Received November 6, 2017, accepted December 1, 2017, date of publication December 27, 2017,
date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2782672

Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks

HONG ZHONG[1], BO HUANG[1], JIE CUI[1], YAN XU[1] AND LU LIU[2]

[1]School of Computer Science and Technology, Anhui University, Hefei 230601, China
[2]Department of Computing and Mathematics, University of Derby, Derby DE22 1GB, U.K.

Corresponding author: Jie Cui (cuijie@mail.ustc.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572001, Grant 61502008, and Grant 61702005, in part by the Natural Science Foundation of Anhui Province under Grant 1508085QF132 and Grant 1708085QF136, and in part by the Doctoral Research Start-up Funds Project of Anhui University.

ABSTRACT Vehicular ad hoc networks (VANETs) have increased in popularity in recent years and play an extremely important role in the intelligent transportation field. However, the demands of larger communication networks and the integrated message verification process for ensuring security incur more communication and computation overheads, and directly affect the efficiency of existing VANET schemes. To address this issue, this paper proposes a novel and practical conditional privacy-preserving authentication scheme, which uses the registration list instead of the revocation list to reduce the communication overhead. Specifically, our scheme can prevent malicious vehicles from disrupting the security features of VANETs. Moreover, we do not use the bilinear pairing operation, which is the most complicated operation in modern cryptography, thus significantly reducing the computation overhead and communication overhead. Security and performance analyses demonstrate that our proposed scheme is more secure and efficient than current schemes, and that the proposed scheme is more suitable for VANET deployments.

INDEX TERMS Registration list, resistance to continuous disruption, modification of passwords, conditional privacy, elliptic curve.

I. INTRODUCTION

A vehicular ad hoc network (VANET) is a special type of mobile ad hoc network that enables communication through multi-hops among the nodes in a wireless network. VANETs, which are increasing in popularity, can provide real-time information exchange by establishing connections among vehicles on roads and road-side infrastructures [1]. VANETs are efficient in providing travel assistance and can effectively reduce the driver's workload through automatic and intelligent driving controls, and facilitate higher comfort and rich travel experience for passengers. VANETs can also provide personal entertainment and in-car office functions by facilitating Internet access to drivers and passengers [2], [3]. In short, VANETs extend the functionalities and facilities of vehicles as mobile information platforms rather than simple transport entities, which significantly enrich the functions and applications of vehicle systems.

The structure of VANETs generally consists of three modules, namely a Trusted Authority (TA), a Road Side Unit (RSU), and an On-Board Unit (OBU) [4]. TA is a trusted third party with high computing power and large storage capacity that is responsible for generating the system parameters and distributing secret materials. RSU is a communication node deployed as a road-side infrastructure that can communicate with vehicles on a section of a road through wireless channels. OBU, which is placed in vehicles, is responsible for issuing and receiving traffic-related messages so that drivers can obtain a better driving experience. In addition, a Tamper-Proof Device (TPD) is used in some VANETs, which is equated to a black box that prevents access to attackers. However, manufacturing overheads of TPD are relatively expensive, so it has not generally been deployed on VANETs on a large scale.

However, security remains one of the prevailing concerns in VANET applications. Adversaries can control communication with ease because communication is often enabled through a wireless channel. There are two immediate implications; first, it is fairly straightforward for attackers to issue illegal messages in order to affect traffic patterns, or to forge malicious information for the purpose of causing traffic accidents. Second, attackers can easily track a vehicle, thus violating user privacy. These two malicious behaviors have had serious impacts upon the efficiency of VANETs in the recent past and have threatened the safety of passenger lives and property in some cases [5].

Also, VANET requires that the sender of the message needs to be tracked quickly [6], and at the same time it should has the ability to disqualify malicious vehicles from sending messages quickly.Nowadays, many people make the same password in different agencies for convenience, for example, the bank card password and the vehicle password are the same. Then the owner will not convenient tell the password to other people directly while many drivers share a vehicle. At this point, the function of modification of the password quickly and convenient is very important and necessary.

In summary, VANETs require further study to enhance security features, robustness, and reliability. To this end, this paper proposes a novel and practical conditional privacy-preserving authentication (CPPA) scheme, which uses the registration list instead of the revocation list for reducing the communication overhead. Important contributions of this paper include the following:

1) Reduction in the retrieval time of the revocation list when it is represented by the registration list in order to reduce the think time available to attackers. Moreover, the proposed scheme can prevent the attacker from continually issuing malicious information, which effectively improves the security of VANETs.
2) The proposed scheme allows the owner of a vehicle to modify passwords anytime, anywhere, which provides more flexibility and privileges to the VANET user.
3) The proposed scheme does not use bilinear pairing, which is the most complicated operation in modern cryptography, and additionally reduces the message length to minimize both the computation and communication overheads in VANETs.

The remainder of the paper is organized as follows. Section introduces the related research of CPPA schemes in VANETs. The background knowledge and system model are introduced in Section III. Section IV describes our proposed scheme in detail and Section V presents the security analysis of the proposed scheme. Section VI presents the performance evaluation, including calculation overhead and communication overhead comparisons. Finally, Section VII discusses the conclusion and future research.

II. RELATED WORK

A wide range of research has focused on enhancing the safety and efficiencies of VANETs in the recent past.

Raya *et al.* [7] proposed a CPPA scheme based on the public key infrastructure (PKI), which used public/private key pairs and corresponding certificates to hide a vehicle's true identity. However, there are two obvious shortcomings: first, the OBU of each vehicle requires large storage space to save the public/private key pairs and the corresponding certificates; second, the TA must carry out a complete traversal in its storage space while seeking the true identity of the attacker, thus resulting in larger time and memory overheads.

Zhang *et al.* [8] highlighted that the computation power of the OBU in vehicles is not capable of performing complex computational operations within a short time when the number of vehicles in the VANET is relatively large. Allowing the nearby RSU to verify the message can assist the OBU in the computation, but a more effective method of reducing the OBUs computation and communication overheads in VANETs is an urgent problem.

Wu *et al.* [9] and Zhang *et al.* [10] proposed a CPPA scheme based on a group signature in which the OBU no longer needs to store more private data and the TA can effectively track the true identity of an attacker based on the revocation list without incurring the overheads caused by the retrieval of the revocation list. However, because the speed of the vehicle is fast and network topology changes quickly as the vehicle progresses, it is difficult to update and select the group managers and group members dynamically.

Chim *et al.* [11] proposed a scheme using a software-based bilinear pairing operation in which the RSU uses a pseudo identity to protect its true identity during message communication by establishing a shared key in the handshaking phase between the RSU and the TA, where the TA can also track the true identity behind the pseudo identity. In the certification phase, the RSU issues a notification message with a Bloom filter to reduce the OBUs computation overhead. But Horng *et al.* [12] later pointed out that the scheme proposed by Chim *et al.* [11] cannot resist an impersonation attack; that is, malicious vehicles can disguise themselves as legitimate vehicles to send a malicious message after intercepting a legal message.

