Hindawi
Mobile Information Systems
Volume 2019, Article ID 7593138, 19 pages
https://doi.org/10.1155/2019/7593138

Research Article

Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs

Yang Ming[1] **and Hongliang Cheng**[2]

[1]*School of Information Engineering, Chang'an University, Xi'an, Shaanxi 710064, China*
[2]*School of Electronic and Control Engineering, Chang'an University, Xi'an, Shaanxi 710064, China*

Correspondence should be addressed to Yang Ming; yangming@chd.edu.cn

Received 17 July 2018; Revised 1 October 2018; Accepted 26 November 2018; Published 3 February 2019

Academic Editor: Francesco Gringoli

Vehicular ad hoc networks (VANETs) are an increasing important paradigm for greatly enhancing roadway system efficiency and traffic safety. To widely deploy VANETs in real life, it is critical to deal with the security and privacy issues in VANETs. In this paper, we propose a certificateless conditional privacy preserving authentication (CCPPA) scheme based on certificateless cryptography and elliptic curve cryptography for secure vehicle-to-infrastructure communication in VANETs. In the proposed scheme, a roadside unit (RSU) can simultaneously verify plenty of received messages such that the total verification time may be sharply decreased. Furthermore, the security analysis indicates that the proposed scheme is provably secure in the random oracle model and fulfills all the requirements on security and privacy. To further improve efficiency, both map-to-point hash operation and bilinear pairing operation are not employed. Compared with previous CCPPA schemes, the proposed scheme prominently cuts down computation delay of message signing and verification by 66.9%–85.5% and 91.8%–93.4%, respectively, and reduces communication cost by 44.4%. Extensive simulations show that the proposed scheme is practicable and achieves prominent performances of very little average message delay and average message loss ratio and thus is appropriate for realistic applications.

1. Introduction

The speedy evolution of wireless technology has elevated Intelligent Transportation System (ITS) to higher levels and also made vehicular ad hoc networks (VANETs) more attractive from academia and industry [1]. VANETs, as a special application of Mobile Ad Hoc Networks (MANETs), are an important component of ITS, rapidly changing, and self-configuring and employ multiple-hops topologies on wireless links [2].

A typical architecture of the VANETs is shown in Figure 1. Usually, the VANETs system comprises four main components, i.e., the Trusted Authorities (TAs), the Application Servers (ASs), the Roadside Units (RSUs), and the vehicles, which is equipped with Onboard Units (OBUs). The responsibility of TAs is to maintain the whole system. The work of ASs is to provide a further data analysis. The RSUs are along the roadside deployment, which serve as transfer stations or carry out the authentication works to lighten the burden of the TAs. The OBUs are embedded in the vehicles to collect and process the traffic-related information and communicate with other entities. The communications mode in VANETs can be classified into two basic types, i.e., Vehicle-to-Infrastructure (V2I) communication and Vehicle-to-Vehicle (V2V) communication. In V2I communication, the vehicles communicate directly with the RSUs fixed in roadside. The vehicles communicate directly with each other to exchange the information in V2V communication. The vehicles (OBUs) communicate with the RUSs and other vehicles via a public wireless channel. Through the wired channel, the RSUs also connect with TAs and ASs. In VANETs, utilizing Dedicated Short Range Communications (DSRC) standard [3], each vehicle periodically broadcasts the vehicle-related condition messages

(e.g., speed, turning intention, direction, and position) and traffic-related safety messages (e.g., congestion state, traffic events, and weather) every 100–300 milliseconds (ms). One side, all the messages are forwarded to the traffic control center (AS) by the RSUs through wired connection. Based on the received messages, the management strategy and optimized control can be generated by the traffic control center to improve efficiency and traffic safety through analyzing the current traffic load in each intersection. On the other side, an early response can be made by the vehicles under the specific situations such as emergent braking, traffic jams, accidents, etc.

The appearing of VANETs stems from enhancing the safe driving conditions and road safety. As the traffic-related messages are transmitted in the wireless channel, the malicious attackers can easily eavesdrop, modify, replay, and delete the messages. Hence, for the practical applications of VANETs, the security and privacy challenges are needed to be tackled.

Facing all kinds of security attacks mentioned above, the message authentication is a crucial security problem for VANETs. In practice, the messages from the vehicle (OBU) need to be integrity-checked and authenticated before depended on. The reason is that an attacker can replace or modify the original safety messages or even impersonate a vehicle to broadcast bogus messages. The message authentication, which consists of identity authentication check and the message integrity check, is implemented to allow vehicle to differentiate trustworthy messages from broadcast messages and to resist impersonation attacks and modification attacks. The digital signature technology would be used to solve this problem in VANETs, which not only allows the receiver to identify the sender, but also prevents the message contents from being altered in transmission.

In addition, privacy is also a significant issue in VANETs. In real life, the vehicle-related privacy information like a vehicle's real identity should be hidden; otherwise, the moving patterns and location of the vehicle can be traced by the attacker. For instance, the leakage of vehicle's traveling routes information will disclose privacy of the vehicle and lead to serious consequences since the information may be utilized for crimes or traffic collisions. Therefore, the vehicles' privacy must be ensured in VANETs. Nonetheless, sometimes there is a conflict between the security and the privacy. The former needs to know the message's origin and integrity, while the latter requires that no entity can trace a message to its generator. Hence, conditional privacy is usually considered in VANETs. That is to say, vehicle's privacy is normally guaranteed, but if a malicious vehicle broadcasts fake messages and causes accidents or crimes, a legal authority will be capable to trace or retrieve the messages of vehicle through revealing the vehicle's real identity.

The conditional privacy-preserving authentication (CPPA) mechanism, which is able to achieve message authentication and conditional privacy simultaneously, is fully appropriate for solving the security and privacy issues in VANETs.

Several research works about privacy preserving authentication for VANETs have been proposed in recent years, which include public key infrastructure based (PKI-based) CPPA schemes [2, 4–6], identity-based (ID-based) CPPA schemes from bilinear pairing [7–19], binary authentication tree [20, 21] and elliptic curve [22–29], and certificateless CPPA schemes [30, 31]. Although certificateless conditional privacy preserving authentication (CCPPA) schemes for VANETs [30, 31] solve the public key certification management problem in PKI-based CPPA schemes and the key escrow problem in ID-based CPPA schemes, the performance of [30, 31] is not efficient owing to the need of map-to-point hash and bilinear pairing operations. We know that these two operations are more complex, which means they need more time to execute than other operations. Therefore, it is important for secure and practical VANETs to design a CCPPA scheme without map-to-point hash and bilinear pairing operations.

Based on certificateless cryptography [32] and elliptic curve cryptography (ECC) [33, 34], an efficient CCPPA scheme for VANETs is proposed in this paper. The major contributions are as follows:

(i) An efficient CCPPA scheme for VANETs is proposed without employing map-to-point hash and bilinear pairing operations. The proposed scheme achieves the fast batch message verification.

(ii) The security analysis shows that the proposed scheme is provably secure under the assumption of elliptic curve discrete logarithm in the random oracle model and satisfies all security and privacy requirements.

(iii) The performances in computation delay and communication overhead are evaluated. The experimental simulations indicate that the proposed CCPPA scheme is more efficient than schemes in [30, 31] for VANETs.

(iv) An extensive simulation is conducted, and the results demonstrate that the proposed CCPPA scheme has extremely low average message delay and average message loss ratio.

The remainder of this paper is organized as follows. In Section 2, we provide a review of the previous related works. The system model, security requirements, and elliptic curve group are presented in Section 3. We propose a concrete CCPPA scheme for secure V2I communication in Section 4 and the security analysis for the proposed scheme in Section 5. Section 6 conducts the performance evaluation and experimental simulations of the proposed scheme with other schemes. Finally, we conclude the paper in Section 7.

2. Related Works

In VANETs, the security and privacy problems have attracted strong interest and research from industry and academia. Recently, lots of CPPA schemes for VANETs have been put forward and roughly classified into three categories:

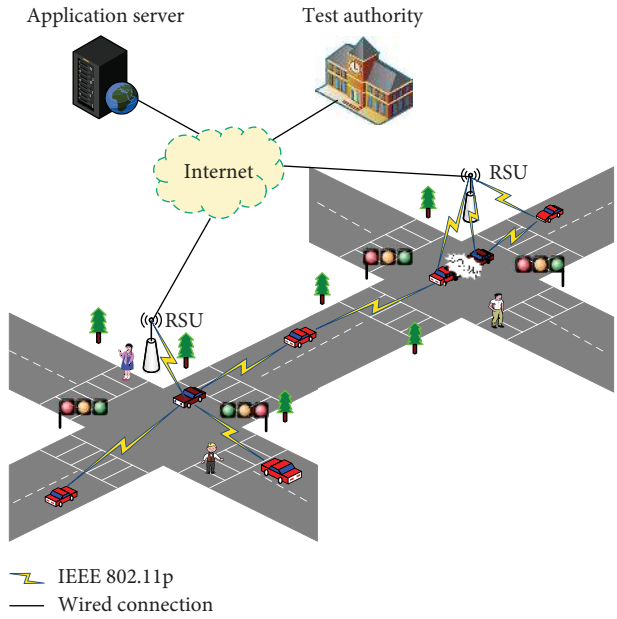

Figure 1: A typical architecture of VANETs.

PKI-based schemes, ID-based schemes, and certificateless schemes.

In 2004, Hubaux et al. [4] firstly pointed out the security and privacy issues in VANETs and declared that the public key infrastructure (PKI) technology could be used to protect transmitted messages in the vehicles. In 2007, based on anonymous certificates, an anonymous authentication scheme for VANETs was proposed by Raya and Hubaux [2]. They showed that the proposed scheme can provide message authentication and conditional privacy preservation. In this scheme, each vehicle requires to preload a huge quantity of anonymous public/private key pairs and corresponding public key certificates and then to sign a message using one of the private keys for anonymity in each communication. Therefore, a huge storage space is needed to store keys and corresponding certificates in all vehicles, while the certificate authority also needs to store all vehicles' certificates. In 2008, Lu et al. [5] put forward an efficient conditional privacy preservation (ECPP) scheme for VANETs to solve the problem of a large storage space for the vehicles in [2] by employing the temporary anonymous certificates. Based on the hash message authentication code (HMAC) and k-anonymity approach, an efficient RSU-aided message authentication scheme was proposed by Zhang et al. [6] to realize the privacy preserving of the vehicles. In summary, all the PKI-based authentication schemes for VANETs have a bottleneck problem on the storage and management of certificates.

To tackle the problem mentioned above, identity-based (ID-based) authentication schemes for VANETs have been proposed. Based on the ID-based cryptography [35], Zhang et al. [7, 8] proposed ID-based CPPA schemes. In their schemes, both the vehicle (OBU) and RSU use the identity information (such as license plate number, device number) as the public keys and the corresponding private keys are generated by a trusted third party, called the Private Key Generator (PKG). Therefore, these schemes can eliminate the need for certificates storage in vehicles and RSUs. Also, the technology of batch message verification can be provided to realize the function of verifying large number of messages simultaneously. In 2011, Chim et al. [9] claimed that Zhang et al.'s schemes [7, 8] are vulnerable to the impersonation attack and antitraceability attack. Using the two shared secrets, Chim et al. [9] also proposed a communication scheme for VANETs. The new scheme not only satisfies the requirements of the security and privacy and but also has lower communication overhead. In 2012, based on the pseudo-identity-based signature, an ID-based CPPA scheme for VANETs was established in [10] which provided the batch message verification. In 2013, Lee and Lai [11] showed that scheme in [7] was insecure against repudiation and relay attacks. And, an improved ID-based privacy-preserving authentication scheme for VANETs was put forward to overcome the weaknesses in [7] and maintain the efficiency. Horng et al. [12] pointed out that scheme in [9] is vulnerable to impersonation attack and gave a new scheme to remedy the security flaw mentioned in [9]. In 2014, Liu et al. [13] indicated that the underlying Shim's identity-based signature scheme in [10] was insecure and thus the corresponding authentication mechanism suffers from modification attacks. An improved ID-based CPPA scheme was proposed in [14] to make up for the weaknesses in [11] and maintain the efficiency as scheme in [11]. In 2015, Bayat et al. [15], aiming at the security flaw in [11], proposed a new scheme. In 2016, exploring the ID-based signature with message recovery, Liu et al. [16] presented an efficient authentication scheme for VANETs that realized the anonymity of vehicles and batch message authentication. Based on bilinear pairing, a CPPA scheme for VANETs was proposed by Wang et al. [17]. This scheme is proven secure under the computational

Differ–Hellman (CDH) assumption in the random oracle model. Based on HMAC and identity based signature, an anonymous batch authentication protocol for VANETs was proposed by Jiang et al. [18]. In 2017, Tzeng et al. [19] found that the scheme in [11] was exposed to some security risks in VANETs and proposed a secure scheme in the random oracle model. In 2009, Jiang et al. [20] firstly presented an ID-based authentication algorithm for V2I communication using a binary authentication tree. This scheme achieves high efficiency when verifying many signatures and filtering bogus messages. However, Shim [21] claimed that Jiang et al.'s scheme in [20] was unable to resist replay, forgery and sybil attacks, and proposed an improved scheme using aggregate signature, ID-based signature, and binary authentication tree. In 2015, by utilizing the ECC, He et al. [22] firstly proposed an ID-based CPPA scheme for VANETs without using map-to-point hash as well as bilinear pairing operations. This scheme has better performances in terms of computation and communication costs. Based on BLS short signature [36] and ECC, Xie et al. [23, 24] put forward ID-based conditional privacy preserving authentication schemes for VANETs, respectively. These schemes satisfy the security and privacy requirements in VANETs and achieve lower computation costs. For the secure communication and vehicle privacy in VANETs, Lo and Tsai [25] presented an efficient CPPA scheme, which does not need map-to-point hash and bilinear pairing operations to achieve better performances. Zhong et al. [26] proposed a provably secure CPPA scheme in the random oracle model which provides a practical service application for VANETs. In 2017, based on the ECC, Wu et al. [27] established an efficient location-based CPPA protocol for VANETs without using the bilinear pairing and tamper-proof device, which could satisfy the security and privacy requirements. Exploiting the binary search and cuckoo filter techniques, Cui et al. [28] proposed a secure privacy-preserving authentication scheme with high success rate in batch verification. In 2018, Li et al. [29] put forward an efficient and anonymous CPPA scheme, which achieves an optimal performance in terms of computation and communication costs. In the aforementioned ID-based CPPA schemes, all the entities' private keys are generated by PKG, which eliminates the management and storage of certificates in PKI-based schemes. However, the schemes suffer from the inherent key escrow problem, i.e., PKG knows the private keys of all vehicles and RSUs and thus literally decrypts any ciphertexts and forges signatures on any messages as any entity. Therefore, it seems that ID-based schemes may not suitable for VANETs.

