On the Security of a Secure Batch Verification with Group Testing for VANET

Zhang Jianhong[1], Xu Min[2], and Liu Liying[3]
(Corresponding author: Zhang Jianhong)

College of sciences & North China University of Technology[1]
Shijingshan District Beijing 100144
Department of Education & Baoding University[2]
Baoding, Hebei 071000
Department of Mathematics & Handan College[3]
Handan, Hebei 056005, China
(Email: jhzhang@ncut.edu.cn)
(Received Apr. 9, 2013; revised and accepted June 10, 2013)

Abstract

Vehicular communication networking can provide well-suited traffic messages, emergency warning messages and infotainment dissemination, and improve driving condition for drivers. The authentication of these information is particularly important in VANET since the wrong traffic information may result in traffic accident and traffic jam. And VANET requires short verifying delay to response messages. To identify invalid messages and reduce verifying delay, a lot of schemes have been proposed to verify the information of VANET by batch verification technique. Recently, Lee et al.' proposed an improved authentication scheme with batch verification based on bilinear pairing to make VANET more secure, efficient, and more suitable for practical use. Unfortunately, their scheme is shown to be insecure and cannot achieve replay attacking, tracing and non-repudiation of message. Finally, to overcome the above flaws, an improved authentication scheme is proposed. And the security proof and performance analysis are presented. By comparing with Lee et al.s'scheme and Zhang et al.'s scheme in terms of verifying delay, our scheme is more efficient than Zhang et al.'s scheme. And Batch verification time in our scheme is more 0.6ms than that of Lee et al.'s scheme, however, Lee et al.'s is insecure.

Keywords: Authentication protocol, non-repudiation, replay attacking, security analysis, verifying delay

1 Introduction

Vehicular Ad hoc Network (VANET) is an important component part of intelligent transportation systems. As an open wireless network, VANETs is an application of Ad-Hoc Network for vehicle communication. It mainly consists of the vehicles with on-board units (OBUs), and the roadside units (RSUs). To provide and share information, there are two kinds of communications types: one is vehicle-to-vehicle (V-2-V) communication, the other is roadside-to-vehicle communications (V-2-R). By V-2-V communication, people can obtain more information and use the shared information to improve road safety. By V-2-R communication, people can communicate with RSU to access internet for downloading and updating files or inquire neighborhood location information. Thus, compared with the traditional pure infrastructure-based network, the hybrid of V-2-V and V-2-R communications is promising since it can not only overcome the disadvantages of infrastructure-based network, but also overcome the disadvantage of non-infrastructure-based network.

The appearing of VANETs comes from improving the road safety and the safe driving condition. Therefore, before deploying VANET for practical application, security and privacy issues must be addressed. Otherwise, the VANETs would be confronted with many potential attacks, for instance, malicious attacks, route tracing and sybil attack, and so on.

Among of VANETs security issues, it is an important challenge how to avoid invalid messages and falsified message, since these invalid messages and falsified message maybe cause road accidents and traffic jams. It will result in serious consequences to the traffic system. To ensure both identity authentication and message integrity in VANETs, a simplest solution to resist invalid message and falsified message is to adopt digital signature technology. Before the message is sent, it is signed with a digital signature by the vehicle. If the sent message is an invalid message or falsified message, any one can distinguish the real origin of the message to punish the vehicle by the authentication and non-repudiation of digital signature. In

2007, Raya and Hubaux [2, 10, 11]included PKI (Public Key Infrastructure) certificate architecture in VANET to achieve authentication of between entities and message's validity.

However, According to Dedicated Short Range Communications (DSRC) protocol [1], each vehicle needs to broadcast a traffic related message every 100-300 ms in VANETs. It means that a vehicle could receive hundreds of message from the surrounding vehicles at the same time, and verifying a large number of these signatures need take a long time since digital signatures rely on time-consuming cryptographic operation. It results in a serious problem which is many useful safety messages maybe be discarded since they cannot be verified within the stipulated time. Thus, it makes that traditional digital signature schemes that verify the message-signature one by one can not satisfy the stringent time requirement for safety related messages. At the same time, to protect the identity privacy of the vehicle, the vehicle's identity must be preserved due to opening property of VANET.

