Research Article

Efficient Message Authentication Scheme with Conditional Privacy-Preserving and Signature Aggregation for Vehicular Cloud Network

Yong Xie ¹, **Fang Xu** ², **Dong Li**¹ and **Yu Nie**³

¹Department of Computer Technology and Application, Qinghai University, China

²School of Computer and Information Science, Hubei Engineering University, Xiaogan, China

³School of Computer and Information Science, Jingdezhen Ceramic Institute, Jingdezhen, China

Correspondence should be addressed to Fang Xu; xf2012@whu.edu.cn

Received 11 April 2018; Revised 10 August 2018; Accepted 30 August 2018; Published 23 September 2018

Academic Editor: Kim-Kwang Raymond Choo

Copyright © 2018 Yong Xie et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Vehicular cloud network (VCN) is deemed as the most promising platform for providing transportation safety, road optimization, and valued-added application services. Because VCN is of distinguishing feature with super-large scale and unstable communication, it is a challenging task to study efficient authentication scheme for VCN without losing security and conditional privacy-preserving. To meet the challenge, a new efficient message authentication scheme is proposed in this paper. A batch message verification and signature aggregation are included in the proposed scheme to improve the authentication efficiency and decrease the communication cost. Compared with the similar conditional privacy-preserving authentication schemes, the proposed scheme has superior performance in computation and communication cost. Simulation analysis further proves that the proposed scheme has better advantages in reducing the verification loss rate and message delay in the application of VCN.

1. Introduction

As the growing demand for transportation safety, driver comfort, and traffic efficiency, it is crucial for vehicles to obtain current traffic-related information accurately and timely. To meet the goal, vehicular ad hoc networks (VANETs) have been raised and caused heated joint researches among researchers, car manufactures, and governments in recent years [1]. Due to the specific features and applications of VANETs, people expect that a vehicle can perform all the tasks of communication, computing, sensing, and storage. On the one hand, a vehicle has some in-car resources, such as sensor, power, CPU, communication units, and actuator, and it should schedule the in-car resource harmoniously to achieve optimal efficiency. On the other hand, a vehicle should cooperate with other units, such as other vehicles and Roadside Units (RSUs), to make use of the unstable external resources in an effective way [2]. Therefore, vehicle will gradually become a complicated integrated intelligent system with computing, mechanical, and communication function in the near future.

Because cloud computing technology has shown many outstanding advantages in practice application, some researchers have proposed vehicular cloud computing, which has been a new paradigm employed by vehicle (driver) to leverage services as a utility and handle a mass of data on demand at any time and anywhere [3]. Thus, to improve efficiency of vehicle-related services to vehicles, some interesting vehicular cloud network (VCN) architectures over VANETs have been proposed recently [4, 5]. A general VCN architecture consists of three tiers: the top tier includes the trusted authority (TA) and cloud servers; the middle tier includes intermediate units including road side units (RSUs), 3/4G base stations (BSs), and other network access units; the bottom tier includes in-car units of vehicles including On-Board Unit (OBU), sensors, 3/4G module, and other modules, as shown in Figure 1. RSUs and BSs are placed on the side of road and can communicate with TA and cloud servers via wired communication. OBU is in charge of communication with other vehicle's OBUs by Vehicle-to-Vehicle (V2V) communication technology, and it also can communicate with RSUs by Vehicle-to-Infrastructure (V2I)

FIGURE 1: A general VCN architecture.

communication technology. Ranging from transportation safety to valued-added application services, VCN is regarded as one of the most promising platforms for future vehicle-centered applications [6].

Nonetheless, benefits usually come with challenges. Because messages in VCN are usually life-critical, the foremost issue is security that the messages must be authenticated and reliable [7]. Nowadays, privacy protection has become the most urgent requirement that users are most concerned about in the open and insecure wireless communication environment [8, 9]. If an attacker could retrieve the private information of a vehicle by linking the messages, the most promising VCN will be gutted. Therefore, the second important issue is privacy-preserving. However, privacy-preserving is the double-edged sword of VCN: A honest vehicle is willing to broadcast real message to its neighbor vehicles; a malicious vehicle may send wrong messages for personal gain by abusing the privacy protection mechanisms, where wrong message has a valid signature and untrue content. Because a wrong message may cause inestimable damage to the traffic system or people's personal safety, there must be one and only one (usually is the TA) that should have the ability to trace the real identity of wrong message generator. Therefore, conditional privacy-preserving (CPP) should be involved in VCN. It is generally known that a huge volume of messages of VCN may be produced in a short time and the communication instability problems of VCN is particularly serious. In order to improve the quality of VCN service, it should decrease communication cost and computation cost. Therefore, the third key issue is to improve authentication efficiency and decrease communication cost without losing security and cryptographic witnesses. To solve the three challenges, industry and academia have done a lot of research works and put forward a lot of interesting results [10].

1.1. Motivations and Contributions. In VCN, there are usually millions of messages being produced in a very short time, and many messages must be processed timely because they

are time sensitive and life-critical. However, it is an arduous task for OBUs or RSUs to verify vast messages timely [11]. Thus, it is a significant challenge to design a practical message authentication scheme for VCN under the precondition of ensuring safety and conditional privacy-preserving.

To meet this challenge, we propose a new message authentication scheme with CPP and signature aggregation. In short, our main contributions can be summarized as follows:

(i) A new efficient message authentication scheme is proposed for VCN using elliptic curves cryptography (ECC). Signature aggregation and batch verification are involved to improve verification efficiency further, where the batch verification allows verifier to verify multiple messages simultaneously and the signature aggregation allows verifiers to aggregate multiple signatures into a single one before forwarding them to its top manager (e.g., cloud servers).

(ii) A rigorous security analysis shows that the proposed scheme could satisfy all security requirements of VCN and provides CPP.

(iii) Performance analysis indicates that our proposed scheme can perform much better in terms of computation cost and the communication cost than most recent schemes proposed in [12–14]. The signature aggregation of the proposed scheme could further decrease communication cost. Simulations show that the proposed scheme also could reduce verification loss rate and message delay in VCN scenario.

