Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6692568, 13 pages
https://doi.org/10.1155/2021/6692568

Research Article

A Novel Privacy-Preserving Authentication Protocol Using Bilinear Pairings for the VANET Environment

Junsong Zhang,[1] Qikun Zhang,[1] Xianling Lu,[2] and Yong Gan[1,2]

[1]*School of Computer and Communication Engineering, Zhengzhou University of Light Industry Zhengzhou, 450002, China*
[2]*School of Information Engineering, Zhengzhou University of Industrial Technology Zhengzhou, 450002, China*

Correspondence should be addressed to Xianling Lu; 2014102@zzuli.edu.cn

Received 7 December 2020; Revised 17 February 2021; Accepted 21 May 2021; Published 28 June 2021

Academic Editor: Keping Yu

With the rapid development of communication and microelectronic technology, the vehicular ad hoc network (VANET) has received extensive attention. However, due to the open nature of wireless communication links, it will cause VANET to generate many network security issues such as data leakage, network hijacking, and eavesdropping. To solve the above problem, this paper proposes a new authentication protocol which uses bilinear pairings and temporary pseudonyms. The proposed authentication protocol can realize functions such as the identity authentication of the vehicle and the verification of the message sent by the vehicle. Moreover, the proposed authentication protocol is capable of preventing any party (peer vehicles, service providers, etc.) from tracking the vehicle. To improve the efficiency of message verification, this paper also presents a batch authentication method for the vehicle to verify all messages received within a certain period of time. Finally, through security and performance analysis, it is actually easy to find that the proposed authentication protocol can not only resist various security threats but also have good computing and communication performance in the VANET environment.

1. Introduction

In recent years, the vehicular ad hoc network (VANET) has attracted more and more attention in improving people's lives. The VANET is a special mobile self-organizing network used in the intelligent transportation field [1]. In this application scenario, a vehicle can share the information with other vehicles via vehicle-to-vehicle (V2V) or vehicle-to-roadside unit (V2R) communications, respectively [2]. And both the above two communication scenarios follow the dedicated short-range communication (DSRC) protocol [3]. According to the DSRC protocol, each vehicle must periodically broadcast traffic-related messages. The traffic-related message mainly includes the vehicle's location, speed, and traffic status. Due to the open nature of wireless connections, the messages transmitted between the vehicles and the roadside unit (RSU) are easily intercepted or eavesdropped on by attackers [4]. Consequently, the security and privacy protection of the message is one of the key components towards the success of VANET applications.

The user privacy should be preserved during authentication in VANET [5]. In order to hide the actual identities of the vehicles, the anonymity of vehicles is required for VANET. On the other hand, the VANET backend server must have the ability to extract a vehicle's actual identity for tracing the malicious vehicles' activities [6]. Otherwise, a malicious vehicle will randomly send a large amount of false messages in VANET, which will lead to serious consequences [7]. Therefore, privacy preservation and traceability are two seemly conflicting requirements, and hence, we must solve them properly. In addition, unlike other types of self-organizing networks, the VANET has the characteristics of very high node movement speed [8]. Consequently, during the authentication period, the communication time among different nodes will be very short. We must improve the efficiency of the authentication protocol as much as possible.

To solve the above issues, in this paper, we present an authentication protocol based on bilinear pairings and temporary pseudonyms. The contributions of this work can be summarized as follows:

(1) We propose a bilinear pairing-based vehicle authentication and the message verification protocol. In addition, to protect privacy, the proposed protocol uses temporary pseudoidentity to identify the messages transmitted between vehicles

(2) To improve the authentication efficiency, the proposed protocol verifies the messages with the single or batch authentication manner on the recipient's side

(3) In our proposed protocol, the TA and RSU have the ability to trace and revoke a compromised vehicle. The TA is also able to find the RSU who has authenticated the compromised vehicle by the traffic-related message that was sent from the compromised vehicle

(4) The detailed security analysis demonstrated that the proposed vehicle authentication and the message verification protocol can not only resist various security threats but also have good security features, such as unforgeability of identity and message integrity

(5) We evaluate the performance of the proposed authentication protocol and compare it with the related authentication protocols in terms of computation and transmission overheads. In addition, we also have analyzed the relationship between different factors and the message loss rate or the message delay of the authentication protocol

The remainder of this paper is organized as follows. Section 2 summarizes the related work. Section 3 explains the system model and some mathematics-related preliminaries. In Section 4, the proposed privacy-preserving anonymous mutual authentication protocol is given. Moreover, we give the security analysis and performance evaluation of the proposed authentication protocol in Sections 5 and 6, respectively. Finally, Section 7 concludes the paper.

2. Related Work

In the past few years, many researchers have focused on the VANET's security and privacy issues. Many solutions based on pseudonyms, group signatures, symmetric cryptography, and identity identifier encryption have been proposed. The existing research works in VANETs can be classified into the following main categories: pseudonym-based authentication protocols [9–14], group signature-based authentication protocols [15–17], and hybrid-based authentication protocols [18, 19].

2.1. Pseudonym-Based Authentication Protocols. The main idea of the pseudonym-based protocol [13] is to use the pseudonyms generated by random functions or other methods instead of the vehicles' identities in the process of authentication in VANET. One of the earliest works in this field is proposed by Raya and Hubaux [9]. The main idea of Raya and Hubaux's protocol is that the vehicles need to preload a huge number of anonymous certificates and their corresponding private keys based on the anonymity level they require. The main drawback of this protocol is that vehicles need to check a long list of revoked certificates when verifying the received signed message, which is very time-consuming. Sun et al. [10] proposed a pseudonym-based authentication protocol. Their protocol allows RSU to distribute certificate service and allows a vehicle to update its certificate on the way.

Although the above method can hide the user's real identity information successfully, the background server cannot complete the trajectory of the vehicle, which is necessary for certain scenarios. Then, Shen et al. [11] presented an ECC-based privacy-preserving authentication protocol with authority traceability for VANET. Li et al. [12] proposed an ID and pseudonym generation-based privacy-preserving authentication for VANET. He et al. [13] proposed an ID-based conditional privacy-preserving authentication protocol for VANETs based on elliptic curve cryptography. To improve performance further, the batch verification method is introduced in their protocol. Wang et al. [14] proposed a hybrid authentication protocol based on the PKI and identity-based signature, which can meet the requirements of security and conditional privacy in VANETs. However, in most of the abovementioned protocols, they cannot avoid the time-consuming identity legality detection in the message verification process.

2.2. Group Signature-Based Authentication Protocols. Another category of privacy-preserving authentication protocols is the group-based protocol [15–17, 20, 21]. In group-based authentication protocols, each group member can sign on behalf of the group without revealing its real identity when it sends traffic-related messages. Other vehicles can only verify that these messages are from a valid group member, but there is no way to determine who sent them. For example, Hao et al. [15] proposed a group signature-based distributed key management scheme for VANETs, which is expected to considerably facilitate location privacy protection and heterogeneous security policies. Later, Zhu et al. [16] presented an efficient privacy-preserving authentication protocol based on group signatures for VANET. In Zhu et al.'s protocol, they use a hash message authentication code (HMAC) to avoid time-consuming CRL checking and to ensure the integrity of messages before batch group authentication. Shao et al. [17] innovatively grouped the vehicle by RSU and proposed a new group signature-based authentication protocol for VANET.

With the assistance of the new group signature scheme, the proposed authentication protocol is featured with threshold authentication, efficient revocation, unforgeability, anonymity, and traceability. Wang and Yao [20] proposed a group signature-based conditional privacy-preserving authentication for VANET. In addition, their authentication protocol also supports batch verification. Islam et al. [21] proposed a password-based conditional privacy-preserving authentication and group key generation protocol for VANET. Their protocol offers group key generation, user joining and leaving, and password change facilities. Besides the group-based signature scheme, other techniques have also been proposed to achieve anonymity within a group. For example, Zhang et al. [22] used the k-anonymity concept

to protect the user privacy so that a vehicle is indistinguishable from $k-1$ vehicles. In addition, some researchers use the ring signature or blind signature to build the privacy-preserving authentication protocol [23, 24].