To solve the key escrow problem of ID-based schemes as well as the certificate management problem in PKI-based schemes, Horng et al. [30] proposed a provable secure CCPPA scheme for VANETs based on the certificateless cryptography [32]. In CCPPA scheme, only the partial private key for the users (vehicles and RSUs) is generated by the trusted Key Generator Center (KGC). The user chooses a secret value itself and combines the partial private key to form the private key and hence KGC cannot obtain the private keys of the users. Note that the certificates are no longer required to guarantee the authenticity of public keys in CCPPA scheme. In 2016, Li et al. [31] pointed out that the scheme in [30] was insecure under the malicious-but-passive KGC attack, i.e., KGC can forge a signature or decrypt a ciphertext using maliciously embedded trapdoors in the public parameters. Furthermore, an improved scheme was put forward. In 2018, based on the new paradigm of certificateless signature with message signature (CLS-MR), Ming and Shen [37] proposed a CCPPA scheme for VANETs. The advantage is that the scheme achieved better communication efficiency. The only imperfection is that the maximum message length was limited to k_2, where k_2 is a positive integer such that k_2 less than a prime number p. In this paper, the certificateless signature technology is used to design an efficient CCPPA scheme, where the length of message is arbitrary size. Hence, this scheme is more suitable for practical VANETs system.

3. Preliminaries

3.1. System Model. The system model of the proposed scheme is shown in Figure 2. This model consists of two layers. The lower layer comprises OBUs installed in the vehicles and RSUs along with roadsides. The communication between RSU and OBU is based on the DSRC protocol [3]. The upper layer includes two trust authorities (TAs), i.e., Key Generator Center (KGC) and Trace Authority (TRA), and Application Servers (ASs) (data analysis center or traffic control center), where message exchange would be implemented over the secure channel provided by the transport layer security (TLS) protocol.

KGC. The KGC is assumed to be a trusted third party and has sufficient storage space and computing power. KGC is in charge of producing public system parameters and preloading them on RSUs and OBUs in the off-line mode. Furthermore, it also generates and distributes the partial private keys for RSUs and OBUs.

TRA. The TRA is assumed to be a trusted third party and has sufficient storage space and computing power. TRA is responsible for the registration of RSUs and OBUs. It can trace messages to their sources and reveal the real identities of the vehicles.

AS. The AS is a safety-related application server, like a traffic-data analysis center, or a traffic manage center. AS is working for first gathering the traffic-related messages including current location, time, and traffic accidents from RSUs and then making further analysis and/or providing feedbacks to them. The AS communicates with KGC, TRA, and RSUs via the wired channel.

RSU. The RSU is located along the roadside with higher computation capabilities. It can communicate with OBU of the vehicle in their coverage region by a wireless channel and communicate with KGC, TRA, and AS via a secure wired channel. In VANETs, the RSU is assumed to be a fully

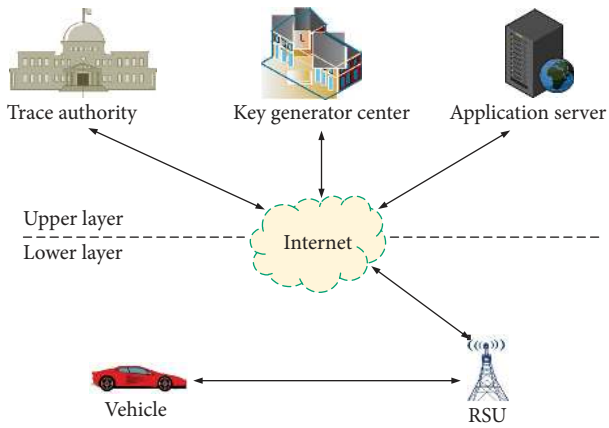

Figure 2: System model of VANETs.

trusted party and is used for verifying messages and processing them locally or sending them to TA or AS when received traffic-related messages.

OBU. The OBU is embedded in the vehicle to communicate with other OBUs and RSUs using Dedicated Short Range Communication (DSRC) [3] technology recognized as IEEE 802.11p (5.9 GHz). It warns the driver about jams and to avoid road accidents through periodically broadcasting the traffic-related status messages like speed, direction, and position to other vehicles.

3.2. Security Requirements. In V2I communication scenario, the following security requirements are needed to be satisfied in the proposed CCPPA scheme.

Message Authentication. The receiver should be able to verify the traffic-related messages and appended signatures in VANETs in order to preserve the integrity of messages sent by the vehicle.

Identity Privacy Preserving. The real identity of each vehicle should be kept secret from other entities in VANETs. Any entity ought not break the vehicle's privacy and disclose the real identity of the vehicle by analyzing transmitted messages.

Traceability. The TRA, as a trusted party must have the capability to expose the real identity of any malicious vehicle, which has broadcasted forged messages to other vehicles in order to disrupt the traffic.

Unlinkability. In addition to TRA, it is difficult to determine for anyone whether two messages are sent by the same vehicle.

Role Separation. Two trusted authorities TRA and KGC are involved in VANETs. TRA is in charge of constructing pseudo identities of the vehicle and if necessary, tracing the vehicle's real identity. KGC is for creating the vehicle's partial private key on the pseudo identity.

Key Escrow Resilience. In VANETs, KGC is normally a semitrusted commercial organization rather than full-trusted and trustworthy entity. Therefore, it is required that KGC cannot impersonate the legitimate vehicle and to generate a valid signature using the vehicle's private key.

Resistance to Attack. Apart from the conventional security and privacy requirements, the CCPPA scheme must be capable to resist various common attacks in the lower layer communication, for example, the impersonation attack, modification attack, replay attack, and man-in-the-middle attack.

3.3. Elliptic Curve Group. The elliptic curve cryptography (ECC) was initially introduced by Miller [33] and Koblitz [34].

An elliptic curve E over a finite field F_p, where p is a large prime, is defined by the following equation:

$$y^2 = x^3 + ax + b \pmod{p} \quad a, b \in F_p, \tag{1}$$

where $(4a^3 + 27b^2) \bmod p \neq 0$.

An infinity point O and all points $(x, y) \in E$ form an additive cyclic group $\mathbb{G}$. Scalar multiplication over $\mathbb{G}$ is defines as

$$kP = P + P + \cdots + P \quad (k \text{ times}), \tag{2}$$

where $P \in \mathbb{G}$.

Elliptic curve discrete logarithm (ECDL) problem [22, 37]: given two random points P and Q on the elliptic curve E, find an integer x, such that $Q = xP$.

Elliptic curve discrete logarithm (ECDL) assumption [22, 37]: the ECDL assumption means that there are no know polynomial-time algorithms to solve the ECDL problem with non-negligible probability.

Elliptic curve computational Differ–Hellman (ECCDH) problem [22, 37]: given two random points $R = xP$ and $Q = yP$ on the elliptic curve E, where x, y are two unknown integers, compute the point xyP.

Elliptic curve computational Differ–Hellman (ECCDH) assumption [22, 37]: the ECCDH assumption means that there are no know polynomial-time algorithms to solve the ECCDH problem with non-negligible probability.

4. The Proposed Scheme

This section describes a CCPPA scheme for V2I communication. The proposed CCPPA scheme includes the following four phases: system initialization, pseudo identity generation and partial private key extraction, private key generation and message signing, and message verification. The definition of notations used in the present paper is listed in Table 1.

4.1. System Initialization. This phase is executed by the two TAs (KGC and TRA) to generate system parameters for all RSUs and OBUs. The following steps are performed in this phase:

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

(2) The TAs pick a group $\mathbb{G}$ of elliptic curve points with prime order q and a generator P of $\mathbb{G}$.

(3) The KGC randomly chooses $s \in \mathbb{Z}_q^*$ as the master key for partial private key extraction and computes $P_{pub} = sP$.

(4) The TRA randomly selects $t \in \mathbb{Z}_q^*$ as the master key for identity traceability and computes $T_{pub} = tP$.

(5) The TAs choose four one-way hash functions: $H_1 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$, $H_3 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$ and $H_4 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$.

The TAs publish $\text{params} = \{p, q, \mathbb{G}, P, P_{pub}, T_{pub}, H_1, H_2, H_3, H_4\}$ as the public system parameters and send them to all RSUs and vehicles (OBUs). The master keys s and t are kept secretly by KGC and TRA, respectively. Here, the system parameters params are preloaded into the tamper-proof devices (TPD) of all vehicles in VANETs.

4.2. Pseudo Identity Generation and Partial Private Key Extraction. This phase is executed between the vehicles and the TAs (TRA, KGC). The TRA calculates the pseudo identities for the vehicle V_i, and then the KGC generates the partial private keys corresponding to the pseudo identities, when TRA receiving the real identity RID_i from V_i, where RID_i uniquely identifies the vehicle V_i. Based on this fact, the TRA and KGC preload the pseudo identities and partial private keys in TPD of vehicle V_i after successful completion of own offline registration. The following steps are executed in this phase:

(1) The vehicle V_i transmits the real identity RID_i to the TRA in a secure manner.

(2) After confirming the real identity RID_i, the TRA randomly chooses $w_i \in \mathbb{Z}_q^*$ and computes

$$\begin{aligned} \text{PID}_{i,1} &= w_i P, \\ \text{PID}_{i,2} &= \text{RID}_i \oplus H_1\left(w_i T_{pub}, T_i\right), \end{aligned} \tag{3}$$

where T_i defines the valid period of this pseudo identity. Then, a pseudo identity $\text{PID}_i = \left\{\text{PID}_{i,1}, \text{PID}_{i,2}, T_i\right\}$ is delivered to the KGC in a secure channel.

(3) For a given pseudo identity $\text{PID}_i = \{\text{PID}_{i,1}, \text{PID}_{i,2}, T_i\}$, the KGC randomly chooses $d_i \in \mathbb{Z}_q^*$ and computes the partial private key (D_i, k_i), where

$$\begin{aligned} D_i &= d_i P, \\ k_i &= d_i + sH_2\left(\text{PID}_i, D_i, T_{pub}, P_{pub}\right). \end{aligned} \tag{4}$$

The KGC sends the pseudo identity and partial private key $\{\text{PID}_i, D_i, k_i\}$ to the vehicle V_i.

4.3. Private Key Generation and Message Signing. At the private key generation and message signing phase, the vehicle V_i generates private key and signs messages. Then, the vehicle V_i broadcasts a message including the pseudo identity, traffic-related message and signature, public key, and timestamp, to nearby RUSs. This phase is depicted as follows:

(1) The vehicle V_i randomly picks $x_i \in \mathbb{Z}_q^*$ and sets x_i as the secret value and computes $P_i = x_i P$. Then, the vehicle V_i's private key is $\{D_i, k_i, x_i\}$ and the public key is P_i.

(2) The vehicle V_i randomly chooses a pseudo identity PID_i from its storage and a current timestamp t_i, which supports the freshness of message so as to resist the replay attack. Given a traffic-related message M_i, the vehicle V_i randomly selects $r_i \in \mathbb{Z}_q^*$ and computes

$$\begin{aligned} R_i &= r_i P, \\ \sigma_i &= k_i + x_i H_3\left(M_i, \text{PID}_i, D_i, P_i, t_i\right) \\ &\quad + r_i H_4\left(M_i, \text{PID}_i, D_i, R_i, t_i\right). \end{aligned} \tag{5}$$

Table 1: Notations.