1.2. Organization of the Paper. The rest of the paper is organized as follows. Preliminaries and background are introduced in Section 2. Section 3 shows background and Section 4 puts forward a new message authentication scheme for VCN. Section 5 demonstrates security proof and analysis. Section 6 discusses complexity analysis and comparisons. The last section concludes the current and future works.

2. Related Work

To achieve CPP authentication, some researchers have proposed classic authentication schemes by using group signature [15–18]. Before a vehicle communicates with other vehicles, it should join in the group to get signing key from the group manager. After then the vehicle uses signing key to sign messages on behalf of the group. Only the group manager can retrieve the identity of message signer, so this kind of authentication schemes can meet conditional privacy-preserving requirement. But, these authentications have much higher communication and computation cost than traditional signatures and have inextricable problem on member revocation [19].

To decrease communication and computation cost, Raya et al. [20] adopted anonymous certificate based on Public Key Infrastructure (PKI) to construct an anonymous authentication scheme for vehicle network. Later, some similar CPP authentication scheme has been proposed [16, 21, 22]. However, it is extremely difficult for these schemes using PKI to overcome issues related to certificate management.

To overcome certificate issues, researchers introduced identity-based public key cryptosystem (ID-PKC) [23] to design message authentication scheme for vehicle network, where no certificate is needed to bind to public key pairs. Zhang et al. [24] used bilinear pairing to construct message authentication scheme based on IP-PKC. Zhang et al.'s scheme [24] no longer needs any certificates. Unfortunately, relay attack and impersonation attack can be launched easily in their scheme. By using two shared secrets, Chim et al. [25] put forward one identity-based authentication scheme. Under the condition of providing anonymity, Chim et al.'s scheme need less communication cost than Zhang et al.'s [24]. But, Chim et al.'s scheme is demonstrated to suffer from impersonation attack. Lee et al. [4] presented a new message authentication scheme employing bilinear pairing. Unfortunately, their scheme could not provide tracing and nonrepudiation and also suffers from relay attacking. To overcome secure issues, Bayat et al.'s [12] presented an reformative authentication scheme over Lee et al.'s scheme [4]. They demonstrated security analysis to show that their scheme can resist various security attacks. However, the aforementioned schemes based on PKC use complex bilinear pairing operations, which is quit complex cryptographic operation in modern cryptography and not suited for OBUs that is limited in computational capacity. To wipe off bilinear pairing, He et al.'s [14] proposed a new conditional preserving scheme by using ECC. He et al. demonstrated that their scheme takes more lower computation cost and communication cost, which makes their scheme more suited for deployment in VCN. Xie et al. [26] proposed an identity-based message authentication scheme for vehicle network using ECC. Their scheme provides not only single message verification but also batch message verification; it can decrease much authentication costs. Unfortunately, it can not provide aggregate authentication. Kang et al. [27] used homomorphic encryption to allow every vehicle to generate any number of authenticated identities to realize anonymity in vehicle network. Recently, Liu et al. [28] proposed a mutual authentication and key agreement scheme for secure vehicle-to-vehicle communication. But the TA should include each authentication process in their scheme, which brings a very large computational overhead to the TA.

Signature aggregation on cryptographic witnesses has drawn more attention due to its special way to improve system performance. Zhang et al. [19] proposed an aggregate privacy-preserving authentication scheme for VANETs. In their scheme, aggregate signature technique is used as an important way to decrease computation and communication overhead during data transmission and signature authentication. But when a vehicle joins a RSU authentication group, the RSU must forward vehicle's information to the root TA through a secure channel. Wasef et al. [29] proposed aggregation protocols based on PKI in vehicle ad hoc network, respectively. The two protocols can aggregate multiple signatures into a single one but cannot aggregate different certificates, which remains a problem on certificate management. To eliminate problem on certificate management, signature aggregation based on identity-based PKC was proposed in [30]. Zhang et al. [13] proposed a hierarchical aggregation to suit for hierarchical

management in VANETs. In their scheme, a secure channel must be preestablished between an RSU and the KGC for vehicle's identity authentication.

All kinds of identity-based schemes for vehicle networks proposed during the last decades can be divided into two major categories. One is using traditional authentication way without using Tamper-proof devices (TPD) [31]; the other more efficient authentication way is by using TPDs. Compared with non-TPD, schemes using TPD are more efficient. Therefore, we construct the proposed scheme using TPD to solve the very arduous message authentication tasks in vehicular cloud network.

3. Background

3.1. System Architecture of VCN. The three-tier architecture proposed in [32] is used in this paper. The top tier consists of the trusted authority (TA) and cloud services, the middle tier consists of intermediate units, the bottom tier consists of in-car units of vehicles, as shown in Figure 1.

(i) *Top Tier.* The same assumption applies with [13]; the TA is a fully trusted administrator, and it is in charge of generating system parameters and allocating Tamper-proof devices (TPD) to each registered role, such as RSUs, vehicles, and cloud serves. A secure access password will be set according to the rules proposed in [33, 34] for each TPD and can be used when the user inputs the correct password. In the system, only the TA is able to retrieve the real identities from valid messages when necessary. The TA is assumed to be never compromised by any adversaries. The cloud services are provided cloud servers by using cloud computing technique and are usually made up of road traffic monitoring, diver body monitoring, whether information, entertainment service, and other services that can be customized by users.

(ii) *Middle Tier.* This tier consists of communication entities, such as RSU, Base stations, and satellite (for connecting to Internet), GPS module (for connecting to satellite network), and 3/4G communication module (for connecting 3/4G wireless network). RSUs are a number of substance units placed on the side of roads. A RSU communicates with vehicles' OBUs by using DSRC protocol and with TA and cloud servers using wired channel. A RSU must verify signatures as soon as receiving messages from vehicles and decides whether to process them locally or deliver them to the top server (including cloud service). BS and satellite connect the 3/4G module and GPS module of vehicles, respectively.

(iii) *Bottom Tier.* This tier consists of On-Board Unit (OBU), TPD, GPS module, 3/4G module, sensors and reactors, and other in-car units. The TA will issue a TPD for each registered vehicle. TPD has high-level ability to withstand any security attacks and no one can extract any data from TPDs, such as secret key and codes [12, 16]. Any message will be signed by TPD before being broadcasted. The OBU collects raw data from other in-car units and then broadcasts messages about traffic status and other service request message. In addition, it is also responsible for communicating with other OBUs and

RSUs under DSRC protocol. The 3/4G module is responsible for communicating with the BS.