K. A. Shim. [13] proposed a security ID-based CPPA scheme in which the RSU supports batch authentication of messages to reduce the computation overhead of the RSU when the number of messages is large. However, the TA must consume more time in retrieving the entire revocation list, and furthermore it does not address the additional authentication overheads caused by illegal information.

Zhang *et al.* [14] proposed another ID-based CPPA scheme to optimize the computation overheads in the message signature and authentication process, while the scheme also supports batch authentication in order to improve the efficiency of identity authentication. However, Lee *et al.* [15] later pointed out that this scheme cannot achieve the function of non-repudiation, and Liu *et al.* [16] pointed out that the scheme cannot resist a modification attack.

In order to improve the communication efficiency while ensuring the conditional privacy protection of the vehicles in VANETs, He *et al.* [17] proposed an efficient and fast signature scheme without using the bilinear pairing operation. This scheme reduces the computation overhead significantly while meeting security requirements.

Zhong *et al.* [18] proposed a CPPA scheme to optimize the computation process and to reduce the computation overhead based on the scheme proposed by He *et al.* [17]. However, the schemes proposed by He *et al.* [17] and Zhong *et al.* [18] include several security assumptions, as it is difficult to equip each vehicle with a TPD in practice. During an attack, TA can track the true identity of the attacker but cannot prevent it from sending additional malicious messages.

In order to solve the above problems, this paper proposes a novel and practical conditional privacy protection scheme based on the scheme of He *et al.* [19], which improves communication efficiency under the premise of reducing the demands in the security hypothesis. Additionally, our scheme can effectively prevent the attacker from continually sending malicious information because of the presence of the registration list, which improves the security features of VANETs.

III. BACKGROUND

In this section, we introduce the system model of our scheme and a background on the security requirements in VANETs.

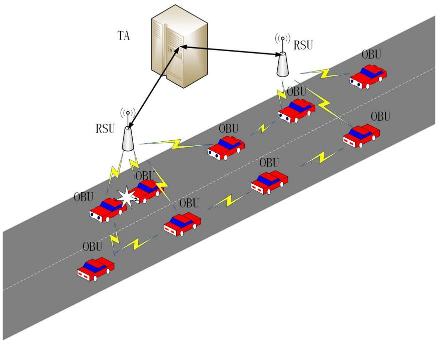


FIGURE 1. System Model.

A. SYSTEM MODEL

The structure of VANETs consists of three parts in general: Trusted Authority (TA), Road Side Unit (RSU) and On Board Unit (OBU), as showed in Fig. 1.

Information among OBUs or between OBU and RSU is transmitted over the wireless channel, and information between TA and RSU is transmitted over the wired channel [20].

TA, a trusted third party with very high computing power and storage capacity, is responsible for generating the system parameters and distributing the secret material. It is also responsible for the offline registration of OBU and RSU and stores the registration list of RSU and OBU.

RSU, a trusted roadside node with high computing power and storage capacity, verifies the validity and integrity of the message and then broadcasts the relevant message to the surrounding vehicles by the notification message. It can also identify the real identity of the attacker if necessary, and then notify the real identity to the TA. Because the number of RSU is less than OBU, and RSU is easier to be maintained than the OBU in VANETs, RSUs are more equipped with TPD than OBU in practice.

OBU is a semi-trusted computing unit with lower computing power and storage capacity load on the vehicle. It is responsible for calculating and issuing traffic-related messages and receiving notification messages from the RSU.

System assumptions in our scheme are as follows:

1) TA is completely trustworthy and will not be compromised by attackers in anytime.
2) The time in various parts of the entire VANET is synchronized.
3) RSU's computing power and storage capacity are lower than TA and higher than OBUs.

B. SECURITY REQUIREMENTS

1) *Identity privacy preservation:* The attacker should not be able to obtain the real identity of the vehicles through the messages sent by the vehicles. Only the TA can track the real identity of the sender of a given message.
2) *Traceability:* The TA should be able to track the real identity of the attacker through malicious messages and counteract if necessary.
3) *Non-repudiation:* When the vehicle sends a message, it cannot deny it.
4) *Un-linkability:* The attacker should not be able to determine whether the messages are issued by the same vehicle through the message content.
5) *Resistant to continuous disruption:* As a kind of real-time network, VANETs should not only be able to trace the real identity when the attacker appears, but should also possess the ability to cease the continuous malicious behaviors.
6) *Modification of passwords:* The owner of a vehicle should be able to modify the passwords anytime, anywhere.
7) *Resistance to ordinary attacks:* The CPPA scheme in VANETs should have the ability to resist some ordinary attacks, such as replay attack, modification attack and impersonation attack.

C. PRELIMINARY KNOWLEDGE

1) The one-way hash function $h(\cdot)$ is said to be secure if the following properties are satisfied [21]:
   - h can take a message of arbitrary length as input and produces a message digest of a fixed-length output;
   - Given x, it is easy to compute $y = h(x)$. However, given y, it is hard to compute $x = h^{-1}(y)$;
   - Given x, it is computationally infeasible to find $x' \neq x$ that $h(x') \neq h(x)$.
2) Elliptic Curve Discrete Logarithm Problem (ECDLP):

   The ECDLP problem [22] is to determine the integer $x, 0 \leq x \leq q-1$, such as $Q = xP$,while two points P, Q of order q are on a given elliptic curve.
3) Computation Diffie-Hellman problem (CDH):

   The CDH problem [22] is to compute $abP \in G$, while $P, aP, bP \in G$ is given and $a, b \in Z_q^*$ is unknown.
4) Bloom Filter:

   A bloom filter [11] is an algorithm for representing a set $A = a_1, a_2, a_3, \ldots a_n$ of n elements to support

TABLE 1. Notation.

Notation	Descriptions
p, q	Two large prime numbers.
E	An elliptic curve defined by the equation $y^2 = x^3 + ax + b\mathrm{mod}p$,where$a, b \in F_p$.
G	An additive group which consists of all points on the elliptic curve E.
ID_R, T_{RSU}^{reg}	The real identity is associated with the location and its corresponding registration time of RSU.
ID_V, T_{OBU}^{reg}	The real identity and its responding registration time of Vehicle.
PW_1, PW_2	Two passwords of vehicle.
PK_{RSU}, SK_{RSU}	The public key and corresponding private key of RSU.
L_{RSU}	The registration lists of RSU that saved in TA.
L_{OBU}	The registration lists of vehicle that saved in TA.
L_m	The message list that saved in RSU.
$h(\cdot)$	A secure hash function.

membership queries. The idea is to allocate a vector v_n with m bits, initially all set to 0, and a secure hash functions $h(\cdot)$, and used to compute the hash value of element, if the element in the set A, and then the bit of the corresponding position is set to 1. To determine whether a given value b is in A, we can check the bits at positions $h(b)$. If this position is set as 1, then b is definitely in the set A.