Symbol	Description
V_i	The ith vehicle
RSU	A roadside unit
OBU	A onboard unit
KGC	A key generation center
TRA	A trace authority
p, q	Two large prime numbers
F_p	The finite field over p
$\mathbb{G}$	An additive group with the order q on the elliptic curve E over F_p
P	A generator of $\mathbb{G}$
RID_i	The V_i's real identity
PID_i	The V_i's pseudo identity
$H_1(\cdot), H_2(\cdot), H_3(\cdot), H_4(\cdot)$	Four one-way hash functions, $H_1, H_2, H_3, H_4 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$
(P_{pub}, s)	The KGC's public key and private key
(T_{pub}, t)	The TRA's public key and private key
(P_i, x_i)	The V_i's public key and secret value
d_i	The V_i's partial private key
$\oplus$	The exclusive OR operation
t_i	The current timestamp
T_i	The valid period of the pseudo identity

The signature of a traffic-related message M_i is $\{D_i, R_i, \sigma_i\}$. Then, the vehicle V_i issues the message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$ to nearby RSUs.

4.4. Message Verification. The verifier (RSU) performs a validity check on the received traffic-related messages in this phase, who can verify the correctness of the signature to ensure that the corresponding vehicle is not attempting to impersonate any other legitimate vehicles or disseminate false messages. The single message verification and batch message verification are as follows, respectively.

4.4.1. Single Message Verification. The verifier receives the message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$ to verify the validity of the message by the performing the following steps:

(1) The verifier checks whether T_i is valid and t_i is fresh. If T_i is not valid or t_i is not fresh, the message will be dropped.

(2) The verifier checks whether the equation

$$\begin{aligned}\sigma_i P = {} & D_i + H_2\left(\mathrm{PID}_i, D_i, T_{\mathrm{pub}}, P_{\mathrm{pub}}\right)P_{\mathrm{pub}} \\ & + H_3\left(M_i, \mathrm{PID}_i, D_i, P_i, t_i\right)P_i + H_4\left(M_i, \mathrm{PID}_i, D_i, R_i, t_i\right)R_i,\end{aligned} \tag{6}$$

holds or not. If it holds, accept the message.

4.4.2. Batch Message Verification. The batch message verification can be used to verify multiple messages simultaneously in order to enhance the efficiency of verification. When receiving the distinct n messages $\{M_1, \mathrm{PID}_1, t_1, P_1, D_1, R_1, \sigma_1\}, \{M_2, \mathrm{PID}_2, t_2, P_2, D_2, R_2, \sigma_2\}, \ldots, \{M_n, \mathrm{PID}_n, t_n, P_n, D_n, R_n, \sigma_n\}$ generated by the different vehicles, respectively, the verifier checks the validity of the messages as follows:

(1) The verifier checks whether T_i is valid and t_i is fresh, where $i = 1, 2, \ldots, n$. If any T_i is not valid or t_i is not fresh, the messages will be dropped.

(2) The verifier checks whether the equation

$$\begin{aligned}\left(\sum_{i=1}^{n}\sigma_i\right)P = {} & \sum_{i=1}^{n} D_i + \left(\sum_{i=1}^{n} H_2\left(\mathrm{PID}_i, D_i, T_{\mathrm{pub}}, P_{\mathrm{pub}}\right)P_{\mathrm{pub}}\right) \\ & + \left(\sum_{i=1}^{n} H_3\left(M_i, \mathrm{PID}_i, D_i, P_i, t_i\right)P_i\right) \\ & + \left(\sum_{i=1}^{n} H_4\left(M_i, \mathrm{PID}_i, D_i, R_i, t_i\right)R_i\right),\end{aligned} \tag{7}$$

holds or not. If it holds, accept the messages.

To detect any invalid signature in batch message verification of n messages, we use the small exponent test technology [14, 16] to realize batch message verification. The verifier checks whether the following equation

$$\begin{aligned}\left(\sum_{i=1}^{n} v_i \cdot \sigma_i\right)P_i = {} & \sum_{i=1}^{n}\left(v_i \cdot D_i\right) \\ & + \left(\sum_{i=1}^{n} v_i \cdot H_2\left(\mathrm{PID}_i, D_i, T_{\mathrm{pub}}, P_{\mathrm{pub}}\right)P_{\mathrm{pub}}\right) \\ & + \left(\sum_{i=1}^{n} v_i \cdot H_3\left(M_i, \mathrm{PID}_i, D_i, P_i, t_i\right)P_i\right) \\ & + \left(\sum_{i=1}^{n} v_i \cdot H_4\left(M_i, \mathrm{PID}_i, D_i, R_i, t_i\right)R_i\right),\end{aligned} \tag{8}$$

holds or not. If it holds, accept the messages, where $v_i \in [1, 2^l]$ and l is a small integer.

5. Security Proof and Analysis

In this section, the security analysis of the proposed CCPPA scheme for VANETs is provided. We describe the security model and prove the security of the proposed scheme under the random oracle model. Then, an evaluation on the security requirements of the proposed scheme as well as its comparison with other schemes in [22, 25, 27, 30, 31] is conducted.

5.1. Security Model. According to certificateless cryptography [32, 38–41], there are two types of adversaries with different capabilities: Type I adversary $\mathscr{A}_1$ and Type II adversary $\mathscr{A}_2$. The adversary $\mathscr{A}_1$ models an outside adversary and acts as a malicious third party while the adversary $\mathscr{A}_2$ models an inside adversary and serves as a malicious-but-passive KGC.

(i) *Type I adversary* $\mathscr{A}_1$. The adversary $\mathscr{A}_1$ cannot access the master key, but has the ability to replace the vehicle's public key with a value chosen by itself.

(ii) *Type II adversary* $\mathscr{A}_2$. The adversary $\mathscr{A}_2$ can access the master key, but cannot replace the vehicle's public key.

The following queries can be made by $\mathscr{A}_1$ and $\mathscr{A}_2$ adversaries.

(i) *Hash* H_1, H_2, H_3, H_4 *queries*. Given a query, output a random value.

(ii) *Create vehicle queries*. Given a query on the pseudo identity PID_i of the vehicle, output the vehicle's public key P_i.

(iii) *Partial private key queries*. Given a query on the pseudo identity PID_i of the vehicle, output the vehicle's partial private key $\{D_i, k_i\}$.

(iv) *Secret value queries*. Given a query on the pseudo identity PID_i of the vehicle, output the vehicle's secret value x_i if the public key has not been replaced; otherwise, output symbol $\perp$.

(v) *Vehicle public key replacement queries*. Given a query on the pseudo identity PID_i of the vehicle and a new vehicle's public key P_i', replace the corresponding vehicle's public key with a new public key P_i'.

(vi) *Sign queries*. Given a query on the traffic-related message M_i under $\{\mathrm{PID}_i, t_i, P_i\}$, output a signature $\{D_i, R_i, \sigma_i\}$.

The security of the proposed CCPPA scheme is defined by the following two interaction games: Game 1 and Game 2 between the adversary $\mathscr{A}_1$ or $\mathscr{A}_2$ and a challenger $\mathscr{C}$.

Game 1. Security against the Adversary $\mathscr{A}_1$. This game is played between the adversary $\mathscr{A}_1$ and the challenger $\mathscr{C}$ for the proposed CCPPA scheme as follows:

(i) *Initialization*. The challenger $\mathscr{C}$ runs the algorithm *System Initialization* to generate master key and the system parameters params. Then $\mathscr{C}$ returns params to $\mathscr{A}_1$.

(ii) *Queries*. The adversary $\mathscr{A}_1$ can adaptively issue H_1, H_2, H_3, H_4 and create vehicle, partial private key, secret value, vehicle public key replacement, and sign queries to $\mathscr{C}$.

(iii) *Forgery*. Eventually, $\mathscr{A}_1$ outputs the signature $\{D_i^*, R_i^*, \sigma_i^*\}$ on M_i^* under $\{\mathrm{PID}_i^*, t_i^*, P_i^*\}$ such that

(a) $\{D_i^*, R_i^*, \sigma_i^*\}$ is a valid signature on M_i^* under $\{\mathrm{PID}_i^*, t_i^*, P_i^*\}$.

(b) $\{M_i^*, \mathrm{PID}_i^*, t_i^*, P_i^*\}$ has not been requested as one of the *sign* queries.

(c) PID_i^* has not been requested as one of the *secret value* queries and the *partial private key* queries.

The success probability of the adversary $\mathscr{A}_1$ wins in *Game 1* is defined as $\mathrm{Succ}_{\mathscr{A}_1}^{\mathrm{AUTH}}$.

Definition 1. A CCPPA scheme for VANETs is secure against Type I adversary $\mathscr{A}_1$ if $\mathrm{Succ}_{\mathscr{A}_1}^{\mathrm{AUTH}}$ is negligible.

Game 2. Security against the Adversary $\mathscr{A}_2$. This game is played between the adversary $\mathscr{A}_2$ and the challenger $\mathscr{C}$ for the proposed CCPPA scheme as follows:

(i) *Initialization*. The challenger $\mathscr{C}$ runs the algorithm *System Initialization* to generate the master key and system parameters params. Then, $\mathscr{C}$ returns the master key and params to $\mathscr{A}_2$.

(ii) *Queries*. $\mathscr{A}_2$ can adaptively issue H_1, H_2, H_3, H_4, create vehicle, secret value, and sign queries to $\mathscr{C}$. Note that here $\mathscr{A}_2$ does not need to issue any partial private key queries, because he has known the master key and has the ability to compute the partial private keys of any vehicles. $\mathscr{A}_2$ also cannot replace any public keys of the vehicles.

(iii) *Forgery*. Eventually, $\mathscr{A}_2$ outputs the signature $\{D_i^*, R_i^*, \sigma_i^*\}$ on M_i^* under $\{\mathrm{PID}_i^*, t_i^*, P_i^*\}$ such that

(a) $\{D_i^*, R_i^*, \sigma_i^*\}$ is a valid signature on M_i^* under $\{\mathrm{PID}_i^*, t_i^*, P_i^*\}$.

(b) $\{M_i^*, \mathrm{PID}_i^*, t_i^*, P_i^*\}$ has not been requested as one of the *sign* queries.

The success probability of the adversary $\mathscr{A}_2$ wins in Game 2 is defined as $\mathrm{Succ}_{\mathscr{A}_2}^{\mathrm{AUTH}}$.

Definition 2. A CCPPA scheme for VANETs is secure against Type II adversary $\mathscr{A}_2$ if $\mathrm{Succ}_{\mathscr{A}_2}^{\mathrm{AUTH}}$ is negligible.

5.2. Provable Security

Theorem 1. *The proposed CCPPA scheme for VANETs is existentially unforgeable under the ECDL assumption in the random oracle model.*

Proof. This theorem is proved based on *Lemma 1* and *Lemma 2*. □

Lemma 1. *The proposed CCPPA scheme for VANETs is existential unforgeable against Type I adversary* $\mathscr{A}_1$ *under the ECDL assumption in the random oracle model.*

Proof. Assuming that polynomially bounded Type I adversary $\mathscr{A}_1$, who can break our proposed scheme with probability ε in time t, there exists an algorithm $\mathscr{B}$ that can compute x with a non-negligible probability when receiving a random ECDL problem instance $\{P, xP = Q\}$. The algorithm $\mathscr{B}$ runs $\mathscr{A}_1$ as subroutine and acts as the challenger $\mathscr{C}$ in Game 1 and interacts with $\mathscr{A}_1$ as described below.

Initialization. The algorithm $\mathscr{B}$ sets $P_{\mathrm{pub}} = Q$ and sends system parameters $\mathrm{params} = \{p, q, \mathbb{G}, P, P_{\mathrm{pub}}, T_{\mathrm{pub}}, H_1, H_2, H_3, H_4\}$ to $\mathscr{A}_1$. Here, hash functions H_1, H_2, H_3, H_4 are considered as random oracles in the proof.

To keep the consistency and rapidly response, $\mathscr{B}$ maintains the initially empty lists as follows:

(i) H_1 *list* $L_{H_1}^{\mathrm{list}}$. This list consists of tuples (Δ_i, T_i, τ_i).

(ii) H_2 *list* $L_{H_2}^{\mathrm{list}}$. This list consists of tuples $(\mathrm{PID}_i, D_i, T_{\mathrm{pub}}, P_{\mathrm{pub}}, l_i)$.

(iii) H_3 *list* $L_{H_3}^{\mathrm{list}}$. This list consists of tuples $(M_i, \mathrm{PID}_i, D_i, P_i, t_i, h_i)$.

(iv) H_4 *list* $L_{H_4}^{\mathrm{list}}$. This list consists of tuples $(M_i, \mathrm{PID}_i, D_i, R_i, t_i, \gamma_i)$.

(v) $L_{\mathrm{PID}}^{\mathrm{list}}$. This list consists of tuples $(\mathrm{PID}_i, P_i, D_i, k_i, x_i)$.