Therefore, it puts forth a challenge how to quickly verifying a number of signatures under the condition that conditional privacy needs to be taken into consideration as well. In 2006, Raya et al.[9] proposed a secure traffic aggregation scheme to minimize the communication overhead and initiate a tradeoff between the security and efficiency by including a group leader which aggregates messages of the whole group. However, group leader changes frequently and executes a number of computation cost. Subsequently, Picconi et al. proposed a PKI-based authentication scheme in VANETs in [7]. The schemes in [9] and [7] mainly focuses on aggregating messages, rather than aggregating digital signature. In 2007, Lin et al. proposed an anonymous authentication scheme [6] to improve authentication efficiency by combining group signature scheme based on bilinear pairing and ID-based signature. In [6], a verifier can verify multiple signatures simultaneously, verification efficiency of signatures is improved. The cost of computation time is not grow linearly with the amount of the signature. Nevertheless, Lin *et al.*'s scheme still need complex computing process due to using a lot of exponent operations. In 2008, Zhu *et al.*proposed an aggregated emergency message authentication scheme in [18] by adopting batch verification technique for efficient emergency messages verification. In 2009, Wasef et al.[12] gave an efficient authentication scheme which can employ aggregation technologies to enable each vehicle to simultaneously verify signatures and their certificates in the PKI scenario. In 2011, Zhang et al.proposed a privacy-preserving authentication scheme [16] by incorporating identity-based cryptography, aggregate signature and one-time signature.

Recently, Zhang et al. presented an authentication protocol [15] for VANET by using an identity-based batch signature verification scheme. Unfortunately, Lee et al. showed that Zhang et al's scheme in [15] was vulnerable to the replaying attack and did not achieve the signature non-repudiation. Then, they proposed an improved scheme [4] to overcome the above flaws. However, in this paper, we show that Lee et al.'s scheme[15] is also insecure and it exists a serious security flaw. Any one can produce a forged signature on message m in name of the other vehicle's identity. Finally, to overcome this serious flaw, an improved scheme is presented. Our improved scheme overcomes the security flaw which exists in the Lee et al.'s scheme,and it has the same efficiency as Lee et al.'s scheme.

Figure 1: The two-lay network model

2 Reviews of Lee et al.'s Batch Verification for VANET

Recently, Lee et al. point out that Zhang et al.'s batch verification scheme for VANET [15] is insecure in [4]. Then they give an improved scheme to overcome these flaws and show that the improved scheme can prevent replay attack and forgery attack. In the following, we briefly review Lee et al.'s improved scheme which includes key generation and pre-distribution phase, pseudo identity generation and message signing phase, identity tracing and message verification phase.

A two-layer vehicular network model was adopted in Lee et al.'s scheme [4] and Zhang et al.'s scheme [15]. The network model is shown in Fig 1. In the model, a trust authority (TA) belongs to the top layer and is responsible for pre-assigning secure information for each vehicle, and the vehicles and RSUs belongs to the lower layer. All notions in this paper are denoted as Table 1.

2.1 Key Generation an Pre-distribution Phase

Let $\mathbb{G}$ and $\mathbb{G}_T$ be a cyclic additive group and a cyclic multiplicative group with the same prime order q, respectively.P is a generator of group $\mathbb{G}$, $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a bilinear map. TA randomly chooses two random numbers $s_1, s_2 \in Z_q$ as its two master keys, and compute the corresponding public key $P_{pub1} = s_1P, P_{pub2} = s_2P$. In

Table 1: Notions in this paper

V_i	the ith vehicle
RSU	A roadside unit
TA	A trust authority
TPD	A tamper-proof device
s_1, s_2	The private key of TA
P_{pub1}, P_{pub2}	The public key of TA
RID_i	The real identity of $V_i, RID_i \in \mathbb{G}$
PWD_i	A password of the vehicle V_i
ID^i	A pseudo identity of the vehicle $V_i, ID^i = (ID_1^i, ID_2^i)$
SK^i	A private key of the vehicle $V_i, SK^i = (SK_1^i 1, SK_2^i)$
M_i	A sent message by the vehicle V_i
$h(), h_2()$	two one-way hash functions
$H()$	A map to point hash function, $H : \{0,1\}^* \rightarrow G$
$\|\|$	messages concatenation operation
T_i	A timestamp generated by the vehicle V_i
Vec_i	A component i vector Vec used to distinguish signature

general, these two master keys (s_1, s_2) of the TA are pre-loaded in each vehicles tamper-proof device. At the same time, the public parameters $(\mathbb{G}, \mathbb{G}_T, q, P, P_{pub1}, P_{pub2})$ are pre-loaded in each RSU and vehicle.

