Hindawi
Security and Communication Networks
Volume 2021, Article ID 6698099, 12 pages
https://doi.org/10.1155/2021/6698099

Research Article

An Improved and Privacy-Preserving Mutual Authentication Scheme with Forward Secrecy in VANETs

Mengting Yao, Xiaoming Wang, Qingqing Gan, Yijian Lin, and Chengpeng Huang

Department of Computer Science, Jinan University, Guangzhou 510632, China

Correspondence should be addressed to Xiaoming Wang; twxm@jnu.edu.cn

Received 12 December 2020; Revised 20 March 2021; Accepted 2 April 2021; Published 21 April 2021

Academic Editor: Stelvio Cimato

Vehicular ad hoc network (VANETs) plays a major part in intelligent transportation to enhance traffic efficiency and safety. Security and privacy are the essential matters needed to be tackled due to the open communication channel. Most of the existing schemes only provide message authentication without identity authentication, especially the inability to support forward secrecy which is a major security goal of authentication schemes. In this article, we propose a privacy-preserving mutual authentication scheme with batch verification for VANETs which support both message authentication and identity authentication. More importantly, the proposed scheme achieves forward secrecy, which means the exposure of the shared key will not compromise the previous interaction. The security proof shows that our scheme can withstand various known security attacks, such as the impersonation attack and forgery attack. The experiment analysis results based on communication and computation cost demonstrate that our scheme is more efficient compared with the related schemes.

1. Introduction

With the rapid development of wireless communication technology, VANETs has drawn widespread attention in society over the decades. VANETs will bring great benefits to people in many ways. It can not only help drivers obtain traffic information in advance and provide better routes to ensure traffic safety and reduce traffic burden but also supply other services, such as toll collection and car infotainment and location-based services [1].

In spite of the huge advantages offered by VANETs, it is still confronted with some problems that need to be solved such as privacy preserving and secure authentication since the communication in VANETs is on an open channel. Numerous schemes [2–5] have provided message authentication. The receiver must first verify the legality and integrity of the messages broadcast by other vehicles before it trusts them. However, in these schemes, the identity of the vehicle is not authenticated before it communicates with others. So, any vehicle can join the communication range and broadcast messages to others. If there are numerous vicious vehicles in communication area, a lot of false information will be generated and broadcast in the Internet of vehicle system, which has an adverse impact on the efficiency of the entire system. Therefore, the identity authentication before communication is also essential for VANETs.

Recently, Cui et al. [6] proposed a mutual authentication scheme for VANETs. In their scheme, the mutual authentication process between the vehicle and TA needs to be executed before the vehicle can communicate with other vehicles and RSUs. However, we find their scheme actually has some security defects. It is vulnerable to forgery attack and impersonation attack and does not provide forward secrecy which is an important security property of authentication scheme. In addition, their scheme cannot meet batch verification. Batch verification allows the verifier to check the validity of many signatures at the same time, which can greatly reduce delay. Many schemes [7–10] with batch verification have been proposed using bilinear pairing or based on elliptic curve.

In this paper, we present an improved mutual authentication scheme with forward secrecy for VANETs in order

to withstand various known attacks. Concretely, the main contributions of our scheme are given as follows:

(1) We identify and analyze security flaws in Cui et al.'s scheme for VANETs. Their scheme exits forgery attack and impersonation attack.

(2) We propose an improved mutual authentication scheme for VANETs to resist the security attacks in Cui et al.'s scheme. Our solution provides not only message authentication but also identity authentication. Moreover, our scheme can also achieve batch verification without using bilinear pairing.

(3) Finally, the proposed scheme can provide stronger security property, forward secrecy. That is to say, even if the current shared key is exposed, the adversary cannot construct the previous shared key. The security proof and analysis indicate that our scheme is secure. Performance evaluation shows that our scheme has low computation and communication overhead.

The rest of the paper is organized as follows. The related work is introduced in Section 2. Section 3 presents the system model, security assumptions, and security requirements. In Section 4, we briefly review the scheme of Cui et al. In Section 5, we analyze the security attacks of their scheme. Section 6 introduces the improved mutual authentication scheme with forward secrecy. In Section 7, we give the security proof and analysis. Section 8 presents the performance analysis. Finally, Section 9 shows the conclusion of this paper.