IV. THE PROPOSED SCHEME

The proposed scheme in our paper mainly includes two main phases such as the offline registration and the driving stage. Offline registration includes the initialization of TA and registration of RSUs and vehicles. The driving stage includes five phases including mutual authentication, release of traffic information, message verification, release of notification message and receiving messages. The main symbols used in our scheme and their definitions are illustrated in Table 1.

A. OFFLINE REGISTRATION

In this section, we introduce the system initialization phase. RSU and OBU get registered offline while in the factory or annual inspection. TA is responsible for the corresponding identity (ID) distribution and management.

- **a. Initialization of TA**

TA is a trusted third party with a high computing power and storage capacity that coordinates and controls the operation of the entire VANETs. Details of TAs Initialization are as follows:

1) TA chooses two large prime numbers p, q and an additive group G with the order q and its generator is P, which consists of all points on the elliptic curve E defined by the equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$.
2) TA chooses a random number $s \in Z_q^*$ as the master private key, and computes $P_{pub} = s \cdot P$ as the master public key.
3) TA chooses a secure hash function $h(\cdot)$.
4) TA broadcasts the system parameter $\{p, q, a, b, P, P_{pub}, h\}$ periodicity.

- **b. Registration of RSU**

TA chooses the identity ID_R of RSU according to its location, and computes $K_R = h(ID_R||s)$, where T_{RSU}^{reg} is the corresponding registration time. After that, TA saves $< T_{RSU}^{reg}, ID_R >$ to registration list L_{RSU} and sends $\{K_R, ID_R\}$ to RSU.

- **c. Registration of Vehicle**

TA chooses the identity ID_V and two passwords PW_1, PW_2 and then calculates $K_V = h(ID_V||s)$ and$Z_V = K_V \oplus h(PW_1||PW_2)$, where T_{OBU}^{reg} is the corresponding registration time, K_V and Z_V will be used in the modification of passwords if needed. After that, TA saves $< T_{OBU}^{reg}, ID_V >$ to registration list L_{OBU}, and then sends $\{ID_V, PW_1, PW_2, Z_V, T_{OBU}^{reg}\}$ and $\{ID_V, PW_1, PW_2\}$ to OBU and the owner of the vehicle respectively.

B. DRIVING STAGE

At this phase, RSU periodicity broadcasts message $\{ID_R, PK_{RSU}\}$ to all vehicles in its range, where PK_{RSU} is the public key of RSU. Whenever a given vehicle enters the range of a new RSU, OBU generates a pseudo identity and sends it to the corresponding RSU. After that, RSU sends the message related to the vehicles pseudo identity to the TA after receiving and processing the message from the vehicle. TA returns the message to the RSU after confirming the legal presence of RSU and OBU in the registration list based on the timestamp. RSU the broadcasts the corresponding message after the computation process. When the vehicle receives the message and confirms its legitimacy, OBU, RSU and TA should have completed the mutual authentication process. After the authentication process, OBU can issue the traffic information with the help of RSU. The details are as follows:

- **a. Mutual Authentication**

1) Driver needs to input the identity and two passwords ID_V, PW_1, PW_2 to start OBU, and then OBU will check whether ID_V and PW_1, PW_2 are identical to the stored ones. If so, OBU computes $K_V = Z_V \oplus h(PW_1||PW_2)$. After that, OBU chooses a random number $x \in Z_q^*$, and computes $X = x \cdot P$, $X^* = x \cdot P_{pub}$ and $PID_V = ID_V \oplus h(X^*)$. Obviously, the above calculation process can be done off-line in advance.

   When a vehicle enters the range of a new RSU, it computes the two signature hash equations $\sigma_{OBU} = h(T_1||ID_V||ID_R||K_V||X||X^*)$and $\sigma_{check} = h(T_{OBU}^{reg}||T_1||X||PID_V||\sigma_{OBU})$.

   Finally, OBU sends $\{T_{OBU}^{reg}, T_1, X, PID_V, \sigma_{OBU}, \sigma_{check}\}$ to RSU.
2) Upon receiving the message $\{T_{OBU}^{reg}, T_1, X, PID_V, \sigma_{OBU}\}$ sent by the vehicle, RSU checks whether the timestamp T_1 is the latest or not. All the timestamps are tested in the following way: t_1 is the value that the current time value minus the time value contained in the received timestamp, t_2 is the value that the clock difference value plus the time delay value, and then judge that whether t_1 is less than t_2. If yes, that

means it is the latest, than RSU checks whether the equation $\sigma_{check} \overset{?}{=} h(T_{OBU}^{reg}||T_1||X||PID_V||\sigma_{OBU})$ exists. If so, RSU chooses a random number $y \in Z_q^*$ and computes $Y = y{\cdot}P, Y^* = y{\cdot}P_{pub}, PID_R = ID_R{\oplus}h(Y^*)$ and $\sigma_{RSU} = h(T_2||PID_V||X||\sigma_{OBU}||ID_R||K_V||Y||Y^*)$.

Now, RSU saves the item $< T_2, X, Y, Y^* >$ to the handshaking list L_{hs} stored in TPD, and then sends $\{T_{RSU}^{reg}, T_2, Y, PID_R, \sigma_{RSU}, T_{OBU}^{reg}, T_1, X, PID_V, \sigma_{OBU}\}$ to TA. Data stored in TPD are periodically deleted in order to reduce its storage burden.

3) Upon receiving the message $\{T_{RSU}^{reg}, T_2, Y, PID_R, \sigma_{RSU}, T_{OBU}^{reg}, T_1, X, PID_V, \sigma_{OBU}\}$, TA checks whether the timestamp T_2 is the latest. If it is the latest, TA computes $Y^* = Y \cdot s$ and $ID_R = PID_R \oplus h(Y^*)$.

   Now TA checks whether ID_R is contained in the registration list L_{RSU} according to the timestamp T_{RSU}^{reg}. If so, TA computes $K_R = h(ID_R||s)$ and checks whether the equation $\sigma_{RSU} \overset{?}{=} h(T_2||PID_V||X||\sigma_{OBU}||ID_R||K_V||Y||Y^*)$ holds. exists. If so, TA computes $X^* = X \cdot s$ and $ID_V = PID_V \oplus h(X^*)$.