Finally, each vehicle is assigned its real identity, denoted as $RID \in \mathbb{G}$, and password, denoted as PWD. Both RID and PWD are stored in the tamper-proof device.

2.2 Pseudo Identity Generation and Message Signing Phase

When each vehicle communicates with other vehicles or RSU, it must anonymously send message to protect its privacy. Therefore, it has to produce a pseudonym before communication. The details are shown as follows:

1) First, the vehicle V_i inputs its real identity RID_i and password PWD_i to initiate a pseudo-identity generation process.

2) After verifying the validity of RID_i and PWD_i, TPD randomly chooses a $r \in Z_q$ to compute pseudo identity $IDi = \{ID_1^i, ID_2^i\}$ and $SK^i = \{SK_1^i, SK_2^i\}$,

$$ID_1^i = rP$$
$$ID_2^i = RID_i \oplus H(rP_{pub1})$$
$$SK_1^i = s_1 ID_1^i$$
$$SK_2^i = s_2 h_2(ID_1^i || ID_2^i || T_i)P$$

where T_i is a current timestamp.

3) After TPD outputs ID^i and SK^i, V_i can produce a messages-signature

$$\delta_i = SK_1^i + h(M_i)SK_2^i$$

on message M_i using ID^i and SK^i.

4) Subsequently, V_i sends the final message $(ID_i, M_i, \delta_i, T_i)$ to its neighboring RSU.

2.3 Identity Tracing

If V_i broadcasts a malicious message, TA can trace the real identity RID_i of V_i by computing $RID_i = ID_2^i \oplus H(s_1 ID_1^i)$: Therefore, once a signature is in dispute, the TA has the tracing ability to find the real identity RID of vehicle from the disputed message.

2.4 Message Verification Phase

When the RSU receives any final message $(ID_i, M_i, \delta_i, T_i))$ from a vehicle, it checks the timestamp T_i. If $T_r - T_i < T_\Delta$, then RSU continues the following verification process, otherwise, reject this message, where T_r denotes the received-time of the message and T_Δ be the predefined endurable transmission delay. The message verification process is divided into two versions: single message verification and batch message verification. The details of these two versions are described as follows.

2.4.1 Single message verification

Upon receiving a message-signature $(ID_i, M_i, \delta_i, T_i))$, it verifies whether the following equation holds.

$$e(\delta_i, P) = e(ID_1^i, P_{pub1})e(h(M_i)h_2(ID_1^i||ID_2^i||T_i)P, P_{pub2})$$

If it holds, the message is accepted, otherwise, reject it.

2.4.2 Batch message verification

If a RSU receives a number of message-signatures, denoted as $(ID_1, M_1, \delta_1, T_1)$,$(ID_2, M_2, \delta_2, T_2), (ID_3, M_3, \delta_3, T_3), \cdots,$ $(ID_n, M_n, \delta_n, T_n)$, the RSU randomly chooses a vector $Vec = (Vec_1, Vec_2, \cdots, V_n)$ where $Vec_i \in [1, x]$ and x is a small value. Then it can simultaneously verify the validity of these messages by batch message verification.

$$e(\sum_{i=1}^{n} Vec_i\delta_i, P) = e(\sum_{i=1}^{n} Vec_i ID_1^i, P_{pub1}) \cdot$$
$$e((\sum_{i=1}^{n} Vec_i h(M_i)h_2(ID_1^i||ID_2^i||T_i))P, P_{pub2})$$

Note that the goal to choose a value vector is to resist illegal message-signature.

3 Security Analysis of Lee et al's Batch Verification Scheme

In [4], Lee et al's claimed that their scheme can resist replaying attack and provide the non-repudiation of message-signature. We show that their scheme doesn't satisfy the non-repudiation of message-signature. An important problem is that the flaw in Lee et al's scheme [4] is more serious than one in Zhang et al.'s scheme [15]. Lee et al.'s scheme exists universal forgeability, that is to say, any one can produce a forged signature in name of any identity. At the same time, the scheme is also shown not to satisfy traceability. Given a message-signature of a vehicle, TA cannot trace the real identity of the vehicle which sent this message. Thus, we can infer that Lee et al.'s scheme doesn't satisfy non-repudiation of message-signature and the traceability of malicious vehicle's real identity due to universal forgeability. These detail attacks are given as follow.