3.2. Security Requirements. A lot of attacks threaten the security of VCN, such as privacy disclosure, relay attack, man-in-the-middle attack, and modification attack. To avoid these attacks, the following security requirements should be provided in the authentication scheme.

(1) *Message Authentication.* In VCN, each verifier can authenticate every message and determines whether the message signer is a registered member and judges whether the message is modified by others.

(2) *Conditional Privacy-Preserving (CPP)* [35]. As with other scenarios of privacy protection, the true identity of the vehicle should be anonymous, including other vehicles, RSUs, and attackers. But registered vehicles with malicious behavior may abuse anonymous mechanism and broadcast wrong messages. In order to restrict the registered vehicles to use anonymity mechanism in rational way, the TA must extract the signer of valid message (with valid signature). As a consequence, authentication schemes must provide CCP functionality [36].

(3) *Resistance to Attacks.* To meet the requirements of security, authentication schemes must be able to withstand all possible attacks, e.g., forgery attack and man-in-the-middle attacks.

4. The Proposed Scheme

In this section, we propose a new efficient identity-based authentication scheme for VCN, which achieves CPP functionality. The proposed scheme includes four phases: initialization, pseudonym generation and message signing phase, message verification phase, and identity extraction phase. To improve efficiency, batch message verification and signature aggregation are involved in message verification phase.

In order to understand the phases of the proposed scheme more intuitively, the main phases of proposed scheme are illustrated as in Figure 2. In Figure 2, PMS denotes Pseudonym Generation and Message Signing, which is executed by the messages signer, i.e., vehicles; SMV, BMV, and SA denote single message verification, batch message verification, and signature aggregation, respectively, which are executed by low-level verifier, such as RSUs or vehicles; AMV denotes aggregated messages verification, which is executed by top manager, such as cloud servers or application servers.

Next, we will show the details of each phase as in the following subsections.

4.1. Initialization. In this phase, the system parameter is initialized by the TA, the detailed steps are as follows:

I1: the TA selects an elliptic curve $E_p(a, b)$, which is defined by $y^2 = x^3 + ax + b \mod p$, where p is a large prime number, $a, b \in F_p$. Then the TA chooses a generator point P from $E_p(a, b)$, and generates group G by P with order q .

FIGURE 2: The main phases of proposed scheme.

Next, the TA chooses $s \in {}_R Z_q^*$ as its private key and computes public key $P_{pub} = s \cdot P$.

I2: two hash functions, $h_1 : G \rightarrow Z_q$, $h_2 : \{0, 1\}^* \rightarrow Z_q$, are chosen as cryptographic hash function. Now, $params = \{E_p(a, b), p, q, P, h_1, h_2, P_{pub}\}$ is set as system public parameter.

I3: when a vehicle V_i registers in the system, the TA assigns a TPD to the vehicle, where the TPD will be preloaded parameters $\{RID_i, PWD_i, s, params\}$. Therefore, each vehicle will obtain unique identifier RID_i and password PWD_i .

I4: at last, the public parameter $params$ is published to each registered vehicle, RSU and cloud server.

4.2. Pseudonym Generation and Message Signing Phase. When a vehicle V_i wants to broadcast or send a message, it generates a pseudonym and sign messages by using its TPD as follows.

S0: the user input the valid RID_i and PWD_i to gain the right to use the TPD. To be practical, the user can employ the TPD to generate pseudonym for a period after he/she has input valid RID_i and PWD_i ; i.e., this step will not be run during the next period, while steps **S1-S3** will be run in this phase.

S1; when a message m_i is generated by the OBU or sensors, it is transmitted to the TPD.

S2: on receiving m_i , the TPD chooses $r_i \in {}_R Z_q^*$ and current timestamp T_i and then calculates $PID_{i,1} = r_i \cdot P$, $PID_{i,2} = RID_i \oplus h_1(r_i \cdot P_{pub})$. Let PID_i denote $\{PID_{i,1}, PID_{i,2}\}$. Next, the TPD computes $h_i = h_2(m_i, PID_i, T_i)$, $\delta_i = (r_i + h_i)/s$. Finally, the TPD sends $m_i, PID_i, T_i, \delta_i$ to the OBU.

S3: the vehicle V_i broadcasts $m_i, PID_i, T_i, \delta_i$.

The steps of this phase are outlined in Figure 3.

4.3. Message Verification Phase. It is a normal state in VCN that an entity (such as a vehicle or a RSU) receives a mass of messages in a brief period. To improve the efficiency of message verification, there are two ways to verify that the received messages are presented in our scheme. One is traditional

FIGURE 3: The steps of pseudonym generation and message signing phase.

single message verification for one message. The other is batch verification for multiple messages simultaneously.

(i) *Single Message Verification.* Assume $m_i, PID_i, T_i, \delta_i$ generated by the vehicle V_i is a message needed to be verified. The T_i of message m_i will be checked firstly. If is not fresh, the verifier discards this message. Otherwise, the verifier computes $h_i = h_2(m_i, PID_i, T_i)$ and then examines if this message satisfies the verification equation as follows:

$$\delta_i \cdot P_{pub} = PID_{i,1} + h_i \cdot P \quad (1)$$

If not, this message will be discarded. Or, it will be accepted.

(ii) *Batch Message Verification.* After n messages $\{m_1, PID_1, T_1, \delta_1\}, \{m_2, PID_2, T_2, \delta_2\}, \dots, \{m_n, PID_n, T_n, \delta_n\}$ are received by the verifier, they could be verified simultaneously as the following steps.

B1: the T_i of message m_i ($i = 1, 2, \dots, n$) will firstly be checked. If it is not fresh, the verifier discards m_i .

B2: to reduce false acceptance, the small exponent test technology [4] is included in batch verification. A vector including small random integers is used to distinguish any modification on multiple signatures during batch verification. The verifier chooses $\lambda = \{\lambda_1, \lambda_2, \dots, \lambda_i, \dots, \lambda_n\}$, where λ_i is randomly chosen in $[1, \gamma]$; γ is a very small integer and only causes little computational overhead [4].