2. Related Work

In recent years, the issues of privacy protection and secure authentication for VANETs have drawn more and more attention. To settle the problems mentioned above, many signature and authentication schemes have been proposed. For example, in 2006, a ring signature scheme was first proposed by Gamage et al. [11] to conceal the signer's real identity. However, their scheme is not suitable for VANETs because no entity could trace the real identities of vehicles when false messages are sent by malicious vehicles caused damage. A year later, a PKI-based authentication scheme using anonymous certificates was proposed in [12]. However, in this scheme, vehicles need to store many public-private keys and corresponding anonymous certificates, which would impose storage burden to vehicles and huge certification management burden to TA. Later, Lin et al. [13] introduced a privacy-preserving authentication protocol based on a group signature [14]. Then, an efficient conditional privacy-preserving authentication (CPPA) scheme using bilinear pairing was proposed in [15]. In this scheme, the RSU needs to update the temporary anonymous certificates periodically and stores them, which would cause huge burden for the RSU and have low efficiency.

In order to mitigate the certificate management problem, many identity-based schemes were proposed such as [16–21]. Zhang et al. [16] introduced an identity-based solution with batch verification called IBV. In their paper, the signature key of the vehicle is generated based on its identity. Both vehicles and RSUs do not need to save any certificate. In addition, their solution can simultaneously verify many received messages, which greatly increases the efficiency of verification. Then, the flaws of Zhang et al.'s IBV scheme [16] were found by Lee and Lai [17]. First of all, Zhang et al.'s scheme is subject to the replaying attack. Secondly, the signature nonrepudiation is not achieved in Zhang et al.'s BIV scheme. So, Lee and Lai proposed an improved scheme to resist the above two types of attacks without extra overhead. Unfortunately, Zeng et al. [18] showed Lee and Lai's scheme [17] exits some weakness in VANETs. Firstly, Lee and Lai's approach did not achieve privacy preserving because anyone who only knows the public system parameters can calculate the real identity of the sender. Secondly, a malicious vehicle can imitate a valid vehicle to send false messages and even can use an arbitrary identity to escape the TA tracking. For the above weakness in VANETs, Zeng et al. [18] proposed an improved IBV scheme.

Soon after, many scholars combined certificateless cryptography and aggregation signature and further constructed various certificateless aggregation signature (CLAS) schemes [22–30]. For example, a CLAS scheme was proposed by Xiong et al. [22]; however, He et al. [23] pointed out that the adversary could forge a legal signature of any message in their scheme and presented an improved CLAS scheme. Unluckily, a security drawback in He et al.'s scheme [23] was found by Li et al. [24]. Xu et al. [30] found that the scheme of Horng et al. [25] cannot resist any type of adversary in the certificateless security model and built a new CLAS scheme. Lately, Cui et al. [26] presented an efficient CLS scheme for VANETs, which was proved to be insecure by Kamil and Ogundoyin [27].

To improve the efficiency, some schemes [31–34] have been designed shortly after. For example, in 2015, a new ID-based CPPA scheme for VANETs was firstly introduced by He et al. [31] based on Elliptic Curve Cryptography (ECC) without bilinear pairing. Cui et al. [35] built a secure privacy-preserving authentication (SPACF) scheme for VANETs using cuckoo filter and binary search methods to enhance the efficiency of batch verification. Azees et al. [36] constructed an efficient anonymous authentication (EAAP) protocol with an efficient conditional privacy tracking mechanism for VANETs. Nevertheless, they did not provide batch signatures verification. Soon after, Zhong et al. [37] proposed a privacy-preserving authentication scheme with full aggregation. In their scheme, the RSU could aggregate the signatures of vehicles which are passing through it. However, this scheme has low efficiency due to the use of map-to-point hash functions and bilinear pairing. Later, Ali and Li [38] introduced an efficient CPPA scheme for VANETs based on general one-way hash functions with lower computation overhead. A conditional privacy-preserving authentication protocol based on Chinese remainder theorem (CRT) for VANETs was elaborated by Zhang et al. [39]. In their protocol, they eliminated the need for preloading the master key of the system into Tamper-Proof

Device (TPD) of vehicle, thus avoiding the risk of compromising a vehicle's TPD leading to entire system failure.

Some mutual authentication schemes [40–42] in other different scenarios have been proposed. Recently, Cui et al. [6] introduced a secure mutual authentication for VANETs. However, we find their scheme exits some security weaknesses, such as forgery attack and impersonation attack. In this paper, we introduce an improved mutual authentication scheme with forward secrecy. Meanwhile, we provide batch verification, which greatly increases the efficiency of verification.