2.3. Hybrid-Based Authentication Protocols. Some research activities use a combination of pseudonyms and group signatures to complete the design of authentication protocols in VANET [18, 19, 25]. For instance, Giorgio et al. [18] suggested an authentication protocol for VANET which uses the above methods in combination to protect the messages transmitted between the vehicles. Later, Liu et al. [19] proposed a protocol for VANET which is based on identity-based and group-based signatures. In Liu et al.'s proposal, the vehicles are divided into two different categories: the public vehicles and the private vehicles. The role of a public vehicle is similar to an RSU. The messages sent from the public vehicles and RSUs are authenticated using the identity-based signature [25]. And the messages sent from the private vehicles are authenticated via the group signature for safety reasons.

In general, most of the existing group-based protocols have some disadvantages. First, the group manager has all the knowledge about group members. Hence, there is the possibility of internal privilege attacks. Second, the joining and leaving of group members will result in the need to update the group key. Therefore, when the number of vehicles is large and the movement is frequent, a large amount of computing resources is required for updating the group key.

3. System Model and Preliminaries

3.1. System Model. A typical VANET system model is shown in Figure 1. There are three important components in VANET: the trusted authority (TA), on-board unit (OBU), and roadside unit (RSU) [26]. The TA is mainly responsible for the registration and certification of OBUs and RSUs. It is a trusted management and certification center. Generally, it is assumed that the TA is powerful enough in terms of communication, computation, and storage capabilities, and it is infeasible to compromise by the adversary.

The RSU, deployed on the roadside, can be regarded as the communication medium between OBU and TA. It is generally believed that there is a secure communication channel between RSU and TA, while the channel between RSU and OBU is an insecure wireless communication channel. In addition, due to working in unattended environments, the RSU can send secret information to the attackers when they are compromised. For the above reasons, all the RSUs must be managed and monitored by the TA. The OBU's role is to achieve the communication between vehicles and vehicles or vehicles and RSUs. In addition, it periodically broadcasts traffic-related messages such as location and speed to other vehicles to alert them to avoid traffic jams or accidents [27]. It is generally assumed that the OBU is a tamper-proof device to store the real identity of the vehicle and some other key materials.

3.2. Attacker Model. Since the VANET uses open-featured wireless links to transmit traffic-related messages, attackers can launch various attacks against the VANET through eavesdropping and tampering. In the VANET environment, attackers are mainly divided into the external attacker and internal attacker [28]. The external attacker can eavesdrop or modify all the exchanged information in VANET. Based on these capabilities, the attacker may masquerade as a legitimate vehicle or RSU and communicate with the target entity to obtain illegal benefits. In addition, the external attacker has the ability to launch a denial-of-service attack. And the external attacker may be performed by a single attacker or a group of colluding attackers. In general, the external attacker has more computing and communication capabilities than the vehicle or RSU [29, 30].

The internal attacker mainly refers to the malicious vehicle inside the VANET or the internal administrator [31–33]. The vehicle itself may also be a malicious node that can launch attacks such as the man-in-the-middle attack and replay attack. Besides, the attacker seeks to breach the anonymity of the vehicle. The internal attackers are potent as well since they are part of the system and have access to shared secrets. In addition, the attacker may eavesdrop on the communication link among the vehicles and RSUs. He/she may also attempt to establish the relationship between the successive pseudonyms and link these pseudonyms to a unique real entity.

In addition, the impact of certain human factors will also pose a great threat to the security of the VANET. For example, the OBU may be stolen by the thief. The thief may use the stolen OBU to send false messages to the other vehicle or the RSUs, which may cause new security threats to the VANET. Therefore, we need to take into account the negative impact of the stolen device.

3.3. Elliptic Curve Cryptosystem (ECC). ECC is one of the commonly used public key encryption algorithms, and its security relies on the difficulties of the discrete logarithm problem of the elliptic curve [34]. Compared to the well-known RSA public key encryption algorithm, ECC can achieve the same public key strength as RSA with a shorter key.

Let p be a large prime number, and let $GF(p)$ be a field of integers modulo p. A nonsuper singular elliptic curve E over $GF(p)$ leads to an equation of the following form:

$$y^2 = \left(x^3 + ax + b\right) \bmod p, \tag{1}$$

where $a, b \in GF(p)$ and $4a^3 + 27b^2 \neq 0 (\bmod\ p)$. And then we look at the points on E with coordinates in $GF(p)$ which we denote by the following form:

$$\begin{aligned} E_p(a,b) = \{(x,y)\colon x, y \in GF(p) \text{ satisfy } y^2 \\ = x^3 + ax + b\} \cup \{\infty\}. \end{aligned} \tag{2}$$

The point multiplication over E can be computed by repeated addition as

$$k \cdot P = P + P + \cdots + P (k \text{ times}), \tag{3}$$

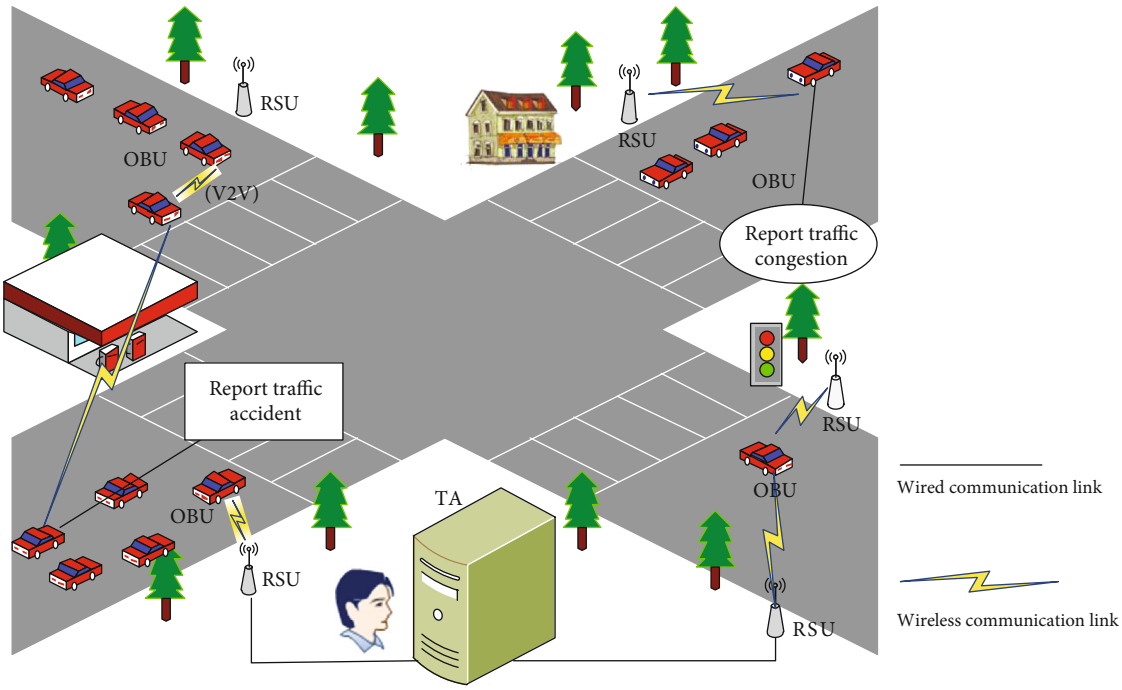

Figure 1: A typical communication model in VANET.

where $k \in GF(p)$ and P is a point $P \in E_p(a, b)$. In view of shortness, we omit the details of ECC and refer to [35, 36].