   Third, TA checks whether ID_V is contained in the registration list L_{OBU} according to timestamp T_{OBU}^{reg}. If yes, TA computes $K_V = h(ID_V||s)$ and checks whether the equation $\sigma_{OBU} \overset{?}{=} h(T_1||ID_V||ID_R||K_V||X||X^*)$ exists. If so, TA computes $TAID_V = ID_V \oplus h(Y||Y^*||K_R)$, $\sigma_{TA-RSU} = h(T_3||ID_V||TAID_V||X||ID_R||Y||K_R)$,$TAID_R = ID_R \oplus h(X||X^*||K_V)$ and $ID_V = PID_V \oplus h(X^*)$.

   Finally, TA sends the message $\{T_3, T_2, T_{OBU}^{reg}, \sigma_{TA-OBU}, \sigma_{TA-RSU}, TAID_V, TAID_R\}$ to RSU.

4) Upon receiving the message $\{T_3, T_2, T_{OBU}^{reg}, \sigma_{TA-OBU}, \sigma_{TA-RSU}, TAID_V, TAID_R\}$, RSU checks whether the timestamp T_3 is the latest. If it is the latest, RSU identifies the item $< T_2, X, Y, Y^* >$ in the handshaking list L_{hs} according to T_2, and computes $ID_V = TAID_V \oplus h(Y||Y^*||K_R)$ and further checks whether the equation $\sigma_{TA-RSU} \overset{?}{=} h(T_3||ID_V||TAID_V||X||ID_R||Y||K_R)$ exists. If so, RSU computes $SK = y \cdot X$ and $\sigma_{RSU-OBU} = h(T_4||ID_V||ID_R||X||Y||SK||\sigma_{TA-OBU})$.

   At last, RSU saves the item $< T_{OBU}^{reg}, ID_V, X, Y, SK, \sigma_{TA-OBU} >$ to the authentication list L_{auth} which is stored in TPD, and sends $\{T_4, TAID_R, \sigma_{TA-OBU}, \sigma_{RSU-OBU}, Y\}$ to RSU. To reduce the storage burden of TPD, the data that stored in it will be deleted periodically.

5) Upon receiving the message $\{T_4, TAID_R, \sigma_{TA-OBU}, \sigma_{RSU-OBU}, Y\}$, OBU checks the whether the timestamp T_4 is the latest. If it is the latest, OBU computes the equation $ID_R = TAID_R \oplus h(X||X^*||K_V)$ and checks whether the equation $\sigma_{TA-OBU} \overset{?}{=} h(ID_V||X||X^*||ID_R||Y||K_V)$ exists. If yes, OBU calculates $SK = x{\cdot}Y$ checks whether the equation $\sigma_{RSU-OBU} = h(T_4||ID_V||ID_R||X||Y||SK||\sigma_{TA-OBU})$ exists.

By now, OBU, RSU and TA should have completed the mutual certification process, therefore, the vehicle is legal and RSU has not been compromised.

- **b. Release of Traffic Information**

If a vehicle in travel wants to issue traffic information , OBU sends $\{T_5, m, \sigma_m\}$ to RSU and to other vehicles, where $\sigma_m = h(T_5||m||ID_R||ID_V||X||Y||SK||\sigma_{TA-OBU})$.

- **c. Message Verification**

Upon receiving the message $\{T_5, m, \sigma_m\}$, RSU checks whether the timestamp T_5 is the latest. If it is the latest, RSU finds out the item$< T_{OBU}^{reg}, ID_V, X, Y, SK, \sigma_{TA-OBU} >$ in the authentication list L_{auth} according to the equation $\sigma_m \overset{?}{=} h(T_5||m||ID_R||ID_V||X||Y||SK||\sigma_{TA-OBU})$. If the equation is not satisfied, the message $\{T_5, m, \sigma_m\}$ is invalid.

- **d. Release of Notification Message**

At this stage, the notification message is issued by the RSU, consisting of the bloom filters (a positive filter and a negative filter). The positive filter stores the hash value of legitimate traffic message and their timestamp, and the negative filter stores the hash value of illegitimate Traffic information and their timestamp. [11]. It is encrypted with the private key SK_{RSU} of the RSU which can prevent an attacker from modifying or forging the notification message.

- **e. Receiving Messages**

Upon receiving the notification message from RSU, OBU decrypts it using the public key PK_{RSU} of RSU. If a vehicle wants to verify the validity of the message $\{T_5, m, \sigma_m\}$ sent by the other vehicles, OBU will compute $h(T_5, m)$ and check whether this value is in the notification message. There are three cases of the results, as showed in Table 2.

TABLE 2. The search results.

Case	Positive Filter	Negative Filter	Result of the Message
1	True	False	Valid
2	False	True	Invalid
3	False	False	Wait for next broadcast

Case 1 means that the message is legitimate, and case 2 indicates that the message is illegitimate. Case 3 depicts that the message has not been authenticated by RSU, therefore, the vehicle just needs to wait for the next notification message from RSU.

V. SECURITY ANLYSIS AND COMPARISONS

Security is one of the basic requirements and core elements of VANETs. In this section, the security features of the proposed scheme is proven to ensure that VANETs security requirements have been met, and further the proposed scheme has been evaluated against a few existing security schemes.

A. SECURITY PROOF

The security model of our scheme is to designed construct a game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$ that is, whether the adversary $\mathcal{A}$ can win the game of overcoming the challenge given by the challenger $\mathcal{C}$ in the polynomial time with a non-negligible probability.

Definition 1: In the game constructed by the security model of the CPPA scheme in VANETs, the scheme is secure if the advantage of the adversary $\mathcal{A}$ is negligible in polynomial time.

Theorem 1: The registration of RSU in the proposed scheme is secure in the random oracle model.

Proof: Suppose there is an adversary $\mathcal{A}$ who can forge a legitimate message $\{ID_R, K_R\}$, we construct a challenger $\mathcal{C}$ that can solve the ECDLP problem with a non-negligible probability by running $\mathcal{A}$ as a subroutine.

Setup − Oracle: $\mathcal{C}$ chooses a random number $s \in Z_q^*$ as the master private key, and computes $P_{pub} = s \cdot P$ as the master public key and generates public parameters $\{p, q, a, b, P, P_{pub}, h\}$.

h − Oracle: $\mathcal{C}$ keeps the list L_h which maintains the item of query from $\mathcal{A}$ along with its corresponding answer $\{ID_R, \tau\}$, while the list is initialized to be empty. Upon receiving a query ID_R from $\mathcal{A}$, $\mathcal{C}$ checks whether the item $\{ID_R, \tau\}$ is in the list or not. If yes, $\mathcal{C}$ sends τ to $\mathcal{A}$. Otherwise $\mathcal{C}$ computes $\tau = h(ID_R||s)$, saves $\{ID_R, \tau\}$ to L_h, and sends τ to $\mathcal{A}$.