3. Preliminaries

In this part, the system model and security requirements will be given.

3.1. System Model. As shown in Figure 1, a typical architecture of VANETs is made up of the following units:

(1) Trusted authority (TA): TA is a trusted third party with large storage capacity and powerful computing capabilities. It is in charge of generating system parameters and authenticating the identity of vehicles. Furthermore, the true identities of vehicles could only be revealed by TA.

(2) Road side unit (RSU): RSU is the roadside infrastructure unit and not fully trusted. It can serve as a bridge between TA and the vehicle communication. And, it can also monitor suspicious message signatures broadcast by vehicles.

(3) Vehicles: each vehicle communicates with other vehicles or RSUs by an open dedicated shortrange communication (DSRC) protocol [43].

3.2. Security Assumptions. The security of our scheme is based on the elliptic curve discrete logarithm (ECDL) problem and the computational Diffie–Hellman (CDH) problem.

(1) ECDL problem: the ECDL problem is to calculate s, where s satisfies the known point $Q = s \cdot P$ on the curve

(2) CDH problem: the CDH problem is to obtain the point $\alpha \cdot \beta \cdot P \in G$ given two random points $\alpha \cdot P$, $\beta \cdot P \in G$, where α and β are secret

3.3. Security Requirements. On the basis of the previous works for VANETs, the following secure requirements should be met in the proposed scheme:

(1) Message authentication: the receiver must check the integrity and validity of the message signatures sent by other vehicles before it trusts them

(2) Identity authentication: the vehicle needs to complete identity authentication to prove it is legal before allowing it to communicate with other RSUs and vehicles

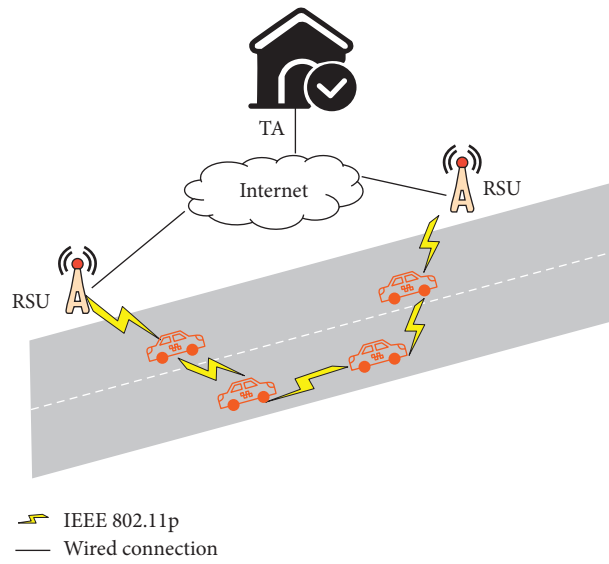

Figure 1: System model.

(3) Traceability: if a malicious vehicle transmits a false message to mislead others, the true identity of it could be traced by TA

(4) Forward secrecy: even if the adversary knows the current shared key, it is impossible to generate the pervious shared key

(5) Resistance against numerous types of attacks: the proposed scheme should be capable of withstanding the following security attacks that exist in VANETs

(1) Replay attack: an adversary may gather and save a message signature and try to send it after the primitive signature becomes invalid

(2) Impersonate attack: a malicious vehicle could diffuse a legal vehicle to send fake messages in order to make profits.

(3) Forgery attack: an adversary could forge some secret information such as identity or authentication credential to generate a signature without being detected

(4) Known key secrecy attack: an adversary could construct the current key if it obtains the key generated in the previous interaction

4. Review of Cui et al.'s Mutual Authentication Scheme

Recently, Cui et al. [6] proposed a secure mutual authentication scheme for VANETs. In this section, we briefly review their scheme.

4.1. TA Initialization Phase

Step 1: TA picks two large prime numbers p, q, an additive group G with order q, which is formed by points on the elliptic curve E ($y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$). P is a generator of G.

Step 2: TA randomly picks a number $s \in Z_q^*$ as its secret key and calculates $P_{\text{pub}} = s \cdot P$ as its public key.

