This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

An Efficient Identity-based Conditional Privacy-preserving Authentication Scheme For Vehicular Ad-hoc Networks

Debiao He, Sherali Zeadally, Baowen Xu and Xinyi Huang

***Abstract*—By broadcasting messages about traffic status to vehicles wirelessly, a Vehicular Ad-Hoc Network (VANET) can improve traffic safety and efficiency. To guarantee secure communication in VANETs, security and privacy issues must be addressed before their deployment. The Conditional Privacy-Preserving Authentication (CPPA) scheme is suitable for solving security and privacy-preserving problems in VANETs because it supports both mutual authentication and privacy protection simultaneously. Many identity-based CPPA schemes for VANETs using bilinear pairings have been proposed over the last few years to enhance security or improve performance. However, it is well known that the bilinear pairing operation is one of the most complex operations in modern cryptography. To achieve better performance and reduce computational complexity of information processing in VANET, the design of a CPPA scheme for the VANET environment that does not use bilinear paring becomes a challenge. To address this challenge, we propose a CPPA scheme for VANETs that does not use bilinear paring and we demonstrate that it could supports both mutual authentication and privacy protection simultaneously. Our proposed CPPA scheme retains most of the benefits obtained with previously proposed CPPA schemes. Moreover, the proposed CPPA scheme yields better performance in terms of computation cost and communication cost making it be suitable for use by VANET safety-related applications.**

***Index Terms*—authentication; bilinear pairing, elliptic curve, vehicular ad-hoc networks**

I. Introduction

The Vehicular Ad-hoc Network (VANET), a variant of the Mobile Ad-hoc Network (MANET), is a continuously self-configuring, infrastructure-less network which has emerged as a result of advances in wireless communications and networking technologies over the last few years [1-4]. Mobile nodes in VANETs are vehicles equipped with On-Board Units (OBUs), which are wireless communication devices. OBUs enable vehicles in VANETs to exchange traffic messages with nearby mobile nodes.

A typical structure of the VANET is shown in Fig. 1. Communications in VANETs can be divided into two types: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication. Both types of communications are controlled by a short-range wireless communication protocol, called the Dedicated Short Range Communication (DSRC) protocol. By using the OBU and the DSRC protocol, each vehicle can communicate with nearby vehicles and Road Side Units (RSUs) located at roadside and can communicate with the traffic control center through the Internet. According to the specification of the DSRC protocol, each vehicle periodically broadcasts messages about road traffic and vehicles' conditions every 100–300 milliseconds, where road traffic conditions include weather conditions, road defects, congestion situation, etc. and vehicle's conditions include location, speed, traffic status, etc. [5, 6]. Upon receipt of these messages, other vehicles could change their traveling routes in order to avoid possible traffic events such as traffic congestion, traffic accident, etc. Besides, RSUs can also send messages about traffic conditions to the traffic control center. Based on received messages, the traffic control center can take some timely actions (such as adjusting traffic lights) to improve traffic safety and efficiency. All the aforementioned benefits make VANET a promising technology for the modern intelligent transportation system.

The work of D. He was supported by the National Natural Science Foundation of China (Nos. 61373169, 61572379, 61501333), the National High-tech R&D Program of China (863 Program) (No. 2015AA016004), the Fujian Provincial Key Laboratory of Network Security & Cryptology Research Fund of Fujian Normal University (No. 15011) and the Natural Science Foundation of Hubei Province of China (No. 2015CFB257). The work of B. Xu was supported by the National Natural Science Foundation of China (No. 91418202, 61472178) and the National Key Basic Research and Development Program of China (No. 2014CB340702). The work of X. Huang was supported by the National Natural Science Foundation of China (61472083, U1405255), the Fok Ying Tung Education Foundation (141065), the Program for New Century Excellent Talents in Fujian University (JA14067), the Distinguished Young Scholars Fund, Fujian Province, China, and the State Key Laboratory of Cryptology Research Fund..

D. He is with the State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan, China and the Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, China (e-mail: hedebiao@163.com).

S. Zeadally is with the College of Communication and Information at the University of Kentucky, USA (e-mail: szeadally@uky.edu).

B. Xu is with the Department of Computer Science and Technology, Nanjing University, Nanjing, China (e-mail: bwxu@nju.edu.cn).

X. Huang (*Corresponding Author*) is with the Fujian Provincial Key Laboratory of Network Security and Cryptology, the School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian, China and the State Key Laboratory of Cryptology, Beijing, China (e-mail: xyhuang81@gmail.com).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

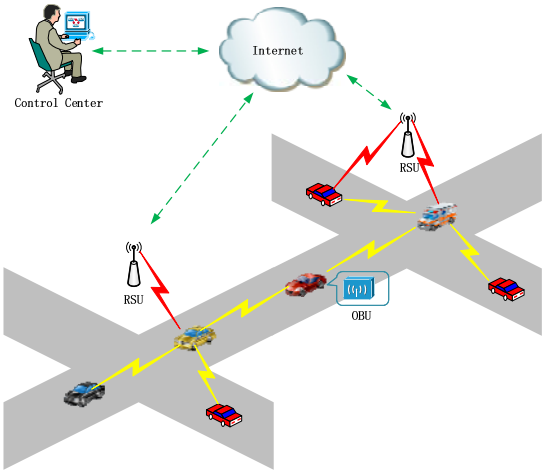

Fig. 1. A typical structure of VANETs

Due to the wireless communication mode, adversaries against VANETs could control communication channels fairly easily, i.e. adversaries could intercept, modify, replay and delete messages transmitted in VANETs easily. Therefore, VANETs are vulnerable to many kinds of attacks [7, 8]. In practice, the vehicle or OBU must verify the validity and integrity of received messages before taking further actions because the adversaries may replace or modify the original messages or impersonate some vehicle to broadcast wrong messages. These messages may cause the traffic control center to make wrong decisions and result in traffic chaos or even lead to traffic accidents. For example, an adversary may impersonate an ambulance to broadcast a message to ask the traffic light to turn green and other vehicles to make way for his/her pass. Therefore, the security of messages transmitted in VANETs is very important for many practical applications [9, 10].

In addition, privacy is another key issue in VANETs [9, 10]. For many applications in VANETs, the vehicle sends its identity to RSUs or other vehicles in plaintext. By capturing the vehicle's messages, the adversary could trace the vehicle's traveling routes. The leakage of traveling routes violates drivers' privacy and may result in serious consequences because those traveling routes may be used for crimes. To address this privacy issue, anonymity must be provided in VANETs but, it should still be possible to extract the real identity from the message by a trusted authority. For example, when a malicious vehicle sends a false message and results in crimes or accidents, the malicious vehicle should be severely punished for its action. Then, traceability becomes an important issue in VANETs. Therefore, conditional privacy should be provided in VANETs. Conditional privacy requires that the trusted authority must be the only one which can extract the real identity from the message.

The Conditional Privacy-Preserving Authentication (CPPA) scheme [11, 12] is suitable for addressing the privacy issue in VANETs because it can support message authentication and conditional privacy. In last several years, several CPPA schemes have been proposed for practical VANET applications [11-24]. Although previously proposed ID-based CPPA schemes [15, 16, 18-24] could solve several weaknesses that exist in some PKI-based CPPA schemes, the performance of such schemes is not satisfactory because a super singular elliptic curve defined over a finite field with large elements should be used to guarantee security. For example, the schemes [15, 16, 18-24] use a bilinear pairing $\bar{e}: G_1 \times G_1 \to G_2$ to achieve the security level of 80 bits (the security level of 1024-bit keys of the RSA algorithm) [25, 26], where G_1 is an additive group generated by a point $\bar{P}$ with the order $\bar{q}$ on the super singular elliptic curve $\bar{E}: y^2 = x^3 + x \bmod \bar{p}$ with a embedding degree 2, $\bar{p}$ is a 512-bit prime number, $\bar{q}$ is a 160-bit prime number and the equation $\bar{p}+1=12\bar{q}\bar{r}$ holds. In this case, the computation costs of the bilinear pairing operation and the scalar multiplication operation are quite complex. We therefore argue that it is far better for practical VANET applications to design an ID-based CPPA scheme for VANETs without bilinear pairing.

