$

TTL is used to ensure the freshness of a message. And $count$ is used to detect repeatedly sent message from the same vehicle, which may imply Sybil attack.

If both checks are false, the message is considered as being valid. A variable num, which is maintained by RSU to represent the number of messages from different vehicles, is increased by 1. When num becomes greater than or equal to the threshold t, RSU believes the messages were sent by at least t different sources, thus being more reliable.

It should be noted that the threshold can adaptively be changed according to the types of messages [24], [29]. For example, if the message is an alert, such as an emergency barking by the vehicle ahead, the threshold can be set low. Otherwise, if the message is an announcement that will affect some other vehicles, the threshold can be set high to improve the trustworthiness.

After verifying the signatures disseminated by vehicles, RSU generates a new message m_R, signs it using its private key, and sends it to *RM*. *RM* verifies the signature using the identity ID_{R_i}. If the verification succeeds, *RM* signs the message and sends it to surrounding RSUs. RSUs that receive the message broadcast it to the vehicles within its coverage. This process transmits the computation intensive operations from OBUs which have limited computing power to RSUs that are more powerful.

H. Membership Traceability

When a vehicle is found to have disputable events or there is a problem in the signature process, for instance, the signature σ on message m is found to be fraudulent, a membership tracing operation is performed to solve the dispute to prevent the occurrence of more serious consequences.

The tracing manager first checks the validity of the signature σ on m and computes A_i according to the formula $A_i \leftarrow T_3/(T_1^{\varepsilon_1}, T_2^{\varepsilon_2})$. It then sends A_i to RM.

RM looks up the record (ID_i, r_i, A_i) in its database to find the corresponding identity ID_i. RM can send information about the compromised OBU to all RSUs, add its identity information (ID_i, A_i) into the local revocation list [32], [33].

IV. Security Analysis

We have proposed a scheme based on group signature. It records the number of times a message has been signed within $\triangle T$ by a count field of the message. The $count$ record enables a priori countermeasures to prevent sybil message attacks [27], [28].Before signing the message, we first examined the count field, if it equals zero then set it equal to one. Otherwise, if time interval between two signatures is less than $\triangle t$, let the count value plus one. Then sign the message and send the message and signature to the receivers.It means if a vehicle produces a signature on a message, then the signature is anonymous to the verifier; however, if a vehicle produces two signatures on the same message, then the verifier can discard the message because it can distinguish that the two signatures are from the same vehicle. By this method, we can construct a priori countermeasures to prevent some fraudulent message attacks.

RSU maintains a threshold value t, which means the number of different vehicles. When RSU receives the same message from at least t different vehicles in the vicinity, the message is believed to be valid. This countermeasure is based on the fact that messages transmitted between vehicles in the same environment should be same or similar. A fraudulent message can be traced or revoked by corresponding posteriori countermeasure. This section analyse security features of the proposed scheme.

A. Authentication and Non-repudiation

Entity authentication means that an entity cannot deny that it has sent a message. In this scheme each vehicle has its own private key, which is unknown to others. Based on existing signature algorithm, such as short signature and re-signature [30], [31], the signature generated by each entity is un-forgeable. Therefore, entity authentication can be achieved by a digital certificate of the owner's signature. Similarly, the message with a veritable signature can guarantee message integrity and non-repudiation.

B. Identity Revocation

In this scheme, if the vehicle is found in violation of the rules, TM and RM will cooperate to complete the revocation of the vehicle and broadcast its identity information to the passing by vehicles. This function can be achieved by publishing the rogue list that contains the compromised vehicles' secret. In order to prohibit previously legal but currently illegal users from generating valid information announcements,revocation can be performed by renewing keys and certificates of issuers' and legitimate signers'.

TABLE II
Computational performance

Name	Party	Computational cost
Sign	Signer	$7 \cdot G_1 + 1 \cdot P$
Threshold-Check	Verifier	Judging the value of count, without multiplication and pairing evaluation
Verify	Verifier	$5 \cdot G_1 + 4 \cdot P$
Trace	Verifier	Verify two signatures $1 \cdot G_1$

C. Conditional Anonymity

In vehicular ad hoc networks, anonymity is a powerful tool to protect the vehicle's privacy. However, in order to remove illegal vehicles, the vehicle identification is necessary to be traced. To solve this conflict, conditional anonymity is provided. According to the characteristics of group signature, we know that the identities of group members are transparent to the recipient. Because the receiver only knows which group the sender belongs to, but not the real identity of the sender. This protects sender's privacy.