Step 3: TA selects symmetric encryption function $E_\pi(\cdot)/D_\pi(.)$ and several hash functions: h: $G \longrightarrow Z_q$, $H_{1\,\text{key}}(\cdot)$: $\{0,1\}^* \longrightarrow \{0,1\}^l$, $H_2(\cdot)$: $\{0,1\}^* \longrightarrow \{0,1\}^l$, $H_3(\cdot)$: $\{0,1\}^* \longrightarrow \Gamma$, where $H_{1\,\text{key}}$ is a hash with key.

Step 4: finally, TA publishes $\psi = \{a, b, q, p, P, h, H_{1\,\text{key}}(\cdot), H_2(\cdot), H_3(\cdot)\}$ as public system parameters.

4.2. Vehicle Setup Phase. The vehicle V_i first transmits real identity RID to TA. Then, TA calculates interpseudonym identity $\text{IPID}_{V_i} = H_1(\text{RID}\|\text{VP}_i)$, where VP_i is the valid period. Then, TA sends IPID_{V_i} to V_i by a secure channel. Finally, V_i randomly picks an integer $\lambda_i \in Z_q^*$ as the encryption key and stores λ_i and IPID_{V_i} into the TPD. Simultaneously, TA saves the tuple (RID, VP_i, IPID_{V_i}, λ_i).

4.3. Mutual Authentication Phase. The mutual authentication process is completed between TA and the vehicle V_i. The details are as follows:

Step 1: firstly, V_i picks a random integer $N_v \in Z_q^*$ and calculates a hash code $\text{HC} = h(\lambda_i\|N_v)$. Then, it encrypts N_v, HC, and IPID_{V_i} using the shared key λ_i. Next, V_i sends the messages $(E_{\lambda_i}(N_v\|\text{HC}\|\text{IPID}_{V_i})\|\text{ID}_{\text{TA}}\|\text{IPID}_{V_i}\|T_1)$ to nearby RSU, where ID_{TA} is the identity of TA, and T_1 is the current timestamp.

Step 2: when RSU obtains a message from V_i, it first inspects the validity of the timestamp. If the timestamp is expired, it fails. Otherwise, RSU attaches its identity ID_{RSU} and a new timestamp T_2 to the message. Then, it uses its private key rsk shared with TA to encrypt messages. Finally, it broadcasts the encrypted messages $\{E_{\text{rsk}}(E_{\lambda_i}(N_v\|\text{HC}\|\text{IPID}_{V_i})\|\text{ID}_{\text{TA}}\|IPID_{V_i}\|\text{ID}_{\text{RSU}}\|T_2)\}$ to TA. When TA receives the messages, it first decrypts to get the tuple $\{E_{\lambda_i}(N_v\|\text{HC}\|\text{IPID}_{V_i})\|\text{ID}_{\text{TA}}\|\text{IPID}_{V_i}\|\text{ID}_{\text{RSU}}\|T_2\}$. Next, it continues to decrypt $E_{\lambda_i}(N_v\|\text{HC}\|\text{IPID}_{V_i})$ to get HC and N_v. Then, it computes $\text{HC}' = h(\lambda_i\|N_v)$. If $\text{HC}' = \text{HC}$, it continues to execute the next step; else it aborts.

Step 3: TA calculates the authentication code $\text{AC} = h(\text{HC}\|s)$. Then, it sends the encrypted messages $E_{\text{rsk}}(E_{\lambda_i}(E_s(\text{IPID}_{V_i}\|T_3\|\text{Lifetime}\|\text{AC}))\|\text{ID}_{\text{TA}})$ to the nearby RSU, where Lifetime is the valid period of AC.

Step 4: as the RSU receives the messages sent by TA, it decrypts the messages to get $\{E_{\lambda_i}(E_s(\text{IPID}_{Vi}\|T_3\|\text{Lifetime}\|\text{AC}))\|\text{ID}_{\text{TA}}\}$. Then, RSU authenticates ID_{TA} if ID_{TA} is invalid, it fails; else it sends $E_{\lambda_i}(E_s(\text{IPID}_{V_i}\|T_3\|\text{Lifetime}\|\text{AC}))$ to V_i. After V_i receives the messages, it first uses λ_i to decrypt them and then uses the system public key P_{pub} to decrypt $E_s(\text{IPID}_{V_i}\|T_3\|\text{Lifetime}\|\text{AC})$ to get IPID_{V_i}. If it is equal to the IPID_{V_i} stored in the TPD, the vehicle V_i successfully completes the mutual authentication with TA and is allowed to broadcast messages to other vehicles and RSU.