A. *Our contributions*

In this paper, we propose an ID-based CPPA scheme for VANETs based on Elliptic Curve Cryptography (ECC), which could achieve the security level of 80 bits by using an additive group G generated by a point P with the order q on a non-singular elliptic curve $E: y^2 = x^3 + ax + b \bmod p$, where p, q are two 160-bit prime numbers and $a, b \in Z_p^*$. To the best of our knowledge, the proposed scheme is the first ID-based CPPA scheme for VANETs without bilinear pairing. To be specific, the major contributions of this paper are threefold:

- First, we propose a new ID-based CPPA scheme for VANETs without using bilinear pairing. To improve performance further, the function of batch verification is included in the proposed ID-based CPPA scheme.
- Second, we perform an in-depth security analysis to demonstrate that the proposed ID-based CPPA scheme could satisfy security and privacy requirements in VANETs.
- Finally, we present an analysis of the computation cost and the communication cost to demonstrate that the proposed ID-based CPPA scheme yields better performance than previously proposed schemes for VANETs.

B. *Organization of the rest paper*

The rest of the paper is organized as follows. Section II reviews related work about CPPA schemes for VANETs Section III introduces some background information used in this paper. Section IV describes the proposed ID-based CPPA scheme for VANETs. Section V presents an in-depth security analysis of the proposed ID-based CPPA scheme. Section VI analyzes both the computation cost and the communication cost of the proposed ID-based CPPA scheme. Finally, some concluding remarks are presented in Section VII.

II. RELATED WORK

To address security and privacy issues in VANETs, Raya and Hubaux [11] used anonymous certificates to design a CPPA scheme. In Raya and Hubaux's scheme, the Public Key

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

Infrastructure (PKI) is modified to implement functions of authentication and integrity. To hide the vehicle's real identity, many public/private key pairs and corresponding certificates are pre-loaded into vehicles' OBUs. In each communication, the vehicle's OBU chooses a pair of public/private key randomly and uses them to implement functions of authentication and integrity. Raya and Hubaux's scheme [9] suffers from the following weaknesses: 1) Each vehicle should have very large storage space to store its public/private key pairs and the corresponding certificates; 2) The authority should also have a very large storage space to store all vehicles' certificates; 3) It is difficult to find the adversary's real identity when he/she sends the wrong message because the authority has to perform an exhaustive search of all stored certificates.

To address the weaknesses in Raya and Hubaux's scheme, Lu et al. [12] proposed a new CPPA scheme using anonymous certificates. The vehicle in Lu et al.'s CPPA scheme obtains a temporary anonymous certificate when it passes by a RSU. To achieve conditional privacy, each vehicle has to request a new anonymous certificate from a RSU frequently because the adversary could trace a vehicle if a certificate is used for a long time. However, frequent interactions with RSUs are not efficient. Therefore, Lu et al.'s CPPA scheme cannot satisfy the requirement of efficiency in VANETs [13]. To overcome the weakness in Lu et al.'s CPPA scheme, Freudiger et al. [13] combined technologies of anonymous certificates and mix-zones to design a new CPPA scheme. However, in this modified CPPA scheme, the vehicles and the RSUs have to store a large number of anonymous certificates. Zhang et al. [14] used the Hash Message Authentication Code (HMAC) to construct an efficient CPPA scheme for VANETs where the key for the HMAC is generated through a key agreement protocol executed between the vehicle and the RSU. To achieve privacy, the vehicle must use different private/public key pair along with the corresponding certificate in each communication with the RSU. Therefore, vehicles have to store a large number of private/public key pairs and the corresponding certificates.

To address the certificate management problem in the above PKI-based CPPA schemes [11-14], Zhang et al. [15, 16] incorporated the IDentity-based Public Key Cryptography (ID-based PKC) into the design of CPPA schemes. The concept of the ID-based PKC was proposed by Shamir [17] in 1984. The identity (such as name, email and phone number) of the user in the ID-based PKC is his/her public key and his/her private key is generated by a trusted third party called the Private Key Generator (PKG). In this case, no certificate is needed to bind the user's identity to his/her public key. Therefore, the ID-based PKC could solve the certificate management problem in the PKI. Zhang et al. [15, 16] proposed an Identity-Based Signature (IBS) scheme and used it in an Identity-based Conditional Privacy-Preserving Authentication (ID-based CPPA) scheme for VANETs. Neither the vehicle nor the RSU in Zhang et al.'s ID-based CPPA scheme needs to store a certificate. Besides, their scheme incurs a lower verification cost because it supports the function of batch verification, i.e., it could verify the validity of many messages simultaneously. Therefore, Zhang et al.' ID-based CPPA scheme could overcome weaknesses in previous PKI-based CPPA schemes [11-14].

However, as Lee and Lai [18] pointed out, Zhang et al.' ID-based CPPA scheme [15, 16] is vulnerable to the replay attack and cannot satisfy the property of non-repudiation. Later, Chim [19] pointed Zhang et al.'s ID-based CPPA scheme is vulnerable to the impersonation attack and the anti-traceability attack. Chim [19] also proposed another ID-based CPPA scheme for VANETs. With only two shared secrets, Chim's ID-based CPPA scheme [19] could satisfy the privacy requirements in VANETs. Besides, Chim's ID-based CPPA scheme [19] has lower communication costs than previously proposed ID-based CPPA schemes. However, Horng et al. [20] found that Chim's ID-based CPPA scheme was vulnerable to the impersonation attack, i.e., a malicious vehicle could impersonate any another vehicle to broadcast counterfeit messages. To improve performance, Shim [21] proposed an efficient IBS scheme and used it to design an efficient ID-based CPPA schemes. Unfortunately, Liu et al. [22] pointed out that a security flaw exists in the proof of Shim's IBS scheme and Shim's ID-based CPPA scheme suffers from a modification attack, i.e., the adversary can generate a new legal message by modifying a previous message.

Recently, Zhang et al. [23] and Bayat et al. [24] found that Lee and Lai's ID-based CPPA scheme [18] cannot withstand the impersonation attack, i.e., a malicious vehicle could impersonate any other vehicle to broadcast a forged message. Zhang et al. [23] also pointed out that Lee and Lai's ID-based CPPA scheme [18] cannot provide non-repudiation of messages. To enhance the security of previous schemes, Zhang et al. [23] and Bayat et al. [24] also proposed two improved ID-based CPPA schemes for VANETs. By modifying the process of generating the anonymous identity and the digital signature, Zhang et al.'s ID-based CPPA scheme [23] and Bayat et al.'s ID-based CPPA scheme [24] could solve security problems in Lee and Lai's ID-based CPPA scheme [18] and have better computation performance results. Despite these improvements, Zhang et al. ID-based CPPA scheme [23] and Bayat et al.'s ID-based CPPA scheme [24] still suffer from the modification attack proposed by Liu et al. [22].

III. BACKGROUND

A. *Network model*

According to novel research [27-29], the two-layer network model is very suitable for VANETs. The various components of the network model are shown in Fig. 1.