B3: the verifier checks whether (2) holds or not.

$$\left(\sum_{i=1}^n \lambda_i \delta_i \right) \cdot P_{pub} = \sum_{i=1}^n (\lambda_i \cdot PID_{i,1}) + \left(\sum_{i=1}^n \lambda_i h_i \right) \cdot P \quad (2)$$

where $h_i = h_2(m_i, PID_i, T_i)$. If (2) holds, the n messages will be accepted. Or, one or more messages are invalid in the n messages. To detect invalid message, the way proposed in [37] is used in the proposed scheme. For more details, please see [37].

If the n messages are valid, the verifier accepts the n messages and can send n messages as $M^* = \{(m_1, PID_1, T_1, \delta_1), (m_2, PID_2, T_2, \delta_2), \dots, (m_n, PID_n, T_n, \delta_n)\}$ to its top manager in traditional ways. To improve efficiency and decrease

communication cost, a signature aggregation is included in the proposed scheme.

(iii) *Signature Aggregation.* To decreasing communication cost, a verifier in the lower layer of system can make aggregate signature on the messages that have been verified before forwarding these messages to its top managers.

Firstly, the verifier computes $\delta_A^* = \sum_{i=1}^n \delta_i$. Then he/she generates the aggregated message $M_A^* = \{(m_1, PID_1, T_1), (m_2, PID_2, T_2), \dots, (m_n, PID_n, T_n), \delta_A^*\}$. At last, the verifier forwards the aggregated message to its top manager.

When the top manager receives $\hat{n}$ aggregated messages $\{(m_1^1, PID_1^1, T_1^1), \dots, (m_n^1, PID_n^1, T_n^1), \delta_A^1\}, \dots, \{(m_1^{\hat{n}}, PID_1^{\hat{n}}, T_1^{\hat{n}}), \dots, (m_n^{\hat{n}}, PID_n^{\hat{n}}, T_n^{\hat{n}}), \delta_A^{\hat{n}}\}$, it can verify single aggregated message by following verification equation (3):

$$\delta_A^* \cdot P_{pub} = \sum_{i=1}^n PID_{i,1} + h_A^* \cdot P \quad (3)$$

where $h_A^* = \sum_{i=1}^n h_2(m_i, PID_i, T_i)$. If (3) holds, the top manager accepts the aggregated message. To improve efficiency, the top manager also can verify the aggregated messages by following verification equation (4):

$$\left(\sum_{j=1}^{\hat{n}} \delta_A^j \right) \cdot P_{pub} = \sum_{j=1}^{\hat{n}} \sum_{i=1}^n PID_{i,1}^j + \left(\sum_{j=1}^{\hat{n}} h_A^j \right) \cdot P \quad (4)$$

If (4) holds, the top manager accepts the $\hat{n}$ aggregated messages.

4.4. Identity Tracing Phase. To obtain profit or disrupt traffic, a registered vehicle V_i perhaps sends false message m_i ; that is, m_i has wrong/untrue context with valid signature. Therefore, the functionality of tracing the identity of false messages must be provided in message authentication scheme. Assume the message m_i in $M^* = \{(m_1, PID_1, T_1), (m_2, PID_2, T_2), \dots, (m_n, PID_n, T_n), \delta^*\}$. Note that the n messages have passed the signature verification. The TA traces the real identity RID_i from m_i by calculating $RID_i = PID_{i,2} \oplus h_1(s \cdot PID_{i,1})$, where s is its private key.

5. Security Proof and Analysis

In this section, we demonstrate that the proposed scheme satisfies the security requirements of VCN described in Section 3.2. In order to prove that the proposed scheme is secure against all types of attacks, we show the nonforgery of the proposed scheme firstly.

5.1. Security Proof. In order to prove the security of the proposed scheme, the security model is defined as a game that is performed by an adversary and a challenger based on the ability of the adversary and the network model.

Theorem 1. *The proposed scheme is existentially unforgeable against an adaptive chosen-message under the random oracle model.*

Proof. Assume an ECDLP instance $(P, Q = xP)$ is given, where P, Q are two points on E/E_p and an adversary $\mathcal{A}$ could forge message $\{m_i, PID_i, T_i, \delta_i\}$. Now, we set up a game between $\mathcal{A}$ and a challenger $\mathcal{C}$, which is able to solve the ECDLP by running $\mathcal{A}$ as a subroutine with a probability that cannot be ignored.

Setup. The challenger $\mathcal{C}$ executes system setup algorithm, lets $P_{pub} = Q = xP$ as system public key, and defines system parameter params= $\{E_p(a, b), p, q, P, h_1, h_2, P_{pub}\}$ and then creates and preserves two lists. One is list L_{h1} formed by $\langle \alpha, \tau_{h1} \rangle$, which contains the queries and answers of h_1 -Oracle and is empty initially. Another is list L_{h2} formed by $\langle m_i, PID_i, T_i, \tau_{h2} \rangle$, which includes the queries and answers of h_2 -Oracle and is empty initially. At last $\mathcal{C}$ sends params to $\mathcal{A}$.

h_1 -Oracle. When $\mathcal{A}$ queries message α , $\mathcal{C}$ checks whether the tuple $\langle \alpha, \tau_{h1} \rangle$ is already in L_{h1} or not. If so, $\mathcal{C}$ sends $\tau_{h1} = h_1(\alpha)$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ chooses $\tau_{h1} \in Z_q^*$ at random and then adds $\langle \alpha, \tau_{h1} \rangle$ to L_{h1} . At last, $\mathcal{C}$ sends $\tau_{h1} = h_1(\alpha)$ to $\mathcal{A}$.

h_2 -Oracle. When $\mathcal{A}$ queries message $\langle m_i, PID_i, T_i, \tau_{h2} \rangle$, $\mathcal{C}$ checks if the tuple $\langle m_i, PID_i, T_i \rangle$ is already in L_{h2} . If so, $\mathcal{C}$ sends $\tau_{h2} = h_2(m_i, PID_i, T_i)$ to $\mathcal{A}$. Or, $\mathcal{C}$ randomly chooses $\tau_{h2} \in Z_q^*$ and then adds $\langle m_i, PID_i, T_i, \tau_{h2} \rangle$ to L_{h2} . At last, $\mathcal{C}$ sends $\tau_{h2} = h_2(m_i, PID_i, T_i)$ to $\mathcal{A}$.