4.4. Vehicle Signature Phase. In this part, V_i randomly chooses a number $r_i \in Z_q^*$ and computes $R_i = r_i \cdot P$. Next, V_i calculates its public pseudonym identity $\text{PPID}_{V_i} = H_2(\text{IPID}_{V_i}\|R_i\|T_i)$. Then, it generates the signature $\delta_i = h(\text{PPID}_{V_i}\|M_i\|\text{AC}\|R_i)$ and broadcasts the messages $\{M_i, \delta_i, \text{PPID}_{V_i}, \text{AC}, R_i\}$ to other RSUs and vehicles.

4.5. Message Verification Phase. As RSU obtains the messages $\{M_i, \delta_i, \text{PPID}_{V_i}, \text{AC}, R_i\}$ from V_i, it calculates $\delta_i^* = h(\text{PPID}_{V_i}\|M_i\|\text{AC}\|R_i)$. If $\delta_i^* = \delta_i$, the message M_i is considered valid; otherwise, the verifier directly discards the messages.

5. Attacks on Cui et al.'s Mutual Authentication Scheme

In this section, we describe some attacks existing in the scheme of Cui et al. [6]. The details are as follows.

5.1. Forgery Attack. According to our analysis, Cui et al.'s scheme exits forgery attack in VANETs. We consider a case in which an attacker forges the authentication code. Then, it can use the authentication code to generate a message signature and the signature can be successfully verified. The details are described as follows.

Suppose an attacker forges an arbitrary authentication code AC^*. Then, it selects a random integer $r_i \in Z_q^*$, computes $R_i = r_i \cdot P$, and generates a signature of false message M_i^* as the following equation:

$$\delta_i^* = h\left(\text{PPID}_{V_i}\|M_i^*\|\text{AC}^*\|R_i\right). \tag{1}$$

Finally, it sends the messages $\{M_i^*, \delta_i^*, \text{PPID}_{V_i}, \text{AC}^*, R_i\}$ to other vehicles and RSUs.

After RSU receives the messages $\{M_i^*, \delta_i^*, \text{PPID}_{V_i}, \text{AC}^*, R_i\}$, it will check that the following equation is satisfied; hence, the message M_i^* will be considered valid:

$$\delta_i^* = h\left(\text{PPID}_{V_i}\|M_i^*\|\text{AC}^*\|R_i\right). \tag{2}$$

From the above, we notice that a vehicle without executing the mutual authentication process can forge the authentication code and uses it as a credential to successfully communicate with others. Essentially, this is because RSU can only verify whether AC sent by V_i has been tampered with the public channel, but cannot verify AC which is distributed by TA.

5.2. Impersonation Attack. We find the scheme of Cui et al. cannot withstand the impersonation attack in VANETs. A malicious vehicle could imitate other valid vehicles to broadcast messages. The details of impersonation attack are as follows.

Suppose an attacker intercepts the authentication code AC and the pseudonym identity PPID_{V_i} on the open channel, and it executes the following steps:

(1) First, it randomly selects an integer $r_i \in Z_q^*$ and calculates $R_i = r_i \cdot P$.

(2) Next, it uses the intercepted AC and PPID_{V_i} to generate the signature of an arbitrary message M_i^* as $\delta_i^* = h(\mathrm{PPID}_{V_i} \| M_i^* \| \mathrm{AC} \| R_i)$. Subsequently, it broadcasts the messages $\{M_i^*, \delta_i^*, \mathrm{PPID}_{V_i}, \mathrm{AC}, R_i\}$ to nearby vehicles and RSUs.

When the verifier receives the messages $\{M_i^*, \delta_i^*, \mathrm{PPID}_{V_i}, \mathrm{AC}, R_i\}$, it will consider the messages to be valid by checking that the following equation holds

$$\delta_i^* = h\left(\mathrm{PPID}_{V_i} \| M_i^* \| \mathrm{AC} \| R_i\right). \tag{3}$$

As a result, when the message M_i^* caused an accident, the TA needs to obtain the true identity of the sender from PPID_{V_i} in order to trace responsibility. However, the TA will obtain the real identity IPID_{V_i} and think the message M_i^* is sent by V_i. Thus, the attacker is able to imitate any vehicle to generate valid signatures of fake messages and escape accountability. Therefore, Cui et al.'s scheme is prone to impersonation attack.