The upper layer of the network model consists of a Trusted Authority (TA) and an Application Server (AS), where they could communicate with each other through a secure channel that can be established through the Secure Socket Layer (SSL) protocol. The bottom layer of the network model consists of a RSU and a vehicle, where they could communicate with each other through the DSRC protocol. The details of those four participants are described as follows.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

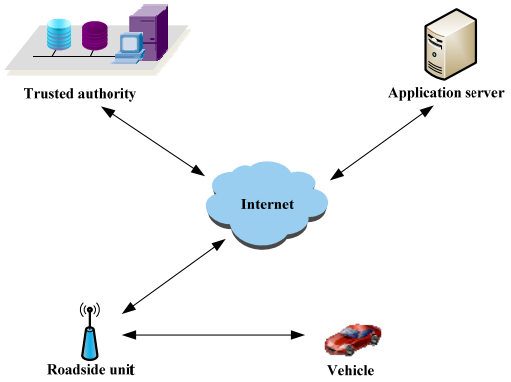

Fig. 2. The network model for VANET

- **TA**: The TA is a trusted third party with high computation and communication capabilities. It is responsible for generating system parameters and preloading them in the OBU of the vehicle offline. It is the only participant that could get the real identity of the vehicle from the intercepted messages.
- **AS**: The AS could support safety-related applications at the traffic management center. The AS could communicate with RSUs for providing application support.
- **RSU**: The RSU is a wireless communication device that uses the DSRC protocol. It is located at roadside and could communicate with vehicles. It can verify the validity of received messages and sends them to the traffic management center or process them locally.
- **Vehicle**: The vehicle is equipped an OBU supporting the DSRC protocol. The OBU is a tamper-proof device and its information is never disclosed. The vehicle communicates wirelessly with RSUs using the OBU.

B. Security and privacy requirements

Both security and privacy are important for secure communications in VANETs. Based on the latest research efforts [17-24, 27-29], an ID-based CPPA scheme for VANETs should meet the following security requirements: message authentication, identity privacy preservation, traceability, un-linkability and resistance to attacks, where the definition of the conditional privacy is expressed by the combination of the identity privacy preservation and traceability.

1) **Message authentication**: RSUs are able to check the validity of the messages sent by vehicles. In addition, RSUs are able to detect any modification of the received message.

2). **Identity privacy preservation**: RSUs and other vehicles are not able to extract the vehicle's real identity. Any third party is not able to get the vehicle's real identity by analyzing intercepted messages.

3) **Traceability**: The TA is able to extract the vehicle's real identity by analyzing its messages when it is necessary. For example, a malicious vehicle sends a false message to mislead others.

4) **Un-linkability**: RSUs and malicious vehicles are not able to link two messages sent by the same vehicle, i.e., they cannot trace the vehicle's action through its messages.

5) **Resistance to attacks**: The ID-based CPPA scheme is able to withstand various common attacks such as the impersonation attack, the modification attack, the replay attack, the man-in-the-middle attack, and the stolen verifier table attack that exist in VANETs.

IV. THE PROPOSED ID-BASED CPPA SCHEME

In this section, we propose our ID-based CPPA scheme without the bilinear pairing for VANETs based on Schnorr's signature scheme [30]. The proposed CPPA scheme could be used for both V2I and V2V communications. There are three phases in the proposed ID-based CPPA scheme: the system initialization phase, the anonymous identity generation and message signing phase and the message verification phase. We define the notations used below as follows:

- p, q : two large prime numbers.
- E : an elliptic curve defined by the equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$.
- G : an additive group with the order q, where G consists of all points on the elliptic curve E and the point at infinity O.
- P : a generator of the group G.
- Discrete Logarithm (DL) problem: Given two random points P and Q on E, the task of the DL problem is computing an integer x to satisfy the equation $Q = xP$.
- Computational Diffie-Hellman (CDH) problem: Given two random points Q and R on E, the task of the CDH problem is computing the point xyP, where $Q = xP$, $R = yP$ and x, y are two unknown integers.
- x : the private key of the system.
- P_{pub} : the public key of the system, where $P_{pub} = x \cdot P$.
- RID : the real identity of a vehicle.
- PWD : the password of the tamper-proof device.
- AID : the anonymous identity of a vehicle.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

- h_1, h_2, h_3 : three secure functions, where $h_1 : G \to Z_q$, $h_2 : \{0,1\}^* \to Z_q$ and $h_3 : \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \to Z_q$.
- $\oplus$: the exclusive-OR operation.
- $||$: the message concatenation operation.

A. System initialization phase

In this phase, the TA generates system parameters (such as a finite filed and an elliptic curve defined on it). The TA pre-loads them into each vehicle's tamper-proof device and sends them to all RSUs. The following steps are executed by the TA in this phase.

1) The TA chooses two large prime numbers p, q and a non-singular elliptic curve E defined by the equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$.

2) The TA chooses a generator P with order q of the group G, which consists of all points on the elliptic curve E and the point at infinity O.

3) The TA chooses a random number $x \in Z_q^*$ as the private key of the system and computes the system public key $P_{pub} = x \cdot P$.

4) The TA chooses three secure hash functions h_1, h_2, h_3, where $h_1 : G \to Z_q$, $h_2 : \{0,1\}^* \to Z_q$ and $h_3 : \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \to Z_q$.

5) The TA assigns a real identity RID and a password PWD for each vehicle and pre-loads $\{RID, PWD, x\}$ into its tamper-proof device.

6) The TA sends the system parameters $parmas = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ to all RSUs and vehicles.

B. Anonymous identity generation and message signing phase

In this phase, the vehicle's tamper-proof device generates an anonymous identity and a digital signature of a message. After that, the vehicle broadcasts the anonymous identities, the message and the digital signature to nearby RSUs and vehicles. The following steps are executed during this phase.

1) The vehicle inputs its real identity RID and password PWD into its tamper-proof device. The tamper-proof device checks if RID and PWD are equal to the stored ones. The tamper-proof device rejects the request if one of them and the corresponding stored one are not equal.

2) The tamper-proof device generates a random number $w_i \in Z_q^*$ and computes $AID_{i,1} = w_i \cdot P$, $AID_{i,2} = RID \oplus h_1(w_i \cdot P_{pub})$, $\alpha_i = h_2(AID_i \,||\, T_i)$, and $sk_i = w_i + \alpha_i \cdot x \bmod q$, where $AID_i = \{AID_{i,1}, AID_{i,2}\}$ and T_i is the current timestamp. Then, the tamper-proof device gives $\{AID_i, sk_i, T_i\}$ to the vehicle.

3) The vehicle generates a random number $r_i \in Z_q^*$, and computes $R_i = r_i \cdot P$, $\beta_i = h_3(AID_i \,||\, T_i \,||\, R_i \,||\, M_i)$ and $\sigma_i = sk_i + \beta_i \cdot r_i \bmod q$, where M_i is a message about traffic status. Then, the vehicle broadcasts $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ to nearby RSUs and vehicles.

C. Message verification phase

In this phase, the verifier (a RSU or a vehicle) checks the validity of received messages. The verifier could check the validity of a received message through the traditional verification process. To improve performance, the proposed ID-based CPPA scheme supports the batch verification function which enables the verifier to check the validity of lots of messages simultaneously. The single verification of one message and the batch verification of multiple messages are described as follows.

● Single verification of one message

Upon receiving a message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ sent by a vehicle, the verifier uses the system parameters $parmas = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ to verify the validity of the message through the following steps.

1) The verifier checks the freshness of T_i. If it is not fresh, the verifier rejects the message.

2) The verifier checks whether the equation $\sigma_i \cdot P = AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i$ holds. If it does not hold, the verifier rejects the message; otherwise, the verifier accepts the message.

