Tsinghua Science and Technology

Volume 21 | Issue 6 Article 4

2016

Efficient Conditional Privacy-Preserving and Authentication Scheme for Secure Service Provision in VANET

Hong Zhong
School of Computer Science and Technology, Anhui University, Hefei 230601, China.

Jingyu Wen
School of Computer Science and Technology, Anhui University, Hefei 230601, China.

Jie Cui
School of Computer Science and Technology, Anhui University, Hefei 230601, China.

Shun Zhang
School of Computer Science and Technology, Anhui University, Hefei 230601, China.

Recommended Citation

Hong Zhong, Jingyu Wen, Jie Cui et al. Efficient Conditional Privacy-Preserving and Authentication Scheme for Secure Service Provision in VANET. Tsinghua Science and Technology 2016, 21(6): 620-629.

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 04/09 pp620-629
Volume 21, Number 6, December 2016

Efficient Conditional Privacy-Preserving and Authentication Scheme for Secure Service Provision in VANET

Hong Zhong, Jingyu Wen, Jie Cui*, and Shun Zhang

Abstract: Vehicle Ad hoc NETworks (VANET) can enhance traffic safety and improve traffic efficiency through cooperative communication among vehicles, roadside infrastructure, and traffic management centers. To guarantee secure service provision in VANET, message authentication is important. Moreover, a vehicle user's private information can also be leaked during service provision. A protection mechanism is needed to prevent such leakage. Therefore, we propose a conditional privacy-preserving and authentication scheme for secure service provision in VANETs. The proposed scheme not only satisfies the security requirements of VANETs, but also optimizes the calculation process of signature generation and verification. We carry out a detailed comparative analysis. The result shows that the proposed scheme is more efficient than existing schemes in terms of communication overhead and computational cost. Therefore, our scheme is suitable for secure service provision in VANETs.

Key words: VANET; message authentication; batch verification; privacy-preserve; elliptic curve

1 Introduction

In the 21st century, with the development of industrial technology and advancement of human civilization, vehicles have become an indispensable part of transportation and are used by most people. Vehicles, such as private cars, police cars, ambulances, trucks, and buses, are spread all over the traffic roads in cities. However, rapid growth in the number of vehicles has created many problems such as increasingly frequent traffic accidents and traffic congestion during the rush hour in major cities, and increased difficulty of traffic management. To solve these problems, researchers have been focusing on vehicle networks and intelligent transportation systems. A Vehicle Ad hoc NETwork (VANET) is constructed by equipping each vehicle with an OnBoard Unit (OBU) for wireless communication and deploying RoadSide Units (RSUs) along the road and at street intersections. A VANET can achieve cooperative communication between vehicles and RSUs and can thus be helpful for enhancing traffic safety, optimizing traffic efficiency, and improving traffic management.

A VANET is a special Mobile Ad hoc NETwork (MANET)[1], in which communications for service provision are divided into two kinds of types: Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Communication between two vehicles has the characteristics of mobile ad-hoc networks that are constantly self-configuring and do not require participation of the network infrastructure. Such communication adopts the Dedicated Short-Range Communication (DSRC) protocol[2]. An OBU broadcasts beacons such as traffic-related information and vehicle status to the network at intervals of 100–300 ms, including current vehicle position, speed, and traffic status.

• Hong Zhong, Jingyu Wen, Jie Cui, and Shun Zhang are with School of Computer Science and Technology, Anhui University, Hefei 230601, China. E-mail: zhongh@ahu.edu.cn; Eskimo4@outlook.com; cuijie@mail.ustc.edu.cn; shzhang27@163.com.

∗ To whom correspondence should be addressed.

Manuscript received: 2016-06-21; revised: 2016-07-26; accepted: 2016-08-01

Owing to the nature of wireless communication, communication for service provision in wireless networks is vulnerable to various attacks such as eavesdropping, tampering, and forgery. Many researchers have worked on secure authentication in various types of wireless networks, such as Wireless Body Area Networks (WBAN) and Wireless Mesh Networks (WMN)[3, 4]. The variety of security threats existing in VANETs cannot be ignored[5]. If a malicious adversary can spread false messages in a VANET, it could be a threat to the interests of vehicle drivers and to traffic safety. Therefore, communication messages should be authenticated securely in a VANET, and other traffic-related operations should be performed from the viewpoint of ensuring message integrity and reliability, which requires that each OBU or RSU authenticate message contents and identify its sender when receiving a message to prevent a malicious third-party from damaging the VANET communication system. In addition, there is the risk of leakage of vehicle users' private information in the communication process, such as user identity, electronic license plate, and traffic routes. To avoid the abovementioned situations, secure authentication schemes for VANETs should also provide privacy preservation[6]. Effective protection of vehicle users' privacy can encourage people to join VANETs and promote the development and application of VANET traffic systems.

In recent years, several authentication schemes have been proposed for secure service provision in VANETs. Although previously proposed authentication schemes could solve a few of the security issues in VANETs, they are not completely safe[7–12]. Moreover, the performance of these previous schemes is not adequate to satisfy the communications, requirements of VANETs. Therefore, we propose an efficient conditional privacy-preserving and secure authentication scheme for a VANET in this paper. The main contributions of this paper are summarized as follows.

- First, we propose a secure authentication scheme for VANET. The proposed scheme employs pseudonym-based signatures for identity authentication. Moreover, we use batch verification to improve computational efficiency of the scheme.
- Then, we perform a rigorous security analysis to show that our scheme can withstand various attacks and satisfy the security requirements of VANETs.
- Finally, we evaluate the performance of our scheme in terms of computation cost and communication overhead. Our scheme is more suitable for service provision in VANETs than the existing schemes.