6. The Proposed Scheme

To overcome the security attacks in Cui et al.'s scheme [6], we construct an improved mutual authentication scheme with forward secrecy. Table 1 displays the notations and descriptions used in the proposed scheme.

6.1. System Initialization.

Step 1: TA picks two large prime numbers p, q and an additive group G with order q formed by points on the elliptic curve E $(y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p)$. Then, TA picks P as a generator of G.

Step 2: TA randomly selects a number $s_T \in Z_q^*$ as its secret key and calculates $P_{\mathrm{pub}} = s_T \cdot P$ as the corresponding public key.

Step 3: TA chooses some hash functions: $H_0(\cdot)$: $G \longrightarrow Z_q^*$, $H_1(\cdot)$: $G \times G \longrightarrow Z_q^*$, $H_2(\cdot)$: $G \times G \times \{0,1\}^* \longrightarrow Z_q^*$, $H_3(\cdot)$: $G \times G \times G \times Z_q^* \longrightarrow Z_q^*$, and $H_4(\cdot)$: $\{0,1\}^* \longrightarrow Z_q^*$. The system parameters $\psi = \{a, b, q, p, P, E, G, H_0, H_1(\cdot), H_2(\cdot), H_3(\cdot), H_4(\cdot), P_{\mathrm{pub}}\}$ are published.

6.2. Vehicle Registration. In this section, the vehicle V_i registers with the TA to get the shared key λ_i, and the process is given as follows.

The vehicle randomly picks an integer $s_i \in Z_q^*$ as its secret key and computes $\mathrm{PID}_{i,1} = s_i \cdot P$. Subsequently, it transmits the real identity RID and $\mathrm{PID}_{i,1}$ to TA via a secure channel. When receiving the information, TA randomly picks an integer $\lambda_i \in Z_q^*$ as the key shared with the vehicle V_i, and calculates $\mathrm{PID}_{i,2} = \mathrm{RID} \oplus H_0(s_T \cdot \mathrm{PID}_{i,1} \| \mathrm{VP}_i)$, where VP_i is the valid period of $\mathrm{PID}_{i,1}$ and $\mathrm{PID}_{i,2}$. Next, TA sends the shared key λ_i and pseudonym identity $\mathrm{PID}_i = \{\mathrm{PID}_{i,1}, \mathrm{PID}_{i,2}, \mathrm{VP}_i\}$ to V_i. Meanwhile, TA saves the tuple $(\mathrm{RID}, \mathrm{VP}_i, \lambda_i)$.

Table 1: Notations and descriptions in our scheme.

Notations	Descriptions
TA	A trusted authority
V_i	The ith vehicle
G	Cycle addition group based on ecliptic curve
P	A generator of G
s_T	The private key of TA
s_i	The private key of V_i
P_{pub}	The public key of TA
λ_i	The shared key between V_i and TA
rsk	The shared key between RSU and TA
PID_i	The pseudonym identity of V_i
RID	The real identity of vehicle
SK_i	The signature key of V_i

6.3. Mutual Authentication and Signing Key Generation. As shown in Table 2, the vehicle V_i completes the mutual authentication process with TA by the help of RSU. After mutual authentication, V_i is considered legal and generates the signing key SK_i.

Step 1: the vehicle V_i first randomly selects numbers $N_v, \alpha \in Z_q^*$ and computes $\eta_1 = H_2(\mathrm{PID}_i \| \lambda_i \| N_v \| \alpha \cdot P)$. Then, it sends the messages $\Phi_1 = \{\eta_1, \mathrm{PID}_i, N_v, \alpha \cdot P, T_1\}$ to nearby RSU, where T_1 is the current timestamp.

Step 2: after getting the messages Φ_1, RSU first checks the validity of T_1. If T_1 is invalid, it ends; otherwise, it chooses a random number $N_r \in Z_q^*$ and calculates $\eta_2 = H_4(\mathrm{ID}_{\mathrm{RSU}} \| \mathrm{rsk} \| N_r)$, where $\mathrm{ID}_{\mathrm{RSU}}$ is the identity of RSU and rsk is only known to TA and RSU. Finally, RSU sends the messages $\Phi_2 = \{\eta_1, \mathrm{PID}_i, N_v, \alpha \cdot P, \eta_2, \mathrm{ID}_{\mathrm{RSU}}, N_r, T_2\}$ to TA, where T_2 is current timestamp.