Sign − Oracle: Upon receiving a query ID_R from $\mathcal{A}$, $\mathcal{A}$ computes $K_R = h(ID_R||s)$ and sends $\{ID_R, K_R\}$ to $\mathcal{A}$. We can know that K_R is the signature of ID_R that is calculated by TA in our scheme.

Output: At last, $\mathcal{A}$ outputs $\{ID'_R, K'_R\}$, and then $\mathcal{C}$ checks whether the equation $K'_R = h(ID'_R||s)$ is satisfied. If not, the game is over and $\mathcal{A}$ fails in the game. If yes, according to the forgery lemma [23], $\mathcal{A}$ will output another valid signature $\{ID''_R, K''_R\}$ when the equation $K''_R = h(ID''_R||s)$ is satisfied.

It means that $\mathcal{A}$ can work out $K''_R - K'_R = h(ID''_R||s) - h(ID'_R||s)$. However, the result is contradictory with the unidirectionality of the secure hash function and the ECDLP is a difficult problem, which means $\mathcal{A}$ cannot work out the above equation. Therefore, theorem 1 is proved.

Theorem 2: The registration of a vehicle in the proposed scheme is secure in the random oracle model.

Proof: Suppose there is an adversary $\mathcal{A}$ who can forge a legitimate message $\{ID_V, K_V, Z_V\}$, we construct a challenger $\mathcal{C}$ that can solve the ECDLP problem with a non-negligible probability by running $\mathcal{A}$ as a subroutine.

Setup − Oracle: $\mathcal{C}$ chooses a random number $s \in Z_q^*$ as the master private key, computes $P_{pub} = s \cdot P$ as the master public key and generates public parameters $\{p, q, a, b, P, P_{pub}, h\}$.

h − Oracle: $\mathcal{C}$ keeps the list L_h which maintains the item of query from $\mathcal{A}$ and its corresponding answer $\{ID_V, \tau\}$, while the list is initialized to be empty. Upon receiving a query ID_V from $\mathcal{A}$, $\mathcal{C}$ checks whether the item $\{ID_V, \tau\}$ is in the list or not. If yes, $\mathcal{C}$ sends τ to $\mathcal{A}$. Otherwise $\mathcal{C}$ computes $\tau = h(ID_V||s)$, saves $\{ID_V, \tau\}$ to , and sends τ to $\mathcal{A}$.

⊕ − Oracle: $\mathcal{C}$ keeps the list $L_\oplus$ which maintains the item of query from $\mathcal{A}$ and its corresponding answer $\{h(PW_1||PW_2), \tau'\}$, while the list is initialized to be empty. Upon receiving a query $h(PW_1||PW_2)$ from $\mathcal{A}$, $\mathcal{C}$ checks whether the item $\{h(PW_1||PW_2), \tau'\}$ is in the list. If yes, $\mathcal{C}$ sends τ' to $\mathcal{A}$. Otherwise $\mathcal{C}$ computes $\tau' = K_V \oplus h(PW_1||PW_2)$, saves $\{h(PW_1||PW_2), \tau'\}$ to $L_\oplus$, and sends τ' to $\mathcal{A}$.

Sign − Oracle: Upon receiving a query ID_V and $h(PW_1||PW_2)$ from $\mathcal{A}$, $\mathcal{C}$ computes $K_V = h(ID_V||s)$ and $Z_V = K_V \oplus h(PW_1||PW_2)$, sends $\{ID_V, h(PW_1||PW_2), K_V, Z_V\}$ to $\mathcal{A}$. We can know that K_V and Z_V is the signature of ID_V and $h(PW_1||PW_2)$ those are calculated by TA in our scheme.

Output: At last, $\mathcal{A}$ outputs $\{ID'_V, h'(PW_1||PW_2), K'_V, Z'_V\}$, and then $\mathcal{C}$ checks whether the equation $K'_V = h(ID'_V||s)$ and $Z'_V = K'_V \oplus h'(PW_1||PW_2)$ is satisfied. If not, the game is over and $\mathcal{A}$ fails in the game. If yes, according to the forgery lemma [23], $\mathcal{A}$ will output another valid signature $\{ID''_V, h''(PW_1||PW_2), K''_V, Z''_V\}$ which the equation $K''_V = h(ID''_V||s)$ and $Z''_V = K''_V \oplus h''(PW_1||PW_2)$ is satisfied.

It means that $\mathcal{A}$ can work out $K''_R - K'_R = h(ID''_V||s) - h(ID'_V||s)$. However, the result is contradictory with the unidirectionality of the secure hash function and the ECDLP is a difficult problem, which means $\mathcal{A}$ cannot work out the above equation. Therefore, theorem 2 is proved.

Theorem 3: The process of sending an authentication message by OBU in the proposed scheme is secure in the random oracle model.

Theorem 4: The process of calculating an authentication message from OBU by RSU in the proposed scheme is secure in the random oracle model.

Theorem 3 and Theorem 4 can be proved by the same way. Therefore, the proposed scheme is secure in the random oracle model.

The next section analyzes the security requirements of the CPPA scheme in VANETs.

1) *Identity privacy preservation:* Normally, the vehicle only sends the pseudo identity once it comes within the range of RSU. Pseudo identity is computed by the equation $X^* = x \cdot P_{pub}$ and $PID_V = ID_V \oplus h(X^*)$, where $x \in Z_q^*$ is a random number. Therefore, no attacker can obtain the real identity ID_V of the vehicle through the pseudo identity PID_V. It means that our proposed scheme has met the requirements of identity privacy preservation.
2) *Traceability:* RSU can search the item $< T^{reg}_{OBU}, T_5, m, ID_V >$ according to T_5 in the message list L_m when it encounters malicious messages, and then sends $< T^{reg}_{OBU}, ID_V >$ to TA. TA can search the item $< T^{reg}_{OBU}, ID_V >$ according to T^{reg}_{OBU} in the registration list L_{RSU} while RSU is comprised.
3) *Non-repudiation:* RSU can search out the item $< T^{reg}_{OBU}, T_5, m, ID_V >$ according to the timestamp T_5 in the message list L_m quickly, which includes the real identity of the vehicle and its registration time. Therefore, our scheme has met the requirements of Non-repudiation.
4) *Un-linkability:* The format of message related to traffic information in our proposed scheme is $\{T_5, m, \sigma_m\}$, where $\sigma_m = h(ID_R||ID_V||X||Y||SK||\sigma_{TA-OBU}||m||T_5)$,

therefore, the attacker cannot determine whether the two given messages are issued by the same vehicle using the message content, which achieves the security requirements of un-linkability.