Due to $P_{pub} = x \cdot P$, $AID_{i,1} = w_i \cdot P$, $AID_{i,2} = RID \oplus h_1(w_i \cdot P_{pub})$, $\alpha_i = h_2(AID_i \,||\, T_i)$, $sk_i = w_i + \alpha_i \cdot x \bmod q$, $R_i = r_i \cdot P$, $\beta_i = h_3(AID_i \,||\, T_i \,||\, R_i \,||\, M_i)$ and $\sigma_i = sk_i + \beta_i \cdot r_i \bmod q$, we could get that

$$\begin{aligned} \sigma_i \cdot P &= (sk_i + \beta_i \cdot r_i) \cdot P \\ &= (w_i + \alpha_i \cdot x + \beta_i \cdot r_i) \cdot P \\ &= w_i \cdot P + \alpha_i \cdot x \cdot P + \beta_i \cdot r_i \cdot P \\ &= AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i \end{aligned} \quad (1)$$

Therefore, the correctness of the single verification of one message is proved.

● Batch verification of multiple messages

To guarantee the non-repudiation of signatures using batch verification, we use the small exponent test technology [20, 23] in the batch verification of multiple messages. A vector, consisting of small random integers, is used to quickly detect any modification of a batch of signatures in the small exponent test technology. Upon receiving multiple messages $\{M_1, AID_1, T_1, R_1, \sigma_1\}$, $\{M_2, AID_2, T_2, R_2, \sigma_2\}$, $\cdots$, $\{M_n, AID_n, T_n, R_n, \sigma_n\}$ sent by some vehicles, the verifier uses the system parameters $parmas = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ to verify the validity of those messages through the following steps.

1) The verifier checks the freshness of T_i, where $i = 1, 2, \cdots, n$. If it is not fresh, the verifier rejects the message.

2) The verifier chooses a vector $v = \{v_1, v_2, \cdots, v_n\}$ randomly, where v_i is a small random integer in $[1, 2^t]$ and t

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

is a small integer and has very little computation overhead. Afterwards, the verifier checks if the following equation holds.

$$\left(\sum_{i=1}^{n} v_i \cdot \sigma_i\right) \cdot P = \sum_{i=1}^{n}\left(v_i \cdot AID_{i,1}\right) + \left(\sum_{i=1}^{n}\left(v_i \cdot \alpha_i\right)\right) \cdot P_{pub} + \sum_{i=1}^{n}\left(v_i \cdot \beta_i \cdot R_i\right) \quad (2)$$

If it does not hold, the verifier rejects the messages; otherwise, the verifier accepts the messages.

Due to $P_{pub} = x \cdot P$, $AID_{i,1} = w_i \cdot P$, $AID_{i,2} = RID \oplus h_1(w_i \cdot P_{pub})$, $\alpha_i = h_2(AID_i \| T_i)$, $sk_i = w_i + \alpha_i \cdot x \bmod q$, $R_i = r_i \cdot P$, $\beta_i = h_3(AID_i \| T_i \| R_i \| M_i)$ and $\sigma_i = sk_i + \beta_i \cdot r_i \bmod q$, we could get that

$$\begin{aligned}
\left(\sum_{i=1}^{n} v_i \cdot \sigma_i\right) \cdot P &= \left(\sum_{i=1}^{n} v_i \cdot \left(sk_i + \beta_i \cdot r_i\right)\right) \cdot P \\
&= \left(\sum_{i=1}^{n} v_i \cdot \left(w_i + \alpha_i \cdot x + \beta_i \cdot r_i\right)\right) \cdot P \\
&= \sum_{i=1}^{n}\left(v_i \cdot \left(w_i \cdot P + \alpha_i \cdot x \cdot P + \beta_i \cdot r_i \cdot P\right)\right) \\
&= \sum_{i=1}^{n}\left(v_i \cdot AID_{i,1} + v_i \cdot \alpha_i \cdot P_{pub} + v_i \cdot \beta_i \cdot R_i\right) \\
&= \sum_{i=1}^{n}\left(v_i \cdot AID_{i,1}\right) + \sum_{i=1}^{n}\left(v_i \cdot \alpha_i \cdot P_{pub}\right) \\
&\quad + \sum_{i=1}^{n}\left(v_i \cdot \beta_i \cdot R_i\right) \\
&= \sum_{i=1}^{n}\left(v_i \cdot AID_{i,1}\right) + \left(\sum_{i=1}^{n}\left(v_i \cdot \alpha_i\right)\right) \cdot P_{pub} \\
&\quad + \sum_{i=1}^{n}\left(v_i \cdot \beta_i \cdot R_i\right)
\end{aligned} \quad (3)$$

Therefore, the correctness of the batch verification of multiple messages is proved.

V. Security Analysis and Comparisons

In this section, we analyze the security of the proposed ID-based CPPA scheme for VANETs. We demonstrate that it is able to meet all security and privacy requirements described in Section 2. First of all, we show that the proposed scheme is able to enforce non-forgery. We also compare the security of the proposed ID-based CPPA scheme for VANETs with three most recently proposed CPPA schemes.

A. Security analysis

Based on the network model and the adversaries' ability, the security model for the CPPA scheme is defined through a game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. The adversary $\mathcal{A}$ could make the following queries in the game.

- *Setup – Oracle*: In this query, $\mathcal{C}$ generates the private key of the system and the system parameters. $\mathcal{C}$ sends the system parameters to $\mathcal{A}$.
- $h_1 - Oracle$: In this query, $\mathcal{C}$ chooses a random number $r \in Z_q$, inserts the tuple (m, r) into the list L_{h_1} and returns r to $\mathcal{A}$.
- $h_2 - Oracle$: In this query, $\mathcal{C}$ chooses a random point $r \in Z_q$, inserts the tuple (m, r) into the list L_{h_2} and returns r to $\mathcal{A}$.
- $h_3 - Oracle$: In this query, $\mathcal{C}$ chooses a random point $r \in Z_q$, inserts the tuple (m, r) into the list L_{h_3} and returns r to $\mathcal{A}$.
- *Sign – Oracle*: In this query, $\mathcal{C}$ generates a request message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ upon receiving the message M_i about traffic status. $\mathcal{C}$ sends $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ to $\mathcal{A}$.

The adversary $\mathcal{A}$ could violate the authentication of the CPPA scheme Γ if it could generate a login request message. Let $Adv_{\Gamma}^{Auth}(\mathcal{A})$ denote the probability that $\mathcal{A}$ could violate the authentication of the CPPA scheme Γ.

Definition 1. A CPPA scheme Γ for VANETs is secure if $Adv_{\Gamma}^{Auth}(\mathcal{A})$ is negligible for any polynomial adversary $\mathcal{A}$.

We have evaluated the security of the proposed ID-based CPPA scheme for VANETs and demonstrated that the proposed scheme is secure in the random oracle.

Theorem 1. The proposed ID-based CPPA scheme for VANETs is secure in the random oracle model.

Proof. Suppose there is an adversary $\mathcal{A}$ that can forge a message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$. We can construct a challenge challenger $\mathcal{C}$, which could solve the DL problem with a non-negligible probability by running $\mathcal{A}$ as a subroutine. Given an instance $(P, Q = x \cdot P)$ of the DL problem, $\mathcal{C}$ simulates oracles queried by $\mathcal{A}$ as follows.

Setup – Oracle: $\mathcal{C}$ sets $P_{pub} \leftarrow Q$, and sends the system parameters $parmas = \{p, q, a, b, P, P_{pub}, h_1, h_2, h_3\}$ to $\mathcal{A}$.