2 Related Work

Secure authentication schemes in VANETs are divided into three types: (1) public key certificate schemes based on Public Key Infrastructure (PKI); (2) group signature-based authentication schemes; and (3) signature authentication schemes based on identities and pseudonyms. Raya and Hubaux[7] proposed a secure communication scheme based on PKI in 2007, in which each vehicle must pre-store a large number of public and private key pairs. A vehicle randomly selects a pair of public and private keys at regular intervals, of which the private key is used to sign transmitted traffic-related messages, while the public key is used to authenticate messages by the receiver. Although this scheme can achieve secure message authentication and protect a vehicle's identity privacy, the public key certificate in the message creates an extra non-negligible communication overhead, and considerable storage space is required in each OBU to store the public and private key pairs. In addition, the traffic management center must store anonymous certificates of all vehicles, which makes it difficult to manage vehicles and increases system operation overhead.

In the same year, Lin et al.[8] used group signature to design an authentication scheme. Several vehicles compose one group in a VANET, and each vehicle in the group has its own private key and a public key shared with all group members. Vehicles sign messages with their own private key, and message receivers can use the public key to verify message reliability and integrity. Moreover, confidentiality of the private key protects the identity of the sender vehicle. However, the high speeds of moving vehicles and the fast-changing network topology of a VANET create difficulties in group manager selection and dynamic group member management. Furthermore, the group signature is much longer than a normal signature, which increases the communication overhead and computation cost associated with signature verification.

Zhang et al.[9, 10] proposed an Identity-Based Verification (IBV) scheme for VANETs in 2008. Shamir[11] first proposed an identity-based signature and encryption system in 1984, in which identity information such as name and telephone number are used as the user's public key, while a trusted third-party uses identity information to generate private keys and distribute them to users. The message sender uses its private key to sign messages, and the recipients verify message security and reliability by using the sender's public key. Zhang et al.'s IBV scheme[9, 10] uses signatures based on vehicle users' identities; thus, the OBU does not need to store large amounts of public and private key pairs and the corresponding certificates. Therefore, the scheme reduces communication and computation costs, in addition to eliminating the need for certificate management. Zhang et al.'s scheme[9, 10] supports batch verification for multiple messages received by an OBU and an RSU, thus improving the efficiency of message authentication in scenarios with high vehicle density. In addition, the real identity of users is not disclosed in the communication process, that is, that any other vehicle, RSU, or malicious attacker cannot derive identity information of the sender from the communication messages. However, trusted authorities, for example, the traffic management department, can determine the real identity of the message sender based on communication messages in the event of traffic accidents or disputes, thus preserving privacy.

However, Lee and Lai[12] pointed out two flaws in Zhang et al.'s scheme[9, 10]. First, the scheme cannot resist the replay attack. A malicious vehicle or attacker can intercept and store communication messages in a VANET and then spread them across the network after a certain time to achieve any malicious purpose. Second, the scheme cannot achieve non-repudiation. Malicious vehicles or attackers broadcast false messages but deny this behavior to escape responsibility in the trace process of trusted authorities. In 2013, Lee and Lai[12] proposed an improved scheme to enhance security and achieve much better efficiency.

In 2015, Horng et al.[13] found a few security holes in Lee and Lai's[12] scheme. First, the real identity of the message sender can be obtained by other vehicles or third parties, so the scheme does not satisfy the requirements of privacy preservation. Second, the scheme is vulnerable to forgery attacks. An attacker can impersonate a legitimate vehicle to broadcast messages cross a VANET, but this illegal behavior cannot be traced back to the attacker's identity by the trusted authority, which means the scheme cannot achieve unforgeability and non-repudiation. Then, Horng et al.[13] proposed an improved IBV scheme that not only fulfills the security requirements of VANETs but is also more efficient in terms of computation and communication costs. Recently, Bayat et al.[14] and He et al.[15] proposed improved security authentication schemes on the basis of Lee and Lai's scheme[12]. However, the signature and verification processes of their schemes require complex cryptography operations, leading to excessive computation cost, which turns into a network bottleneck easily in scenarios with high vehicle density, traffic congestion, and high communication traffic in city centers.

3 Preliminaries

In this section, we introduce the system model, security requirements, and a few mathematical tools for VANETs.

3.1 System model

A VANET system consists of three main entities, namely, OBU, RSU, and Trusted Authority (TA), as shown in Fig. 1.

Detailed descriptions of each part shown in Fig. 1 are given below.

(1) OBU: The OBU is installed on each vehicle, and it uses the 802.11P protocol to communicate with surrounding vehicles or RSUs. According to the 802.11P protocol, an OBU broadcasts a traffic-related beacon message at intervals of 100–300 ms. Moreover, OBUs can provide transportation-related information to vehicle drivers, such as a map of the surrounding roads, information about the nearest gas station, and traffic congestion conditions.

(2) RSU: As base stations, RSUs are deployed on both sides of roads or intersections. An RSU is responsible for managing the communications of all OBUs within its range, usually 300–500 m. In addition,

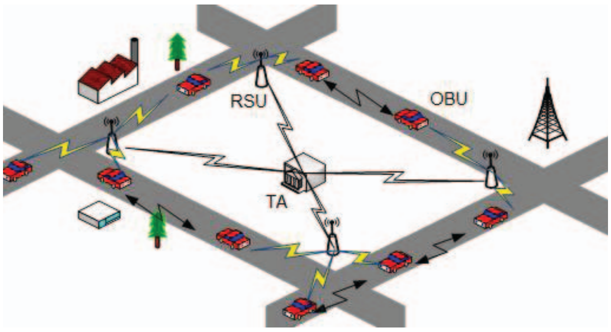


Fig. 1 System model.

RSUs communicate with other RSUs and with the trusted authority in a VANET through a secure channel of wired networks. For example, an RSU can report traffic accidents in the city and so on to the trusted authority.