3.1 Forgeability Attack

Let $\mathcal{A}$ be an attacker, to produce a forged signature of message $\bar{M}$ in name of identity $\overline{RID}$, it executes the following steps:

1) Let $\bar{M}$ be a sent false message.

2) The attacker $\mathcal{A}$ randomly chooses $l \in Z_q$ to compute $I\bar{D}_1^i = lP$ and $I\bar{D}_2^i = \overline{RID} \oplus H(lP_{pub1})$. Then, it sets
$$I\bar{D}^i = (I\bar{D}_1^i, I\bar{D}_2^i)$$

3) the attacker computes
$$\bar{\delta} = lP_{pub1} + h(\bar{M})h_2(I\bar{D}_1^i||I\bar{D}_2^i||\bar{T})P_{pub2}$$
where $\bar{T}$ is a current timestamp.

4) Finally, that attacker outputs $(I\bar{D}_i, \bar{\delta}, \bar{T}, \bar{M})$ as the forged signature on message $\bar{M}$.

In the following, we will show that the forged signature $(I\bar{D}_i, \bar{\delta}, \bar{T}, \bar{M})$ can pass the verification equation. Since

$$\begin{aligned} & e(\bar{\delta}, P) \\ = \ & e(lP_{pub1} + h(\bar{M})h_2(I\bar{D}_1^i||I\bar{D}_2^i||\bar{T})P_{pub2}, P) \\ = \ & e(lP_{pub1}, P)e(h(\bar{M})h_2(I\bar{D}_1^i||I\bar{D}_2^i||\bar{T})P_{pub2}, P) \\ = \ & e(lP, P_{pub1})e(h(\bar{M})h_2(I\bar{D}_1^i||I\bar{D}_2^i||\bar{T})P, P_{pub2}) \\ = \ & e(I\bar{D}_1^i, P_{pub1})e(h(\bar{M})h_2(I\bar{D}_1^i||I\bar{D}_2^i||\bar{T})P, P_{pub2}) \end{aligned}$$

It shows the forged signature can pass verification equation.Thus,it means that our forgery attack is successful.

3.2 Tracing Attack

In Lee et al.'s scheme[4], they also claimed that their scheme could trace the real identity of malicious vehicle if it broadcasted a malicious message. However, we will show that their scheme doesn't achieve the traceability of malicious vehicle's identity by analyzing security of the scheme.

Supposed that $\mathcal{A}$ is a malicious vehicle, to prevent TA from tracing the real identity, The malicious vehicle computes the signature on message in the following form.

1) Let M be a false message.

2) $ID^A = \{ID_1^A = rP, ID_2^A = RID_A \oplus H(rP_{pub1})\}$ is the produced pseudo identity by TPD.

3) $SK^A = \{SK_1^A, SK_2^A\}$ is the corresponding private key to pseudo identity ID^A.

4) The malicious vehicle $\mathcal{A}$ randomly chooses a number $k \in Z_q$ to compute $ID'^A_1 = kID_1^A = krP$, and sets $ID'^A_2 = ID_2^A$

5) Then it sets $SK'^A_1 = kSK_1^A = s_1ID_1^A$ and $SK'^A_2 = h_2(ID'^A_1||ID'^A_2||T)h_2(ID_1^A||ID_2^A||T)^{-1}SK_2^i = s_2h_2(ID'^A_1||ID'^A_2||T)$, where (SK_1^A, SK_2^A) is outputted to the vehicle by TPD.

6) Finally, the malicious vehicle computes
$$\delta_A = SK'^A_1 + h(M)h_2(ID'^A_1||ID'^A_2||T)h_2(ID_1^A||ID_2^A||T)^{-1}SK_2^A$$

7) The resultant signature is
$$\sigma_A = (ID'^A = (ID'^A_1, ID'^A_2), M, \delta_A, T)$$

Obviously, the resultant signature $\sigma_A = (ID'^A = (ID'^A_1, ID'^A_2), M, \delta_A, T)$ can pass verification equation since

$$\begin{aligned} & e(\delta_A, P) \\ = \; & e(SK'^A_1 + h(M)h_2(ID'^A_1||ID'^A_2||T) \\ & \cdot h_2(ID^A_1||ID^A_2||T)^{-1} SK^A_2, P) \\ = \; & e(SK'^A_1, P)e(h(M)h_2(ID'^A_1||ID'^A_2||T) \cdot \\ & h_2(ID^A_1||ID^A_2||T)^{-1} SK^A_2, P) \\ = \; & e(ID'^A_1, P_{pub1})e(h(M)SK'^A_2, P) \\ = \; & e(ID'^A_1, P_{pub1})e(h(M)h_2(ID'^A_1||ID'^A_2||T)P, P_{pub2}) \end{aligned}$$