H_1 *Queries*. Suppose $\mathscr{A}_1$ submits a query on (Δ_i, T_i), $\mathscr{B}$ checks the list $L_{H_1}^{\mathrm{list}}$ and executes as follows:

(i) If the list $L_{H_1}^{\mathrm{list}}$ includes (Δ_i, T_i, τ_i), $\mathscr{B}$ responds with previous value $\tau_i = H_1(\Delta_i, T_i)$ to $\mathscr{A}_1$.

(ii) If the list $L_{H_1}^{\mathrm{list}}$ does not include (Δ_i, T_i, τ_i), $\mathscr{B}$ chooses a random number $\tau_i \in \mathbb{Z}_q$, adds (Δ_i, T_i, τ_i) in $L_{H_1}^{\mathrm{list}}$ and returns $\tau_i = H_1(\Delta_i, T_i)$ to $\mathscr{A}_1$.

H_2 *Queries*. Suppose $\mathscr{A}_1$ submits a query on $(\mathrm{PID}_i, D_i, T_{\mathrm{pub}}, P_{\mathrm{pub}})$, $\mathscr{B}$ checks the list $L_{H_2}^{\mathrm{list}}$ and executes as follows:

(i) If the list $L_{H_2}^{\text{list}}$ includes $(\text{PID}_i, D_i, T_{\text{pub}}, P_{\text{pub}}, l_i)$, $\mathscr{B}$ responds with previous value $l_i = H_2(\text{PID}_i, D_i, T_{\text{pub}}, P_{\text{pub}})$ to $\mathscr{A}_1$.

(ii) If the list $L_{H_2}^{\text{list}}$ does not include $(\text{PID}_i, D_i, T_{\text{pub}}, P_{\text{pub}}, l_i)$, $\mathscr{B}$ chooses a random number $l_i \in \mathbb{Z}_q$, adds $(\text{PID}_i, D_i, T_{\text{pub}}, P_{\text{pub}}, l_i)$ in $L_{H_2}^{\text{list}}$, and returns $l_i = H_2(\text{PID}_i, D_i, T_{\text{pub}}, P_{\text{pub}})$ to $\mathscr{A}_1$.

H_3 Queries. Suppose $\mathscr{A}_1$ submits a query on $(M_i, \text{PID}_i, D_i, P_i, t_i)$, $\mathscr{B}$ checks the list $L_{H_3}^{\text{list}}$, and executes as follows:

(i) If the list $L_{H_3}^{\text{list}}$ includes $(M_i, \text{PID}_i, D_i, P_i, t_i, h_i)$, $\mathscr{B}$ responds with previous value $h_i = H_3(M_i, \text{PID}_i, D_i, P_i, t_i)$ to $\mathscr{A}_1$.

(ii) If the list $L_{H_3}^{\text{list}}$ does not include $(M_i, \text{PID}_i, D_i, P_i, t_i, h_i)$, $\mathscr{B}$ chooses a random number $h_i \in \mathbb{Z}_q$, adds $(M_i, \text{PID}_i, D_i, P_i, t_i, h_i)$ in $L_{H_3}^{list}$, and returns $h_i = H_3(M_i, \text{PID}_i, D_i, P_i, t_i)$ to $\mathscr{A}_1$.

H_4 Queries. Suppose $\mathscr{A}_1$ submits a query on $(M_i, \text{PID}_i, D_i, R_i, t_i)$, $\mathscr{B}$ checks the list $L_{H_4}^{\text{list}}$, and executes as follows:

(i) If the list $L_{H_4}^{\text{list}}$ includes $(M_i, \text{PID}_i, D_i, R_i, t_i, \gamma_i)$, $\mathscr{B}$ responds with previous value $\gamma_i = H_4(M_i, \text{PID}_i, D_i, R_i, t_i)$ to $\mathscr{A}_1$.

(ii) If the list $L_{H_4}^{\text{list}}$ does not include $(M_i, \text{PID}_i, D_i, R_i, t_i, \gamma_i)$, $\mathscr{B}$ chooses a random number $\gamma_i \in \mathbb{Z}_q$, adds $(M_i, \text{PID}_i, D_i, R_i, t_i, \gamma_i)$ in $L_{H_4}^{\text{list}}$, and returns $\gamma_i = H_4(M_i, \text{PID}_i, D_i, R_i, t_i)$ to $\mathscr{A}_1$.

Create Vehicle Queries. Suppose $\mathscr{A}_1$ submits a public key query on a pseudo identity PID_i of the vehicle, $\mathscr{B}$ checks the list $L_{\text{PID}}^{\text{list}}$ and executes as follows:

(i) If the list $L_{\text{PID}}^{\text{list}}$ includes $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ responds with previous value P_i to $\mathscr{A}_1$.

(ii) If the list $L_{\text{PID}}^{\text{list}}$ does not include $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ randomly chooses $x_i \in \mathbb{Z}_q$, and computes $P_i = x_i P$. Finally, $\mathscr{B}$ returns P_i to $\mathscr{A}_1$, and inserts $(\text{PID}_i, P_i, D_i, k_i, x_i)$ to $L_{\text{PID}}^{\text{list}}$.

Partial Private Key Queries. Suppose $\mathscr{A}_1$ submits a partial private key query on a pseudo identity PID_i of the vehicle, $\mathscr{B}$ checks the list $L_{\text{PID}}^{\text{list}}$, and executes as follows:

(i) If the list $L_{\text{PID}}^{\text{list}}$ includes $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ responds with previous value $\{D_i, k_i\}$ to $\mathscr{A}_1$.

(ii) If the list $L_{\text{PID}}^{\text{list}}$ does not include $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ picks random numbers $k_i, l_i \in \mathbb{Z}_q$, and sets $l_i = H_2(\text{PID}_i, D_i, T_{\text{pub}}, P_{\text{pub}})$ and $D_i = k_i P - l_i P_{\text{pub}}$. Finally, $\mathscr{B}$ returns $\{D_i, k_i\}$ to $\mathscr{A}_1$, and inserts $(\text{PID}_i, D_i, T_{\text{pub}}, P_{\text{pub}}, l_i)$ and $(\text{PID}_i, P_i, D_i, k_i, x_i)$ to $L_{H_2}^{\text{list}}$ and $L_{\text{PID}}^{\text{list}}$, respectively.

Secret Value Queries. Suppose $\mathscr{A}_1$ submits a secret value query on a pseudo identity PID_i of the vehicle, $\mathscr{B}$ checks the list $L_{\text{PID}}^{\text{list}}$, and executes as follows:

(i) If the list $L_{\text{PID}}^{\text{list}}$ includes $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ responds with previous value x_i to $\mathscr{A}_1$.

(ii) If the list $L_{\text{PID}}^{\text{list}}$ does not include $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ makes a create vehicle query itself to generate $\{P_i, x_i\}$. Finally, $\mathscr{B}$ returns x_i to $\mathscr{A}_1$ and inserts $(\text{PID}_i, P_i, D_i, k_i, x_i)$ to $L_{\text{PID}}^{\text{list}}$.

Vehicle Public Key Replacement Queries. Suppose $\mathscr{A}_1$ submits a public key replacement query on $\{\text{PID}_i, P_i'\}$, $\mathscr{B}$ checks the list $L_{\text{PID}}^{\text{list}}$, and executes as follows:

(i) If the list $L_{\text{PID}}^{\text{list}}$ includes $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ sets $P_i = P_i'$ and $x_i = \perp$ and updates $(\text{PID}_i, P_i, D_i, k_i, x_i)$ to $L_{\text{PID}}^{\text{list}}$.

(ii) If the list $L_{\text{PID}}^{\text{list}}$ does not include $(\text{PID}_i, P_i, D_i, k_i, x_i)$, $\mathscr{B}$ sets $P_i = P_i'$ and $x_i = \perp$ and inserts $(\text{PID}_i, P_i, D_i, k_i, x_i)$ to $L_{\text{PID}}^{\text{list}}$.

Sign Queries. Suppose $\mathscr{A}_1$ submits a sign query on $\{M_i, \text{PID}_i, t_i, P_i\}$, $\mathscr{B}$ firstly conducts a partial private key query itself to generate $\{D_i, k_i\}$. $\mathscr{B}$ chooses a random value $\sigma_i \in \mathbb{Z}_q^*$ and computes $R_i = \gamma_i^{-1}(\sigma_i P - D_i - l_i P_{\text{pub}} - h_i P_i)$. If the tuple including γ_i already appear on the list $L_{H_4}^{\text{list}}$, $\mathscr{B}$ picks another $\sigma_i \in \mathbb{Z}_q^*$, and tries again. Finally, $\mathscr{B}$ returns $\{D_i, R_i, \sigma_i\}$ to $\mathscr{A}_1$.

Forgery. $\mathscr{A}_1$ outputs a valid signature $\{D_i^*, R_i^*, \sigma_i^*\}$ on M_i^* under $\{\text{PID}_i^*, t_i^*, P_i^*\}$. Based on the Forking Lemma [42], $\mathscr{B}$ can obtain another valid signature $\{D_i^*, R_i^*, \sigma_i^{*'}\}$ on M_i^* under $\{\text{PID}_i^*, t_i^*, P_i^*\}$ by replaying procedure with the same random tape but a different choice of H_2. Then we have

$$\sigma_i^* P = D_i^* + L_i^* P_{\text{pub}} + h_i^* P_i^* + \gamma_i^* R_i^*, \tag{9}$$

$$\sigma_i^{*'} P = D_i^* + L_i^{*'} P_{\text{pub}} + h_i^* P_i^* + \gamma_i^* R_i^*. \tag{10}$$

Following equations (9) and (10), we can obtain

$$\begin{aligned}(\sigma_i^* - \sigma_i^{*'})P &= \sigma_i^* P - \sigma_i^{*'} P = L_i^* P_{\text{pub}} - L_i^{*'} P_{\text{pub}} \\ &= (L_i^* - L_i^{*'})P_{\text{pub}} = (L_i^* - L_i^{*'})xP.\end{aligned} \tag{11}$$

Finally, $\mathscr{B}$ outputs $x = (L_i^* - L_i^{*'})^{-1}(\sigma_i^* - \sigma_i^{*'})$, which is the solution to the ECDL problem.

After completing the above simulation, we will analyze the probability and time of $\mathscr{B}$ to solve the ECDL problem instance.

Assuming that $\mathscr{A}_1$ can make at most q_{H_i} times $H_i (i = 1, 2, 3, 4)$ queries, q_{cv} times create vehicle queries, q_{pp} times partial private key queries, q_{sv} times secret value queries, q_{vp} times vehicle public key replacement queries, and q_{s} times sign queries.

The probability of failure in handling a partial private key query resulted from a conflict on H_2 is at most $q_{H_2} q_{\text{pp}}/q$. The probability of failure in handling a sign query caused by a conflict on H_4 is at most $q_{\text{s}}(q_{H_4} + q_{\text{s}})/q$. In addition, the probability of $\mathscr{A}_1$ outputs a valid forgery without asking the corresponding H_2, H_3, H_4 is at most $3/q$. $\mathscr{B}$ guesses it correctly as the point of rewind, with

probability at least $1/q_{H_2}$. Therefore, the probability of success of $\mathcal{B}$ to solve the ECDL problem is at least $(\varepsilon - (q_{H_2}q_{pp} + q_s(q_{H_4} + q_s) + 3)/q)/q_{H_2}$.

The running time of $\mathcal{B}$ is equal to the running time of $\mathcal{A}_1$ plus the time it takes to respond to q_{cv} create vehicle queries, q_{pp} partial private key queries, q_{sv} secret value queries, and q_s sign queries. Each create vehicle query requires 1 scale multiplication operation in $\mathbb{G}$. Each partial private key query requires 2 scale multiplication operations in $\mathbb{G}$. Each secret value query requires 1 scale multiplication operation in $\mathbb{G}$. Each sign query requires 2 scale multiplication operations in $\mathbb{G}$. Assuming that each scale multiplication in $\mathbb{G}$ needs time t_{sm}, the total running time of $\mathcal{B}$ is at most $t + (2q_{pp} + q_{cv} + q_{sv} + 2q_s)t_{sm}$. □

Lemma 2. *The proposed CCPPA scheme for VANETs is existential unforgeable against Type II adversary $\mathcal{A}_2$ under the ECDL assumption in the random oracle model.*

Proof. Assuming that a polynomially bounded Type II adversary $\mathcal{A}_2$, who can break our proposed scheme with probability ε in time t, there exists an algorithm $\mathcal{B}$ that can compute x with a non-negligible probability when receiving a random ECDL problem instance $\{P, xP = Q\}$. The algorithm $\mathcal{B}$ runs $\mathcal{A}_2$ as subroutine and acts as the challenger $\mathcal{C}$ in Game 2 and interacts with $\mathcal{A}_2$ as described below:

Initialization. The algorithm $\mathcal{B}$ randomly chooses $\theta \in \mathbb{Z}_q$ and sets $\theta P = P_{pub}$, then $\mathcal{B}$ sends master key θ and system parameters $\text{params} = \{p, q, \mathbb{G}, P, P_{pub}, T_{pub}, H_1, H_2, H_3, H_4\}$ to $\mathcal{A}_2$. It should be pointed out $\mathcal{A}_2$ has the master key and does not require to issue any partial private key query. Similar to *Lemma 1*, the lists $L_{H_1}^{list}$, $L_{H_2}^{list}$, $L_{H_3}^{list}$, and $L_{H_4}^{list}$ are maintained by $\mathcal{B}$. $\mathcal{B}$ also keeps a list $L_{PID}^{list} = (PID_i, P_i, D_i, k_i, x_i, c_i)$, which is initial-empty.