(3) TA: The TA is a VANET system management center in charge of issue system parameters, vehicle registration, vehicle management, and traceability. The TA is usually deployed in the traffic management department. Therefore, in our system, the TA is completely credible, while OBUs and RSUs are semi-credible. In the proposed scheme, communications can be either V2V or V2I. This means that the message sender is a vehicle, while the message receiver can be a vehicle or an RSU. We assume that the clocks of all devices are synchronized in our system.

3.2 Security requirements

A VANET security authentication scheme should have the following characteristics.

(1) Message authentication: In VANET communication, a message recipient should be sure that a message is indeed from a legitimate user and has not been tampered with by any third party.

(2) Identity privacy preservation: Any other vehicles, RSUs or malicious attackers should not be able to discern a vehicle's identity information from the messages it transmits.

(3) Traceability: The TA should be able to the real identity of a message sender from a message when necessary. For example, if an attacker or a malicious vehicle attempts to distribute illegal information in the network, the TA should be able to trace their identity and take corresponding measures in time.

(4) Unlinkability: An attacker should not be able to recognize whether two or more messages are from the same vehicle.

(5) Non-repudiation: When the TA traces a message sender's identity, the vehicle should not be able to deny that it has sent the message to the network.

(6) Various attacks resistance: The authentication scheme for a VANET should be able to withstand a variety of network attacks such as replay attacks and Sybil attacks.

3.3 Mathematical tools

Elliptic curve cryptography was proposed by Miller[16] in 1985, and since then, it has been used widely to design digital signatures and security algorithms. We assume F_n denotes a finite field, E represents an elliptic curve defined by the equation $y^2 = x^3 + ax + b \bmod n$ based on the finite field F_n, where n is a large prime number and $a, b \in F_n$. Suppose O is an infinite point, and G is a cyclic additive group based on all points on the elliptic curve E and point O. Let q and P be the order and generator of group G, respectively.

Point addition in G is defined as follows. Assume P and Q are two points on the elliptic curve E. Let L be the connecting line between P and Q or a line tangential to curve E if $P = Q$. L intersects E at point R. Then, the addition of P and Q can be expressed as $P + Q = -R$. Scalar point multiplication in G is defined as $mP = P + P + \cdots + P$, which is equivalent to performing m repetitions of the addition operation on P, where $m \in \mathbf{Z}_n, m > 0, P \in G$.

The Discrete Logarithm Problem (DLP) of an elliptic curve[17] is computationally difficult. Given two points P and Q in an additive group G based on an elliptic curve, the task of DLP is to find an integer x satisfying $Q = xP$.

4 Proposed Scheme

In this section, we introduce our security authentication scheme for VANET. The proposed scheme can be used for both V2V and V2I communication. Our scheme not only protects a vehicle user's identity but also ensures secure exchange of traffic-related messages. The scheme is divided into three main phases: system initialization, pseudonym and key generation, and message signing and verification. Table 1 lists the notations used in this paper.

4.1 System initialization

In the system initialization phase, the TA first generates system parameters. Then, the TA chooses an additive group G of order q on the elliptic curve $y^2 = x^3 + ax + b \bmod n$ and its generator P. Then, the TA randomly selects an integer $s \in \mathbf{Z}_q^*$ as the system private key and generates the following public key $P_{\text{Pub}} = sP$. Thereafter, it selects three secure one-way hash functions $h : \{0,1\}^* \rightarrow \mathbf{Z}_q^*$, $h_1 : \{0,1\}^* \rightarrow \mathbf{Z}_q^*$, $h_2 : \{0,1\}^* \rightarrow \mathbf{Z}_q^*$.

The trusted authority preloads the system's public parameters $\{G, q, P, P_{\text{Pub}}, h, h_1, h_2\}$ into the OBU of each registered vehicle and into all RSUs deployed on the road. In the register phase, the TA preloads the system private keys, vehicles' real identity (RID), and Tamper-Proof Device (TPD) password (PWD) into each

Table 1 Notations used in this paper.

Notation	Description
TA	A trusted authority
RSU	Roadside unit
OBU	Onboard unit
G	Cycle additive group based on elliptic curve
P	A generator of G
q	Order of G
s	Private key of TA
P_{Pub}	Public key of TA
RID	Vehicle's real identity
PWD	Password of TPD on vehicle
r	A random number
ID	Vehicle's pseudonym identity
h_1, h_2, h_3	Three secure one-way hash function
SK	Vehicle's private key
M	Traffic-related message
σ	Signature of the message M
T	A timestamp
$\oplus$	Exclusive-OR operation
$\parallel$	Concatenation operation

vehicle's TPD.

4.2 Pseudonym and key generation

When a vehicle joins a VANET, the tamper-proof device in the vehicle starts executing the pseudonym and key generation phase as follows. Figure 2 shows the message authentication procedure employed in the proposed scheme.

(1) A vehicle user inputs his real identity RID and tamper-proof device password PWD into the TPD. The TPD checks whether RID and PWD are equal to the corresponding stored values; if yes, the TPD executes the subsequent steps for the vehicle user.

(2) The TPD chooses a random number $r \in \mathbf{Z}_q^*$ and calculates $\text{ID}_1 = rP, \text{ID}_2 = \text{RID} \oplus h(r \cdot P_{\text{Pub}})$. The pseudonym ID is determined as $\text{ID} = (\text{ID}_1, \text{ID}_2)$.

(3) The TPD computes a key $\text{SK} = sh_1(\text{ID}_1 \| \text{ID}_2)$ and stores the tuple $\{r, \text{ID}, \text{SK}\}$ in its memory.