Sign-Queries. When $\mathcal{A}$ makes sign-query on message m_i , $\mathcal{C}$ randomly chooses $\delta_i, h_i \in Z_p^*$, $PID_i \in G$, and computes $PID_{i,1} = \delta_i \cdot P_{pub} - h_i \cdot P$. Then, $\mathcal{C}$ adds $\langle m_i, PID_i, T_i, h_i \rangle$ to L_{h2} . At last, $\mathcal{C}$ constructs a message $\{m_i, PID_i, T_i, \delta_i\}$ and sends it to $\mathcal{A}$. According to the rules of the game, each response to the Sign-queries is valid because $\{m_i, PID_i, T_i, \delta_i\}$ answered in the game is able to meet the following equation:

$$\begin{aligned} \delta_i \cdot P_{pub} &= PID_{i,1} + h_i \cdot P = (\delta_i \cdot P_{pub} - h_i \cdot P) + h_i \cdot P \\ &= \delta_i \cdot P_{pub} \end{aligned} \quad (5)$$

Output. At last, $\mathcal{A}$ outputs $\{m_i, PID_i, T_i, \delta_i\}$ as a valid message with nonnegligible probability. $\mathcal{C}$ can verify the message using

$$\delta_i \cdot P_{pub} = PID_{i,1} + h_i \cdot P \quad (6)$$

If it does not hold, $\mathcal{C}$ terminates this progress.

$\mathcal{A}$ could output $\{m_i, PID_i, T_i, \delta_i^*\}$ as another valid message if $\mathcal{A}$ executes the progress with another h_2 -oracle query (let its answer be h_i^*) on the basis of the forgery lemma [38]. Likewise, the message is able to satisfy

$$\delta_i^* \cdot P_{pub} = PID_{i,1} + h_i^* \cdot P \quad (7)$$

According to (6) and (7), we can deduce

$$\begin{aligned} (\delta_i - \delta_i^*) \cdot x \cdot P &= (\delta_i - \delta_i^*) \cdot P_{pub} \\ &= \delta_i \cdot P_{pub} - \delta_i^* \cdot P_{pub} \end{aligned}$$

$$\begin{aligned} &= PID_{i,1} + h_i \cdot P - (PID_{i,1} + h_i^* \cdot P) \\ &= (h_i - h_i^*) \cdot P \end{aligned} \quad (8)$$

From (8), we could obtain (9) as follows:

$$(\delta_i - \delta_i^*) \cdot x = (h_i - h_i^*) \mod q \quad (9)$$

Now, $\mathcal{C}$ outputs $(\delta_i - \delta_i^*)^{-1} \cdot (h_i - h_i^*)$ as a solution for the given instance of the ECDLP. However, it contradicts with the difficulty of solving the ECDLP. So the proposed scheme can resist forgery attack. $\square$

5.2. Security Analysis. In the subsection, we analyze how the proposed scheme meets the security requirements of VCN.

(1) *Message Authentication* [39]. In the proposed scheme, an adversary cannot forge a message with nonnegligible probability to meet the verification equation $\delta_i \cdot P_{pub} = PID_{i,1} + h_i \cdot P$ according to Theorem 1. Therefore, a verifier is able to check the validity of message by the verification equation (1). Not that $h_i = h_2(m_i, PID_i, T_i)$ in signature can also be used to check the integrity of message. Therefore, the proposed scheme is able to accomplish signature and integrity verification for VCN.

(2) *Conditional Privacy-Preserving (CPP)*. Vehicle V_i sends message to others with form of $\{m_i, PID_i, T_i, \delta_i\}$, where $PID_{i,1} = r_i \cdot P$, $PID_{i,2} = RID_i \oplus h(r_i \cdot P_{pub})$. The identity of the vehicle is perfectly protected for $PID_{i,2}$ is a pseudoidentity including a random number. To reveal V_i 's real identity, an adversary needs to compute $RID_i = PID_{i,2} \oplus h(r_i \cdot P_{pub}) = PID_{i,2} \oplus h(r_i xP)$. However, without knowing r_i and x , the adversary cannot reveal RID_i because it is an instance of CDH problem to compute $w_i xP$. On the contrary, only the TA could reveal the identity from the message by calculating $RID_i = PID_{i,2} \oplus h(x \cdot PID_{i,1})$, if it is necessary. Therefore, the proposed scheme can achieve CPP.

(3) *Resistance to Attacks*. The proposed scheme can resist the main security attacks of VCN as follows.

(i) *Replay Attack*. When an attacker launches a replay attack on $\{m_i, PID_i, T_i, \delta_i\}$, it should forge another T_i^* to pass the exam of time freshness. According to Theorem 1, the attacker cannot forge another valid signature δ_i^* to pass message authentication. So this scheme can resist replay attack.

(ii) *Modification Attack* [40]. As the design of scheme, a valid message consists of its digital signature $\{PID_i, \delta_i\}$. If an attacker makes any modification on the message, the verifier can easily find the modification by verifying (1). Thus, the proposed scheme can resist modification attack.

(iii) *Impersonation Attack*. An attacker launches an impersonation attack; it should forge a message [41]. However, the probability of the forged message to meet the verification equation can be negligible according to Theorem 1. Therefore, the proposed scheme can resist the impersonation attack.

TABLE 1: The cryptographic operation and execution time.

Cryptographic operation	Abbr.	Time (ms)
operations related to bilinear pairing	T_{bp}	4.2110
	T_{pm}	1.7090
	T_{ps}	0.0535
	T_{pa}	0.0071
operations related to ECC	T_{em}	0.4420
	T_{es}	0.0138
	T_{ea}	0.0018
Map-To-Point hash function	T_H	4.4060
One-way Hash function	T_h	0.0001

(iv) *Verifier Table Attack*. As attacks on verifier table become a more and more serious security attack, authentication scheme should focus more attention on these attacks. In the proposed scheme, there is no need for a verifier table in the TA, vehicles, or RSUs. Therefore, an attacker cannot launch any attack on verifier table. Therefore, the proposed scheme can resist the verifier table attack.