Hash H_1, H_2, H_3, H_4 queries. It is same to *Lemma 1*.

Create Vehicle Queries. Suppose $\mathcal{A}_2$ submits a public key query on a pseudo identity PID_i of the vehicle, $\mathcal{B}$ checks the list L_{PID}^{list}, and executes as follows:

(i) If the list L_{PID}^{list} includes $(PID_i, P_i, D_i, k_i, x_i, c_i)$, $\mathcal{B}$ responds with previous value P_i to $\mathcal{A}_2$.

(ii) If the list L_{PID}^{list} does not include $(PID_i, P_i, D_i, k_i, x_i, c_i)$, using Coron's technique [43], $\mathcal{B}$ tosses a coin $c_i \in \{0, 1\}$ that yields 1 with probability $1 - \delta$ and 0 with probability δ. $\mathcal{B}$ randomly chooses a value $k_i \in \mathbb{Z}_q$. If $c_i = 0$, $\mathcal{B}$ sets $P_i = k_iQ$; if $c_i = 1$, $\mathcal{B}$ sets $P_i = k_iP$. Finally, $\mathcal{B}$ returns P_i to $\mathcal{A}_2$ and inserts $(PID_i, P_i, D_i, k_i, x_i, c_i)$ to L_{PID}^{list}.

Secret Value Queries. Suppose $\mathcal{A}_2$ submits a secret value query on a pseudo identity PID_i of the vehicle, $\mathcal{B}$ checks the list L_{PID}^{list}, and executes as follows:

(i) If the list L_{PID}^{list} includes $(PID_i, P_i, D_i, k_i, x_i, c_i)$, if $c_i = 0$, $\mathcal{B}$ halts; if $c_i = 1$, $\mathcal{B}$ responds with previous value x_i to $\mathcal{A}_2$.

(ii) If the list L_{PID}^{list} does not include $(PID_i, P_i, D_i, k_i, x_i, c_i)$, $\mathcal{B}$ submits a create vehicle query itself, and inserts $(PID_i, P_i, D_i, k_i, x_i, c_i)$ to L_{PID}^{list}. If $c_i = 0$, $\mathcal{B}$ halts; if $c_i = 1$, $\mathcal{B}$ returns x_i to $\mathcal{A}_2$.

Sign Queries. It is the same to *Lemma 1*.

Forgery. $\mathcal{A}_2$ outputs a valid signature $\{D_i^*, R_i^*, \sigma_i^*\}$ on M_i^* under $\{PID_i^*, t_i^*, P_i^*\}$. Based on the Forking Lemma [42], $\mathcal{B}$ can obtain another valid signature $\{D_i^*, R_i^*, \sigma_i^{*'}\}$ on M_i^* under $\{PID_i^*, t_i^*, P_i^*\}$ by replaying process with the same random tape but a different choice of H_3. Then we have

$$\sigma_i^* P = D_i^* + L_i^* P_{pub} + h_i^* P_i^* + \gamma_i^* R_i^*, \tag{12}$$

$$\sigma_i^{*'} P = D_i^* + L_i^* P_{pub} + h_i^{*'} P_i^* + \gamma_i^* R_i^*, \tag{13}$$

$\mathcal{B}$ checks the L_{PID}^{list}, if $c_i^* = 1$, $\mathcal{B}$ aborts; if $c_i^* = 0$, according to equations (12) and (13), we have

$$\begin{aligned}(\sigma_i^* - \sigma_i^{*'})P &= \sigma_i^* P - \sigma_i^{*'} P = h_i^* P_i^* - h_i^{*'} P_i^* \\ &= (h_i^* - h_i^{*'})P_i^* = (h_i^* - h_i^{*'})k_i^* xP.\end{aligned} \tag{14}$$

Finally, $\mathcal{B}$ outputs $(h_i^* - h_i^{*'})^{-1}(k_i^*)^{-1}(\sigma_i^* - \sigma_i^{*'})$, which is the solution to the ECDL problem.

Same to *Lemma 1*, the analysis on the probability and time of $\mathcal{B}$ is as follows.

Assuming that $\mathcal{A}_2$ can make at most q_{H_i} times $H_i (i = 1, 2, 3, 4)$ queries, q_{cv} times create vehicle queries, q_{sv} times secret value queries, and q_s times sign queries.

The probability of failure in handing a sign query because of a conflict on H_4 is at most $q_s(q_{H_4} + q_s)/q$. In a secret value query and forgery phase, the probability of success is $(1 - \delta)^{q_{sv}}\delta$ according to Coron's technique [43]. When the optimal probability is $\delta = 1/(q_{sv} + 1)$, it is greater than $1/e(q_{sv} + 1)$. The probability of $\mathcal{A}_2$ outputs a valid forgery signature without asking the corresponding H_2 or H_3 or H_4 is at most $3/q$. $\mathcal{B}$ guesses it correctly as the point of rewind, with probability at least $1/q_{H_3}$. Therefore, the probability of success of $\mathcal{B}$ to solve the ECDL problem is at least $(\varepsilon - (q_s(q_{H_4} + q_s) + 3)/q)/(e(q_{sv} + 1)q_{H_3})$.

The running time of $\mathcal{B}$ is equal to the running time of $\mathcal{A}_2$ plus the time it takes to respond to q_{cv} create vehicle queries, q_{sv} secret value queries, and q_s sign queries. Each create vehicle query requires 1 scale multiplication operation in $\mathbb{G}$. Each secret value query requires 1 scale multiplication operation in $\mathbb{G}$. Each sign query requires 2 scale multiplication operations in $\mathbb{G}$. Assuming that each scale multiplication in $\mathbb{G}$ needs time t_{sm}, the total running time of $\mathcal{B}$ is at most $t + (q_{cv} + q_{sv} + 2q_s)t_{sm}$. □

5.3. Analysis and Comparison of Security Requirements. An evaluation on the security of the proposed scheme as well as its comparison with other schemes is conducted in this subsection.

Message Authentication. As Theorem 1, any polynomial-time adversary cannot be able to forge a valid signature

due to the assumption that the ECDL problem is hard. By verifying whether equation (6) holds, a verifier (RSU) can confirm the validity and integrity of a message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$. Therefore, the message authentication can be ensured in the proposed CCPPA scheme.

Identity Privacy Preserving. In the proposed scheme, the vehicle broadcasts the message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$, by $\mathrm{PID}_{i,1} = w_i P$ and $\mathrm{PID}_{i,2} = \mathrm{RID}_i \oplus H_1(w_i T_{\mathrm{pub}}, T_i)$, where the real identity RID_i of the vehicle V_i is perfectly hidden in random pseudo identity PID_i. To extract the vehicle V_i's real identity RID_i, the adversary should compute $\mathrm{PID}_{i,2} = \mathrm{RID}_i \oplus H_1(w_i T_{\mathrm{pub}}, T_i) = \mathrm{RID}_i \oplus H_1(w_i \cdot t \cdot P, T_i)$. However, without knowing w_i and t, it is impossible for any adversary to obtain RID_i because it is an instance of ECCDH problem to solve $w_i \cdot t \cdot P$. Hence, any adversary is not able to obtain the real identity RID_i of the vehicle, even if he/or she knows the pseudo identity PID_i. Therefore, the identity preserving can be ensured in the proposed CCPPA scheme.

Traceability. The real identity RID_i of the vehicle V_i is involved in a pseudo identity PID_i, where $T_{\mathrm{pub}} = tP$, $\mathrm{PID}_{i,1} = w_i P$, $\mathrm{PID}_{i,2} = \mathrm{RID}_i \oplus H_1(w_i T_{\mathrm{pub}}, T_i)$, and $\mathrm{PID}_i = \{\mathrm{PID}_{i,1}, \mathrm{PID}_{i,2}, T_i\}$. By computing $t \cdot \mathrm{PID}_{i,1} = t \cdot w_i \cdot P = w_i \cdot t \cdot P = w_i \cdot T_{\mathrm{pub}}$ and $\mathrm{RID}_i = \mathrm{PID}_{i,2} \oplus H_1(w_i T_{\mathrm{pub}}, T_i)$, the TRA can extract the real identity RID_i using its own master key t. Therefore, the proposed CCPPA scheme satisfies the traceability.

Unlinkability. In the proposed scheme, the TRA, KGC, and the vehicle randomly select $w_i \in \mathbb{Z}_q^*$, $d_i \in \mathbb{Z}_q^*$ and $r_i \in \mathbb{Z}_q^*$, respectively, and generate a message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$, where $\mathrm{PID}_{i,1} = w_i P$, $\mathrm{PID}_{i,2} = \mathrm{RID}_i \oplus H_1(w_i T_{\mathrm{pub}}, T_i)$, $\mathrm{PID}_i = \{\mathrm{PID}_{i,1}, \mathrm{PID}_{i,2}, T_i\}$, $D_i = d_i P$, $k_i = d_i + sH_2(\mathrm{PID}_i, D_i, T_{\mathrm{pub}}, P_{\mathrm{pub}})$, $R_i = r_i P$, and $\sigma_i = k_i + x_i H_3(M_i, \mathrm{PID}_i, D_i, P_i, t_i) + r_i H_4(M_i, \mathrm{PID}_i, D_i, R_i, t_i)$. Owning to the randomness of w_i, d_i, and r_i, any adversary is unable to link two messages sent from the same vehicle or two anonymous pseudo identities. Therefore, the proposed CCPPA scheme realizes the unlinkability.

Role Separation. There are two trusted authorities, namely, KGC and TRA, in the proposed scheme. The real identity of a vehicle can be only revealed by TRA, even if KGC cannot have the capability to do this. Here, t must be strongly protected in order to achieve the vehicle's anonymous, in which the threshold cryptography [44] would be a better candidate. But, the master key s of KGC should not be strongly protected, because no adversaries can generate a valid message under only knowing s without the vehicle's secret value.

Key Escrow Resilience. In the proposed scheme, the private key of the vehicle V_i includes the secret value x_i and partial private key $\{D_i, k_i\}$, where the vehicle V_i calculates the secret value x_i itself, and it cannot be accessed by the KGC. Hence, the malicious KGC cannot impersonate a vehicle to generate a valid signature without knowing the secret value x_i. The key escrow resilience is satisfied in the proposed CCPPA scheme.

Resistance to Attacks. The proposed CCPPA scheme can resist the main security attacks of VANETs as follows:

(i) *Replay attack*. Replay attack is a class of network attack with repeating valid messages fraudulently. In the proposed scheme, the timestamp t_i is involved in a message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$. By checking freshness of t_i, the verifier (RSU) can withstand any replay attacks.

(ii) *Modification attack*. In the proposed CCPPA scheme, a digital signature on the traffic-related message M_i under $\{\mathrm{PID}_i, t_i, P_i\}$ is the tuples $\{D_i, R_i, \sigma_i\}$. According to Theorem 1, any modified message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$ made by an adversary cannot satisfy equations (6).

(iii) *Impersonation attack*. To launch an impersonation attack, an adversary needs to generate a fake message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$ that satisfies equations (6). However, according to Theorem 1, the probability of the forged message for the adversary to satisfy equation (6) can be negligible.

(iv) *Man-in-the-middle attack*. Based on the aforementioned analysis for message authentication and modification attack, any modification about message in transmitting can be found by verifying equation (6).

Table 2 shows the security comparisons of the proposed scheme with related schemes in [22, 25, 27, 30, 31], in which indicates "satisfy" and means "not satisfy".

According to Table 2, He et al.'s scheme [22], Lo and Tsai's scheme [25], and Wu et al.'s scheme [27] cannot provide key escrow resilience, i.e., the vehicles' private key is entirely generated by the KGC, and it is not fully trusted, it can impersonate any legal vehicle whenever it wants. This may be a strong assumption in VANETs that the KGC is fully trusted for solving key escrow problem. In addition, Horng et al.'s scheme [30] cannot achieve message authentication and resist modification attack, impersonation attack and man-in-the-middle attack. In contrast, the proposed scheme can satisfy all security requirements. Therefore, the proposed scheme has better security than the schemes in [22, 25, 27, 30].

6. Performance Evaluation and Simulation

In this section, the computation delay and communication overhead of the proposed CCPPA scheme are compared with the identity-based CPPA schemes [22, 25, 27] and the certificateless CCPPA schemes [30, 31]. In addition, an extensive simulation is performed using ns-3.26 simulator [45] and the simulation of urban mobility (SUMO) [46]. The ns-3.26 simulator is used for wireless network simulation and SUMO, a traffic simulation tool, provides the realistic traffic mobility model. The simulations are evaluating the average message delay and average message loss ratio in real scenario.