In order to prove the security of our proposed protocol, here, we present two important mathematical problems on elliptic curves as follows:

Elliptic curve discrete logarithm problem (ECDLP). Given an elliptic curve E defined over a finite field $GF(p)$, and two points $P, Q \in E$ of order q, it is hard to find an integer $k \in Z_q^*$ such that $Q = kP$.

Computational Diffie-Hellman problem (CDHP). Given an elliptic curve E defined over a finite field $GF(p)$, and the points $P, aP, bP \in E$, it is hard to compute abP.

3.4. Bilinear Pairings. The bilinear mapping defines three multiplicative cyclic groups with prime order $q : G_1, G_2, G_T$. Let $\hat{e} : G_1 \times G_2 \to G_T$ be a computable bilinear map, which satisfies the following properties:

Bilinearity. For any $P, Q \in G$ and $a, b \in Z_q^*$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, where $Z_q^* = \{j \mid 1 \le j \le q-1\}$. This can be restated in the following way: for any $P, Q \in G$ and $a, \in Z_q^*$, $\hat{e}(a \cdot P, Q) = \hat{e}(P, a \cdot Q) = \hat{e}(P, Q)^a$.

Nondegenerate. For any $P \in G$, $\hat{e}(P, P) \ne e$, where e is the identity element of the group G_T.

Computability. There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P \in G_1$ and $Q \in G_2$.

Then, we called e a bilinear map. The bilinear mapping can be constructed by Tate pairs or Weil pairs on elliptic curves over a finite field.

4. The Proposed Authentication Scheme

In this section, we present a bilinear pairing-based vehicle authentication and the message authentication protocol to improve the security and efficiency of communication in VANET. It contains seven phases, namely, system initialization, registration, RSU temporary key retrieval, vehicle authentication, vehicle verification, message signing, and message verification. To facilitate the subsequent description, the various symbols used in this paper are listed in Table 1.

Table 1: The symbols used in this paper.

Notations	Description
R_i	The ith roadside unit (RSU)
RID_i	The identity of the RSU R_i
TA	The trusted authority
V_j	The jth vehicle
pID_j	The pseudoidentity of the vehicle which contains $\mathrm{pID}_j = \{\mathrm{pID}_j^1, \mathrm{pID}_j^2\}$
s, P_{pub}	The master and public keys of TA
rprk_i, rpuk_i	The master and public keys of the ith RSU
uprk_j, upuk_j	The master and public keys of the jth OBU
$h(\cdot)$	$h : \{0,1\}^* \to Z_q^*$ is a secure hash function
$H(\cdot)$	$H : E_p(a, b) \to \{0,1\}^l$, where l is the length of the string
$H_1(\cdot)$	$H_1 : \{0,1\}^* \to G$ is a map-to-point hash function
$\oplus$	The bitwise XOR operation
$\|$	String concatenation operation

4.1. Initialization. In the initialization phase, TA sets the required parameters used in the proposed scheme:

Step I_1. TA first selects a prime number p and an appropriate elliptic curve E over the finite field $GF(p)$ and then selects a base point P over the elliptic curve E, and the order of P is q. Let G be a cyclic additive group generated by P and G_T be a cyclic multiplicative group with the same order q. Then, TA constructs an appropriate bilinear map $\hat{e} : G \times G \rightarrow G_T$.

Step I_2. The TA selects two secure cryptographic hash functions $h(\cdot)$, $H(\cdot)$, and $H_1(\cdot)$, where $h : \{0,1\}^* \rightarrow Z_q^*$ is a secure hash function, $H : E_p(a,b) \rightarrow \{0,1\}^l$, where l is the length of the string, and $H_1 : \{0,1\}^* \rightarrow G$ is a map-to-point hash function.

Step I_3. Next, TA chooses its private key $s \in Z_q^*$ and computes its corresponding public key $P_{\text{pub}} = s \cdot P$. Then, TA selects two secret values $x, y \in Z_q^*$ and saves them properly.

Step I_4. After completing the above operations, the TA publishes the system parameters $\{E, q, P, G, G_T, h(\cdot), H(\cdot), P_{\text{pub}}\}$.

4.2. Registration Phase. Due to different roles and characteristics, the registration phase is divided into two parts: OBU registration and RSU registration.

4.2.1. OBU Registration. When the vehicle V_j wants to accept the services provided by VANET, it must be registered by the TA:

Step OR_1. The vehicle V_j selects a unique identity ID_{vj} and a password PW_{vj}. Then, it chooses a random number $b_{vj} \in Z_q^*$ and computes $B_{vj} = h(b_{vj} \| \text{PW}_{vj})$. Next, the V_j sends $\{\text{ID}_{vj}, B_{vj}\}$ to the TA through a secure channel.

Step OR_2. Upon receiving the message $\{\text{ID}_{vj}, B_{vj}\}$, the TA randomly generates a number r_{vj} and then calculates

$$\begin{aligned} A_{vj} &= h\left(x \| r_{vj}\right), \\ C_{vj} &= A_{vj} \oplus B_{vj}, \\ D_{vj} &= h\left(\text{ID}_{vj} \| B_{vj} \| A_{vj}\right). \end{aligned} \tag{4}$$

Then, TA chooses a random number $\text{uprk}_j \in Z_q^*$ as the user's private key and computes the corresponding public key $\text{upuk}_j = \text{uprk}_j \cdot P$.

Step OR_3. Next, the TA embedded the information $\{C_{vj}, D_{vj}, r_{vj}, h(\cdot), H(\cdot), q, \text{uprk}_j, \text{upuk}_j\}$ into the V_j's tamper-proof device (TPD) and keeps $(\text{ID}_{vj}, \text{upuk}_j)$ in its tracking list.

4.2.2. RSU Registration. The registration process of the RSU R_i, $i \in \{1, 2, 3, \cdots, n\}$, is explained as follows:

Step RR_1. The RSU R_i sends the information about the network to which it is connected to the TA securely.

Step RR_2. The TA chooses a random value $\text{rprk}_i \in Z_q^*$ as R_i's private key and computes the corresponding public key $\text{rpuk}_i = \text{rprk}_i \cdot P$.

Step RR_3. The TA generates the signature $\text{Sign}_{ri} = h(y \| \text{RID}_i)$, where RID_i is R_i's identifier number. Then, TA injects the information $\{\text{RID}_i, \text{Sign}_{ri}, \text{rprk}_i, \text{rpuk}_i\}$ into the RSU via a secure channel.

4.3. RSU Temporary Key Retrieval Phase. In order to improve the efficiency of message verification, RSU is responsible for regularly distributing its local temporary keys for the vehicles which enter into the RSU's communication range.

The RSU R_i randomly chooses a value $\delta_i \in Z_q^*$ and calculates the temporary master key $\text{MK}_i = h(\text{rprk}_i \oplus \delta_i)$. Then, the RSU stores the temporary master key in its TPD. And then, the RSU calculates the corresponding temporary public key $\text{RPK}_i = \text{MK}_i P$.

Next, the RSU releases its temporary public key RPK_i together with the random number δ_i in its coverage area periodically.

4.4. The Vehicle Authentication Phase. When a vehicle arrives at the area covered by the RSU R_i, it first checks the identity of R_i and determines whether it is a new RSU. If so, the vehicle V_j should be authenticated to R_i to get the of RSU_i's temporary master key. Then, V_j calculates its anonymous identity via the R_i's temporary master key.