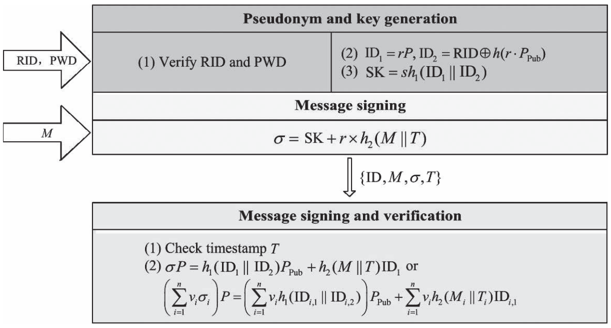

RID, PWD
Pseudonym and key generation
(1) Verify RID and PWD
(2) $\text{ID}_1 = rP, \text{ID}_2 = \text{RID}\oplus h(r \cdot P_{\text{Pub}})$
(3) $\text{SK} = sh_1(\text{ID}_1 \parallel \text{ID}_2)$
M
Message signing
$\sigma = \text{SK} + r \times h_2(M \parallel T)$
$\{\text{ID}, M, \sigma, T\}$
Message signing and verification
(1) Check timestamp T
(2) $\sigma P = h_1(\text{ID}_1 \parallel \text{ID}_2)P_{\text{Pub}} + h_2(M \parallel T)\text{ID}_1$ or
$\left(\sum_{i=1}^{n} v_i\sigma_i\right)P = \left(\sum_{i=1}^{n} v_i h_1(\text{ID}_{i,1} \parallel \text{ID}_{i,2})\right)P_{\text{Pub}} + \sum_{i=1}^{n} v_i h_2(M_i \parallel T_i)\text{ID}_{i,1}$

Fig. 2 Message authentication procedure.

4.3 Message signing and verification

(1) When an OBU needs to send a message M, it inputs M to the TPD. Then, the TPD uses its stored tuple $\{r, \text{ID}, \text{SK}\}$ to generate signature $\sigma = \text{SK} + r \times h_2(M \| T)$, where T is the current timestamp and σ is the signature of message M. TPD outputs $\{\text{ID}, M, \sigma, T\}$ to the OBU, and then, OBU sends them to the network.

(2) After one OBU or RSU receives the message $\{\text{ID}, M, \sigma, T\}$, it first checks the validity of timestamp T. Suppose T_{rec} is the time at which the message is received, and ΔT is the predefined endurable transmission delay. If $\Delta T > T_{\text{rec}} - T$, the timestamp is valid, and the recipient continues verifying the message according to the following equation.

$$\sigma P = h_1(\text{ID}_1 \parallel \text{ID}_2)P_{\text{Pub}} + h_2(M \parallel T)\text{ID}_1 \qquad (1)$$

If the equation holds, the signature is deemed valid and legal, and the recipient is clear to accept the message; else, the recipient rejects the message.

(3) In the case of frequent traffic message communication, an OBU or RSU will receive a large number of messages that would be required to be verified in a very short time. This requires our scheme to support batch verification of messages, as described below.

When a recipient receives multiple messages $\{\text{ID}_i, M_i, \sigma_i, T_i\}$ $(1 < i < n)$, it first validates the timestamp of each message. Messages with invalid timestamps are rejected by the recipient. To ensure non-repudiation of batch verification, we use the small exponent test technology. The message recipient chooses a random vector $\boldsymbol{v} = \{v_1, v_2, \ldots, v_n\}$, where $v_i \in [1, 2^t]$ and t is a small integer that does not increase computational cost considerably. Then, the recipient verifies the following equation.

$$\left(\sum_{i=1}^{n} v_i\sigma_i\right)P = \left(\sum_{i=1}^{n} v_i h_1(\text{ID}_{i,1} \parallel \text{ID}_{i,2})\right)P_{\text{Pub}} + \sum_{i=1}^{n} v_i h_2(M_i \parallel T_i)\text{ID}_{i,1} \qquad (2)$$

If the equation holds, the messages are considered legitimate and can be accepted.

5 Analysis and Comparison

In this section, we analyze the proposed scheme and give proof of its security, in addition to comparing it with several existing schemes in terms of computation cost and communication overhead. The results illustrate that our scheme is adequately secure for use in VANETs, and reduces computation cost and communication overhead.

5.1 Security proof

The security model of the proposed scheme is established on a game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ based on the adversary's ability and the network model of VANET.

Theorem 1 The proposed secure authentication scheme for VANET is able to enforce non-forgery of messages under adaptive chosen message attack in the random oracle model.

Proof Suppose there is an adversary $\mathcal{A}$ who can forge a legitimate message $\{\mathrm{ID}_i, M_i, \sigma_i, T_i\}$. Then, we construct another challenger $\mathcal{C}$ to solve the DLP with a non-negligible probability by running $\mathcal{A}$ as a subroutine. Given an instance $(P, Q = xP)$ of DLP, $\mathcal{C}$ executes the following steps.

Initialization: Challenger $\mathcal{C}$ sets $P_{\mathrm{Pub}} = Q = xP$ as a system public key and generates public parameters para $= \{G, q, P, P_{\mathrm{Pub}}, h, h_1, h_2\}$. Then, $\mathcal{C}$ constructs and maintains three lists L_h, L_{h_1}, and L_{h_2}.

h-Oracle: $\mathcal{C}$ maintains list L_h in the form $\langle \alpha, \tau_h \rangle$ and list L_h is initialized to empty. Upon receiving a query from $\mathcal{A}$ with the message α, $\mathcal{C}$ checks whether the tuple $\langle \alpha, \tau_h \rangle$ is in the list first. If so, $\mathcal{C}$ sends $\tau_h = h(\alpha)$ to $\mathcal{A}$; else, $\mathcal{C}$ selects $\tau_h \in \mathbf{Z}_q^*$ randomly and adds $\langle \alpha, \tau_h \rangle$ to the list. Then, $\mathcal{C}$ sends $\tau_h = h(\alpha)$ to $\mathcal{A}$.