Table 2: Security comparisons.

Security	[22]	[25]	[27]	[30]	[31]	The proposed scheme
Message authentication						
Identity privacy preserving						
Traceability						
Unlinkability						
Role separation						
Key escrow resilience						
Resistance to replay attack						
Resistance to modification attack						
Resistance to impersonation attack						
Resistance to man-in-the-middle attack						

6.1. Computation Delay. The computation delay for the message signing and message verification is evaluated. For computation complexity estimation, the time cost for performing the cryptographic operations is defined below. Let T_{p} be the time for performing a bilinear pairing operation, T_{mtp} be the time for performing a map-to-point hash function operation. The time for performing a scale multiplication operation in bilinear pairing and ECC are denoted as T_{m} and $T_{\mathrm{m-ecc}}$, respectively. Because the v_i used in batch verification is very small, the computation cost can be negligible. Other lightweight operations (one-way hash function and point addition) are not taken into account.

In terms of the proposed CCPPA scheme, He et al.'s scheme [22], Lo and Tsai's scheme [25], and Wu et al.'s scheme [27], the ECC for the security level of 80 bits can be established as follows: $\mathbb{G}$ is an additive group generated by a point P on a non-singular elliptic curve $E : y^2 = x^3 + ax + b \bmod p$, the order of it is q, where $a = -3$, b is a random 160-bit prime number and p and q are two 160-bit prime numbers. For the CCPPA schemes in [30, 31], the symmetric bilinear pairing for the security level of 80 bits can be constructed as follows: $e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_T$, where $\mathbb{G}_1$ is an additive group formed by a generator P with the order q on a super singular elliptic curve $E : y^2 = x^3 + x \bmod p$ with embedding degree 2. p is 512-bit prime number, and q is 160-bit Solinas prime number, which satisfy $q \cdot 12 \cdot r = p + 1$.

To quantify the running time of the cryptographic operations, the MIRACL Crypto SDK [47] is used in this paper. The experiment is performed on Intel Corei5-4590, 3.3 GHz CPU, 8 gigabytes memory with Windows 7. The average execution times of T_{p}, T_{mtp}, T_{m}, and $T_{\mathrm{m-ecc}}$ are listed in Table 3.

Based on the experiment results, the computation delay of the proposed CCPPA scheme, He et al.'s scheme [22], Lo and Tsai's scheme [25], Wu et al.'s scheme [27], Horng et al.'s scheme [30], and Li et al.'s scheme [31] are summarized and shown in Table 4.

In terms of the computation delay of one message signing, He et al.'s scheme [22], Lo and Tsai's scheme [25], and Wu et al.'s scheme [27] require two scalar multiplication operations in ECC. Therefore, the total signing time is $2T_{\mathrm{m-ecc}} = 1.6620$ ms. Horng et al.'s scheme [30] requires two scalar multiplication operations in bilinear pairing. Therefore, the total signing time is $2T_{\mathrm{m}} = 7.5540$ ms. Li et al.'s scheme [31] requires two scalar multiplication operations in bilinear pairing and one map-to-point hash operation. Therefore, the total signing time is $2T_{\mathrm{m}} + T_{\mathrm{mtp}} = 17.2592$ ms. The proposed scheme requires three scalar multiplication operations in ECC. Therefore, the total signing time is $3T_{\mathrm{m-ecc}} = 2.4930$ ms.

In terms of the computation delay of one message verification, He et al.'s scheme [22] and Lo and Tsai's scheme [25] require three scalar multiplication operations in ECC. Therefore, the total verification time is $3T_{\mathrm{m-ecc}} = 2.4930$ ms. Wu et al.'s scheme [27] requires four scalar multiplication operations in ECC. Therefore, the total verification time is $4T_{\mathrm{m-ecc}} = 3.3240$ ms. Horng et al.'s scheme [30] requires three bilinear pairing operations, one scalar multiplication operation in bilinear pairing and one map-to-point hash operation. Therefore, the total verification time is $3T_{\mathrm{p}} + T_{\mathrm{m}} + T_{\mathrm{mtp}} = 40.7195$ ms. Li et al.'s scheme [31] requires three bilinear pairing operations, one scalar multiplication operation in bilinear pairing, and two map-to-point hash operations. Therefore, the total verification time is $3T_{\mathrm{p}} + T_{\mathrm{m}} + 2T_{\mathrm{mtp}} = 50.4247$ ms. The proposed scheme requires four scalar multiplication operations in ECC. Therefore, the total verification time is $4T_{\mathrm{m-ecc}} = 3.3240$ ms.

The computation delay for one message and its correlation with the number of messages (n) are shown in Figure 3. It is known from Table 4 and Figure 3(a), the computation delay of a message signing is 2.4930 ms in the proposed scheme, which decreases by 66.9% and 85.5% compared with those in Horng et al.'s scheme [30] and Li et al.'s scheme [31], respectively. In terms of computation delay of a message verification, the proposed scheme needs 3.3240 ms, which decreases by 91.8% and 93.4% compared with those in Horng et al.'s scheme [30] and Li et al.'s scheme [31], respectively.

To obtain computation delay of multiple (n) messages signing, the computation delay of one message signing should be repeated n times. Therefore, the total n messages signing times in the proposed scheme, He et al.'s scheme [22], Lo and Tsai's scheme [25], Wu et al.'s scheme [27], Horng et al.'s scheme [30], and Li et al.'s scheme [31] are $2.4930n$ ms, $1.6620n$ ms, $1.6620n$ ms, $1.6620n$ ms, $7.5540n$ ms, and $17.2592n$ ms, respectively. To obtain the computation delay of multiple (n) messages verification, He et al.'s scheme [22] and Lo and Tsai's scheme [25] require $(n + 2)$ scalar multiplication operations in ECC. Therefore, the total verification time is $(n + 2)T_{\mathrm{m-ecc}} = 0.8310n + 1.6620$ ms. Wu et al.'s scheme [27] requires $(2n + 2)$ scalar multiplication operations in ECC. Therefore, the total

Table 3: Execution time of cryptographic operation (in milliseconds).

Cryptographic operation	Execution time
Bilinear pairing T_p	9.0791
Map-to-point hash function in bilinear pairing T_{mtp}	9.7052
Scalar multiplication in bilinear pairing T_m	3.7770
Scalar multiplication in ECC T_{m-ecc}	0.8310

verification time is $(2n+2)T_{m-ecc} = 1.6620n + 1.6620$ ms. Horng et al.'s scheme [30] requires three bilinear pairing operations, n scalar multiplication operations in bilinear pairing, and n map-to-point hash operations. Therefore, the total verification time is $3T_p + nT_m + nT_{mtp} = 13.4822n + 27.2373$ ms. Li et al.'s scheme [31] requires three bilinear pairing operations, n scalar multiplication operations in bilinear pairing, and $(n+1)$ map-to-point hash operations. Therefore, the total verification time is $3T_p + nT_m + (n+1)T_{mtp} = 13.4822n + 36.9425$ ms. The proposed scheme requires $(2n+2)$ scalar multiplication operations in ECC. Therefore, the total verification time is $(2n+2)T_{m-ecc} = 1.6620n + 1.6620$ ms.

As is shown in Figure 3(b) and Figure 3(c), that with the increase of number of messages, the signing delay and verification delay grows linearly in all schemes. And the proposed scheme has the lowest slope compared with schemes [30, 31]. It is shown in Figure 3(c), the verification delay of the schemes in [22, 25, 27, 30] and [31] and the proposed scheme, respectively, is 9.9720 ms, 9.9720 ms, 18.2820 ms, 162.0593 ms, 171.7645 ms, and 18.2820 ms when $n = 10$, and 51.5520 ms, 51.5520 ms, 101.3830 ms, 836.1693 ms, 845.8745 ms, and 101.3830 ms when $n = 60$. Apparently, the proposed scheme achieves the lowest verification delay as the number of messages grows in all CCPPA schemes.

Therefore, the proposed scheme has much more superiority than other CCPPA schemes in [30, 31] in the signing and verification process, regardless of the number of messages, and is more suitable for VANETs. The proposed CCPPA scheme is slightly less efficient than He et al.'s scheme [22], Lo and Tsai's scheme [25], and Wu et al.'s scheme [27]. This degradation is forgivable due to the fact that the proposed scheme is a certificateless system and provides key escrow resilience, however, is not the case in [22, 25, 27].

6.2. Communication Cost. In this subsection, the proposed scheme is compared with He et al.'s scheme [22], Lo and Tsai's scheme [25], Wu et al.'s scheme [27], Horng et al.'s scheme [30], and Li et al.'s scheme [31] in terms of the communication cost. In V2I communication, the communication cost refers to the size of message transmitted from a vehicle (OBU) to an RSU. Just as the before analysis, the length of p is 512 bits (64 bytes) and that of q is 160 bits (20 bytes), so the length of elements in $\mathbb{G}_1$ and $\mathbb{G}$, respectively, are 64 bytes and 20 bytes. Assuming the length of output of general one-way hash function is 160 bits (20 bytes), and the length of a timestamp is 32 bits (4 bytes). According to the IEEE Trial-Use standard [48] for VANET security, the length of message is defined as 67 bytes. Table 5 illustrates the comparison of communication costs.

In He et al.'s scheme [22], the message $\{M_i, \mathrm{PID}_i, t_i, R_i, \sigma_i\}$ is sent from the vehicle to a RSU, where $\mathrm{PID}_i = (\mathrm{PID}_{i,1}, \mathrm{PID}_{i,2}, T_i)$, $\mathrm{PID}_{i,1} \in \mathbb{G}$, $\mathrm{PID}_{i,2} \in \mathbb{Z}_q$, and T_i is the timestamp. Thus, the communication cost of He et al.'s scheme is 155 bytes as

$$|M_i| + |PID_i| + |t_i| + |R_i| + |\sigma_i| = 67 + 44 + 4 + 20 + 20 = 155 \text{ bytes.} \quad (15)$$

In Lo and Tsai's scheme [25], the message $\{M_i, \mathrm{PID}_i, tt_i, K_i, R_i, V_i\}$ is sent from the vehicle to a RSU, where $\mathrm{PID}_i = (\mathrm{PID}_{i,1}, \mathrm{PID}_{i,2}, t_i)$, $\mathrm{PID}_{i,1} \in \mathbb{G}$, $\mathrm{PID}_{i,2} \in \mathbb{Z}_q$ and t_i is the timestamp. Thus, the communication cost of Lo and Tsai's scheme is 175 bytes as

$$|M_i| + |\mathrm{PID}_i| + |tt_i| + |K_i| + |R_i| + |V_i| = 67 + 44 + 4 + 20 + 20 + 20 = 175 \text{ bytes.} \quad (16)$$

In Wu et al.'s scheme [27], the message $\{M_i, \mathrm{PID}_i, T_i, h_i, R_i, \delta_i\}$ is sent from the vehicle to a RSU, where $\mathrm{PID}_i = (\mathrm{PID}_{vi}, k_{vi}, T_{vi})$, $\mathrm{PID}_{vi} \in \mathbb{G}$, $k_{vi} \in \mathbb{Z}_q$, and T_{vi} is the timestamp. Thus, the communication cost of Wu et al.'s scheme is 175 bytes as

$$|M_i| + |\mathrm{PID}_i| + |T_i| + |h_i| + |R_i| + |\delta_i| = 67 + 44 + 4 + 20 + 20 + 20 = 175 \text{ bytes.} \quad (17)$$

In Horng et al.'s scheme [30] and Li et al.'s scheme [31], the message $\{M_i, \mathrm{PID}_i, t_i, P_i, R_i, S_i\}$ is sent from the vehicle to a RSU, where $\mathrm{PID}_i = (\mathrm{PID}_{i,1}, \mathrm{PID}_{i,2}, T_i)$, $\mathrm{PID}_{i,1} \in \mathbb{G}_1$, $\mathrm{PID}_{i,2} \in \mathbb{Z}_q$, and T_i is the timestamp. Thus, the communication cost of these two schemes is 351 bytes as

$$|M_i| + |PID_i| + |t_i| + |P|_i + |R_i| + |S_i| = 67 + 88 + 4 + 64 + 64 + 64 = 351 \text{ bytes.} \quad (18)$$

In the proposed scheme, the message $\{M_i, \mathrm{PID}_i, t_i, P_i, D_i, R_i, \sigma_i\}$ is sent from the vehicle to a RSU, where PID_i is the same one as [22]. Thus, the communication cost of the proposed scheme is 195 bytes as

$$|M_i| + |\mathrm{PID}_i| + |t_i| + |P_i| + |D_i| + |R_i| + |\sigma_i| = 67 + 44 + 4 + 20 + 20 + 20 + 20 = 195 \text{ bytes.} \quad (19)$$

The comparison on the communication costs of one message and multiple messages is shown in Figure 4. Clearly, the communication costs increase linearly as the number of messages increases in six schemes. The same communication costs exist in the ID-based schemes [25, 27] and the

Table 4: Comparison of computation delay.