6. Performance Analysis and Comparison

In this section, we analyze the performance of the proposed scheme in terms of computation cost and communication cost. The performance comparisons are demonstrated between the proposed scheme and several newly proposed CPP authentication schemes for vehicle network, which are Bayat et al.'s scheme [12] (BAS-CPP, for short), Zhang et al.'s scheme [13] (ZAS-CPP, for short), and He et al.'s scheme [14] (HAS-CPP, for short). Then, the impact on system performance posed by signature aggregation is analyzed. At last, detailed simulations and analysis are shown to evaluate the performance of the proposed scheme according to verification loss rate and message delay.

6.1. Computation Cost Analysis and Comparison. Due to the difference in design, BAS-CPP [12] and ZAS-CPP's [13] cryptographic operations are built on bilinear pairings, while HAS-CPP [14] and our proposed scheme's cryptographic operations are built on ECC. We construct a bilinear pairing cryptography system and an ECC system at 80-bit security level. Table 1 lists the cryptographic operations and corresponding abbreviations and execution times in the four schemes.

Column Abbr. lists the abbreviation of cryptographic operations. Bilinear pairing operation is abbreviated as T_{bp} . Three operations related to bilinear pairing, i.e., scale multiplication, small scale multiplication, and point addition, are abbreviated as T_{pm} , T_{ps} , and T_{pa} , respectively. Three operations related to ECC, i.e., normal scale multiplication, small scale multiplication, and point addition, are abbreviated as T_{em} , T_{es} , and T_{ea} , respectively.

Pseudonym-generating and message signing phase, single message verification phase, and batch message verification phase are called PMS, SMV, and BMV for short.

FIGURE 4: The computation cost comparison of batch verification.

In BAS-CPP [12], the PMS includes five scalar-multiplication operations, one point-addition operation, one Map-To-Point function operation, and two one-way hash operations. The total execution time of BAS-CPP's PMS is $5T_{pm} + 1T_{pa} + 1T_H + 2T_h \approx 12.9583$ ms. The SMV includes three bilinear pairing operations, one point-addition operation, one operation of Map-To-Point function, and one operation of one-way hash function. So the total execution time of BAS-CPP's SMV is $3T_{bp} + 1T_{pa} + 1T_H + 1T_h \approx 18.7481$ ms. The BMV includes three bilinear pairings, $(n + 1)$ operations of scalar multiplication, n small scalar-multiplication operations, $3n - 3$ point-addition operations, and n one-way hash function operations. So the total execution time of BAS-CPP's BMV is $3T_{bp} + (n)T_{pm} + 2nT_{ps} + (3n - 3)T_{pa} + nT_h \approx 6.1364n + 12.6117$ ms. We also can compute ZAS-CPP's [13] computation cost in the same way. For simplicity, the detailed analysis of its computation cost is not presented here.

The PMS of the proposed scheme includes two scalar-multiplication operations and two one-way hash function operations. So the total execution time of PMS in the proposed scheme is $2T_{em} + 2T_h = 0.8842$ ms. The SMV of the proposed scheme includes two scalar-multiplication operations, one point-addition operation, and one one-way hash function operation. So the total execution time of SMV in the proposed scheme is $2T_{em} + 1T_{ea} + 1T_h \approx 0.8859$ ms. The BMV of the proposed scheme includes two scalar-multiplication operations, n small-scalar-multiplication operations, n point-addition operations, and n one-way hash function operations. So the total execution time of BMV in the proposed scheme is $2T_{em} + nT_{es} + nT_{ea} + nT_h \approx 0.0157n + 0.8840$ ms. The cryptographic construction of the HAS-CPP [14] is same as the proposed scheme. For simplicity, the detail analysis of its computation cost is not presented here.

Therefore, we can compute the computation cost of each phase of the four schemes according to Table 1, as shown in Table 2. The result indicates that the proposed scheme has the higher superiority in the computation cost.

Figure 4 illustrates the computation costs of BMV for the different number of messages. As shown in Figure 4, the

TABLE 2: The computation cost of the four authentication schemes.

	PMS	SMV	BMV
BAS-CPP [12]	12.9583 ms	18.7481 ms	$6.1364n + 12.6117$ ms
ZAS-CPP [13]	9.5473 ms	16.0584 ms	$3.4715n + 12.6330$ ms
HAS-CPP [14]	1.3263 ms	1.3298 ms	$0.4752n + 0.8822$ ms
The proposed scheme	0.8842 ms	0.8859 ms	$0.0157n + 0.8840$ ms
The improvement of the proposed scheme over other schemes			
BAS-CPP [12]	93.17%	95.27%	99.48% ($n=50$)
ZAS-CPP [13]	90.73%	94.48%	99.10% ($n=50$)
HAS-CPP [14]	33.33%	33.38%	93.23% ($n=50$)

TABLE 3: The comparison of communication cost.

	The component of single message	size
BAS-CPP [12]	$\{m_i, AID_i^1, AID_i^2, T_i, \delta_i\}$	280 bytes
ZAS-CPP [13]	$\{m_i, S_{i,1}, S_{i,2}, STP_{i,j}\}$	276 bytes
HAS-CPP [14]	$\{m_i, AID_{i,1}, AID_{i,2}, T_i, R_i, \delta_i\}$	144 bytes
The proposed scheme	$\{m_i, PID_{i,1}, PID_{i,2}, T_i, \delta_i\}$	84 bytes

proposed scheme is more efficient than the three others in BMV phase regardless of the number of messages

6.2. Communication Cost Analysis and Comparison. In this subsection, the proposed scheme is compared with BAS-CPP [12], ZAS-CPP [13], and HAS-CPP [14] in communication cost. According to the definition in previous section, the size of a bilinear pairing group element is 128 bytes, and the size of an ECC system group element is 40 bytes. Let the sizes of a timestamp and a one-way hash output be 4 and 20 bytes. Here we do not consider original content in message for it is the same to all schemes. According to the component of single message of the four schemes, Table 3 shows their communication costs. Obviously, compared with BAS-CPP, ZAS-CPP, and HAS-CPP, the proposed scheme requires less communication cost.