$h_1 - Oracle$: $\mathcal{C}$ keeps a list L_{h_1} with the form of $< \Gamma, \tau >$, which is initialized to empty. Upon receiving $\mathcal{A}$'s query with the message Γ, $\mathcal{C}$ checks whether a tuple $< \Gamma, \tau >$ exists in L_{h_1} first. If so, $\mathcal{C}$ sends $\tau = h_1(\Gamma)$ to $\mathcal{A}$; otherwise, $\mathcal{C}$ generates a random number $\tau \in Z_q$, adds $< \Gamma, \tau >$ in L_{h_1} and sends $\tau = h_1(\Gamma)$ to $\mathcal{A}$.

$h_2 - Oracle$: $\mathcal{C}$ keeps a list L_{h_2} with the form of $< AID_i, T_i, \tau >$, which is initialized to empty. Upon receiving $\mathcal{A}$'s query with the message (AID_i, T_i), $\mathcal{C}$ checks whether a tuple $< AID_i, T_i, \tau >$ exists in L_{h_2} first. If so, $\mathcal{C}$ sends $\tau = h_2(AID_i \| T_i)$ to $\mathcal{A}$; otherwise, $\mathcal{C}$ generates a random number $\tau \in Z_q$, adds $< AID_i, T_i, \tau >$ in L_{h_2} and sends $\tau = h_2(AID_i \| T_i)$ to $\mathcal{A}$.

$h_3 - Oracle$: $\mathcal{C}$ keeps a list L_{h_3} with the form of $< AID_i, T_i, R_i, M_i, \tau >$, which is initialized to empty. Upon

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

receiving $\mathscr{A}$'s query with the message (AID_i, T_i, R_i, M_i), $\mathscr{C}$ checks if a tuple $< AID_i, T_i, R_i, M_i, \tau >$ exists in L_{h_3} first. If so, $\mathscr{C}$ sends $\tau = h_3(AID_i \| T_i \| R_i \| M_i)$ to $\mathscr{A}$; otherwise, $\mathscr{C}$ generates a random number $\tau \in Z_q$, adds $< AID_i, T_i, R_i, M_i, \tau >$ in L_{h_3} and sends $\tau = h_3(AID_i \| T_i \| R_i \| M_i)$ to $\mathscr{A}$.

Sign−Oracle: Upon receiving $\mathscr{A}$'s query with the message M_i, $\mathscr{C}$ generates three random numbers $\sigma_i, \alpha_i, \beta_i \in Z_q^*$, chooses a random point $AID_{i,2}$ and computes $AID_{i,1} = \sigma_i \cdot P - \alpha_i \cdot P_{pub} - \beta_i \cdot R_i$. $\mathscr{C}$ adds $< AID_i, T_i, \alpha_i >$ and $< AID_i, T_i, R_i, M_i, \beta_i >$ into L_{h_2} and L_{h_3} respectively, where $AID_i = \{AID_{i,1}, AID_{i,2}\}$. Finally, $\mathscr{C}$ sends the message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ to $\mathscr{A}$. It is easy to verify the equation $\sigma_i \cdot P = AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i$ holds. Therefore, all signatures generated by $\mathscr{C}$ are indistinguishable from those generated by legal vehicles.

At last, $\mathscr{A}$ outputs a message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$. $\mathscr{C}$ checks whether the following equation holds.

$$\sigma_i \cdot P = AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i \quad (4)$$

If it does not hold, $\mathscr{C}$ aborts the process. According to the forgery lemma [31], $\mathscr{A}$ could output another valid message $\{M_i, AID_i, T_i, R_i, \sigma_i'\}$ if we repeat the process with a different choice of h_2. In this case, we could get the following equation.

$$\sigma_i' \cdot P = AID_{i,1} + \alpha_i' \cdot P_{pub} + \beta_i \cdot R_i \quad (5)$$

According to equations (3) and (4), we could get

$$\begin{aligned}(\sigma_i - \sigma_i') \cdot P &= \sigma_i \cdot P - \sigma_i' \cdot P \\ &= AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i - \\ &(AID_{i,1} + \alpha_i' \cdot P_{pub} + \beta_i \cdot R_i) \\ &= (\alpha_i - \alpha_i') \cdot P_{pub} = (\alpha_i - \alpha_i') \cdot x \cdot P\end{aligned} \quad (6)$$

and

$$\sigma_i - \sigma_i' = (\alpha_i - \alpha_i') \cdot x \bmod q \quad (7)$$

$\mathscr{C}$ outputs $(\alpha_i - \alpha_i')^{-1}(\sigma_i - \sigma_i')$ as the answer of the instance of the DL problem. The ability of solving the DL problem contradicts the hardness of the DL problem. Therefore, the proposed ID-based CPPA scheme for VANETs is secure against forgery under adaptive chosen message attack in the random oracle model.

1) **Message authentication**: According to Theorem 1, we know that no polynomial adversary can forge a valid message if the DL problem is hard. Therefore, the verifier could check the validity and integrity of the message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ by verifying whether the equation $\sigma_i \cdot P = AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i$ holds. Thus, the proposed ID-based CPPA scheme for VANETs provides message authentication.

2) **Preserving identity privacy**: The vehicle's real identity *RID* is involved in AID_i generated by the vehicle, where $P_{pub} = x \cdot P$, $AID_{i,1} = w_i \cdot P$, $AID_{i,2} = RID \oplus h_1(w_i \cdot P_{pub})$ and $AID_i = \{AID_{i,1}, AID_{i,2}\}$. To extract *RID* from $AID_{i,2} = RID \oplus h_1(w_i \cdot P_{pub})$, the adversary computes $w_i \cdot P_{pub} = w_i \cdot x \cdot P$ from $P_{pub} = x \cdot P$ and $AID_{i,1} = w_i \cdot P$. Therefore, the adversary has to solve the CDH problem. According to the hardness of the CDH problem, we conclude that the proposed ID-based CPPA scheme for VANETs preserves identity privacy.

3) **Traceability**: The vehicle's real identity *RID* is involved in AID_i generated by the vehicle, where $P_{pub} = x \cdot P$, $AID_{i,1} = w_i \cdot P$, $AID_{i,2} = RID \oplus h_1(w_i \cdot P_{pub})$ and $AID_i = \{AID_{i,1}, AID_{i,2}\}$. Using the private key of the system, TA computes $x \cdot AID_{i,1} = x \cdot w_i \cdot P = w_i \cdot x \cdot P = w_i \cdot P_{pub}$ and extracts the real identity by computing $RID = AID_{i,2} \oplus h_1(x \cdot AID_{i,1})$. Therefore, the proposed ID-based CPPA scheme for VANETs could provide traceability.

4) **Un-linkability**: To generate a message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$, the tamper-proof device and the vehicle in the proposed ID-based CPPA scheme generates two random $w_i \in Z_q^*$ and $r_i \in Z_q^*$ separately, where $AID_{i,1} = w_i \cdot P$, $AID_{i,2} = RID \oplus h_1(w_i \cdot P_{pub})$, $AID_i = \{AID_{i,1}, AID_{i,2}\}$, $sk_i = w_i + \alpha_i \cdot x \bmod q$, $\alpha_i = h_2(AID_i \| T_i)$, $R_i = r_i \cdot P$, $\beta_i = h_3(AID_i \| T_i \| R_i \| M_i)$ and $\sigma_i = sk_i + \beta_i \cdot r_i \bmod q$. Due to the randomness of w_i and r_i, no adversary could link two anonymous identities or two signatures generated by the same vehicle. Therefore, the proposed ID-based CPPA scheme for VANETs provides un-linkability.

5) **Resistant against various types of attacks**: We show that the proposed ID-based CPPA scheme for VANETs could withstand the impersonation attack, the modification attack, the replay attack, the man-in-the-middle attack, and the stolen verifier table attack as follows.