5) *Resistant to continuous disruption:* TA will delete the registration form in the corresponding registration list when either the real identity of a malicious vehicle or a compromised RSU is detected. Therefore, when either a malicious vehicle is authenticated by a valid RSU or a legitimate vehicle is authenticated by a compromised RSU, TA will immediately stop the certification process to prevent continuous damage.
6) *Modification of passwords:* The owner of a vehicle can change the passwords anytime anywhere whenever he considers the passwords is not secure and the details are as follows. Owner inputs $ID_V, PW_1^{old}, PW_2, PW_1^{new}$ to start OBU. OBU will check whether ID_V and PW_1^{old}, PW_2 are identical to the stored ones. If yes, OBU computes $K_V = Z_V \oplus h(PW_1^{old}||PW_2)$ and $Z_V^{new} = K_V \oplus h(PW_1^{new}||PW_2)$. At last, OBU only needs to replace Z_V^{old} with Z_V^{new}.
7) *Resistance to ordinary attacks:*
    - *Replay attack:* RSU will check the timestamp while receiving a message, once it is found not to be the latest, RSU will drop it immediately.
    - *Modification attack:* It is impossible that the attacker can modify a legal message $\{T_5, m, \sigma_m\}$ to $\{T_5, m', \sigma'_m\}$ where $\sigma'_m = h(ID_R||ID_V||X||Y|| SK||\sigma_{TA-OBU}||m'||T_5)$, while the sent real identity of a vehicle $\{T_5, m, \sigma_m\}$ is unknown.
    - *Impersonation attack:* If the attacker wants to send a legal message by impersonating the legal vehicle, it must obtain the real identity of the vehicle. However the attacker cannot obtain the real identity of the vehicle according to the preceding knowledge. Therefore, our proposed scheme can resist the impersonation attack.

B. SECURITY COMPARISONS

In general, the security requirements of VANETs mainly span across message authentication, preservation of identity privacy, traceability, un-linkability, resistant to continuous disruption, modification of passwords, and resistance to ordinary attacks. We evaluate the performance of our scheme against four existing schemes in terms of the security requirements of VANETs. The results are presented in Table 3.

Among the evaluated schemes, the other four schemes are not resistant to continuous disruption and modification of passwords. Though, our proposed scheme effectively satisfies all the security requirements of VANETs.

VI. PERFORMANCE ANALYSIS

The performance of VANETs is susceptible to computation and communication overheads due to the rapid speed of the vehicles and the rapid changes in the network topology.

TABLE 3. Security comparisons.

	Shim et al.[13]	Zhang et al.[14]	He et al.[17]	Zhong et al.[18]	The proposed scheme
Preservation of identity privacy	√	√	√	√	√
Traceability	√	√	√	√	√
Un-linkability	×	√	√	√	√
Resistant to continuous disruption	×	×	×	×	√
Modification of passwords	×	×	×	×	√

TABLE 4. The definition and execution time of related operations.

Operation	Definition	Execution time(ms)
T_{sm-bp}	The time of a scale multiplication operation in a group based on bilinear pairing	0.694
T_{sm-ecc}	The time required for performing a scalar point multiplication in a group based on ECC	0.3218
$T_{sm-bp-s}$	The time required for performing a small scalar point multiplication in a group based on ECC	0.0736
$T_{sm-ecc-s}$	The time of a scale multiplication operation in a group based on bilinear pairing	0.0246
T_{pa-bp}	The time of a point addition operation in a group based on bilinear pairing	0.0018
T_{pa-ecc}	The execution time of a point addition operation based on ECC	0.0024
T_{bp}	The time required to execute a bilinear pairing operation.	5.086
T_h	The execution time of a general hash function operation	0.001
T_{mtp}	The time required for executing a hash function that maps a string to a point in group	0.0992

A. COMPUTATION OVERHEAD ANALYSIS

The CPPA schemes proposed by Shim *et al.* [13] and Zhang *et al.* [14] are based on bilinear pairing, where the additive group G with the order q and its generator Pconstitutes all points on the elliptic curve E defined by the equation $y^2 = x^3 + x \bmod p$, where p is a 512-bit prime number and q is a 160-bit prime number. The schemes proposed by He *et al.* [17] and Zhong *et al.* [18] are based on Elliptic Curve Cryptography (ECC) to achieve the same level of security, where the additive group $\overline{G}$ with the order q and its generator $\overline{p}$constitutes all points on the elliptic curve $\overline{E}$ defined by the equation $y^2 = x^3 + ax + b \bmod \overline{p}$, where $a, b \in F_p, \overline{p}$ and q is a 160-bit prime number. The cryptography library used in our experiment is MIRACL[30], which is a well-known and widely used cryptographic library in computing the time required for various cryptographic operations. And our hardware platform consists of an Intel I7-6700 processor8 gigabytes memory and runs Windows 7 operating system. The definition and execution time of related operations in cryptography are shown in Table 4.

TABLE 5. The comparison of the execution time.

Scheme	Single traffic-related message	n traffic-related messages
Shim et al.[13]	$3T_{sm-bp}$ $+2T_{pa-bp}+1T_h$ ≈ 2.0866ms	$(3n)T_{sm-bp}$ $+(2n)T_{pa-bp}$ $+nT_h$ $\approx 2.0866n$ ms
Zhang et al.[14]	$6T_{sm-bp}+2T_{pa-bp}$ $+1T_{mtp}+4T_h$ ≈ 4.2708 ms	$(6n)T_{sm-bp}$ $+(2n)T_{pa-bp}$ $+(4n)T_h$ $\approx 4.2708n$ ms
He et al.[17]	$3T_{sm-ecc}+3T_h$ ≈ 0.9684 ms	$(3n)T_{sm-ecc}$ $+(3n)T_h$ $\approx 0.9684n$ ms
Zhong et al.[18]	$2T_{sm-ecc}+2T_h$ ≈ 0.6456 ms	$(2n)T_{sm-ecc}$ $+(2n)T_h$ $\approx 0.6456n$ ms
The proposed scheme	$1T_{sm-ecc}+6T_h$ ≈ 0.3278 m	The worst case: $nT_{sm-ecc}+(6n)T_h$ $\approx 0.3278n$ ms The best case: $1T_{sm-ecc}+(n+5)T_h$ $\approx 0.001n+0.3218$ ms

The calculation and storage capacity of OBU are low and the number of vehicles is more than RSU, therefore one of the purposes of our scheme is to reduce the OBUs computation overhead. The performance evaluation of the schemes in terms of the execution time consumed to send traffic-related message (that is generating the pseudo identity and message signature) by OBU is shown in Table 5.

In the scheme of Jianhong *et al.* [14], the execution time of issuing single traffic-related messages is $6T_{sm-bp}+2T_{pa-bp}+1T_{mtp}+4T_h \approx 14.6746$ ms and the execution time of issue n traffic-related message is $(6n)T_{sm-bp}+(2n)T_{pa-bp}+(4n)T_h \approx 14.6746n$ ms, while the execution time in the scheme proposed by Zhong *et al.* [18] is $2T_{sm-ecc}+2T_h \approx 0.8842$ ms and $(2n)T_{sm-ecc}+(2n)T_h \approx 0.8842n$ ms respectively.