6.3. Signature Aggregation Analysis. In this subsection, we show the performance improvement of signature aggregation over traditional ways, i.e., forwarding message one by one.

BAS-CPP [12] and HAS-CPP [14] do not offer signature aggregation. Different from them, the proposed scheme and ZAS-CPP [13] provide signature aggregation. As shown in message verification phase in Section 4, after the verifier has checked n messages, the verifier forwards the n messages to top managers one by one. To decrease communication and computation cost, the verifier can aggregate multiple signatures into a single one, i.e., the verifier could make n messages into an aggregated signature $M_A^* = \{(m_1, PID_1, T_1), (m_2, PID_2, T_2), \dots, (m_n, PID_n, T_n), \delta_A^*\}$, where the size of δ_A^* in M_A^* is identical to the size of δ_i in a single message $\{m_i, PID_i, T_i, \delta_i\}$, regardless of the number of messages. During forwarding 50 messages to top managers, the verifier in our scheme can decrease communication cost by 1000 bytes using signature aggregation compared to using traditional way, details shown in Figure 5. As far as signature aggregation is concerned, ZAS-CPP [13]

FIGURE 5: The communication cost comparison of signature aggregation.

can decrease more communication cost, though it needs more sign and verification cost. Therefore, our scheme and ZAS-CPP [13] can further decrease communication cost by signature aggregation.

From the above performance analysis and comparison, it is easy to draw a conclusion that the proposed scheme has more advantages. Compared with BAS-CPP and HAS-CPP, the proposed scheme not only has less computation and communication cost in message signing phase, single message verification phase, and batch message verification phase, but also decreases communications cost by signature aggregation. Compared with ZAS-CPP, although the proposed scheme is insufficient in signature aggregation, it has a great advantage in computation and communication cost in signing phase and verification phase. Table 4 shows the comprehensive comparison results of the four schemes in terms of the computation costs of PMS, SMV, and BMV, the communication cost (C-cost for short), and the signature aggregation functionality (SA-func for short). It obviously shows that the proposed scheme has most advantages. Therefore, the proposed scheme can further satisfy the requirements of VCN.

TABLE 4: The comprehensive comparison results of the four schemes.

scheme name	PMS	SMV	BMV	C-Cost	SA-func
BAS-CPP [12]	High	High	High	High	No
ZAS-CPP [13]	High	High	High	High	Yes
HAS-CPP [14]	Middle	Middle	Middle	Middle	No
The proposed scheme	Low	Low	Low	low	Yes

FIGURE 6: The simulation scenario.

6.4. Simulation and Analysis. In this section, we evaluate the performance of the proposed scheme by several simulations. The simulation scenarios are constructed in the Veins framework [42] and the OMNeT++ simulation platform [43] with the surrounding roads of Wuhan University, as shown in Figure 6, where all roads are two-way multilane. The main goal of this simulation is to test the advantages and disadvantages of the proposed scheme in terms of loss rate and message delay.

In the simulation, one RSU is deployed every 2 km along the roads, and it can send messages to vehicles within 800 m; vehicles run along roads and communicate with others within 250 m. Let each vehicle generate a traffic message every 300 ms and send it to RSUs and other vehicles; then RSUs verify and aggregate the messages to cloud sever. Let the size of a message be 200 bytes, the wired communication bandwidth between RSUs and cloud server is 10 mb/s, and the wireless communication bandwidth between vehicles is 200 kb/s. The vehicle density (the number of vehicles in the scenario) in the scene is set between 200 and 800. Let 2% vehicles be malicious ones that have invalid signature messages. The speed of vehicles is randomly generated by the system in a normal distribution between 40 and 90 km/h.

In order to test the impact of batch authentication time interval setting on the proposed scheme, four batch verification simulations with different intervals are designed, where the intervals T are 20 ms, 30 ms, 40 ms, and 50 ms. The verification loss rate and message delay during the simulations are shown in Figures 7 and 8.

The T in Figure 7 denotes the interval for batch verification, and the verification loss rate has a certain function with vehicle density under different T . It shows that the greater the vehicle density, the greater the communication overhead of the whole system. Meanwhile, the verification loss rate

FIGURE 7: Verification loss rate related to vehicle density and interval.

FIGURE 8: Message delay related to vehicle density and interval.

is rising as communication overhead is rising under any T . Of course, as T decreases, the verification loss rate of the proposed scheme increases, but its increase is in a smaller range.

Figure 8 shows the relationship between message delay and vehicle density in the proposed scheme. It shows that the greater the vehicle density is, the greater the communication overhead is, which results in adding the instability of the

FIGURE 9: The comparison of verification loss rate among three schemes.

communication system. Therefore, message delay is rising as vehicle density is rising under any T . However, the message delay increases slightly as T decreases.

Next, the comparison simulations are executed among the proposed scheme, BAS-CPP [12], and HAS-CPP [14] in terms of verification loss rate and message delay. In these simulations, $T = 30$ ms. Figure 9 shows the comparison of verification loss rate among three schemes in the simulations. As can be seen from Figure 9, as the vehicle density increases, the message loss rate of the three schemes increases. The verification loss rate of BAS-CPP is increasing rapidly, and the rates of HAS-CPP and the proposed scheme are relatively slow, which could prove that the improved message verification efficiency can improve the speed of receiving and processing messages and reduce the loss rate.

Figure 10 shows the comparison of message delay among three schemes. As the vehicle density increases, the message delay of the proposed scheme and HAS-CPP increases, but the delay growth rate is smaller than BAS-CPP. The simulation results further prove that the proposed scheme can reduce the message delay and improve the performance of the VCN system.

7. Conclusion

A new efficient message authentication scheme for VCN is presented in this paper, and it achieves conditional privacy-preserving. In order to solve urgent authentication issue for life-critical message in VCN, batch message verification and signature aggregation are included in the proposed scheme, which is suitable for VCN because verifiers are limited in computation capacity and communication channel is very strained in VCN. The security proof and analysis show that the proposed scheme could satisfy the security requirements of VCN. The performance analyses show that the proposed scheme has obvious advantages in decreasing

FIGURE 10: The comparison of message delay among three schemes.

communication and computation cost when compared with recent proposed identity-based authentication schemes. A detailed simulations and analysis are shown to evaluate the performance of the proposed scheme according to verification loss rate and message delay, which prove that the proposed scheme can reduce verification loss rate and message delay, and improve the performance of the VCN system.