However, when TA need to trace the real identity of the vehicle which produces signature $\sigma_A = (ID'^A = (ID'^A_1, ID'^A_2), M, \delta_A, T)$, TA computes

$$\begin{aligned} ID'^A_2 \oplus H(s_1 ID'^A_1) &= RID_A \oplus H(rP_{pub1}) \oplus H(s_1 ID'^A_1) \\ &= RID_A \oplus H(rP_{pub1}) \oplus H(rkP_{pub1}) \\ &\neq RID_A \end{aligned}$$

According to the above result, we know that given a message-signature δ_A, TA cannot trace the real identity of a malicious vehicle from this signature δ_A. Thus, Lee et al.'s scheme doesn't achieve traceability.

4 An Improved batch verification with group testing for VANET

4.1 Key Generation an Pre-distribution Phase

In the phase, the system parameters are the same ones of Lee et al.'scheme except that TA still randomly chooses two elements $Q, P_1 \in \mathbb{G}$. Thus, system parameters are

$$(\mathbb{G}, \mathbb{G}_T, q, P, Q, P_1, P_{pub1}, P_{pub2}, h, H, h_2)$$

where $P_{pub1} = s_1 P, P_{pub2} = s_2 P$, $s_1, s_2 \in Z_q$ are secretly kept by TA. For bilinear map group system parameters' choice, please refer to [13, 14, 5, 17] for the detail.

4.2 Pseudo Identity Generation and Message Signing Phase

Before each vehicle communicate with other vehicles or RSU, the pseudonym of the vehicle is produced as follows:

1) First, the vehicle V_i inputs its real identity RID_i and password PWD_i to initiate a pseudo-identity generation process.

2) After verifying the validity of RID_i and PWD_i, TPD randomly chooses a $r \in Z_q$ to compute pseudo identity $IDi = \{ID^i_1, ID^i_2\}$ and $SK^i = \{SK^i_1, SK^i_2\}$, where

$$\begin{aligned} ID^i_1 &= rP \\ ID^i_2 &= RID_i \oplus H(rP_{pub1}) \\ SK^i_1 &= s_1 ID^i_1 \\ SK^i_2 &= s_2 h_2(ID^i_1||ID^i_2||T_i)P_1 + s_1 h(ID^i_1)Q \end{aligned}$$

where T_i is a current timestamp.

3) After TPD outputs ID^i and SK^i, V_i can produce a signature on messages M_i

$$\delta_i = SK^i_1 + h(M_i)SK^i_2$$

on message M_i using ID^i and SK^i.

4) Finally, V_i sends the signature $(ID_i, M_i, \delta_i, T_i)$ on message M_i to its neighboring RSU or the other vehicles.

4.3 Identity Tracing

If V_i broadcasts a malicious message, TA can trace the real identity RID_i of V_i by computing $RID_i = ID^i_2 \oplus H(s_1 ID^i_1)$: Therefore, once a signature is in dispute, the TA has the tracing ability to find the real identity RID of vehicle from the disputed message.

4.4 Message Verification Phase

When the RSU receives any final message $(ID_i, M_i, \delta_i, T_i))$ from a vehicle, it first checks the timestamp T_i. If $T_r - T_i < T_\Delta$, then RSU executes the following verification process, otherwise, reject this message, where T_r denotes the received-time of the message and T_Δ be the predefined endurable transmission delay. The message verification process is divided into two versions: single message verification and batch message verification. The details of these two versions are described as follows.

4.4.1 Single message verification

Upon receiving a message-signature $(ID_i, M_i, \delta_i, T_i))$, it verifies whether the following equation holds.

$$\begin{aligned} e(\delta_i, P) = \; & e(ID^i_1 + h(ID^i_1)Q, P_{pub1}) \\ & \cdot e(h(M_i)h_2(ID^i_1||ID^i_2||T_i)P_1, P_{pub2}) \end{aligned}$$

If it holds, the message is accepted, otherwise, reject it.