In our scheme, whenever the vehicle enters the range of a new RSU, it is necessary to send the identity authentication message to RSU, and the RSU will send messages to TA after processing the identity authentication message which ensures that no malicious vehicle or compromised RSU is involved in the transmission process of traffic-related message. When n traffic-related messages needs to be sent, the worst case is that the OBU sends an identity authentication message to the RSU for each traffic-related messages. Therefore the execution time of OBU is $nT_{sm-ecc}+(6n)T_h \approx 0.4426n$ ms. While the best case is when OBU sends the identity authentication message only once in the range of RSU, therefore the execution time of the OBU is $1T_{sm-ecc}+(n+5)T_h \approx 0.0001n+0.4435$ ms.

Consider, the coverage of the RSU is about 600 m, the vehicle speed is between 0 km/h and 120 km/h [7] and the time taken for sending traffic information message is 100-300 ms [24]. Now, OBU needs to send at least 50 traffic-related messages in the range of RSU. From Fig. 2, the execution time required by OBU to issue traffic-related message in our proposed scheme is much less than that of the other four schemes even in the worst case.

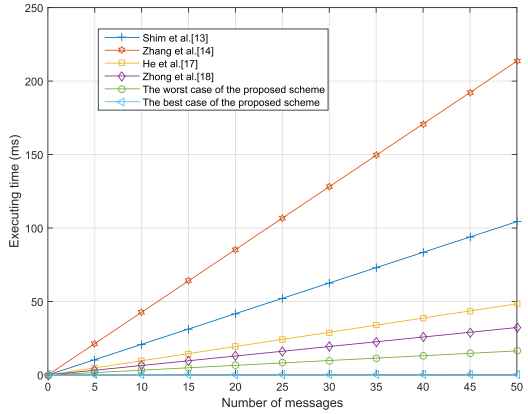


FIGURE 2. The comparison of the execution time.

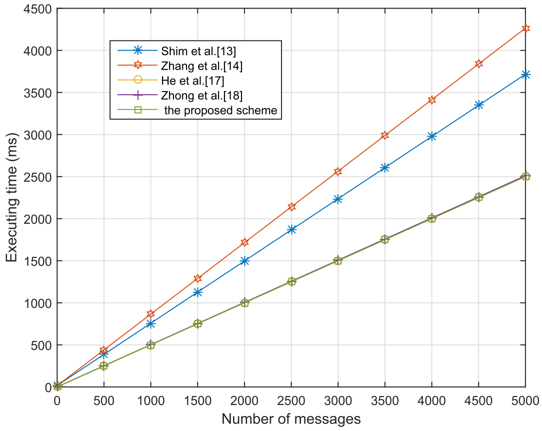


FIGURE 3. The comparison of authenticating message time.

The speed of traffic-related message verification process also determines the computation efficiency of VANETs. Assuming there are 500 vehicles in the range of RSU, the RSU needs to verify 2500-5000 messages per second [25].

Traffic-related message verification process in our scheme is carried out by RSU which usually comprises more storage and computing power. RSU issues the notification information which is encrypted with the private key and the OBU only needs to decrypt the notification information using the public key, and the operation time of decryption is negligible. Upon receiving the traffic information message, the RSU will find out the item $< T_{OBU}^{reg}, ID_V, X, Y, SK, \sigma_{TA-OBU} >$ in the list L_{auth} which satisfies the signature equation. Considering the storage capacity of TPD in the VANETs, TPD will delete the private data before a certain time. Therefore, the data in the list L_{auth} will be deleted periodically, and the number of item in the list is usually maintained at a level more than that of vehicles in order to continue the process when the vehicle speed is low. Assuming there are 500 vehicles within the RSU coverage, the number of item saved in the list L_{auth} is 1000, the best case in message authentication process is that only one hash function is performed and the worst case is carried out with 1000 hash functions. The execution time of the message verification process with 500 hash functions by all the evaluated schemes is depicted in Table 6.

TABLE 6. The execution time of message verification process.

Scheme	Single traffic information	n traffic information
Shim et al.[13]	$3T_{bp} + 2T_{sm-bp}$ $+1T_{pa-bp} + 2T_h$ ≈ 16.6498ms	$3T_{bp} + (2+1)T_{sm-bp}$ $+(3n-3)T_{pa-bp} + 2nT_h$ $\approx 0.74n + 17.3346$ ms
Zhang et al.[14]	$3T_{bp} + 2T_{sm-bp}$ $+1T_{pa-bp} + 3T$ ≈ 16.6508 ms	$3T_{bp} + (n+1)T_{sm-bp}$ $+(2n)T_{sm-bp-s}$ $+T_h(3n-2)T_{pa-bp}$ $+(3n)T_h$ $\approx 0.8496n + 15.9484$ ms
He et al.[17]	$3T_{sm-ecc} + 2T_h$ $+2T_{pa-ecc}$ ≈ 0.9722 ms	$(n+2)T_{sm-ecc}$ $+(2n)T_{sm-ecc-s}$ $+(3n-1)T_{pa-ecc}$ $+(2n)T_h$ $\approx 0.5003n + 0.6412$ ms
Zhong et al.[18]	$3T_{sm-ecc} + 2T_h$ $+1T_{pa-ecc}$ ≈ 0.9698 ms	$(n+2)T_{sm-ecc}$ $+(2n)T_{sm-ecc-s}$ $+(2n-1)T_{pa-ecc}$ $+(2n)T_h$ $\approx 0.5021n + 0.6412$ ms
The proposed scheme	$500T_h$ ≈ 0.5 ms	$(500n)T_h$ $\approx 0.5n$ ms

From Fig.3, it can be observed that the time consumed to authenticate a message in the schemes proposed by Shim *et al.* [13] and Jianhong *et al.* [14] is similar, and the time consumed in our scheme is significantly lower than them. Yet, the result is almost the same to the schemes proposed by He *et al.* [17] and Zhong *et al.* [18]. However, the above results are based on the fact that all of the authenticated messages are legitimate, but batch authentication usually fails when illegal messages appear. Under such a scenario, the TA only detects the illegal messages by adopting the binary search strategy [11], which will lead to obvious reduction in the efficiency of batch authentication. Although our proposed scheme does not support batch certification, the efficiency of the message verification process is relatively stable, thus our scheme is superior to the other evaluated schemes in VANETs.