Our next research will focus on improving the signature aggregation to decrease more communication cost while keeping the efficiency of signature and verification.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was supported in part by the National Natural Science Foundation of China under Grant 61862052, the MOE (Ministry of Education in China) Project of Humanities and Social Sciences (17YJCZH203), and the Hubei Provincial Department of Education research projects (D20182702).

References

- [1] M. S. Kakkasageri and S. S. Manvi, "Information management in vehicular ad hoc networks: a review," *Journal of Network and Computer Applications*, vol. 39, no. 1, pp. 334–350, 2014.
- [2] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Comments on 'dual authentication and key management techniques for

- secure data transmission in vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, 2017.
- [3] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, “Toward Cloud-based vehicular networks with efficient resource management,” *IEEE Network*, vol. 27, no. 5, pp. 48–55, 2013.
 - [4] 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.
 - [5] J. Wang, J. Cho, S. Lee, and T. Ma, “Real time services for future cloud computing enabled vehicle networks,” in *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP ’11)*, pp. 1–5, November 2011.
 - [6] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, “A survey on vehicular cloud computing,” *Journal of Network and Computer Applications*, vol. 40, no. 1, pp. 325–344, 2014.
 - [7] J. Cui, J. Zhang, H. Zhong, and Y. Xu, “SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283–10295, 2017.
 - [8] D. Hughes and V. Shmatikov, “Information hiding, anonymity and privacy: A modular approach,” *Journal of Computer Security*, vol. 12, no. 1, pp. 3–36, 2004.
 - [9] D. Wang, H. Cheng, H. Debiao, and P. Wang, “On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices,” *IEEE Systems Journal*, vol. 12, no. 1, pp. 916–925, 2018.
 - [10] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication,” *Vehicular Communications*, vol. 9, pp. 19–30, 2017.
 - [11] T. Gao, X. Deng, N. Guo, and X. Wang, “An anonymous authentication scheme based on PMIPv6 for VANETs,” *IEEE Access*, vol. 6, pp. 14686–14698, 2018.
 - [12] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, “A secure authentication scheme for VANETs with batch verification,” *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.
 - [13] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, “Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response,” *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562–2574, 2016.
 - [14] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.
 - [15] 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.
 - [16] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: efficient conditional privacy preservation protocol for secure vehicular communications,” in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM ’08)*, pp. 1229–1237, April 2008.
 - [17] 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.
 - [18] Y. Liu, W. Guo, Q. Zhong, and G. Yao, “LVAP: Lightweight V2I authentication protocol using group communication in VANETs,” *International Journal of Communication Systems*, vol. 30, no. 16, 2017.
 - [19] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, “Distributed aggregate privacy-preserving authentication in VANETs,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.
 - [20] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.
 - [21] J. Freudiger, R. Maxim, M. Félegyházi, P. Papadimitratos, and H. Jean-Pierre, “Mix-zones for location privacy in vehicular networks,” in *Proceedings of the ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS ’07)*, number LCA-CONF-2007-016, 2007.
 - [22] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, “RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks,” in *Proceedings of the IEEE International Conference on Communications (ICC ’08)*, pp. 1451–1457, May 2008.
 - [23] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO ’84)*, vol. 196, pp. 47–53, Springer, 1984.
 - [24] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,” in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM ’08)*, pp. 246–250, April 2008.
 - [25] 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 Networks*, vol. 9, no. 2, pp. 189–203, 2011.
 - [26] Y. Xie, L. Wu, J. Shen, and A. Alelaiwi, “ELIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs,” *Telecommunication Systems*, vol. 65, no. 2, pp. 229–240, 2017.
 - [27] J. Kang, D. Lin, W. Jiang, and E. Bertino, “Highly efficient randomized authentication in VANETs,” *Pervasive and Mobile Computing*, vol. 44, pp. 31–44, 2018.
 - [28] Y. Liu, Y. Wang, and G. Chang, “Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.
 - [29] A. Wasef and X. Shen, “ASIC: Aggregate signatures and certificates verification scheme for vehicular networks,” in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM ’09)*, pp. 1–6, December 2009.
 - [30] R. W. Van Der Heijden, S. Dietzel, and F. Kargl, “SeDyA: Secure dynamic aggregation in VANETs,” in *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec ’13)*, pp. 131–142, April 2013.
 - [31] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, “Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks,” *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, 2017.
 - [32] E. Lee, E.-K. Lee, M. Gerla, and S. Y. Oh, “Vehicular cloud networking: architecture and design principles,” *IEEE Communications Magazine*, vol. 52, no. 2, pp. 148–155, 2014.
 - [33] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, “Zipf’s Law in Passwords,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.
 - [34] D. Wang and P. Wang, “Two birds with one stone: two-factor authentication with security beyond conventional bound,” *IEEE Transactions on Dependable and Secure Computing*, 2016.

- [35] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 28–35, 2018.
- [36] X. Hu, J. Zhang, Z. Zhang, and F. Liu, "Anonymous password authenticated key exchange protocol in the standard model," *Wireless Personal Communications*, vol. 96, no. 1, pp. 1451–1474, 2017.
- [37] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.
- [38] D. Hankerson, S. Vanstone, and A. J. Menezes, *Guide to Elliptic Curve Cryptography*, Springer, New York, NY, USA, 2004.
- [39] Q. Jiang, C. Zhiren, L. Bingyan, J. Shen, L. Yang, and M. Jianfeng, "Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1061–1073, 2018.
- [40] X. Hu, J. Zhang, Z. Zhang, and J. Xu, "Universally composable anonymous password authenticated key exchange," *Science China Information Sciences*, vol. 60, no. 5, 2017.
- [41] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Computers and Electrical Engineering*, vol. 63, pp. 182–195, 2017.
- [42] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. L. Cigno, "Plexe: A platooning extension for Veins," in *Proceedings of the IEEE Vehicular Networking Conference (VNC '14)*, pp. 53–60, Paderborn, Germany, December 2014.
- [43] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (ICST '08)*, pp. 60–69, March 2008.