4.4.2 Batch message verification

If a RSU receives a number of message-signatures, denoted as $(ID_1, M_1, \delta_1, T_1)$,$(ID_2, M_2, \delta_2, T_2)$, $(ID_3, M_3, \delta_3, T_3), \cdots,$ $(ID_n, M_n, \delta_n, T_n)$, the RSU randomly chooses a small value vector $Vec = (Vec_1, Vec_2, \cdots, V_n)$ where

$Vec_i \in [1, x]$ and x is a small value. Then it verifies as follows.

$$e(\sum_{i=1}^{n} Vec_i\delta_i, P) = e(\sum_{i=1}^{n} Vec_i(ID_1^i + h(ID_1^i)Q), P_{pub1})$$
$$\cdot e((\sum_{i=1}^{n} Vec_i h(M_i)h_2(ID_1^i||ID_2^i||T_i))P_1, P_{pub2})$$

In the following, we will show that our improved scheme is secure.

Theorem 1. *If there exists an adversary $\mathcal{A}$ which can break the improved scheme, then Then there exists an algorithm $\mathcal{B}$ who can solve the CDH problem.*

Proof. Given an instance (P, aP, bP) of the CDH problem, its goal is to compute abP. The whole system parameters is set up as follows.

Let $Q = aP$ and $P_{pub1} = bP$. Algorithm $\mathcal{B}$ randomly choose $s \in Z_q$ to set $P_{pub2} = sP$. Finally, the algorithm $\mathcal{B}$ sends $(Q, P, P_{pub1}, P_{pub2}, h, h_2)$ to the adversary $\mathcal{A}$. In the game, hash function h is thought of as a random oracle.

When the adversary $\mathcal{A}$ make a signing query with M, the algorithm $\mathcal{B}$ randomly chooses $l_1, l_2 \in Z_q$ and $ID_2 \in \{0,1\}^*$ to set $ID_1^i = l_1P - l_2Q$ and $h(ID_1^i) = l_2$. If ID_1^i has already existed in the h-list which is initially empty, then the algorithm $\mathcal{B}$ needs to reselect l_1, l_2. Finally, it computes $\delta = l_1P_{pub1} + h(M_i)h_2(ID_1^i||ID_2^i||T)P_{pub2}$ and returns (ID_1^i, M_i, δ, T) to the adversary $\mathcal{A}$.

Eventually, the adversary $\mathcal{A}$ outputs a forged signature $(ID_1^*, M^*, \delta^*, T^*)$. We apply the Forking Lemma [8]. By replaying the game with the same random tape but different choices of oracle h, at the end of the second run, we obtain another valid forged signature $(ID_1^*, M^*, \delta^*, T^*)$, where $ID_1^* = ID'^*_1$. Then we have

$$\begin{aligned} e(\delta^*, P) &= e(ID_1^* + h(ID_1^*)Q, P_{pub1}) \\ &\quad \cdot e(h(M^*)h_2(ID_1^*||ID_2^*||T^*)P, P_{pub2}) \end{aligned}$$

and

$$\begin{aligned} e(\delta'^*, P) &= e(ID'^*_1 + h(ID'^*_1)Q, P_{pub1}) \\ &\quad \cdot e(h(M^*)h_2(ID'^*_1||ID'^*_2||T^*)P, P_{pub2}) \end{aligned}$$

Thus, we can obtain

$$e(\delta^* - (\delta')^* + R, P) = e((h(ID_1^*) - h(ID'^*_1))Q, P_{pub1})$$

where

$$\begin{aligned} R &= (h(M^*)h_2(ID'^*_1||ID'^*_2||T^*) \\ &\quad -h(M^*)h_2(ID_1^*||ID_2^*||T^*))P_{pub2} \end{aligned}$$

It means that

$$abP = (\delta^* - (\delta')^* + R)^{(h(ID_1^*) - h(ID'^*_1))^{-1}}$$

However, we know that it is difficulty of solving the CDH problem. This fully demonstrates our improved scheme is secure. □

4.5 Security Evaluation

In VANET, digital signature is an important tool to provide message authentication and source authentication. To achieve secure authentication, a basic condition is that the adopted digital signature must be able to achieve adaptive unforgeability. It makes that the sender can deny the sent message. At the same time, a secure authentication protocol must resist forgery attack, replay attack, and so on. In [4], Lee et al. showed that Zhang et al.'s scheme [15] exists replay attack and can not achieve non-repudiation in the batch verification. They includes time-stamp and a short vector to prevent replay attack and achieve non-repudiation. However, their scheme results in more serious security problems. The adopted digital signature is secure in Lee et al.'s scheme, any one can produce a forged signature. Thus, Lee et al.'s scheme cannot achieve resisting replay attacking, non-repudiation and tracing. In our scheme, we overcome the above security flaws and provide stronger security. In Table II, we compare our scheme with Lee *et al.*s' scheme [4] and Zhang et al.'s scheme [15] in terms of security. From Table II, we can know that our improved is securer than Lee *et al.*'s scheme and Zhang *et al.*'s scheme.