When a dispute event was detected, ***TM*** which has the vehicle's private key will compute its pseudonymous identity and send it to ***RM*** who hold the real identity of the vehicle. ***RM*** removes (ID_i, A_i) from its own database. This feature meets the requirements for malicious vehicle tracking.

V. Performance analysis

As observed in [25], under normal circumstances, the realization of an exponential operation in G_T cost about 4 scalar multiplications in G_1. This means that we can change all exponentiation formulas in G_T required in our scheme into scalar multiplication formulas in G_1 to obtain a faster implementation. For instance, in order to calculate $e(S, X)^x$ in the Sign algorithm we can first compute $x \cdot S$ and then get the value of $e(S, X)^x$ by computing $e(x \cdot S, X)$. This trick also applies to other algorithms in this process [14]. According to this rule, we can get detailed power consumption in each part of the program, as show in Table II. $n \cdot G_1$ means n scalar multiplication in G_1, and $m \cdot P$ denotes m pairing operations.

In this subsection, we compare our scheme with three relevant schemes, GSIS [11],TAA [14] and BST-P [12].Specifically,we conduct our comparison in two categories, including functionalities and computation time.

- **Functionalities**. Table III compares three schemes with respect to the features of auditability, reliability, and privacy. Entity authentication and data integrity are satisfied in all three solutions because messages are signed with digital signature. However, only our scheme provides non-repudiation and prevents DOS attacks at the same time. All schemes can achieve anonymity and revocation because they use techniques of group signature.Finally,neither GSIS nor BTSP can achieve non-repudiation,because the issuer also have the group signing key of a vehicle.
- **Computation time**. According to the experiment results given in [26], to achieve 80-bit security level we can set

TABLE III
COMPARISON OF FUNCTIONALITIES

Name	Auth.	Integ.	Thres.	Anonym.	Unlink.	Trace.	Revoc.	Non-rep.	DOS
GSIS [11]	√	√	×	√	√	√	√	×	×
TAA [14]	√	√	√	√	√	√	√	√	×
BTSP [12]	√	√	√	√	√	√	√	×	×
Our Sch.	√	√	√	√	√	√	√	√	√

Sch.: scheme; Auth.: entity authentication; Integ.: data integrity; Thres.: threshold verification; Anony.: anonymity; Unlink.: unlinkability; Trace.: traceability; Revoc.: revocation; Non-repud.: non-repudiation.

TABLE IV
COMPARISON OF EXECUTION TIME (MS)

Name	Sign	Verify	Revocation Check	Threshold Check	Trace
GSIS [11]	7.5	13.8	$13.5 \times n$	$--$	1.2
TAA [14]	9.9	27.3	$0.6 \times n$	0	0.6
BTSP [12]	7.2	16.2	$10.2 \times n$	4.5	2.4
Our Sch.	8.7	21.1	$0.8 \times n$	0	0.6

n means the length of the revocation list

$|p| = 160$ and $|G_1| = 161$. Therefore, multiplications in G_1 and one pairing evaluation can be done within 0.6ms and 4.5ms respectively [14]. As shown in Table IV, further experiments compares the execution time of three solutions.From this table we can see that signing a message in our scheme takes much more time than GSIS and BTSP, but less than TAA. We are even more incredible to see that the time for verifying a signature in our scheme is approximately doubled. The main reason is because that a few pairing evaluations in GSIS can be pre-computed, but can not be pre-computed in our scheme. On the other hand, we are pleased to see that revocation check is significantly faster in our scheme than in GSIS an takes almost the same time as in TAA.

Based on the experiment results, we can conclude that our scheme maintains similar performance to existing solutions, while improving the detection rate of fraudulent messages.

VI. CONCLUSION

Privacy and security are two important issues in VANETs. Addressing these needs, we have presented a novel privacy-preserving scheme for VANETs communication based on a priori and posteriori countermeasures by using group signature with counting method. The scheme supports non-repudiation and distinguishability of messages that signed by a vehicle many times. When there is a dispute event happens, efficient traceability can be achieved without the overhead of managing a large number of stored certificates at *TM* and *RM*. *TM* and *RM* can cooperate to revoke misbehaving OBUs to avoid further harm to VANETs.

ACKNOWLEDGEMENT

The research work reported in this paper is supported by National Science Foundation of China under Grant No. 61100172, No. 61272512, and No. 61300177. It is also supported by Program for New Century Excellent Talents in University (NCET-12-0046), and Beijing Natural Science Foundation (No. 4121001).