In this phase, the vehicle V_j generates an anonymous identity and constructs a message authentication code. Then, the TA verifies the authentication message to verify the legality of the vehicle V_j. The detailed message authentication process is described as follows:

Step A_1. The user of the vehicle V_j enters the identity ID_{vj} and the password PW_{vj} into the OBU_j. The OBU of the vehicle V_j calculates the following formulas:

$$\begin{aligned} B_{vj}^* &= h\left(b_{vj} \| \text{PW}_{vj}\right), \\ A_{vj}^* &= B_{vj}^* \oplus C_{vj}, \\ D_{vj}^* &= h\left(\text{ID}_{vj} \| B_{vj}^* \| A_{vj}^*\right). \end{aligned} \tag{5}$$

And then, it verifies whether $D_{vj}^* = D_{vj}$ holds. If they are not equal, the OBU_j will require the user to enter the correct identity and password again. Otherwise, the OBU_j generates a timestamp T_{vj} and computes $\text{TID}_{vj} = \text{ID}_{vj} \oplus h(A_{vj} \| T_{vj})$ and $\text{Cert}_{vj} = h(A_{vj} \| \text{ID}_{vj} \| T_{vj})$.

Step A_2. Then, the OBU of the vehicle V_j sends the message $M_1 = \{\text{TID}_{vj}, r_{vj}, T_{vj}, \text{upuk}_j, \text{Cert}_{vj}\}$ to the RSU_i via a public communication channel.

Step A_3. Upon receiving the message, the R_i first checks the freshness of the timestamp T_{vj}. If it holds, the RSU_i then computes $\text{Cert}_{ri} = H(\text{rprk}_i \cdot P_{\text{pub}}) \oplus (\text{TID}_{vj} \| \text{Cert}_{vj} \| \| \text{Sign}_{ri} \| T_{c1})$ and sends the message $\{M_1, \text{Cert}_{ri}, \text{RID}_i, \text{rpuk}_i, T_{c1}\}$ to the TA via a public channel.

4.5. The Vehicle Verification Phase. Step V_1. Upon receiving the message $\{M_1, \text{Cert}_{ri}, \text{RID}_i, \text{rpuk}_i, T_{c1}\}$, the TA first checks the timestamp T_{c1}. If the condition holds, the TA computes

$$\begin{aligned} \mathrm{Sign}_{ri}^{*} &= h(y \| \mathrm{RID}_i), \\ H(s \cdot \mathrm{rpuk}_i) \oplus \mathrm{Cert}_{ri} &= \left(\mathrm{TID}_{vj} \| \mathrm{Cert}_{vj} \| \mathrm{Sign}_{ri} \| T_{c1}\right). \end{aligned} \tag{6}$$

Then, TA determines whether the equation $\mathrm{Sign}_{ri}^{*} = \mathrm{Sign}_{ri}$ is true. If they are equal, the TA considers R_i to be a legitimate RSU.

Step V_2. Next, the TA extracts the message M_1 and continues to calculate

$$\begin{aligned} A_{vj}^{*} &= h\left(x \| r_{vj}\right), \\ \mathrm{ID}_{vj}^{*} &= \mathrm{TID}_{vj} \oplus h\left(A_{vj}^{*} \| T_{vj}\right), \\ \mathrm{Cert}_{vj}^{*} &= h\left(A_{vj}^{*} \| \mathrm{ID}_{vj}^{*} \| T_{vj}\right). \end{aligned} \tag{7}$$

And then it checks whether $\mathrm{Cert}_{vj}^{*} = \mathrm{Cert}_{vj}$ holds. If they are equal, the TA considers V_j to be a legitimate vehicle.

Step V_3. The TA computes $\mathrm{Cert}_{\mathrm{TA}} = H(s \cdot \mathrm{rpuk}_i) \oplus (\mathrm{TID}_{vj} \| h(y \| \mathrm{RID}_i) \| T_{c1} \| T_{c2})$ and sends the message $\{\mathrm{Cert}_{\mathrm{TA}}, T_{c2}\}$ to R_i via a public channel to tell R_i the vehicle V_j is a legitimate vehicle. Upon receiving the message, R_i computes $C_1 = H(\mathrm{rprk}_i \cdot \mathrm{upuk}_j) \oplus (\mathrm{TID}_{vj} \| \mathrm{MK}_i \| T_{c1} \| T_{c2})$ and sends C_1 to the vehicle V_j via a public communication channel.

Step V_4. Upon receiving the message, the vehicle V_j computes $C_1 \oplus H(\mathrm{uprk}_j \cdot \mathrm{rpuk}_i) = (\mathrm{TID}_{vj} \| \mathrm{MK}_i \| T_{c1} \| T_{c2})$ and extracts R_i's local master keys MK_i to prepare for the next message signing phase. The sequence diagram of the vehicle's login and certification steps is described in Figure 2.

4.6. Message Signing Phase. As discussed previously, the vehicle driving on the road needs to send out traffic-related messages periodically. To protect the privacy of the vehicle, the message should be signed with the vehicle's pseudoidentity. However, in order to ensure the legitimacy of the received traffic-related messages, the receiver needs to verify the messages. Hence, message authentication is very important in VANET. The receiver checks the integrity and validity of the traffic-related message by verifying the correctness of the signature. The details of the signing phase can be described as follows:

Step M_1. The vehicle V_j first chooses a random number $\sigma \in Z_q^{*}$ and generates its pseudo-ID $\mathrm{pID}_j = \{\mathrm{pID}_j^1, \mathrm{pID}_j^2\}$ and the corresponding private key $\mathrm{SK}_j = \{\mathrm{SK}_j^1, \mathrm{SK}_j^2\}$ as follows:

$$\begin{aligned} \mathrm{pID}_j^1 &= \sigma \cdot P, \\ \mathrm{pID}_j^2 &= \mathrm{ID}_{vj} \oplus h(\sigma \| \mathrm{MK}_i), \\ \mathrm{SK}_j^1 &= \mathrm{MK}_i \cdot \mathrm{pID}_j^1, \\ \mathrm{SK}_j^2 &= \mathrm{MK}_i \cdot H_1\left(\mathrm{pID}_j^1 \| \mathrm{pID}_j^2 \| \delta_i\right). \end{aligned} \tag{8}$$

Step M_2. The vehicle V_j then generates a traffic message M_s which includes the timestamp and the traffic information related to the vehicle. Next, V_j signs the message M_s as follows:

$$\theta_j = \mathrm{SK}_j^1 + h(M_s) \cdot \mathrm{SK}_j^2. \tag{9}$$

Step M_3. Finally, the vehicle V_j releases the traffic-related message $\{\mathrm{pID}_j, \theta_j, M_s, \mathrm{RID}_i\}$. Here, RID_i is the identity of the RSU R_i. It is used to let the verifier know that the traffic-related message is signed by the key which is based on the temporary master key of R_i.

4.7. Message Verification Phase. When the traffic-related message $\{\mathrm{pID}_j, \theta_j, M_s, \mathrm{RID}_i\}$ is received by other recipients, they should check the validity of this message. And the validity of the traffic-related message can be verified when the value of the following equation is true:

$$\begin{aligned} \hat{e}(\theta_j, P) = \hat{e}\left(\mathrm{pID}_j^1, \mathrm{RPK}_i\right) \times \hat{e}\Big(h(M_s) \\ \cdot H_1\left(\mathrm{pID}_j^1 \| \mathrm{pID}_j^2 \| \delta_i\right), \mathrm{RPK}_i\Big). \end{aligned} \tag{10}$$