4.6 Performance Analysis

Efficiency of verifying a signature is a very important factor in the authentication protocol of VANET. It determines time which the vehicles responds to emergency message. In the following, we evaluate the performance of the improved scheme in terms of verification delay.

For convenience,we define the time cost of the cryptographic operations required in each verification. Let T_{mul} be the time to compute one point multiplication over an elliptic curve, T_{m2p} be the time of a MapToPoint hash function, and T_e be the time of computing a pairing operator. Because the above three operators are more time-consuming than the other operators, we only consider these operations. In our experiment, we adopt the MNT curve [3, 15, 16] which embeds degree $k = 6$ and 160-bit q, running on an Intel Pentium IV 3.0 GHZ machine. By experiment, the following results are obtained: T_{mul} is 0.6ms, T_{m2p} is 0.6ms and T_{par} is 4.5ms.

Next, we compare our improved scheme with Lee *et al.*s' scheme [4] and Zhang et al.'s scheme [15] in terms of the verification delay. Table III shows the computational time of the three signature schemes in terms of verifying a single signature and n signatures, respectively. Like Lee et al.'s scheme [4], our scheme doesn't consider $Vec_i\delta_i$, $Vec_iID_1^i$ and $Vec_ih(M_i)h_2(ID_1^i||ID_2^i||T_i)$ since Vec_i is very small, such as $Vec_i \in [1, 9]$, and the cost of Vec_is computation is negligible.

According to DSRC transmission protocol, a vehicle sends a safety related message every 100-300 ms. And the transmission range of a vehicle is around 300m. We consider the number of signatures to be verified in 300 ms. When utilizing the results of the MNT curve and the

Table 2: Comparisons of security in three signature schemes

	Batch verification	replaying attack	non-repudiation of simple message	non-repudiation of batch message	Tracing
Zhang et al.'s scheme	✓	✓	✓	×	×
Lee et al.'s scheme	✓	✓	×	×	×
Our scheme	✓	×	✓	✓	✓

Table 3: Comparisons of verifying time of the three signature schemes

	Verifying a single signature	Verifying n signatures
Zhang et al.'s scheme	$3T_e + T_{m2p} + T_{mul}$	$3T_e + nT_{m2p} + nT_{mul}$
Lee et al.'s scheme	$3T_e + T_{mul}$	$3T_e + T_{mul}$
Our scheme	$3T_e + 2T_{mul}$	$3T_e + 2T_{mul}$

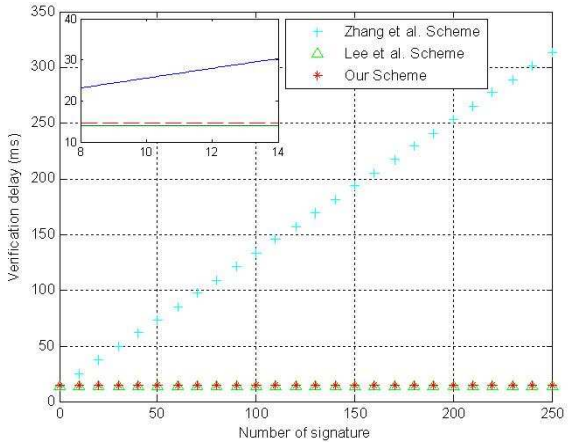

Figure 2: Influence on the batch verification delay in three schemes

value of performance comparison to estimate the effect on the batch verification, Fig 2 shows the relationship between the verification delay and the number of vehicles in three schemes. The embedded small figure is a local zoom-in with verifying signature numbers ranging from 0 to 5. From Figure 2, we can observe that the verification delay in our scheme is almost completely same as ones in Lee et al.'s scheme.