h_1-Oracle: $\mathcal{C}$ maintains list L_{h_1} of the form $\langle \mathrm{ID}_1, \mathrm{ID}_2, \tau_{h_1} \rangle$ and list L_{h_1} is initialized to empty. Upon receiving a query from $\mathcal{A}$ with the message $(\mathrm{ID}_1, \mathrm{ID}_2)$, $\mathcal{C}$ first checks whether the tuple $\langle \mathrm{ID}_1, \mathrm{ID}_2, \tau_{h_1} \rangle$ is in the list. If yes, $\mathcal{C}$ sends $\tau_{h_1} = h_1(\mathrm{ID}_1 \parallel \mathrm{ID}_2)$ to $\mathcal{A}$; otherwise, $\mathcal{C}$ selects $\tau_{h_1} \in \mathbf{Z}_q^*$ randomly and adds $\langle \mathrm{ID}_1, \mathrm{ID}_2, \tau_{h_1} \rangle$ to the list. Then, $\mathcal{C}$ sends $\tau_{h_1} = h_1(\mathrm{ID}_1 \parallel \mathrm{ID}_2)$ to $\mathcal{A}$.

h_2-Oracle: $\mathcal{C}$ maintains a list L_{h_2} of the form $\langle M, T, \tau_{h_2} \rangle$ and list L_{h_2} is initialized to empty. Upon receiving a query from $\mathcal{A}$ with the message (M, T), $\mathcal{C}$ first checks whether the tuple $\langle M, T, \tau_{h_2} \rangle$ is in the list. If yes, $\mathcal{C}$ sends $\tau_{h_2} = h_2(M \parallel T)$ to $\mathcal{A}$; otherwise, $\mathcal{C}$ selects $\tau_{h_2} \in \mathbf{Z}_q^*$ randomly and adds $\langle M, T, \tau_{h_2} \rangle$ to the list. Then, $\mathcal{C}$ sends $\tau_{h_2} = h_2(M \parallel T)$ to $\mathcal{A}$.

Sign-Oracle: When $\mathcal{C}$ receives a query from $\mathcal{A}$ with the message M, $\mathcal{C}$ generates three random numbers $\sigma, h_{i,1}, h_{i,2} \in \mathbf{Z}_q^*$. Then, $\mathcal{C}$ selects a random point $\mathrm{ID}_2 \in G$ and calculates $\mathrm{ID}_1 = (\sigma P - h_{i,1} P_{\mathrm{Pub}})/h_{i,2}$. $\mathcal{C}$ adds the tuple $\langle \mathrm{ID}_1, \mathrm{ID}_2, h_{i,1} \rangle$ to list L_{h_i} and adds $\langle M, T, h_{i,2} \rangle$ to list L_{h_2}. Finally, $\mathcal{C}$ constructs a message $\{\mathrm{ID}, M, \sigma, T\}$ and sends it to $\mathcal{A}$, where $\mathrm{ID} = (\mathrm{ID}_1, \mathrm{ID}_2)$. It can be checked that the message satisfies the following equation.

$$\sigma P = h_{i,1} P_{\mathrm{Pub}} + h_{i,2} \mathrm{ID}_1 = \\ h_{i,1} P_{\mathrm{Pub}} + (\sigma P - h_{i,1} P_{\mathrm{Pub}}) = \sigma P \tag{3}$$

So the message and signature $\{\mathrm{ID}, M, \sigma, T\}$, which $\mathcal{A}$ obtained from the query, is valid.

Output: At last, $\mathcal{A}$ outputs a message $\{\mathrm{ID}, M, \sigma, T\}$. $\mathcal{C}$ verifies the message by the following equation.

$$\sigma P = h_{i,1} P_{\mathrm{Pub}} + h_{i,2} \mathrm{ID}_1 \tag{4}$$

If it does not hold, $\mathcal{C}$ terminates the game process. According to the forking lemma[12], if $\mathcal{A}$ chooses a different h_1-query, $\mathcal{A}$ can output another valid message $\{\mathrm{ID}, M, \sigma', T\}$ that satisfies $\sigma' P = h'_{i,1} P_{\mathrm{Pub}} + h_{i,2} \mathrm{ID}_1$.

Based on the above two equations, we can obtain

$$(\sigma - \sigma')P = \sigma P - \sigma' P = h_{i,1} P_{\mathrm{Pub}} - h'_{i,1} P_{\mathrm{Pub}} = \\ (h_{i,1} - h'_{i,1}) P_{\mathrm{Pub}} = (h_{i,1} - h'_{i,1}) xP \tag{5}$$

Then, we can get $\sigma - \sigma' = (h_{i,1} - h'_{i,1}) \cdot x \bmod n$.

$\mathcal{C}$ outputs $(\sigma - \sigma') \cdot (h_{i,1} - h'_{i,1})^{-1}$ as a solution of the given DLP instance. However, DLP is a difficult problem to solve. Therefore, the proposed scheme is resistant to message forgery under adaptive chosen message attack in the random oracle model. ■

5.2 Security analysis

Here we continue to analyze the various security features of our scheme.

(1) Message authentication: According to Theorem 1, we have learned that an adversary cannot forge messages to meet the verification equation $\sigma P = h_1(\mathrm{ID}_1 \parallel \mathrm{ID}_2) P_{\mathrm{Pub}} + h_2(M \parallel T)\mathrm{ID}_1$ in the proposed scheme. Therefore, the message recipient can verify the validity and legality of message $\{\mathrm{ID}, M, \sigma, T\}$ by using the verification equation. Thus, the proposed scheme satisfies the message authentication requirement of VANETs.

(2) Identity privacy preservation: A vehicle's RID is hidden in a pseudonym ID generated by the TPD according to the equation $\mathrm{ID}_1 = rP$, $\mathrm{ID}_2 = \mathrm{RID} \oplus h(r \cdot P_{\mathrm{Pub}})$. According to DLP, no vehicle or attacker can calculate r or s from ID_1 and P_{Pub}. Therefore, any vehicle or attacker cannot obtain RID information even if the pseudonym $\mathrm{ID} = (\mathrm{ID}_1, \mathrm{ID}_2)$ is disclosed. Thus, the proposed scheme satisfies the identity privacy preservation requirement.