Equation (10) can be derived as follow:

$$\begin{aligned} \mathrm{L.H.S} &= \hat{e}(\theta_j, P) = \hat{e}\left(\mathrm{SK}_j^1 + h(M_s) \cdot \mathrm{SK}_j^2, P\right) \\ &= \hat{e}\left(\mathrm{SK}_j^1, P\right) \times \hat{e}\left(h(M_s) \cdot \mathrm{SK}_j^2, P\right) \\ &= \hat{e}\left(\mathrm{MK}_i \cdot \mathrm{pID}_j^1, P\right) \times \hat{e}(h(M_s) \cdot \mathrm{MK}_i \\ &\quad \cdot H_1\left(\mathrm{pID}_j^1 \| \mathrm{ID}_j^2 \| \delta_i\right), P\Big) \\ &= \hat{e}\left(\mathrm{pID}_j^1, \mathrm{MK}_i \cdot P\right) \times \hat{e}(h(M_s) \\ &\quad \cdot H_1\left(\mathrm{pID}_j^1 \| \mathrm{pID}_j^2 \| \delta_i\right), \mathrm{MK}_i \cdot P) \\ &= \hat{e}\left(\mathrm{pID}_j^1, \mathrm{RPK}_i\right) \times \hat{e}(h(M_s) \\ &\quad \cdot H_1\left(\mathrm{pID}_j^1 \| \mathrm{pID}_j^2 \| \delta_i\right), \mathrm{RPK}_i) = \mathrm{R.H.S.} \end{aligned} \tag{11}$$

The recipients have obtained the system parameter P, the RSU's temporary public key RPK_i, and the random number δ_i. After receiving vehicle V_j's traffic-related message, they can get the traffic-related message M_s, the signature θ_j, and the anonymous identity pID_j. If the above formula is true, it proves that the sender of the traffic-related message is legal, and the integrity of this message can also be confirmed.

When the recipient receives multiple messages at the same time, the recipient can use the batch verification method to verify these messages. Suppose these messages are marked as $\{\{\mathrm{pID}_1, \theta_1, M_{s1}, \mathrm{RID}_i\}, \{\mathrm{pID}_2, \theta_2, M_{s2}, \mathrm{RID}_i\}, \cdots, \{\mathrm{pID}_n, \theta_n, M_{sn}, \mathrm{RID}_i\}\}$. The batch verification of these messages uses the following equation:

$$\begin{aligned} \hat{e}\left(\sum_{j=1}^{n} \theta_j, P\right) = \hat{e}\left(\sum_{j=1}^{n} \mathrm{pID}_j^1, \mathrm{RPK}_i\right) \times \hat{e}\Bigg(\sum_{j=1}^{n} h(zM_{sj}) \\ \cdot H_1\left(\mathrm{pID}_j^1 \| \mathrm{pID}_j^2 \| \delta_i\right), \mathrm{RPK}_i\Bigg). \end{aligned} \tag{12}$$

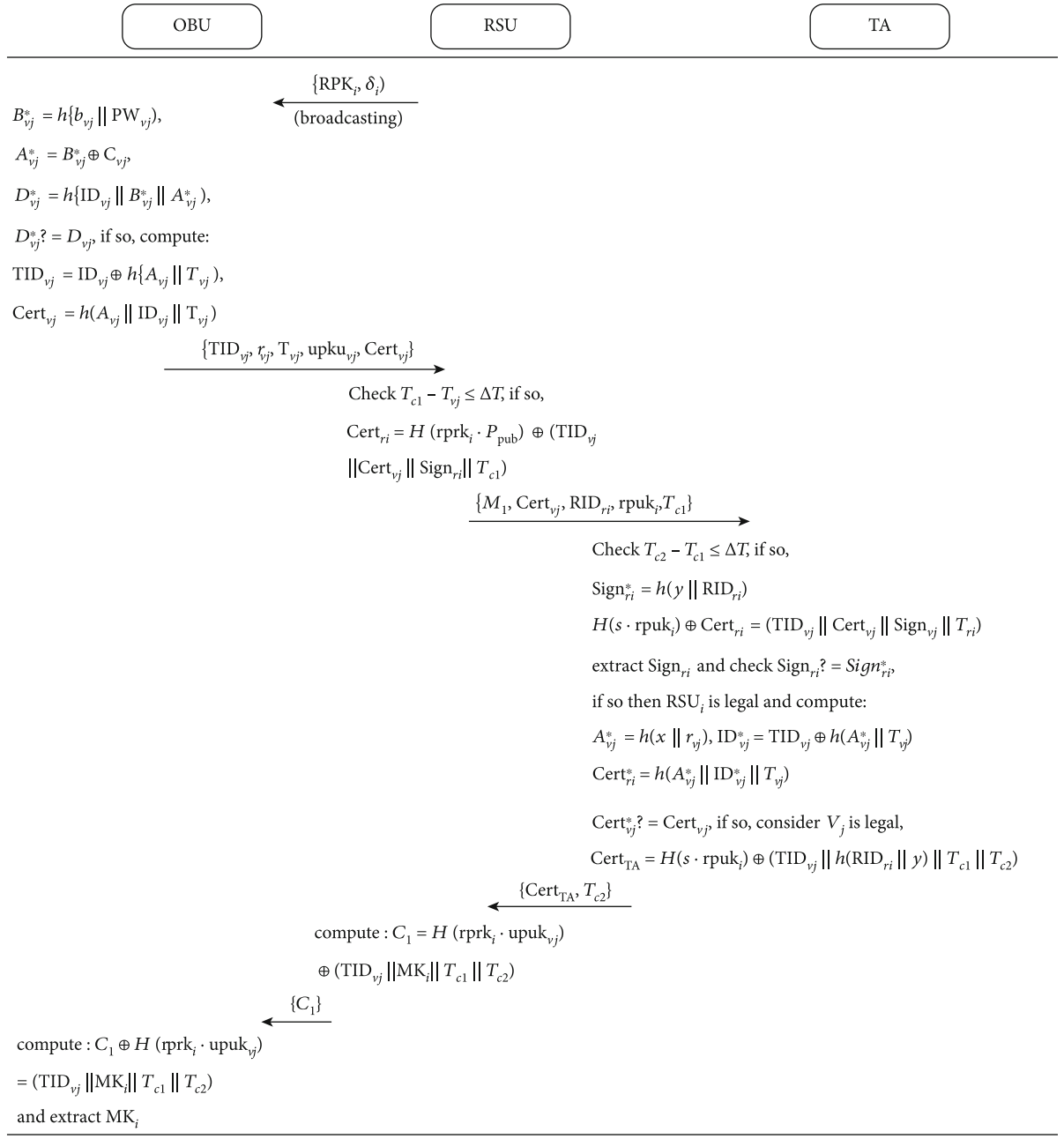

Figure 2: The vehicle's login and certification process.

Verifying a number of signatures with the batch verification method is much faster than verifying them individually. In addition, the proof process of formula (12) is similar to that of formula (10). For brevity, we omit the proof process of formula (12). The sequence diagram of the message signing and verification processes is described in Figure 3.

4.8. Real Identity Tracking and Revocation. In the proposed authentication protocol, the traffic-related messages are signed with pseudoidentities to protect privacy. When an OBU is compromised and releases false traffic-related messages, TA should have the ability to reveal its real identity and revoke its long-term certificate. In the proposed protocol, only the TA and RSU have the ability to trace and revoke a compromised vehicle. Therefore, TA is able to find the compromised vehicle by the RID_i which is contained in the traffic-related messages. Then, TA calculates the real identity of the compromised vehicle using the following equation:

$$\mathrm{pID}_j^2 \oplus h(\sigma \| \mathrm{MK}_i) = \mathrm{ID}_{vj}. \tag{13}$$

Next, TA adds the genuine identity ID_{vj} of this vehicle to its compromised vehicle list (CVL) and sends the updated CVL to all RSUs. When a vehicle is compromised, the RSU will discard its request message in the early stages of mutual