5 Conclusion

In this paper, we first analyze the security of Lee et al.'s scheme and show that their scheme exists a serious security issue. It can not only exist replay attack and repudiation attack, but also achieve trace the real identity of malicious sender. To overcame the weaknesses of Lee et al.'s scheme, we proposed an improved authentication scheme with batch verification for VANET, which can maintain the same efficiency as Lee et al.'s scheme. At the same time, it can also achieve resist replay attack and repudiation attack, and realize the traceability of malicious vehicle. In the future, we would like to further enhance the features of batch scheme for VANET, such as identifying illegal signatures, designing new schemes in order to gain more efficiency.

Acknowledgments

This study is supported by beijing natural science foundation (no:4122024), and the nova programma (no:2007b-001) and beijing natural science foundation programm and scientific research key program of beijing municipal commission of education (no:kz2008 10009005).

References

[1] "Dedicated short range communications (dsrc),". http://grouper.ieee.org/groups/scc32/dsrc/index.html.

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

[3] K. Karabina and E. Teske, "On prime-order elliptic curves with embedding degrees k = 3, 4, and 6," in *The 8th International Conference on Algorithmic Number Theory*, LNCS 5011, pp. 102–117, Springer-Verlag, 2008.

[4] C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for vanet," *Wireless Networks*, vol. 18, no. 2, pp. 61–70, 2012.

[5] J. Li and S. Wang, "New efficient proxy blind signature scheme using verifiable self-certified public key," *International Journal of Network Security*, vol. 4, no. 2, pp. 193–200, 2007.

[6] X. Lin, X. Sun, P. H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[7] F. Picconi and M. Gruteser, "Probabilistic validation of aggregated data in vehicular ad hoc networks," in *ACM VANET 2006*, pp. 76–85, 2006.

[8] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, pp. 361–396, 2000.

[9] M. Raya, A. Aziz, and J. P. Hubaux, "Efficient secure aggregation in VANETs," in *Proceedings of International workshop on Vehicular Ad Hoc Networks*, pp. 67–75, 2006.

[10] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[11] M. Stanek, "A note on security protocol for multicast communications," *International Journal of Network Security*, vol. 14, no. 1, pp. 59–60, 2012.

[12] A. Wasef and X. Shen, "ASIC: Aggregate signatures and certificates verification scheme for vehicular networks," in *Proceedings of GLOBECOM '09*, pp. 4489–4494, 2009.

[13] S. Wu and Y. Zhu, "Proof of forward security for password-based authenticated key exchange," *International Journal of Network Security*, vol. 7, no. 3, pp. 335–341, 2008.

[14] Z. Yong, M. Jianfeng, , and S. Moon, "An improvement on a three-party password-based key exchange protocol using weil pairing," *International Journal of Network Security*, vol. 11, no. 1, pp. 14–19, 2010.

[15] C. Zhang, P. H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, no. 8, pp. 1851–1865, 2011.

[16] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "APPA: Aggregate privacy-preserving authentication in vehicular ad hoc networks," in *The 14th Information Security Conference (ISC 2011)*, LNCS 7001, pp. 293–308, Springer-Verlag, 2011.

[17] Z. M. Zhao, "ID-based weak blind signature from bilinear pairings," *International Journal of Network Security*, vol. 7, no. 2, pp. 265–268, 2008.

[18] H. Zhu, X. Lin, R. Lu, P. Ho, and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in *IEEE ICC 2008*, pp. 1436–1440, 2008.

Jianhong Zhang received his Ph.D. degrees in Cryptography from Xidian University, Xian, Shanxi, in 2004 and his M.S. degree in Computer Software from Guizhou University, Guiyang, Guizhou, in 2001. He was engaging in postdoctoral research at Peking University from October 2005 to December 2007. He has been an Assistant Processor of College of Sciences, North China University of Technology, Beijing China, since 2001. His research interests include computer networks, cryptography, electronic commerce security, computer software.

Min Xu received the MS. in Mathematics and Education from Hebei Normal University in 2004. She is now an Associate Professor in College of Science, Baoding University, Baoding, China. She has published more than 30 papers in international conferences and journals. His research interest includes applied mathematics, education theory and multimedia processing.

Liying Liu received the MS. in Mathematics from Hebei University in 2004. She is now an Associate Professor in College of Science, Handan University, Handan, China. She has published more than 10 papers in international conferences and journals. His research interest includes applied mathematics, economic mathematics, computer software and multimedia processing.