- **Impersonation attack**: To impersonate a vehicle to RSUs or other vehicles, the adversary must generate a message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ satisfying the equation $\sigma_i \cdot P = AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i$. According to Theorem 1, the adversary cannot generate such messages. RSUs and other vehicles could detect the attack easily by checking whether the above equation holds. Therefore, the proposed ID-based CPPA scheme for VANETs could withstand the impersonation attack.
- **Modification attack**: According to description of the proposed ID-based CPPA scheme, we know that $\{AID_i, R_i, \sigma_i\}$ is a digital signature of $\{M_i, T_i\}$. Based on Theorem 1, any modification of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ could be found by checking whether the equation $\sigma_i \cdot P = AID_{i,1} + \alpha_i \cdot P_{pub} + \beta_i \cdot R_i$ holds. Therefore, the proposed ID-based CPPA scheme for VANETs could withstand the modification attack.

- **Replay attack**: The timestamp T_i is included in the message $\{M_i, AID_i, T_i, R_i, \sigma_i\}$ and $\{AID_i, R_i, \sigma_i\}$ is a digital signature of $\{M_i, T_i\}$. Then, RSUs and other vehicles could find the replay of the message by checking the freshness of the timestamp T_i. Therefore, the proposed ID-based CPPA scheme for VANETs could withstand the replay attack.
- **Man-in-the-middle attack**: According to the above analysis about message authentication, we know the proposed ID-based CPPA scheme for VANETs could provide authentication between the sender and the receiver. Therefore, the proposed ID-based CPPA scheme for VANETs could withstand the man-in-the-middle attack.
- **Stolen verifier table attack**: Neither the RSU nor the vehicle maintains a verifier table for message authentication because they just needs to store their own private key. Then, the adversary cannot steal any verifier table for malicious attacks. Therefore, the proposed ID-based CPPA scheme for VANETs could withstand the stolen verifier table attack.

B. Security comparisons

We compare the security of our proposed ID-based CPPA scheme for VANETs with three recently proposed ID-based CPPA schemes [19, 21, 22] for VANETs. Let $SR-1$, $SR-2$, $SR-3$, $SR-4$ and $SR-5$ denote message authentication, preservation of identity privacy, traceability, un-linkability and resistance to attacks respectively. The security comparisons of the various schemes are listed in Table 1.

According to Table 1, none of the three schemes (i.e., Shim's ID-based CPPA scheme [19], Zhang et al.'s ID-based CPPA scheme and Bayat et al.'s ID-based CPPA scheme) can satisfy all 5 security requirements (SR-1 to SR-5). Besides, Shim's ID-based CPPA scheme [19] is not able to provide un-linkability because the vehicle's anonymous identity is a constant. In contrast, our proposed ID-based CPPA scheme could satisfy all five security requirements in VANETs.

Table 1. Security comparisons of past schemes and our proposed scheme

	Shim's scheme [19]	Zhang et al.'s scheme [21]	Bayat et al.'s scheme [22]	Our proposed scheme
$SR-1$	√	√	√	√
$SR-2$	√	√	√	√
$SR-3$	√	√	√	√
$SR-4$	×	√	√	√
$SR-5$	×	×	×	√

√: The requirement is satisfied.
×: The requirement is not satisfied.

VI. Performance analysis

In this section, we analyze the performance of the proposed ID-based CPPA scheme for VANETs. We analyze both the computation cost and the communication cost in the next two subsections. Besides, we also compare the performance of the proposed ID-based CPPA scheme for VANETs with three most recent ID-based CPPA schemes proposed in the literature.

For bilinear pairings based ID-based CPPA schemes for VANETs [19, 21, 22], we use a bilinear pairings $\bar{e}: G_1 \times G_1 \to G_2$ to achieve the security level of 80 bits, where G_1 is an additive group generated by a point $\bar{P}$ with the order $\bar{q}$ on the super singular elliptic curve $\bar{E}: y^2 = x^3 + x \bmod \bar{p}$ with embedding degree 2, $\bar{p}$ is a 512-bit prime number, $\bar{q}$ is a 160-bit Solinas prime number and the equation $\bar{p}+1=12\bar{q}\bar{r}$ holds. For ECC-based ID-based CPPA schemes for VANETs (the proposed scheme), we use an additive group G generated by a point P with the order q on a non-singular elliptic curve $E: y^2 = x^3 + ax + b \bmod p$ to achieve the security level of 80 bits, where p, q are two 160-bit prime numbers and $a, b \in Z_p^*$.

A. Computation cost analysis

In this subsection, we analyze the computation cost of related ID-based CPPA schemes for VANETs. For convenience, we define some notations about execution time as follows.

- T_{bp}: the execution time of a bilinear pairing operation $\bar{e}(S,T)$, where $\bar{S}, \bar{T} \in G_1$.
- T_{sm-bp}: the execution time of a scale multiplication operation $\bar{x} \cdot \bar{P}$ related to the bilinear pairing, where $\bar{x} \in Z_{\bar{q}}^*$ and $\bar{P} \in G_1$.
- $T_{sm-bp-s}$: the execution time of a small scale multiplication operation $v_i \cdot \bar{P}$ related to the bilinear pairing, which is used in the small exponent test, where $\bar{P} \in G_1$, v_i is a small random integer in $[1, 2^t]$ and t is a small integer.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

- T_{pa-bp} : the execution time of a point addition operation $\overline{S}+\overline{T}$ related to the bilinear pairing, where $\overline{S},\overline{T}\in G_1$.
- T_{mtp} : the execution time of a hash-to-point operation related to the bilinear pairing, where the hash function maps a string to a point of G_1.
- T_{sm-ecc} : the execution time of a scale multiplication operation $x\cdot P$ related to the ECC, where $x\in Z_q^*$ and $P\in G$.
- $T_{sm-ecc-s}$: the execution time of a small scale multiplication operation $v_i\cdot P$ used in the small exponent test technology, where $P\in G$, v_i is a small random integer in $[1,2^t]$ and t is a small integer.
- T_{pa-ecc} : the execution time of a point addition operation $S+T$ related to the ECC, where $S,T\in G$.
- T_h : the execution time of a general hash function operation.

To compare the computation cost of related ID-based CPPA schemes for VANETs, we compute the execution time of above cryptographic operations using MIRACL [32], which is a famous cryptographic library and has been widely used to implement cryptographic operations in many environments. Our hardware platform consists of an Intel I7-4770 processor with 3.40 GHz clock frequency, 4 gigabytes memory and runs Windows 7 operating system. The execution time of the above cryptographic operations are listed in Table 2.

Table 2. Execution time of different cryptographic operations

Cryptographic operation	**Execution time (milliseconds)**
T_{bp}	4.211
T_{sm-bp}	1.709
$T_{sm-bp-s}(t=5)$	0.0535
$T_{sm-bp-s}(t=10)$	0.1068
T_{pa-bp}	0.0071
T_{mtp}	4.406
T_{sm-ecc}	0.442
$T_{sm-ecc-s}(t=5)$	0.0138
$T_{sm-ecc-s}(t=10)$	0.0276
T_{pa-ecc}	0.0018
T_h	0.0001

Let *AIDGMS* and *SVOM* and *BVMM* denote the anonymous identity generation and message signing, the single verification of one message and the batch verification of multiple messages steps respectively. We only present the detailed analysis of Bayat et al.'s scheme [22] and the proposed scheme. The detailed analysis of other schemes [19, 21] could be achieved using the same method. The comparisons of computation costs for each step are presented in Table 3.