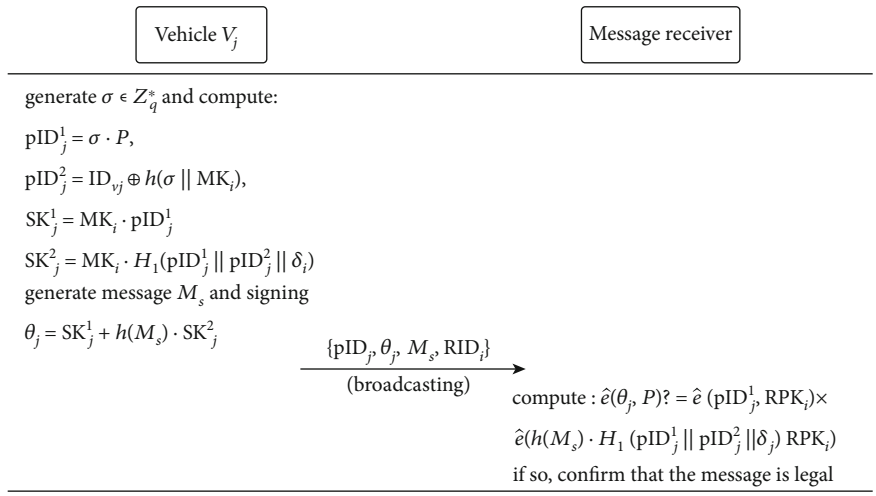

Figure 3: The message signing and verification processes.

authentication. Consequently, the compromised vehicle will not get the RSU's local master keys. And it cannot calculate the corresponding temporary key to release the malicious wrong traffic-related message.

5. Security Analysis

In this section, we analyze the security and privacy features of the proposed authentication protocol as follows.

5.1. Unforgeability of Identity. The proposed protocol guarantees that no one can use an identity that does not belong to him/her to take part in the system. When the vehicle V_j needs to be authenticated at the RSU_i, the message $\{TID_{vj}, r_{vj}, T_{vj}, upuk_j, Cert_{vj}\}$ sent by V_j does contain its real identity ID_{vj}. However, due to the one-way nature of the hash function, the attacker cannot get ID_{vj} from the above message.

On the other hand, the attacker also cannot pretend to be an RSU to spoof. Even if the attacker obtains the RSU_i's identity RID_i and the corresponding public key $rpuk_i$, the attacker is unable to calculate the parameter $H(rprk_i \cdot P_{pub})$ for authentication with the TA because it cannot obtain the RSU_i's private key $rprk_i$. Then, the attacker is unable to establish a secure connection with the vehicle V_j and perform subsequent operations.

5.2. Replay Attacks. Due to the open nature of the wireless channel, the message can be easily captured or modified by the attacker. Therefore, the attacker may use the captured traffic-related message to launch a replay attack. In our proposed scheme, the timestamp T_{vj} is used to keep the freshness of the messages and resist the replay attack in the vehicle authentication phase. Although the attacker may obtain another vehicle's authentication message $\{TID_{vj}, r_{vj}, T_{vj}, upuk_j, Cert_{vj}\}$, without knowing the secure variable A_{vj}, he/she cannot get the session key and finish the authentication successfully.

Similarly, the attacker cannot replay the traffic-related message. The reason is that the traffic-related message contains the random number σ and the corresponding private key SK_{vj} which is only owned by the vehicle V_j. If an attacker replays this data, he/she will not be able to structure a valid signature about the traffic-related message. Through the above analysis, it is clear that the proposed authentication protocol has the ability to resist the replay attack.

5.3. Message Integrity and Authentication. For VANET, which is composed of open communication links, the integrity and authenticity of the message must be guaranteed. In the proposed authentication protocol, the TA injects the relevant secret information into every RSU's and OBU's memory in the registration phase. In V2R communication, the vehicle V_j sends the request message to RSU_i to authenticate with the RSU_i and obtain its local master keys MK_i. Then, the RSU_i returns its local master key MK_i to the requested vehicle. All the messages mentioned above are encrypted with the secret values obtained from the TA. Therefore, the receiver can easily verify the integrity and identity of the messages.

After mutual authentication, the vehicle V_j obtains the local master key from the RSU_i. In the next V2V communication, the vehicle V_j uses the RSU_i's local master key MK_i to generate its pseudo-ID $pID_j = \{pID_j^1, pID_j^2\}$ and the corresponding private key $SK_j = \{SK_j^1, SK_j^2\}$. Because of the use of identity-based signature algorithms, the receiver can easily verify the integrity of the traffic-related messages broadcasted by vehicle V_j. With the above analysis, we can find that our proposed protocol satisfies the requirements of message integrity and authentication.

5.4. Conditional Privacy-Preserving Property. As described earlier, in the authentication phase, the main role of RSU is to distribute the temporary public key to the vehicles nearby it. However, the privacy of the vehicle's identity must be protected in this environment. The proposed authentication protocol achieves the conditional privacy-preserving property in two aspects.

Table 2: Parameters used in the experimental simulation platform.

Bit rate	20 Mbps
Minimum frequency	5.890*e*9 Hz
Maximum transmission	20 mW
Minimum signal attenuation threshold	-80 dBm
Application packet length	Uniform (256 bits, 15000 bits)

First, when a vehicle V_j moves near the RSU, V_j needs to generate a fresh timestamp T_{vj} and uses it to calculate with the user's real identity ID_{vj} via the hash function to generate an authentication message. Since the timestamp T_{vj} used to calculate the authentication message is different each time and the hash function has a strong collision resistance property, the adversary cannot get the genuine identity information of the vehicle V_j through the message $M_1 = \{TID_{vj}, r_{vj}, T_{vj}, upuk_j, Cert_{vj}\}$.

Second, when the vehicle V_j joins an RSU R_i's group, it obtains the R_i's local master key MK_i and the corresponding temporary public key RPK_i. And then, it generates a new pseudo-ID and the corresponding private key to sign the traffic-related message by the temporary master key of R_i. Since the traffic-related message is signed with different temporary master keys of R_i at different time, no entity except TA and R_i can establish the link between signatures and pseudo-IDs of the vehicle V_j. In summary, we can find that the proposed authentication protocol satisfies the conditional privacy-preserving property.

5.5. Traceability and Revocability. In the proposed authentication protocol, only the TA can get the authentic identity ID_{vj} of the vehicle V_j from its authentication request message. Other participants (including vehicles and attackers) cannot extract the authentic identity ID_{vj} of the vehicle V_j from the authentication request message.

In addition, to protect privacy, the proposed protocol signs the traffic-related messages with different pseudo-IDs in the message signing phase. And the TA can get the authentic identity ID_{vj} of the vehicle V_j by using equation (13). Consequently, when a vehicle is compromised, the TA could reveal its authentic identity to other entities. As a result, the revoked vehicle cannot join the RSU's communication group to release any messages. This means that the proposed authentication protocol supports the traceability and revocability property.

6. Performance Evaluations

In this section, we evaluate the performance of the proposed authentication protocol and compare it with the related authentication protocols in terms of computation and transmission overheads. In our implementation, we use a PC with Intel Core i7 CPU 2.6 GHz and 8 GB memory to run the verification authentication protocol. Then, we use currently very popular experimental platforms, OMNeT++ and SUMO, to implement the proposed authentication protocol and test the indicators of communication performance and reliability.

Table 3: Execution time of the related pairing-based operations.

Symbols	Execution time for various operations	Running time (ms)
T_h	One-way hash function $H(\cdot)$ or $h(\cdot)$	<1
T_{Gh}	Map-to-point hash function $H_1(\cdot)$	<1
T_{pair}	Bilinear pairing computation	3.61
T_{add}	Addition operation of points in ECC	<1
T_{exp}	Exponential operation	2.74
T_{mul}	Scalar multiplication of elliptic curves	1.63
T_{en}	Symmetric encryption algorithm AES (128-bit key)	<1

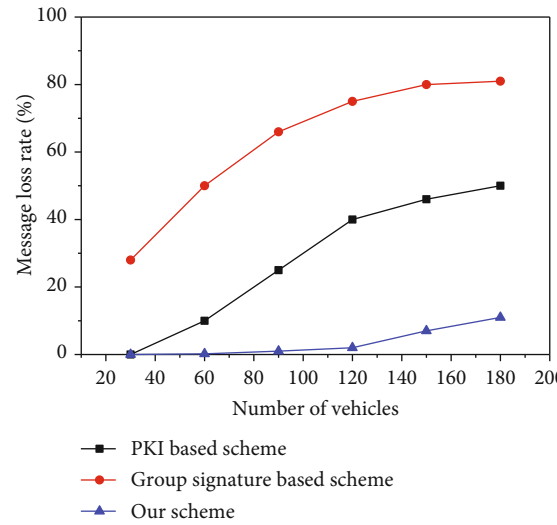

Figure 4: The relationship between the number of vehicles and the loss rate of messages.