Step 3: when TA receives the messages Φ_2, it first inspects the expiration date of T_2. If T_2 is expired, it aborts; else it checks the identity of the RSU. It computes $\eta_2^* = H_4(\mathrm{ID}_{\mathrm{RSU}} \| \mathrm{rsk} \| N_r)$; if $\eta_2^* \neq \eta_2$, it aborts; else, it continues to authenticate V_i. TA computes $\eta_1^* = H_2(\mathrm{PID}_i \| \lambda_i \| N_v \| \alpha \cdot P)$; if $\eta_1^* \neq \eta_1$, it ends; otherwise, V_i is successfully authenticated by TA. Then, TA randomly selects numbers $\beta, \omega_i \in Z_q^*$ and computes $W_i = \omega_i \cdot P$, $X_i = H_1(\mathrm{PID}_i \| W_i)$, $S_i' = \omega_i + s_T \cdot X_i$, $Q = H_3(\lambda_i \| \mathrm{PID}_i \| N_v \| S_i' \| \beta \cdot P \| W_i)$, $\eta_3 = H_4(\mathrm{rsk} \| N_r)$, and $\eta_4 = S_i' \oplus \beta \cdot \alpha \cdot P$. Finally, TA sends the messages $\Phi_3 = \{\eta_3, \eta_4, Q, \beta \cdot P, W_i, T_3\}$ to nearby RSU, where T_3 is current timestamp. At the same time, TA updates the shared key λ_i^* as $H_0(\beta \cdot \alpha \cdot P)$.

Step 4: upon getting the message Φ_3, RSU first checks the freshness of T_3 and then calculates $\eta_3^* = H_4(\mathrm{rsk} \| N_r)$. If $\eta_3^* = \eta_3$, it forwards the messages $\Phi_4 = \{\eta_4, Q, \beta \cdot P, W_i, T_4\}$ to the vehicle V_i, otherwise it aborts.

Table 2: Mutual authentication phase between TA and the vehicle.

V_i	RSU	TA
Selects $N_v, \alpha \in Z_q^*$ Computes $\eta_1 = H_2(\mathrm{PID}_i \Vert \lambda_i \Vert N_v \Vert \alpha \cdot P)$ $\Phi_1 = \{\eta_1, \mathrm{PID}_i, \alpha \cdot P, T_1\}$ $\longrightarrow$		
	Verifies $T_1^* - T_1 \le \Delta T$ Selects $N_r \in Z_q^*$, Computes $\eta_2 = H_4(\mathrm{ID}_{\mathrm{RSU}} \Vert \mathrm{rsk} \Vert N_v)$ $\Phi_2 = \{\Phi_1, \eta_2, \mathrm{ID}_{\mathrm{RSU}}, T_2\}$ $\longrightarrow$	
		First verifies $T_2^* - T_2 \le \Delta T$ Computes $\eta_2^* = H_4(\mathrm{ID}_{\mathrm{RSU}} \Vert \mathrm{rsk} \Vert N_r)$, Checks $\eta_2^* \stackrel{?}{=} \eta_2$ Computes $\eta_1^* = H_2(\mathrm{PID}_i \Vert \lambda_i \Vert N_v \Vert \alpha \cdot P)$, Checks $\eta_1^* \stackrel{?}{=} \eta_1$ Selects $\beta, \omega_i \in Z_q^*$ Computes $W_i = \omega_i \cdot P$ Computes $X_i = H_1(\mathrm{PID}_i \Vert W_i), Si' = \omega_i + s_T \cdot X_i$ Computes $Q = H_3(\lambda_i \Vert \mathrm{PID}_i \Vert N_v \Vert S_i' \Vert \beta \cdot P \Vert W_i)$ Computes $\eta_3 = H_4(\mathrm{rsk} \Vert N_r)$ Computes $\eta_4 = S_i' \oplus \beta \cdot \alpha \cdot P$ Updates $\lambda_i^* = H_0(\beta \cdot \alpha \cdot P)$ $\Phi_3 = (\eta_3, \eta_4, Q, \beta \cdot P, W_i, T_3)$ $\longleftarrow$
	Verifies $T_3^* - T_3 \le \Delta T$ Computes $\eta_3^* = H_4(\mathrm{rsk} \Vert N_r)$ Checks $\eta_3^* \stackrel{?}{=} \eta_3$ $\Phi_4 = (\eta_4, Q, \beta \cdot P, W_i, T_4)$ $\longleftarrow$	
$T_4^* - T_4 \le \Delta T$ Retrieves $S_{i,}' = \eta_4 \oplus \alpha \cdot \beta \cdot P$ Checks $Q^* \stackrel{?}{=} Q$ Updates $\lambda_i^* = H_0(\alpha \cdot \beta \cdot P)$ Generates the signing key: $\mathrm{SK}_i = s_i^{-1} \cdot S_i' = s_i^{-1} \cdot (\omega_i + s_T \cdot X_i)$		