REFERENCES

[1] J. Blau, "Car talk," IEEE Spectr., vol. 45, no. 10, p. 16, Oct. 2008.
[2] F. Dotzer, "Privacy issues in vehicular ad hoc networks," in Proc. PET, vol. 3856, Lecture Notes in Computer Science, 2005, pp. 197-209.
[3] KVH Industries, Inc. [Online]. Available: http://www.kvh.com/
[4] MSN TV. [Online]. Available: http://www.msntv.com/
[5] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in Proc. Eur. Wireless, 2002, pp. 270-274.
[6] 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.
[7] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in Proc. 3rd VANET, 2006, pp. 67-75.
[8] F. Picconi, N. Ravi, M. Gruteser, and L. Iftode, "Probabilistic validation of aggregated data in vehicular ad-hoc networks," in Proc. 3rd VANET, 2006, pp. 76-85.
[9] L. Chen and S. L. Ng. Comments on "Proving reliability of anonymous information in VANETs" by Kounga et al. IEEE Trans. Veh. Technol., volume 59(3), pp. 1503-1505, March 2010.
[10] T. Nakanishi, T. Fujiwara, and H. Watanabe, "A linkable group signature and its application to secret voting," Trans. Inf. Process. Soc. Jpn., vol. 40, no. 7, pp. 3085-3096, 1999.
[11] X. Lin, X. Sun, P.-H. Ho and X. Shen. GSIS: Secure vehicular communications with privacy preserving. IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442-3456, 2007
[12] Wu Q, Domingo-Ferrer J, Gonzlez-Nicols. Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications. IEEE Transactions on Vehicular Technology 2010;59
[13] Raya M, Hubaux JP. Securing vehicular ad hoc networks. Journal of Computer Security 2007; 15(1):39-68.
[14] Chen L, Ng S-L, Wang G. Threshold anonymous announcement in VANETs. IEEE Journal on Selected Areas in Communications 2011; 29(3):605-612.
[15] Privacy-preserving authentication protocols with efficient verification in VANETs;2013
[16] E. Gallery, An overview of trusted computing technology, in C. Mitchell, editor, Trusted Computing, chapter 3. IEE, 2005.
[17] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. Mobile Netw. Veh. Environ., Anchorage, AK, May 2007, pp. 103-108.
[18] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. INFOCOM, Phoenix, AZ, Apr. 2008, pp. 1229-1237.
[19] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," IEEE Trans. Wireless Commun., vol. 8, no. 4, pp. 1974-1983, Apr. 2009.

[20] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in Proc. 4th ACM Int. Workshop VANET, Montreal, QC, Canada, 2007, pp. 19-28
[21] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39-68, Jan. 2007.
[22] K. Laberteaux, J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," in Proc. 5th ACM Int. Workshop VANET, San Francisco, CA, 2008, pp. 88-89.
[23] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in Proc. 5th ACM Int. Workshop VANET, San Francisco, CA, 2008, pp. 86-87.
[24] Yipin Sun,Rongxing Lu,Xiaodong Lin and Xuemin Shen," An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications" in IEEE transaction on vol59 no7 ,2010
[25] L. Chen and P. Morrissey and N. P. Smart. DAA: Fixing the pairing based protocols. Cryptology ePrint Archive: Report 2009/198, available at http://eprint.iacr.org/2009/198 Last accessed December 10, 2009.
[26] M. Scott. Efficient implementation of cryptographic pairings, 2007. http: //ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf Last accessed December 10, 2009.
[27] Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC)
[28] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442-3456, Nov. 2007.
[29] Wu Q, Domingo-Ferrer J, Gonzlez-Nicols. Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications. IEEE Transactions on Vehicular Technology 2011; 59(2):559-573
[30] Y. Zhang, W. Liu, W. Lou, Y. Fang, Securing mobile ad hoc networks with certificateless public keys, IEEE Transactions on Dependable and Secure Computing 3 (4) (2006) 386C399.
[31] B. Sieka, A.D. Kshemkalyani, Establishing authenticated channels and secure identifiers in ad-hoc networks, International Journal of Network Security 5 (1) (2007) 51C61.
[32] J. van der Merwe, D. Dawoud, S. Mcdonald, A survey on peer-topeer key management for mobile ad hoc networks, ACM Computing Surveys 39 (1) (2007) 1C45.
[33] D. Jungels, M. Raya, P. Papadimitratos, I. Aad, J.P. Hubaux, Certificate revocation in vehicular ad hoc networks, Technical LCAReport- 2006-006, LCA, 2006.
[34] Chenxi Zhang,Rongxing Lu,Xiaodong Lin,Pin-Han Ho,and Xuemin(Sherman)Shen,"An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks" in Proc.INFOCOM 2008. The 27th Conference on Computer Communications IEEE.