The various parameters used in the experimental simulation platform are shown in Table 2. In the implementation of our protocol, the point multiplication operations of ECC are based on a 160-bit private key. And we select SHA-256 as the elementary hash function to structure the hash functions used in the proposed authentication protocol (i.e., $h(\cdot)$, $H(\cdot)$). We use the pairing-based cryptography library [37] for algorithm experimental verification. The computation overhead of the proposed authentication protocol consists of the vehicle authentication phase and the signature verification phase.

6.1. Computation Overhead Analysis. Table 3 illustrates the experimental results for related pairing-based operations on the Intel Core i7 CPU 2.6 GHz machine. In our simulation, each randomized ID is 1024 bits, and the size of the ECC point is 160 bits. From the results, we observe that the bilinear pairing operation takes 3.61 milliseconds at the application server when averaging over 10 experiments to run the pairing-based operation. Figure 4 further shows the results on Intel Core i7 CPU 2.6 GHz for the above metrics.

Table 4: Execution time of the proposed scheme in different phases.

Different phases	On the OBU side	On the RSU side
Vehicle authentication	$4T_h \approx 4$ ms	$T_{mul} + T_h \approx 2.63$ ms
Vehicle verification	$T_{mul} + T_h \approx 2.63$ ms	$2T_{mul} + 4T_h \approx 7.26$ ms
Message signing	$3T_{mul} + T_{add} + T_h + T_{Gh} \approx 7.89$ ms	—
Message verification	$3T_{pair} + T_{mul} + T_{Gh} + T_h \approx 14.46$ ms	—

Table 5: Comparisons between the related research and our protocol.

Protocols	Vehicle authentication phase	Message signing phase
Wang and Yao [20]	$T_{mul} + T_{en} + T_h \approx 3.63$ ms	$5T_{mul} + T_{add} + 2T_h \approx 11.15$ ms
Islam et al. [21]	$3T_{en} + T_{pair} + T_h \approx 7.61$ ms	$T_{mul} + 2T_{en} + 4T_h \approx 7.63$ ms
Ahamed et al. [29]	$3T_{mul} + 2T_{pair} + 2T_h \approx 10.85$ ms	$3T_{exp} + T_{mul} \approx 9.22$ ms
The proposed	$T_{mul} + T_h \approx 2.63$ ms	$3T_{mul} + T_{add} + T_h + T_{Gh} \approx 7.89$ ms

Table 6: Length of the elements used in our protocol.

Element	ID_{vj}	RID_i	Timestamp	Point of ECC	Pseudo-ID	Nonce	M_s (traffic message)
Length	17 bytes	20 bytes	8 bytes	40 bytes	72 bytes	8 bytes	200 bytes

Furthermore, if the proposed authentication protocol is implemented on a more powerful high-end server, the running time will be greatly reduced, as shown in Table 3.

The main computational cost involved in the proposed authentication protocol is the registration phase, vehicle authentication phase, and message verification phase. However, in the proposed authentication protocol, it is not required to register a large number of vehicles and RSUs at the same time. Therefore, the time consumed in this phase does not require counting in the real-time running process. We focus on the time-consuming vehicle authentication phase and message signing and verification phases. In Table 4, we illustrate the running time of the proposed authentication protocol in different phases.

On the TA side, it is only involved in the system initialization phase and the vehicle verification phase. Note that the system initialization phase can be computed offline, and thus, we omit the computational overhead of this phase. And the TA's computation cost in the vehicle verification phase is 3 $T_{mul} + 6T_h \approx 10.89$ ms. On the OBU side, it is involved in the vehicle authentication phase, vehicle verification phase, message signing phase, and message verification phase. On the RSU side, it is only involved in the following stages: vehicle authentication and vehicle verification. From the proposed authentication, it is easy to find that the OBU is involved in almost all phases, except the identity tracking and revocation phase. Table 4 gives the detailed numbers.

From Table 4, we can see that if there are many message signatures for the OBU to verify, it will take a long time to run the message verification phase. To speed up the verification process, the proposed authentication protocol uses the batch authentication manner (see equation (12)) to reduce the time of pairing computation. We can analyze that the computation overhead in the single authentication manner is $(n+1)T_{mul} + nT_{Gh} + 3nT_{pair}$ from equation (10). And the computation overhead in the batch authentication manner is only $(n+1)T_{mul} + nT_{Gh} + 3T_{pair}$ from equation (12). As a result, we can reduce the number of pairing computation from $3n$ to only 3. In Table 5, we have compared the computational cost of the proposed authentication protocol with the related works for each step.

6.2. Communication Overhead Analysis. We assume that the vehicles and RSUs have the same communication speed. Then, the communication overhead can be estimated by the length of messages. In our implementation, we adopt SHA-256 as the elementary hash function to structure the hash function, whose output length is 32 bytes. We use the vehicle identification number (VIN) [38] proposed by the International Organization for Standardization as the identifier of the vehicle. In Table 6, we illustrate the default length of the elements used in the proposed authentication protocol.

In the vehicle authentication phase, the communication overhead is mainly caused by the authentication request message $\{TID_{vj}, r_{vj}, T_{vj}, upuk_j, Cert_{vj}\}$. Just as summarized in the previous part, the sizes of TID_{vj} and $Cert_{vj}$ are 32 bytes. And the sizes of r_{vj}, T_{vj}, and $upuk_j$ are 8 bytes, 8 bytes, and 40 bytes, respectively. Therefore, the size of the authentication message is $32 + 32 + 8 + 8 + 40 = 120$ bytes. Similarly, the size of the safety-related message $\{pID_j, \theta_j, M_s, RID_i\}$ is $40 + 40 + 200 + 20 = 300$ bytes. From Table 7, the communication cost of our protocol is slightly higher than that of the protocols in [25]. However, the proposed protocol provides more security of the vehicle authentication than the related research.

Table 7: Communication cost comparisons between the related research and our protocol.

Protocols	Vehicle authentication	Message authentication
Wang and Yao [20]	181 bytes	352 bytes
Islam et al. [21]	324 bytes	388 bytes
Ahamed et al. [29]	108 bytes	288 bytes
The proposed	120 bytes	300 bytes

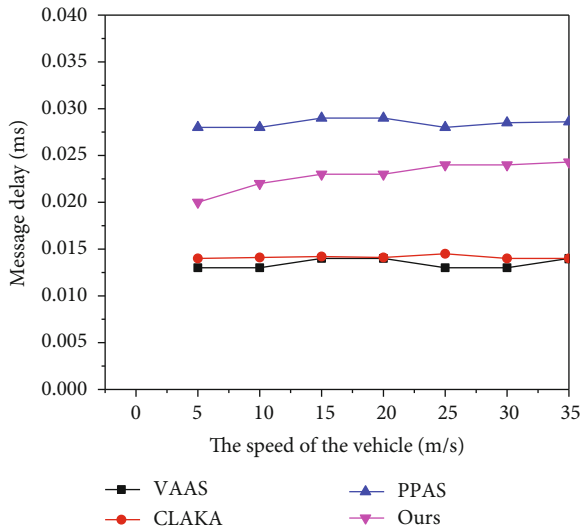

Figure 5: The relationship between the speed of vehicles and the delay of messages.