Scheme	A message signing	A message verification	n message signing	n message batch verification
[22]	$2T_{m-ecc} = 1.6620$ ms	$3T_{m-ecc} = 2.4930$ ms	$2nT_{m-ecc} = 1.6620n$ ms	$(n+2)T_{m-ecc} = 0.8310n + 1.6620$ ms
[25]	$2T_{m-ecc} = 1.6620$ ms	$3T_{m-ecc} = 2.4930$ ms	$2nT_{m-ecc} = 1.6620n$ ms	$(n+2)T_{m-ecc} = 0.8310n + 1.6620$ ms
[27]	$2T_{m-ecc} = 1.6620$ ms	$4T_{m-ecc} = 3.3240$ ms	$2nT_{m-ecc} = 1.6620n$ ms	$(2n+2)T_{m-ecc} = 1.6620n + 1.6620$ ms
[30]	$2T_m = 7.5540$ ms	$3T_p + T_m + T_{mtp} = 40.7195$ ms	$2nT_m = 7.5540n$ ms	$3T_p + nT_m + nT_{mtp} = 13.4822n + 27.2373$ ms
[31]	$2T_m + T_{mtp} = 17.2592$ ms	$3T_p + T_m + 2T_{mtp} = 50.4247$ ms	$2nT_m + nT_{mtp} = 17.2592n$ ms	$3T_p + nT_m + (n+1)T_{mtp} = 13.4822n + 36.9425$ ms
The proposed scheme	$3T_{m-ecc} = 2.4930$ ms	$4T_{m-ecc} = 3.3240$ ms	$3nT_{m-ecc} = 2.4930n$ ms	$(2n+2)T_{m-ecc} = 1.6620n + 1.6620$ ms

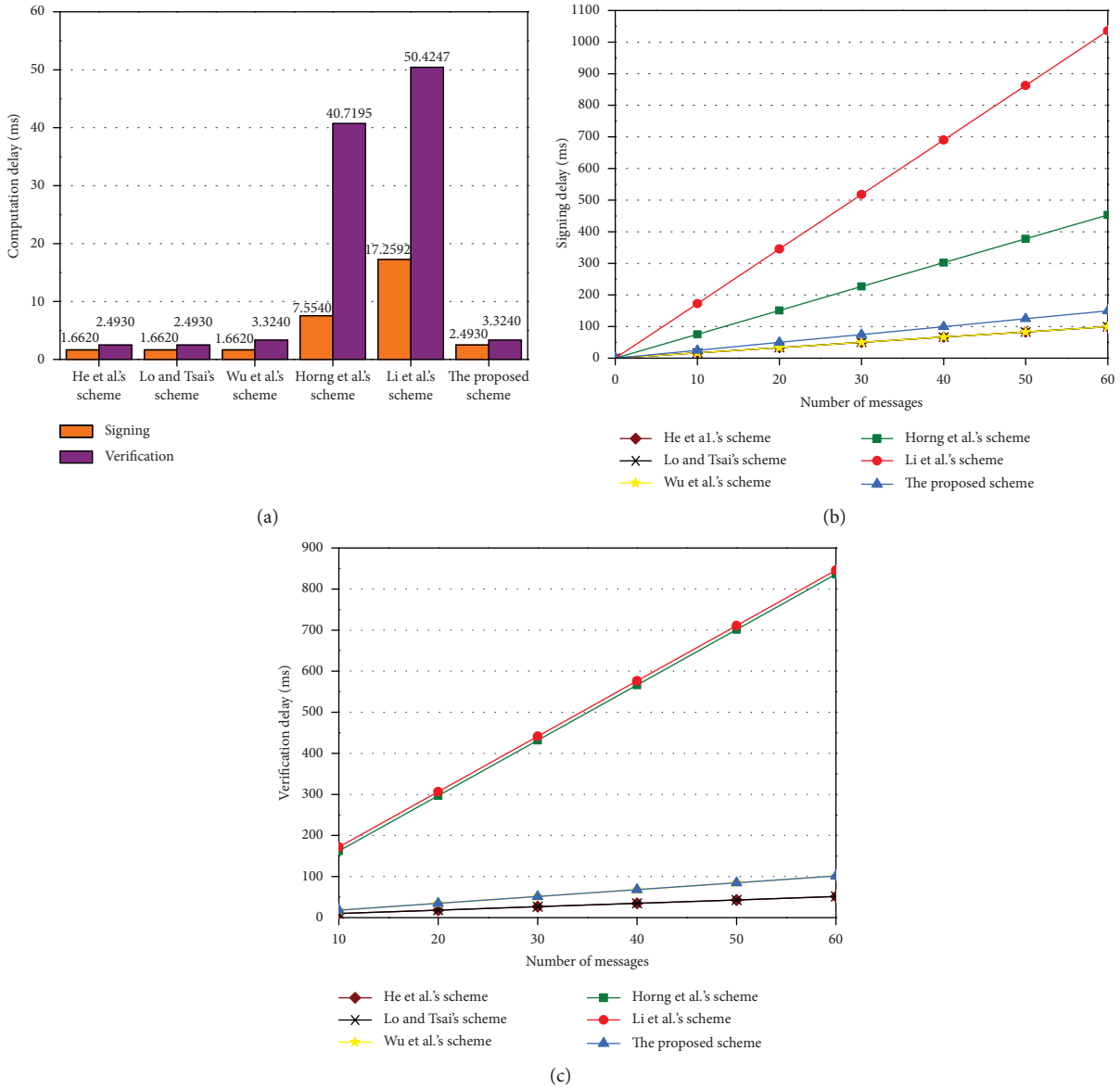

Figure 3: Computation delay. (a) Computation delay in one message signing and verification. (b) Signing delay vs number of messages. (c) Verification delay vs number of messages.

Table 5: Comparison of communication cost.

Scheme	Send a message	Send n messages
[22]	155 bytes	$155n$ bytes
[25]	175 bytes	$175n$ bytes
[27]	175 bytes	$175n$ bytes
[30]	351 bytes	$351n$ bytes
[31]	351 bytes	$351n$ bytes
The proposed scheme	195 bytes	$195n$ bytes

certificateless schemes [30, 31], whether one message or multiple messages are transmitted. The communication cost of the proposed scheme is the lowest in the CCPPA schemes, which significantly decreases by 44.44%. When the number of messages rises to 30 000, the proposed scheme can save 4.46 MB of bandwidth compared with the schemes in [30, 31]. The communication cost of the proposed scheme is slightly larger than that of He et al.'s scheme [22], Lo and Tsai's scheme [25], and Wu et al.'s scheme [27]. The reason is that the proposed scheme is a certificatless scheme, in which an additional user's public key is needed to transmit.

6.3. Simulations. The popular network simulator ns-3.26 [45] on a Ubuntu platform is adopted to evaluate the performances of the proposed CCPPA scheme by comparing with those of He et al.'s scheme [22], Lo and Tsai's scheme [25], Wu et al.'s scheme [27], Horng et al.'s scheme [30], and Li et al.'s scheme [31]. In addition, a road traffic simulator SUMO [46] is used to generate a realistic traffic mobility trace for the road scenario shown in Figure 5.

In our road scenario, the RSUs are assigned every 500 m along each road, and each vehicle broadcasts traffic-related messages every 300 ms. The vehicles are distributed at random on the road and move toward randomly selected intersections. The important simulation parameters are summarized in Table 6.

Generally, the average message delay (avgMD) and average message loss ratio (avgMLR) in RSUs are adopted to estimate the performances.

The avgMD is defined as

$$\text{avgMD} = \frac{\sum_{i=1}^{N_V} \sum_{j=1}^{N_R} \sum_{k=1}^{N_M^i} \left(T^{\text{Recv}}_{V_i \longrightarrow R_j, M_k} - T^{\text{Send}}_{V_i \longrightarrow R_j, M_k} \right)}{\sum_{i=1}^{N_V} N_M^i} + T^{\text{Verify}}_{\text{avg}}, \tag{20}$$

where N_V and N_R indicates the number of vehicles and RSUs in simulation area, respectively. N_M^i represents the number of messages that sent from vehicle V_i. $T^{\text{Recv}}_{V_i \longrightarrow R_j, M_k}$ is the time for R_j (a RSU) receiving a message M_k from V_i and $T^{\text{Send}}_{V_i \longrightarrow R_j, M_k}$ is the time for V_i sending a message M_k to R_j (a RSU). $T^{\text{Verify}}_{\text{avg}}$ means the average verification time for each message.

The avgMLR refers to the ratio of the number of messages dropped over the total number of messages received by the RSUs, which is defined as

$$\text{avgMLR} = \frac{1}{N_R} \sum_{j=1}^{N_R} \frac{N^j_{\text{Dropped}}}{N^j_{\text{Received}}}, \tag{21}$$

where N^j_{Dropped} indicates the number of messages dropped by R_j (a RSU) in the application layer and N^j_{Received} represents the number of messages received by R_j (a RSU) in MAC layer. We emphasize that the avgMLR occurs by the security protocol and the buffer space of the RSU, rather than the wireless transmission channel.

6.3.1. Impact of Vehicle Density. Two experiments are conducted to analyze the influence of the vehicle density on avgMD and avgMLR. The number of vehicles varies from 20 to 100, and the average speed of vehicles is approximately 20 m/s (72 km/h). The simulation results under the different vehicle densities are shown in Figure 6.

Figure 6(a) reveals the relationship between avgMD and the number of vehicles. The avgMD for RSUs increases with the number of vehicles. The avgMD is 0.005 s, 0.004 s, 0.006 s, 2.94 s, 2.98 s, and 0.006 s in He et al.'s scheme [22], Lo and Tsai's scheme [25], Wu et al.'s scheme [27], Horng et al.'s scheme [30], Li et al.'s scheme [31], and the proposed scheme, respectively. Clearly, the avgMD of the proposed scheme and schemes in [22, 25, 27] is very low and hardly affected by vehicle density.

Figure 6(b) describes the relationship between avgMLR and the number of vehicles. While the number of vehicles in the communication range is larger than 20, the avgMLR increases along with the number of vehicles in Horng et al.'s scheme [30] and Li et al.'s scheme [31] and reaches as high as 57% when the number of vehicles is 100. However, for the proposed scheme and schemes in [22, 25, 27], the avgMLR remains nearly 0 regardless of the vehicle density.

6.3.2. Impact of Vehicle Speed. Two experiments are conducted to evaluate the impact of speed of vehicles on avgMD and avgMLR. The average vehicle speed is varies from 10 to 50 m/s (36 to 180 km/h) and the number of vehicles is 50. The results obtained from the simulation under varying speed of vehicles are depicted in Figure 7.

Figure 7(a) shows the relationship between avgMD and the speed of vehicles. Obviously, when the vehicle density is constant, the avgMD hardly changes, showing that it is merely little influenced by the speed of vehicles.

Figure 7(b) depicts the relationship between avgMLR and the speed of vehicles. When the speed of vehicles is higher than 20 m/s, the avgMLRs in Horng et al.'s scheme [30] and Li et al.'s scheme [31] are slightly influenced. As speed of vehicles gets larger, the avgMLR of the proposed scheme and schemes in [22, 25, 27] has been steady at a very low level.

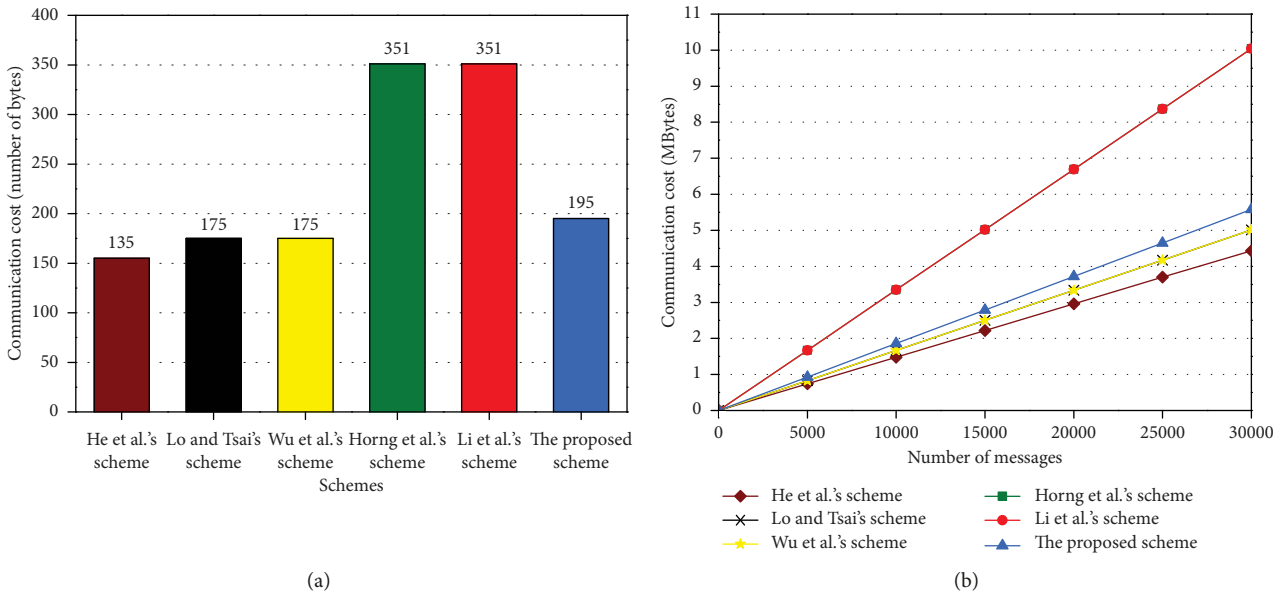

Figure 4: Communication cost. (a) Communication cost of one message. (b) Communication cost vs number of messages.