Table 3. Comparison of computation cost

	AIDGMS	*SVOM*	*BVMM*
Shim's scheme [19]	$3\,T_{sm-bp}+2\,T_{pa-bp}+1\,T_h\approx$ 5.1413 ms	$3\,T_{bp}+2\,T_{sm-bp}+1\,T_{pa-bp}+2\,T_h\approx$ 16.0583 ms	$3\,T_{bp}+(n+1)\,T_{sm-bp}+(3n-3)\,T_{pa-bp}+(2n)\,T_h\approx$ 1.7035 n +14.3207ms
Zhang et al.'s scheme [21]	$6\,T_{sm-bp}+2\,T_{pa-bp}+1\,T_{mtp}+4\,T_h\approx$ 14.6746 ms	$3\,T_{bp}+2\,T_{sm-bp}+1\,T_{pa-bp}+3\,T_h\approx$ 16.0584 ms	$3\,T_{bp}+(n+1)\,T_{sm-bp}+(2n)\,T_{sm-bp-s}+(3n-2)\,T_{pa-bp}+(3n)\,T_h\approx$ 1.8376 n +14.3276/ 1.9442 n +14.3276 ms
Bayat et al.'s scheme [22]	$5\,T_{sm-bp}+1\,T_{pa-bp}+1\,T_{mtp}+2\,T_h\approx$ 12.9583ms	$3\,T_{bp}+1\,T_{sm-bp}+1\,T_{mtp}+1\,T_h\approx$ 18.7481ms	$3\,T_{bp}+(n)\,T_{sm-bp-s}+(3n-3)\,T_{pa-bp}+(n)\,T_{mtp}+(n)\,T_h\approx$ 6.1364 n +12.6117ms
Our proposed scheme	$3\,T_{sm-ecc}+3\,T_h\approx$ 1.3263 ms	$3\,T_{sm-ecc}+2\,T_h+2\,T_{pa-ecc}\approx$ 1.3298 ms	$(n+2)\,T_{sm-ecc}+(2n)\,T_{sm-ecc-s}+(3n-1)\,T_{pa-ecc}+(2n)\,T_h\approx$ 0.4252 n +0.8822 / 0.5027 n +0.8822 ms
% Improvement of proposed scheme over three other schemes	74.20 % improvement over Shim's scheme [19]	91.72 % improvement over Shim's scheme [19]	70.95 % improvement over Shim's scheme [19]
	90.96 % improvement over Zhang et al.'s scheme [21]	91.72 % improvement over Zhang et al.'s scheme [21]	72.64% improvement over Zhang et al.'s scheme [21]
	89.76% improvement over Bayat et al.'s scheme [22]	92.89 % improvement over Bayat et al.'s scheme [22]	91.81 % improvement over Bayat et al.'s scheme [22]

For the *AIDGMS* step of Bayat et al.'s ID-based CPPA scheme [22], the vehicle needs to execute five scalar multiplication operations related to the bilinear pairing, one point addition operation related to the bilinear pairing, one hash-to-point operation related to the bilinear pairing and one general hash function operation. Therefore, the execution time of this step is $5\,T_{sm-bp}+1\,T_{pa-bp}+1\,T_{mtp}+2\,T_h\approx$ 12.9583 ms. For

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

the *SVOM* step of Bayat et al.'s ID-based CPPA scheme [22], the verifier needs to execute three bilinear pairing operations, one scalar multiplication operation related to the bilinear pairing, one hash-to-point operation related to the bilinear pairing and one general hash function operation. Therefore, the execution time of this step is $3\ T_{bp} + 1\ T_{sm-bp} + 1\ T_{mtp} + 1\ T_h \approx 18.7481$ ms. For the *BVMM* step of Bayat et al.'s ID-based CPPA scheme [22], the verifier needs to execute three bilinear pairing operations, (n) scalar multiplication operations related to the bilinear pairing, ($3n$-3) point addition operations related to the bilinear pairing, (n) hash-to-point operations related to the bilinear pairing and (n) general hash function operations. Therefore, the execution time of this step is $3\ T_{bp} + (n)\ T_{sm-bp-s} + (3n-3)\ T_{pa-bp} + (n)\ T_{mtp} + (n)\ T_h \approx 6.1364n + 12.6117$ ms.

For *AIDGMS* step of our proposed ID-based CPPA scheme, the vehicle needs to execute three scalar multiplication operations related to the ECC and three general hash function operations. Therefore, the execution time of the step is $3\ T_{sm-ecc} + 3\ T_h \approx 1.3263$ ms. For the *SVOM* step of the proposed ID-based CPPA scheme, the verifier needs to execute three scalar multiplication operations related to the ECC, two point addition operations related to the ECC and two general hash function operations. Therefore, the execution time of the phase is $3\ T_{sm-ecc} + 2\ T_{pa-ecc} + 2\ T_h \approx 1.3298$ ms. For the *BVMM* step of the proposed ID-based CPPA scheme, the verifier needs to execute ($n+2$) scalar multiplication operations related to the ECC, ($2n$) small scalar multiplication operations related to the ECC, ($3n$-1) point addition operations related to the ECC and ($2n$) general hash function operations. Therefore, the execution time of this step is $(n+2)\ T_{sm-ecc} + (2n)\ T_{sm-ecc-s} + (3n-1)\ T_{pa-ecc} + (2n)\ T_h \approx 0.4252n + 0.8822$ ms ($t=5$) / $0.5027n + 0.8822$ ms ($t=10$). The percentage improvement with the *AIDGMS* step of our proposed scheme over Bayat et al.'s scheme for the total execution time is about $\frac{12.9583 - 1.3263}{12.9583} \approx 89.76\%$. Other percentage improvement could be achieved by using a similar method.

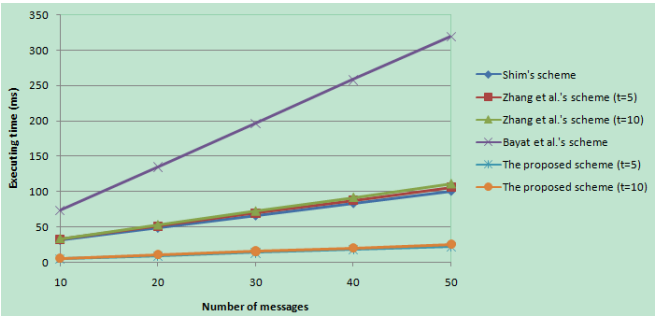

Fig. 3. Execution time for the batch verification of multiple messages

To demonstrate the major benefit of the proposed ID-based CPPA scheme in the batch verification of multiple messages, we compare the execution times of batch verification in the proposed scheme with three most recently proposed ID-based CPPA schemes [19, 21, 22] as shown in Figure 3. Based on the results shown in Table 3 and Figure 3, the proposed ID-based CPPA scheme for VANETs has lower computation cost compared to the three most recently proposed ID-based CPPA schemes for VANETs for all three steps including *AIDGMS*, *SVOM*, and *BVMM*.

B. Communication cost analysis

In this subsection, we analyze the communication cost of related ID-based CPPA schemes for VANETs. Since the sizes of $\overline{p}$ and p are 64 bytes (512 bits) and 20 bytes (160 bits) respectively, then the sizes of the elements in G_1 and G are $64 \times 2 = 128$ bytes and $20 \times 2 = 40$ bytes respectively. Besides, let the sizes of the general hash function's output and timestamp be 20 bytes and 4 bytes respectively. We only consider the size of signature because messages about traffic status are the same in all ID-based CPPA schemes. The comparison of computation costs is presented in Table 4.