B. COMMUNICATION OVERHEAD ANALYSIS

This section evaluated the communication overhead efficiencies of the evaluated schemes. The additive group G with the order q and its generator Pconstitutes all the points on the elliptic curve E defined by the equation $y^2 = x^3 + x \bmod p$, where p is a 512-bit prime number and q is a 160-bit prime number. The additive group $\overline{G}$ with the order q and its generator $\overline{p}$constitutes all the points on the elliptic curve $\overline{E}$ defined by the equation $y^2 = x^3 + ax + b \bmod \overline{p}$, where $a, b \in F_p$, $\overline{p}$ and q is a 160-bit prime number. Therefore, the size of each element in G and $\overline{G}$ is 128 bytes and 40 bytes respectively [26]. We assume that the timestamp and the output of the secure hash function are 4 bytes and 20 bytes respectively [27] and the size of each element in Z_q^* is 20 bytes. If the traffic information in the messages are the same, we only need to consider the message length. Table 7 presents the communication overhead performance of the evaluated schemes.

In CPPA scheme of VANETs, the value T in the traffic-related message denotes the timestamp. As is shown in Table 7, the traffic-related messages in the scheme of He *et al.* [17] are $\{M, AID, T, R, \sigma\}$, where $AID = \{AID_1, AID_2\}$, $AID_1, R \in \overline{G}$ and $AID_2, \sigma \in Z_q^*$, and the length of a single traffic-related message is $40 * 2 + 20 * 2 + 4 = 124$ bytes. Moreover, In the CPPA scheme of Zhong *et al.* [18], the vehicle broadcasts the traffic-related messages $\{AID, M, \sigma, T\}$ to others, where $AID = \{AID_1, AID_2\}$, $AID \in \overline{G}$ and $AID_2, \sigma \in Z_q^*$, and the length of a single traffic-related message is $40 + 20 * 2 + 4 = 84$ bytes. Traffic-related messages are $\{T, m, \sigma\}$ in our proposed scheme, where $\sigma \in Z_q^*$, and the length of a single traffic-related message is $20 + 4 = 24$ bytes.Therefore, the proposed scheme is superior to the other four schemes in terms of reducing the communication overheads. Thus, from the aforementioned comparative evaluations of the schemes in terms of reducing the computation and communication overheads, we can draw the conclusion that our proposed scheme has obvious advantages than the other four schemes in both the aspects. Therefore, our scheme can accommodate more transmission tasks while realizing higher level of security in VANETs, and it is more suitable for VANETs.

TABLE 7. The comparison of communication overhead.

Scheme	Single message	n messages
Shim et al.[13]	644	$644n$
Zhang et al.[14]	388	$388n$
He et al.[17]	124	$124n$
Zhong et al.[18]	84	$84n$
The proposed scheme	24	$24n$

VII. CONCLUSION AND FUTURE WORK

This paper proposed a novel and practical ID-based CPPA scheme based on invocating the registration list to reflect the role of the revocation list. The proposed scheme greatly reduces the time taken to retrieve the registration list and effectively improves the security of VANETs. Moreover, our scheme does not use bilinear pairing, which is the most complicated operation in modern cryptography, and effectively reduces the length of messages sent by vehicles. Therefore, the proposed scheme also effectively improves the communication performance and efficiency of VANETs.

Security analyses showed that the proposed scheme is not only effective in satisfying the basic security requirements of VANETs but also efficient in preventing the malicious vehicle or the compromised RSU from disrupting VANET security protocols because of the presence of the registration list. Performance analyses demonstrated that our proposed scheme achieves better performance in reducing both the computation overhead and the communication overhead compared to existing schemes, and further exhibits better practical application in current VANETs. As future work, we plan to study means of reducing the operation time of the TA and RSU and the delay time between them, which can obviously increase the security and efficiency of VANETs.

ACKNOWLEDGMENT

The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

REFERENCES

[1] P. Papadimitratos, A. De La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 84–95, Nov. 2009.

[2] A. Boukerche, H. A. B. FOliveira, E. F. Nakamura, and A. A. F. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," *Comput. Commun.*, vol. 31, no. 12, pp. 2838–2849, 2008.

[3] *IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages*, IEEE Standard 1609.2a, Intelligent Transportation Systems Committee, 2013.

[4] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[5] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[6] V. Daza, J. Domingo-Ferrer, and F. Sebé, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1876–1886, May 2009.

[7] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[8] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2008, pp. 1451–1457.

[9] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[10] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[11] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, 2011.

[12] S.-J. Horng *et al.*, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[13] K.-A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

[14] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *Int. J. Netw. Secur.*, vol. 16, no. 5, pp. 351–358, 2014.

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

[16] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Expert Syst. Appl.*, vol. 41, no. 5, pp. 2559–2564, 2014.

[17] 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. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[18] H. Zhong, J. Wen, J. Cui, and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET," *Tsinghua Sci. Technol.*, vol. 21, no. 6, pp. 620–629, 2016.

[19] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.

[20] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[21] W. Mao, *Modern Cryptography: Theory and Practice*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2003.

[22] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Des., Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, Mar. 2000.

[23] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.

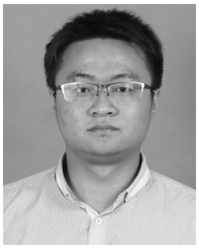
[24] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[25] Y. Liu, L. Wang, and H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3697–3710, Aug. 2014.

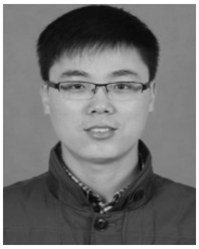
[26] L. Martin, *Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*, document RFC 5091, 2007.

[27] C. Adams and D. Pinkas, *Internet x. 509 Public Key Infrastructure Time Stamp Protocol (TSP)*, document RFC 3161, 2001.

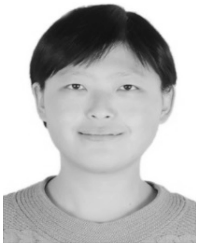
HONG ZHONG received the Ph.D. degree from the University of Science and Technology of China in 2005. She has been a Professor and the Dean of the School of Computer Science and Technology, Anhui University, China, since 2009. She has published over 100 papers. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, and software-defined networking.



BO HUANG is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, Anhui University. His research interest is vehicle ad hoc network.



JIE CUI received the Ph.D. degree in computer science and technology from the University of Science and Technology, China, in 2012. He is currently an Associate Professor with the School of Computer Science and Technology, Anhui University, China. He has published over 50 papers. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, and software-defined networking.



YAN XU received the Ph.D. degree from the University of Science and Technology of China in 2015. She is currently a Lecturer with the School of Computer Science and Technology, Anhui University, China. Her research interests cover network and information security.

LU LIU received the M.Sc. degree in data communication systems from Brunel University, U.K., and the Ph.D. degree from University of Surrey, U.K. (funded by DIF DTC). He is currently a Professor of distributed computing with the University of Derby, U.K. His research interests are in areas of cloud computing, service computing, computer networks and peer-to-peer networking. He is a Fellow of British Computer Society.