(3) Traceability: Although a vehicle's RID is hidden in a pseudonym, it can be calculated by the

equation $\mathrm{RID} = \mathrm{ID}_2 \oplus h(r \cdot P_{\mathrm{Pub}}) = \mathrm{ID}_2 \oplus h(s \cdot \mathrm{ID}_1)$ given that the system private key s is known. Therefore, in some special circumstances such as traffic accidents, the TA can obtain the vehicle's RID based on the pseudonym $\mathrm{ID} = (\mathrm{ID}_1, \mathrm{ID}_2)$ used in communication message $\{\mathrm{ID}, M, \sigma, T\}$, which illustrates that the proposed scheme provides traceability.

(4) Unlinkability: In the signing process of each message, because r is generated randomly during pseudonym calculation, the messages sent by a vehicle at each time contain a unique pseudonym that is different from others, and there is no relationship among different pseudonyms from the attacker's perspective. Moreover, the signature, too, is generated by using a random number r and a unique pseudonym. Therefore, an attacker cannot link two or more anonymous identities or signatures generated by the same vehicle from the messages sent by it. This means the proposed scheme achieves unlinkability.

(5) Non-repudiation: Once the TA has traced the RID of a communication message sent to the network, the message sender cannot deny its signature for this message. Moreover, in the batch verification of messages, we have used the random vector $\boldsymbol{v} = \{v_1, v_2, \ldots, v_n\}$, so an attacker cannot deny its signature in a message sent by exchanging signatures among several different messages[18].

(6) Replay resistance: In the message-signing process $\sigma = \mathrm{SK} + r \times h_2(M \parallel T)$, we use a current timestamp T so that any attacker cannot forge or modify the timestamp in a communication message. In the first step of signature verification, the message would be discarded immediately if the timestamp is expired or invalid. Therefore, the replay attack is ineffective in a network based on the proposed scheme.

5.3 Performance analysis and comparison

In this section, we evaluate the performance of the proposed scheme in terms of computation cost and communication overhead. In addition, we compare the performance of the proposed scheme with that of existing schemes.

5.3.1 Computation cost

In the schemes based on bilinear pairing, such as the ones in Horng et al.[13] and Bayat et al.[14], group G in the bilinear mapping $\hat{e} : G \times G \rightarrow G_T$ is generated based on the elliptic curve $y^2 = x^3 + x \mathrm{mod} n$, where n is a 512-bit prime number and the order q of G is a 160-bit prime number. While in the schemes based on Elliptic Curve Cryptography (ECC), such as the one in He et al.[15] and the proposed scheme in this paper, group G is generated on the elliptic curve $y^2 = x^3 + ax + b \mathrm{mod} n$ to achieve the same security level as in the schemes based on bilinear pairing, where both n and q are 160-bit prime numbers. We define a few major cryptographic operations that dominate the computation cost as follows[19]: T_{bp} denotes the time to execute a bilinear mapping operation. $T_{\text{mp-bp}}$ denotes the time required to perform a scalar point multiplication in a group based on bilinear pairing. $T_{\text{mp-ECC}}$ represents the time required for performing a scalar point multiplication in a group based on ECC. T_{mtp} denotes the time required for executing a hash function that maps a string to a point in group G, also called the MapToPoint operation. The execution times of each operation are as follows: $T_{\mathrm{bp}} = 4.211\,\mathrm{ms}$, $T_{\text{mp-bp}} = 1.709\,\mathrm{ms}$, $T_{\text{mp-ECC}} = 0.442\,\mathrm{ms}$, $T_{\mathrm{mtp}} = 4.406\,\mathrm{ms}$[15].

The communication process in a VANET can be divided into three phases: pseudonym and signature generation, signature verification, and batch verification of multiple signatures. We compare our scheme with schemes of Zhang et al.[20], Horng et al.[13], Bayat et al.[14], and He et al.[15] in term of computation costs in those three phases. Table 2 lists the comparison results.

In Horng et al.'s scheme[13], the calculation to generate pseudonym $\{\mathrm{AID}_{i,1}, \mathrm{AID}_{i,2}\}$ requires two scalar point multiplications and one MapToPoint operation. Then, signing a message using the pseudonym needs one scalar point multiplication operation. Thus, the entire pseudonym and signature generation phase requires $3T_{\text{mp-bp}} + T_{\mathrm{mtp}} = 9.553\,\mathrm{ms}$.

Table 2 Computation cost of each scheme.

Scheme	Pseudonym and signature generation phase	Signature verification phase	Batch verification phase of n signatures
Zhang et al.[20]	$6T_{\text{mp-bp}} + T_{\mathrm{mtp}}$	$3T_{\mathrm{bp}} + 2T_{\text{mp-bp}}$	$3T_{\mathrm{bp}} + (n+1)T_{\text{mp-bp}}$
Horng et al.[13]	$3T_{\text{mp-bp}} + T_{\mathrm{mtp}}$	$2T_{\mathrm{bp}} + T_{\text{mp-bp}}$	$2T_{\mathrm{bp}} + T_{\text{mp-bp}}$
Bayat et al.[14]	$5T_{\text{mp-bp}} + T_{\mathrm{mtp}}$	$3T_{\mathrm{bp}} + T_{\text{mp-bp}} + T_{\mathrm{mtp}}$	$3T_{\mathrm{bp}} + nT_{\text{mp-bp}} + nT_{\mathrm{mtp}}$
He et al.[15]	$3T_{\text{mp-ECC}}$	$3T_{\text{mp-ECC}}$	$(n+2)T_{\text{mp-ECC}}$
The proposed scheme	$2T_{\text{mp-ECC}}$	$3T_{\text{mp-ECC}}$	$(n+2)T_{\text{mp-ECC}}$

In single signature verification, it needs two bilinear mapping operations and one scalar point multiplication operation, so the computation cost is $2T_{\text{bp}} + T_{\text{mp-bp}} = 10.131$ ms. While in the verification of multiple signatures, due to batch verification and the small exponent test technology, the total computation cost to verify n signatures is still $2T_{\text{bp}} + T_{\text{mp-bp}} = 10.131$ ms.