6.3. Authentication Message Loss Rate Analysis. The message loss rate (MLR) is defined by formula (14), where N is used to represent the total number of authentication messages, M^i_{rev} represents the total number of messages received by vehicle V_i, and M^i_{send} represents the total number of authentication messages sent by the RSU.

$$\text{MLR} = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{M^i_{\text{rev}}}{M^i_{\text{send}}}\right). \tag{14}$$

Figure 4 shows the relationship between the message loss rate and the number of vehicles in the system. It can be seen from the simulation results that as the volume of message authentication services increases, the message loss rate is gradually increasing. In addition, in the same environment, we also compare the proposed protocol with the PKI-based protocol and that in [23] in terms of the message loss rate. It can be found that the message loss rate of the authentication protocol proposed in this paper is the lowest.

6.4. Authentication Protocol's Delay Factor Analysis. In the simulation environment, we obtained the relationship between different factors and the delay of the authentication protocol by modifying the relevant parameters, such as the speed of the vehicle and the number of vehicles. Figure 5 reflects the relationship between vehicle speed and message delay, and Figure 6 reflects the relationship between the number of vehicles and the delay of authentication messages.

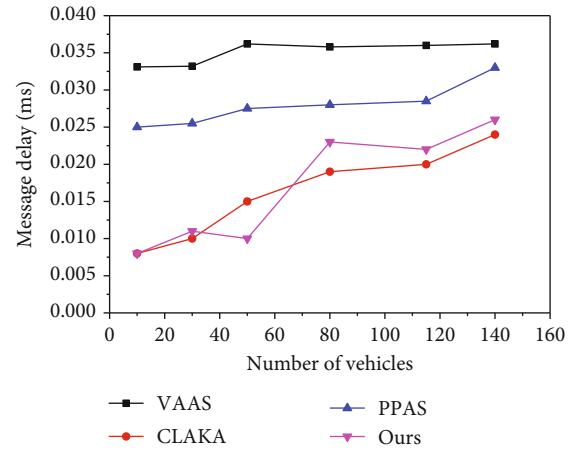

Figure 6: The relationship between the number of vehicles and the delay of messages.

It can be seen from Figure 5 that when the speed is lower than 35 m/s (126 km/h), the increase in vehicle speed does not have much impact on the message delay of the authentication protocol. This shows that the proposed protocol can meet the demand for message delay under the condition of normal vehicle speed. From Figure 6, it is easy to see that when the proposed is used for high traffic density occasions, the authentication message delay time will increase a bit. However, when the number of vehicles in the area covered by an RSU is less than 80, the delay is still relatively small. In fact, the probability that the number of vehicles in the area covered by an RSU exceeds 80 is negligible. Obviously, the message delay of the proposed protocol is very small in the daily traffic environment.

7. Conclusion

In the future smart transportation system, VANET will play an increasingly important role. The communication security and vehicle privacy protection in VANET are the fundamental requirements for its rapid development. In this paper, we proposed a bilinear pairing-based vehicle authentication and the message verification protocol to solve these problems. To protect user privacy, the proposed protocol uses a temporary pseudoidentity-based anonymous method in the message signing and verification phases. In addition, to improve the efficiency of the proposed authentication protocol, the recipients can verify the traffic-related messages with the single or batch authentication manner. Finally, we give the security and performance analysis of the proposed protocol. The security analysis shows that the proposed authentication protocol can resist various security threats and protect user privacy in the VANET environment. The performance analysis results show that the proposed scheme has lower communication overhead and computational cost when compared with the related protocol. Therefore, the proposed authentication protocol is very suitable for the VANET environment.

Data Availability

Data is available from http://crypto.stanford.edu/pbc/.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Grant nos. 61772477 and U1804263) and the Key Scientific Research Project of Colleges and Universities in Henan Province (no. 21A520048).

References

[1] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *2008 Proceedings IEEE INFOCOM - The 27th Conference on Computer Communications*, pp. 1903–1911, Phoenix, AZ, USA, April 2008.

[2] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.

[3] R. Hajlaoui, H. Guyennet, and T. Moulahi, "A survey on heuristic-based routing methods in vehicular ad-hoc network: technical challenges and future trends," *IEEE Sensors Journal*, vol. 16, no. 17, pp. 6782–6792, 2016.

[4] P. Vijayakumar, V. Chang, L. Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, pp. 943–955, 2018.

[5] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 1, pp. 1654–1667, 2020.

[6] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[7] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[8] J. Kang, D. Lin, W. Jiang, and E. Bertino, "Highly efficient randomized authentication in VANETs," *Pervasive and Mobile Computing*, vol. 44, pp. 31–44, 2018.

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

[10] Y. Sun, R. Lu, X. Lin, X. (. S.). Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[11] A.-N. Shen, S. Guo, D. Zeng, and M. Guizani, "A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2543–2548, Paris, France, April 2012.

[12] J. Li, H. Lu, and M. Guizani, "ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[13] 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 & Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[14] Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, "Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs," *International Journal of Network Security*, vol. 18, no. 2, pp. 374–382, 2016.

[15] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, pp. 1–5, New Orleans, LA, USA, November-December 2008.

[16] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2014.

[17] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[18] C. Giorgio, P. Panos, J. B. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks - VANET '07*, pp. 19–28, Montréal, Québec, Canada, 2007.

[19] H. Liu, H. Li, and Z. Ma, "Efficient and secure authentication protocol for VANET," in *2010 International Conference on Computational Intelligence and Security*, pp. 523–527, Nanning, China, December 2010.

[20] S. Wang and N. Yao, "LIAP: a local identity-based anonymous message authentication protocol in VANETs," *Computer Communications*, vol. 112, pp. 154–164, 2017.

[21] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[22] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pp. 246–250, Phoenix, AZ, USA, April 2008.

[23] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Computer Networks*, vol. 177, Article ID 107333, 2020.

[24] S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, 2015.

[25] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular

ad hoc networks," *Cluster Computer*, vol. 20, no. 3, pp. 2439–2450, 2017.

[26] S. 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.

[27] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[28] V. Kanimozhi and S. Karthik, "A survey on multi-constrained optimal path selection schemes and authentication schemes for VANET," in *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, January 2017.

[29] A. B. Shakeel Ahamed, N. Kanagaraj, and M. Azees, "EMBA: an efficient anonymous mutual and batch authentication schemes for VANETs," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 1320–1326, Coimbatore, India, April 2018.

[30] D. Tiwari, M. Bhushan, A. Yadav, and S. Jain, "A novel secure authentication scheme for VANETs," in *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*, pp. 287–297, Ghaziabad, India, February 2016.

[31] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced Security Identity-Based Privacy-Preserving Authentication Scheme Supporting Revocation for VANETs," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5373–5383, 2020.

[32] A. Meddeb-Makhlouf, N. Meddeb, and M. A. B. Ayed, "An enhanced multilevel authentication protocol for VANETs," in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1232–1238, Hammamet, Tunisia, October 2017.

[33] 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.

[34] J. Zhang, J. Ma, and W. Wang, "A secure and efficient remote user authentication scheme for multi-server environments using ECC," *KSII Transactions on Internet & Information Systems*, vol. 8, no. 8, pp. 2930–2947, 2014.

[35] H. Debiao, C. Jianhua, and H. Jin, "An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security," *Information Fusion*, vol. 13, no. 3, pp. 223–230, 2012.

[36] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, New York, NY, USA, 2004.

[37] B. Lynn, "The pairing-based cryptography library," http://crypto.stanford.edu/pbc/.

[38] "Road vehicles—vehicle identification number (VIN)—content and structure, document ISO 3779," 2009, https://www.iso.org/standard/9305.html.