Table 4. Comparison of communication cost

	Sending a single message	Sending n messages
Shim's scheme [19]	644 bytes	644 n bytes
Zhang et al.'s scheme [21]	388 bytes	388 n bytes
Bayat et al.'s scheme [22]	388 bytes	388 n bytes
The proposed scheme	**144 bytes**	**144 n bytes**

In the Shim's ID-based CPPA scheme [19], the vehicle broadcasts the anonymous identity and signature $\{AID_i, T_i, U_i, V_i, W_i\}$ to the verifier, where $AID_i = \{AID_i^1, AID_i^2\}$, $AID_i^1, AID_i^2, U_i, V_i, W_i \in G_1$ and T_i is the timestamp. Therefore, the communication cost of the Shim's ID-based CPPA scheme [19] is $128 \times 5 + 4 = 644$ bytes. In the Zhang et al.'s ID-based CPPA scheme [21] and Bayat et al.'s scheme [22], the vehicle broadcasts the anonymous identity and signature $\{AID_i, T_i, U_i\}$ to the verifier, where $AID_i = \{AID_i^1, AID_i^2\}$, $AID_i^1, AID_i^2, U_i \in G_1$ and T_i is the timestamp. Therefore, the communication cost of Zhang et al.'s ID-based CPPA scheme [21] is $128 \times 3 + 4 = 388$ bytes. The vehicle in the proposed CPPA scheme broadcasts the anonymous identity and signature $\{AID_i, T_i, R_i, \sigma_i\}$ to the verifier, where $AID_i = \{AID_i^1, AID_i^2\}$, $AID_i^1, AID_i^2, R_i \in G$, $\sigma_i \in Z_q$ and T_i is the timestamp. Therefore, the communication cost of the proposed CPPA scheme is $40 \times 3 + 20 + 4 = 144$ bytes. Thus, the proposed CPPA scheme for VANETs incurs a much lower communication cost than the three latest ID-based CPPA schemes for VANETs [19, 21, 22].

VII. Conclusion

In this work, we have proposed a new ID-based CPPA scheme, which could be used for both V2V communication and V2I communication in VANETs. To improve performance, the function of batch verification of multiple messages is included in the proposed ID-based CPPA scheme. The security analysis shows that the proposed scheme can overcome the weaknesses of previously proposed schemes and satisfy the security requirements of ID-based CPPA schemes for VANETs. Our performance analysis results show that the proposed scheme

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2473820, IEEE Transactions on Information Forensics and Security

incurs lower computation cost and communication cost because no bilinear pairings are used in our proposed ID-based CPPA scheme. This makes the proposed scheme more suitable for deployment in the VANET environment.

ACKNOWLEDGMENTS

We thank the Associate Editor and the anonymous reviewers for their useful comments and suggestions which helped us improve the quality and presentation of this paper.

REFERENCES

[1] T. Chim, S. Yiu, L. Hui, and V. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Networks, vol. 9, no. 12, pp. 189-203, 2011.
[2] S. Zeadally, R. Hunt, Y. Chen, A. Irwin, and A. Hassan, "Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges", Telecommunication Systems, Vol. 50, No. 4, 2012
[3] M. Ghosh, A. Varghese, A. Gupta, A. Kherani, and S. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," Ad Hoc Networks, vol. 8, no. 7, pp. 778-790, 2010.
[4] Y. Toor , P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," IEEE Communications Surveys and Tutorials, vol. 10, no. 3, pp. 74–87, 2008.
[5] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," Computer Communications, vol. 31, no. 12, pp. 2838–2849, 2008.
[6] IEEE Trial-Use Standard for Wireless Access in Vehicular Environment-Security Services for Applications and Management Messages, IEEE standard 1609.2-2006, Jul. 2006.
[7] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8-15, 2006.
[8] J. Tellez, S. Zeadally, and J. Camara, "Security Attacks and Solutions for Vehicular Ad-Hoc Networks", IET Communications Journal, vol. 4, no. 7, 2010
[9] 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.
[10] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in Proceeding of Securecomm and Workshops, 2006, pp. 1-5.
[11] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
[12] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," In: INFOCOM 2008, 2008, doi: 10.1109/INFOCOM.2008.179.
[13] J. Freudiger, M. Raya, M. Fe´legyha´zi, and P. Papadimitratos, "Mix-zones for location privacy in vehicular networks," In: Proceedings of the first international workshop on wireless networking for intelligent transportation systems (Win-ITS), 2007.
[14] C. Zhang, X. Lin, R. Lu, and P. Ho, "Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks," In: ICC'08, pp. 1451-1457, 2008.
[15] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM'08, Apr. 2008, pp. 816–824.
[16] 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.
[17] A. Shamir, "Identity-based cryptosystems and signature schemes," In: Proceedings of CRYPTO 84, pp. 47-53,1984.
[18] C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," Wireless Networks, vol. 19, no. 6, pp. 1441-1449, 2013.
[19] T. Chim, S. Yiu, L. Hui, and V. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Networks, vol. 9, no. 2, pp. 189-203, 2011.
[20] S. Horng, S. Tzeng,Y. Pan, and P. Fan, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1860-1875, 2013.
[21] K. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1874-1883, 2012.
[22] J. Liu, T. Yuen, M. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," Expert Systems with Applications, vol. 41, no. 5, 2559-2564, 2014.
[23] 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.
[24] M. Bayat, M. Barmshoory, M. Rahimi, and M. Aref, "A secure authentication scheme for VANETs with batch verification," Wireless Networks, vol. 21, no. 5, pp 1733-1743, 2015.
[25] D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," Journal of Cryptology, vol. 23, no. 2, pp. 224-280, 2010.
[26] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," Information Sciences, vol. 180, no. 15, pp. 2895-2903, 2010.
[27] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 4, pp. 1606–1617, 2010.
[28] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "APPA: aggregate privacy-preserving authentication in vehicular ad hoc networks," In: the 14th Conference on Information Security (ISC2011), 2011, pp. 293-308.
[29] 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.
[30] C. Schnorr, "Efficient signature generation by smart cards," Journal of cryptology, vol. 4, no. 3, pp. 161-174, 1991.
[31] P. David, and S. Jacque, "Security arguments for digital signatures and blind signatures," Journal of Cryptology, vol. 13, no. 3, pp. 361-396, 2000.
[32] Shamus Software Ltd., Miracl library. <http://www.shamus.ie/index.php?page=home>.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, WuhanUniversity in 2009. He is currently an Associate Professor of the State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan, China. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Sherali Zeadally is an Associate Professor withthe College of Communication and Information, University of Kentucky, Lexington, KY, USA. Hereceived the bachelor's and Doctorate degrees incomputer science from the University of Cambridge, England, and the University of Buckingham, England respectively. Heis a fellow of the British Computer Society and the Institution of Engineering Technology, England.

Baowen Xu received the BS, MS, and PhD degrees in computer science from Wuhan University, Huazhong University of Science and Technology, and Beihang University, respectively. He is currently a professor in the

Department of Computer Science & Technology at Nanjing University. His main research interests include programming languages, software testing, software maintenance, and software metrics. He is a member of the IEEE and the IEEE Computer Society.

Xinyi Huang received his Ph.D. degree from the School of Computer Science and Software Engineering, University of Wollongong, Australia. He is currently a Professor at the School of Mathematics and Computer Science, Fujian Normal University, China, and the Co-Director of Fujian Provincial Key Laboratory of Network Security and Cryptology. His research interests include applied cryptography and network security. He has published over 100 research papers in refereed international conferences and journals. His work has been cited more than 1900 times at Google Scholar (H-Index: 25). He is an associate editor of IEEE Transactions on Dependable and Secure Computing, in the Editorial Board of International Journal of Information Security (IJIS, Springer) and has served as the program/general chair or program committee member in over 60 international conferences.