In the signing calculation of the proposed scheme, pseudonym $\text{ID} = (\text{ID}_1, \text{ID}_2)$ and private key $\text{SK} = sh_1(\text{ID}_1 \parallel \text{ID}_2)$ generation only need two scalar point multiplication operations. The process of signature generation $\sigma = \text{SK} + r \times h_2(M \parallel T)$ does not need any scalar point multiplication. Therefore, the entire pseudonym and signature generation phase requires $2T_{\text{mp-ECC}} = 0.884$ ms. In signature verification, the single signature verification process $\sigma P = h_1(\text{ID}_1 \parallel \text{ID}_2)P_{\text{Pub}} + h_2(M \parallel T)\text{ID}_1$ needs three scalar point multiplications, that is, $3T_{\text{mp-ECC}} = 1.326$ ms. In batch verification of n signatures, the random vector $\boldsymbol{v} = \{v_1, v_2, \ldots, v_i\}$ of the small exponent test used in the proposed scheme only needs one v_i in a small range that would not produce excessive additional computation cost. As a result, the batch verification process $\left(\sum_{i=1}^{n} v_i\sigma_i\right)P = \left(\sum_{i=1}^{n} v_i h_1(\text{ID}_{i,1} \parallel \text{ID}_{i,2})\right)P_{\text{Pub}} + \sum_{i=1}^{n} v_i h_2(M_i \parallel T_i)\text{ID}_{i,1}$ needs only $(n+2)$ scalar point multiplication operations, such that the computation cost is $(n+2)T_{\text{mp-ECC}} = (0.442n + 0.884)$ ms. The other schemes compared herein can be analyzed with the same method.

Figure 3 shows the computation cost to sign and verify a single message in each scheme. Given that the cryptography-related operations are ECC-based, the proposed scheme has obvious advantages in terms of computation cost compared to Horng et al.'s[13] and Bayat et al.'s[14] schemes, which are based on bilinear pairing. Moreover, the proposed scheme is also improved in some ways compared to He et al.'s[15] scheme. Figure 4 shows the execution time for batch verification along with the growth of number of messages in each scheme. When 100 messages are to be verified, the total calculation time for batch verification in the proposed scheme is less than 50 ms. Therefore, the proposed scheme can satisfy the communication requirement of VANETs despite traffic congestion and heavy network throughput.

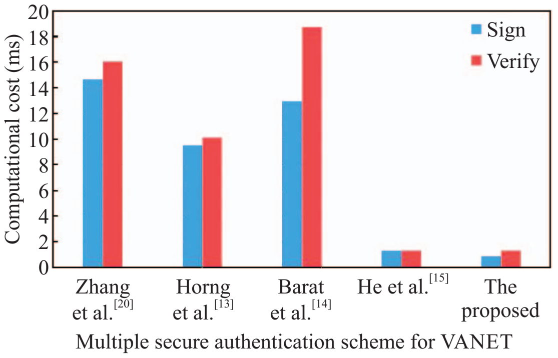


Fig. 3 Comparison of computation cost to sign and verify a single message.

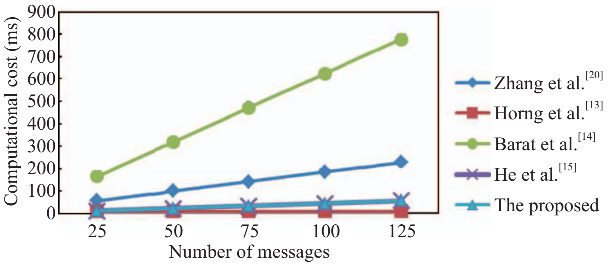


Fig. 4 Computation cost comparison of batch verification.

5.3.2 Communication overhead

In this section, we analyze the communication overhead of the proposed scheme. In the bilinear pairing-based group G_1, n of the elliptic curve $y^2 = x^3 + x \bmod n$ is a 512-bit prime number, so the size of each element in G_1 is 128 bytes[21]. In the ECC-based group G, n of the elliptic curve $y^2 = x^3 + ax + b \bmod n$ is a 160-bit prime number, and the size of each element in G is 40 bytes. We assume that the output of the one-way hash function and the timestamp are 20 bytes and 4 bytes, respectively[22], and the element in integer group $\mathbf{Z}_q^*$ is 20 bytes. The length of a vehicle's traffic-related message (for example, a beacon message) is not considered in the following comparisons[23]. The comparative results of various schemes are listed in Table 3.

Table 3 Comparison of communication overhead.