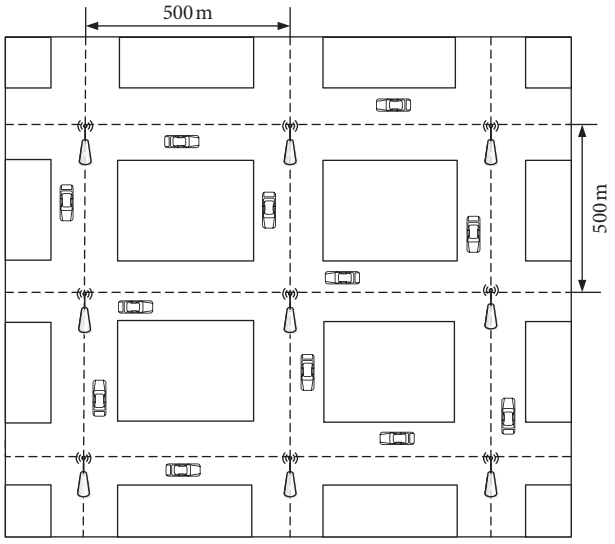

Figure 5: Road scenario for simulation.

Table 6: Simulation parameters.

Parameters	Values
Wireless protocol	802.11p
Channel bandwidth	6 mbs
Buffer size	1 M bytes
Simulation area	1000 m × 1000 m
Number of RSU	9
Simulation time	200 s
Network simulation tool	ns-3.26
Traffic simulation tool	SUMO
Vehicle speed	10–50 m/s

7. Conclusion

This paper has presented a novel and efficient CCPPA scheme in V2I communication for VANETs. Our proposed scheme is not only provably secure in the random oracle model under the ECDL assumption, but also satisfies all security requirements such as message authentication and conditional privacy preserving. Furthermore, the proposed scheme does not need any map-to-point hash operations and bilinear pairing operations. The performance evaluation demonstrates that the proposed scheme has higher efficient

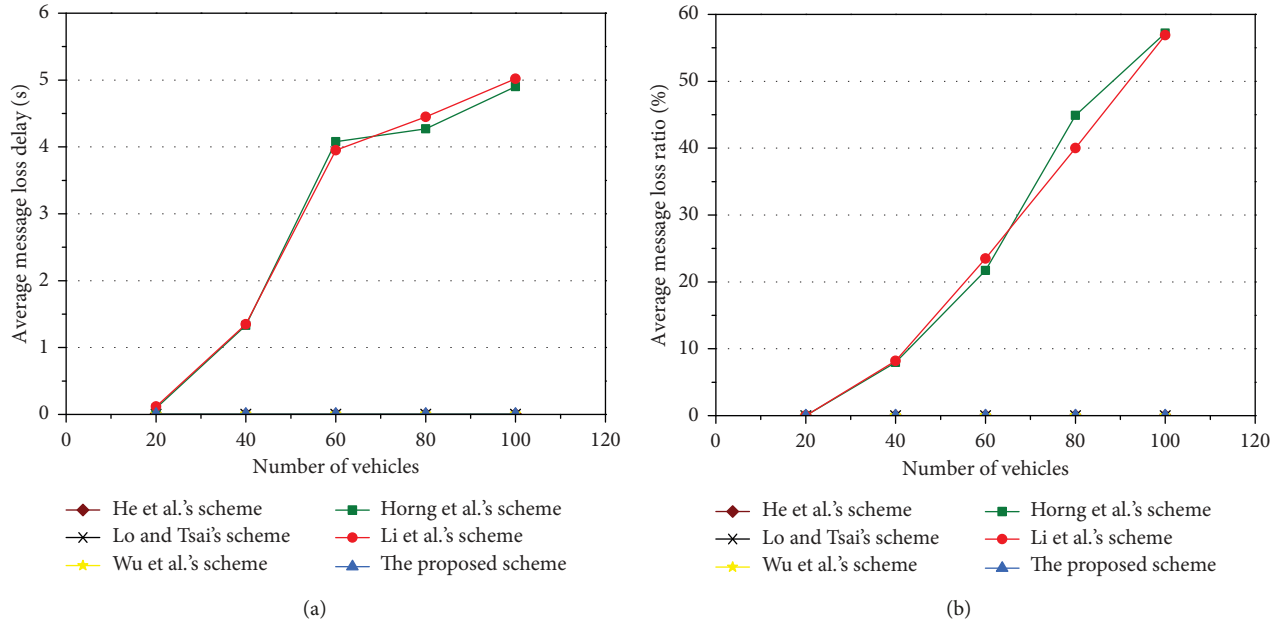

Figure 6: Average message delay and message loss ratio under different number of vehicles. (a) Average message delay vs number of vehicles. (b) Average message loss ratio vs number of vehicles.

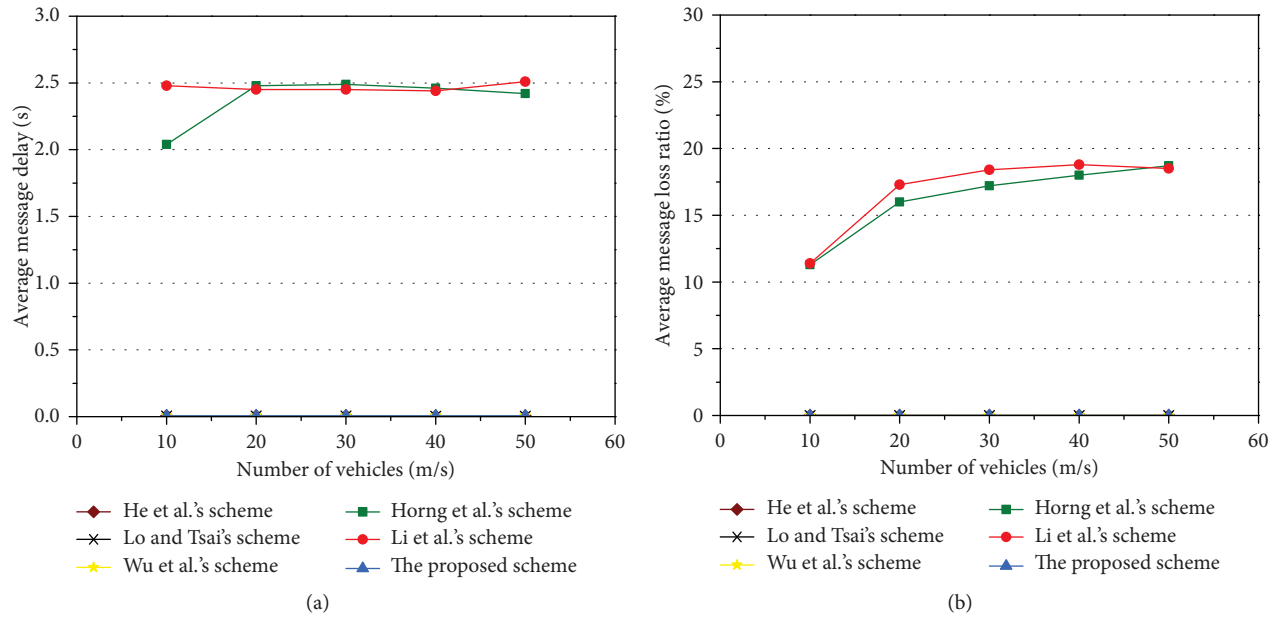

Figure 7: Average message delay and message loss ratio under different speed of vehicles. (a) Average message delay vs speed of vehicles. (b) Average message loss ratio vs speed of vehicles.

in terms of computation delay and communication cost than that of two recently proposed CCPPA schemes. Extensive simulation results indicate that the proposed scheme is feasible in the average message delay and average message loss ratio, and thus the proposed scheme is extremely appropriate in realistic VANETs.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Natural Science Foundation of Shaanxi Province under grant 2018JM6081 and the Project of Science and Technology of Xi'an City under grant 2017088CG/RC051(CADX002).

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, pp. 334–350, 2014.

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

[3] Dedicated short range communications (DSRC)," 2018, http://grouper.ieee.org/groups/scc32/top_lvl3.html/.

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

[5] 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 IEEE INFOCOM—the 27th Conference on Computer Communications*, pp. 1903–1911, Washington, DC, USA, April 2008.

[6] 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 IEEE International Conference on Communications*, pp. 1451–1457, Beijing, China, May 2008.

[7] 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 IEEE INFOCOM—the 27th Conference on Computer Communications*, pp. 816–824, Washington, DC, USA, April 2008.

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

[9] 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.

[10] K. A. Shim, "CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[11] 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.

[12] S. J. Horng, S. F. Tzeng, Y. Pan et al., "b-SPECS+: batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

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

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

[15] 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.

[16] Y. Liu, Z. He, S. Zhao, and L. Wang, "An efficient anonymous authentication protocol using batch operations for VANETs," *Multimedia Tools and Applications*, vol. 75, no. 24, pp. 17689–17709, 2016.

[17] Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, "Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs," *Security and Communication Networks*, vol. 9, no. 18, pp. 5460–5471, 2016.

[18] C. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[19] S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2017.

[20] Y. Jiang, M. Shi, X. S. Shen, and C. Lin, "BAT: a robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974–1983, 2009.

[21] K. A. Shim, "Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree," *IEEE Transactions on Wireless Communications*, vol. 12, no. 11, pp. 5386–5393, 2013.

[22] 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. 2681–2690, 2015.

[23] Y. Xie, L. Wu, J. Shen, and A. Alelaiwi, "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs," *Telecommunication Systems*, vol. 65, no. 2, pp. 229–240, 2016.

[24] Y. Xie, L. Wu, Y. Zhang, and J. Shen, "Efficient and secure authentication scheme with conditional privacy-preserving for VANETs," *Chinese Journal of Electronics*, vol. 25, no. 5, pp. 950–956, 2016.

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

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

[27] 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, Article ID 155014771770089, 2017.

[28] 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.

[29] J. Li, K. K. Raymond Choo, W. Zhang et al., "EPA-CPPA: an efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Vehicular Communications*, vol. 13, pp. 104–113, 2018.

[30] S. J. Horng, S. F. Tzeng, P. H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, pp. 48–66, 2015.

[31] J. Li, H. Yuan, and Y. Zhang, "Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," Cryptology ePrint Archive, 2018, http://eprint.iacr.org/2016/692.

[32] S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'03)*, pp. 452–473, Springer-Verlag, Taipei, Taiwan, December 2003.
[33] V. S. Miller, "Use of elliptic curves in cryptography," in *Proceedings of Conference on the Theory and Application of Cryptographic Techniques (CRYPTO'85)*, pp. 417–426, Springer-Verlag, Santa Barbara, CA, USA, August 1985.
[34] N. Koblitz, "Elliptic curve cryptosystem," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.
[35] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO'84)*, pp. 47–53, Springer-Verlag, Santa Barbara, CA, USA, August 1984.
[36] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.
[37] Y. Ming and X. Shen, "PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks," *Sensors*, vol. 18, no. 5, p. 1573, 2018.
[38] Z. Zhang, D. S. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: security model and efficient construction," in *Proceedings of International Conference on Applied Cryptography and Network Security (ACNS'06)*, pp. 293–308, Springer-Verlag, Singapore, Singapore, June 2006.
[39] J. Li, X. Huang, Y. Mu, and W. Wu, "Cryptanalysis and improvement of an efficient certificateless signature scheme," *Journal of Communications and Networks*, vol. 10, no. 1, pp. 10–17, 2008.
[40] J. Li, H. Yuan, and Y. Zhang, "Cryptanalysis and improvement for certificateless aggregate signature," *Fundamenta Informaticae*, vol. 157, no. 1-2, pp. 111–123, 2018.
[41] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Transactions on Services Computing*, .
[42] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPTO'96)*, pp. 387–398, Springer-Verlag, Saragossa, Spain, May 1996.
[43] J. S. Coron, "On the exact security of full domain hash," in *Proceedings of Annual International Cryptology Conference (CRYPTO'00)*, pp. 229–235, Springer-Verlag, Santa Barbara, CA, USA, August 2000.
[44] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[45] Network simulator N. S.-3," 2018, http://www.nsnam.org/.
[46] "Sumo project," 2018, http://sourceforge.net/projects/sumo/.
[47] Shamus Software Ltd., "Multiprecision integer and rational arithmetic cryptographic library (MIRACL)," 2018, http://www.certivox.com/miracl/.
[48] "IEEE trial-user standard for wireless access in vehicular environments-security services for applications and management messages," IEEE Standard 925 1609 2-2006, 2006.