Scheme	Single message (byte)	n messages (byte)
Zhang et al.[20]	388	388n
Horng et al.[13]	388	388n
Bayat et al.[14]	280	280n
He et al.[15]	144	144n
The proposed scheme	84	84n

As listed in Table 3, the communication message $\{\mathrm{ID}, M, \sigma, T\}$ in Zhang et al.'s scheme[20] includes the pseudonym $\mathrm{ID}_1 \in G_1, \mathrm{ID}_2 \in G_1$ and signature $\sigma \in G_1$. Therefore, the length of a single message is $128\times\ 3 + 4 = 388$ bytes. When sending n messages needs n groups of pseudonyms, signatures and timestamps, so the total length is $388n$ bytes. Moreover, in He et al.'s scheme[15], the vehicle broadcasts anonymous identity and signature $\{\mathrm{AID}, T, R, \sigma\}$ to the verifier, where $\mathrm{AID} = \{\mathrm{AID}_1, \mathrm{AID}_2\}$. Because $\mathrm{AID}_1, \mathrm{AID}_2,\ R \in G, \sigma \in \mathbf{Z}_q^*$, and T is the timestamp, the communication cost of He et al.'s scheme[15] is $40 \times 3+\ 20 + 4 = 144$ bytes. Other schemes could be analyzed in the same way. In the proposed scheme, the length of the communication message, which includes pseudonym $\mathrm{ID}_1 \in G, \mathrm{ID}_2 \in \mathbf{Z}_q^*$ and signature $\sigma \in \mathbf{Z}_q^*$, is $40 + 20 \times 2 + 4 = 84$ bytes. Moreover, n messages need $84n$ bytes. Thus, the proposed scheme has considerably lower communication overhead compared to other schemes for VANET message transmission. Therefore, the proposed scheme is conducive to use the limited communication resources in a VANET efficiently.

6 Conclusion

In this paper, we proposed a conditional privacy-preserving authentication scheme for VANETs that considers the security of communication messages, vehicle users' privacy, and the computational power of vehicle nodes. The security analysis shows that the proposed scheme not only satisfies the security acquirements such as message authentication, non-repudiation, unlinkability, and replay resistance but also preserves the privacy of vehicles while ensuring they can be traced by the TA. Moreover, we prove that the proposed scheme can enforce non-forgery of messages under the adaptive chosen message attack in the random oracle model. The performance evaluation indicates that our scheme is more efficient than the existing schemes in terms of computation cost and communication overhead, which makes it more suitable for deployment in VANET services and applications. In the future, we will continue our research on secure communications for VANETs with a focus private key distribution and management.

Acknowledgment

The work was supported by the National Natural Science Foundation of China (Nos. 61572001 and 61502008), the Research Fund for the Doctoral Program of Higher Education (No. 20133401110004), the Natural Science Foundation of Anhui Province (No. 1508085QF132), and the Doctoral Research Start-up Funds Project of Anhui University. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

References

[1] S. Giordano, Mobile ad hoc networks, in *Handbook of Wireless Networks and Mobile Computing*, I. Stojmenović, ed. Wiley, 2002, pp. 325–346.

[2] J. B. Kenney, Dedicated short-range communications (DSRC) standards in the United States, *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[3] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, Anonymous authentication for wireless body area networks with provable security, *IEEE Systems Journal*, 2016. doi: 10.1109/JSYST.2016.2544805.

[4] P. Guo, J. Wang, B. Li, and S. Lee, A variable threshold-value authentication architecture for wireless mesh networks, *Journal of Internet Technology*, vol. 15, no. 6, pp. 929–936, 2014.

[5] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, Secure vehicular communication systems: Design and architecture, *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

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

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

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

[9] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, presented at the 27th Conference on Computer Communications, INFOCOM, 2008.

[10] 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.

[11] A. Shamir, Identity-based cryptosystems and signature schemes, *Lecture Notes in Computer Science*, vol. 196, pp. 47–53, 2000.

[12] C.-C. Lee and Y. Lai, Toward a secure batch verification with group testing for VANET, *Wireless Networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[13] S.-J. Horng, S.-F. Tzeng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, Enhancing security and privacy for identity-based batch verification scheme in VANET, *IEEE Trans. on Vehicular Technology*, 2015. doi: 10.1109/TVT.2015.2406877

[14] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, A secure authentication scheme for VANETs with batch verification, *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[15] D. He, S. Zeadally, B. Xu, and X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, *IEEE Trans. on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[16] S. V. Miller, Use of elliptic curves in cryptography, in *Conference on the Theory and Application of Cryptographic Techniques*, 1985, pp. 418–426.

[17] N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, *Journal of Cryptology*, vol. 12, no. 3, pp. 193–196, 1999.

[18] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, b-SPECS+: Batch verification for secure pseudonymous authentication in VANET, *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[19] D. He, N. Kumar, H. Shen, and J.-H. Lee, One-to-many authentication for access control in mobile pay-TV systems, *SCIENCE CHINA Information Sciences*, vol. 59, no. 5, pp. 1–14, 2016.

[20] J. Zhang, M. Xu, and L. Liu, On the security of a secure batch verification with group testing for VANET, *International Journal of Network Security*, vol. 16, no. 5, pp. 355–362, 2014.

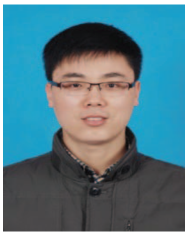
[21] X. Boyen and L. Martin, Identity-based cryptography standard (IBCS): Supersingular curve implementations of the BF and BB1 cryptosystems, No. RFC 5091, 2007.

[22] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato, Internet X. 509 public key infrastructure time-stamp protocol (TSP), http://tools.ietf.org/html/rfc3161, 2001.

[23] N.-W. Lo and J.-L. Tsai, An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings, *IEEE Trans. on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2016.

Hong Zhong is currently a professor (from 2009) and executive dean of School of Computer Science and Technology, Anhui University, China. She received the PhD degree from University of Science and Technology of China in 2005. Her research interests cover network and information security.

Jingyu Wen is currently a master student at School of Computer Science and Technology, Anhui University. He got the bachelor degree from University of Science and Technology of Anhui in 2013. His research interest is vehicle ad hoc network.



Jie Cui is now an associate professor at School of Computer Science and Technology, Anhui University. He received the PhD degree from University of Science and Technology of China in 2012. He has published over 30 papers. His research interests include network and information security.

Shun Zhang is now an associate professor at School of Computer Science and Technology, Anhui University. He received the PhD degree from Beijing Normal University in 2012. He has published over 10 papers. His research interest is information security.