Step 5: upon receiving the message Φ_4, V_i first inspects the validity of T_4. Then, it retrieves $S_i' = \eta_4 \oplus \alpha \cdot \beta \cdot P$ and computes $Q^* = H_3(\lambda_i \Vert \mathrm{PID}_i \Vert N_v \Vert S_i' \Vert \beta \cdot P \Vert W_i)$. If $Q^* \neq Q$, it ends; else, the vehicle V_i successfully authenticates the TA and updates $\lambda_i^* = H_0(\alpha \cdot \beta \cdot P)$. Finally, V_i generates the signing key $\mathrm{SK}_i = s_i^{-1} \cdot S_i' = s_i^{-1} \cdot (\omega_i + s_T \cdot X_i)$.

6.4. Message Signing. When the vehicle V_i is ready to broadcast message M_i to others, it picks a random integer $r_i \in Z_q^*$ and computes $R_i = r_i \cdot \mathrm{PID}_{i,1}, Y_i = H_2(M_i \Vert \mathrm{PID}_i \Vert R_i \Vert T_i)$. Then, it generates the signature $\sigma_i = \mathrm{SK}_i + r_i \cdot Y_i$, where T_i is the current time. Subsequently, it broadcasts the messages $\{M_i, \sigma_i, \mathrm{PID}_i, R_i, W_i, T_i\}$ to nearby vehicles and RSUs.

6.5. Message Verification. When the RSU obtains the messages $\{M_i, \sigma_i, \mathrm{PID}_i, R_i, W_i, T_i\}$, it first checks the freshness of T_i and valid period VP_i of PID_i. Then, it verifies the signature by checking whether $\sigma_i \cdot \mathrm{PID}_{i,1} = W_i + X_i \cdot P_{\mathrm{pub}} + Y_i \cdot R_i$ satisfies. If it satisfies, the RSU accepts the messages; otherwise, it directly discards the messages. The correctness proof of the above equation is as follows.

6.5.1. Correctness Proof

$$\begin{aligned}
\sigma_i \cdot \mathrm{PID}_{i,1} &= (\mathrm{SK}_i + r_i \cdot Y_i) \cdot \mathrm{PID}_{i,1} \\
&= \left(s_i^{-1} \cdot S_i' + r_i \cdot Y_i\right) \cdot \mathrm{PID}_{i,1} \\
&= s_i^{-1} \cdot (w_i + s_T \cdot X_i) \cdot s_i \cdot P + r_i \cdot Y_i \cdot \mathrm{PID}_{i,1} \\
&= (w_i + s_T \cdot X_i) \cdot P + Y_i \cdot R_i \\
&= W_i + X_i \cdot P_{\mathrm{pub}} + Y_i \cdot R_i.
\end{aligned} \tag{4}$$

6.6. Batch Verification. When receiving lots of messages from multiple vehicles, the RSU can verify these messages in batch to effectively reduce the computation cost and raise the efficiency of verification. Assume that the RSU obtains the messages from n vehicles, which are denoted as $\{M_i, \sigma_i, \mathrm{PID}_i, R_i, W_i, T_i\}$, where $i = 1, 2, \ldots, n$. Similar to the single verification, the process of batch verification is executed by the verifier as follows.

The RSU first checks the freshness of T_i and valid period VP_i of PID_i; if T_i is not fresh or VP_i is expired, RSU discards this message; otherwise, it randomly selects a vector $\nu_i = \{\nu_1, \nu_2, \ldots, \nu_n\}$, where $\nu_i \in [1, 2^\varepsilon]$ and ε is a tiny number. Then, it performs batch verification by inspecting the validity of the following equation:

$$\sum_{i=1}^{n} v_i \cdot \sigma_i \cdot \mathrm{PID}_{i,1} = \sum_{i=1}^{n} v_i \cdot W_i + \left(\sum_{i=1}^{n} v_i \cdot X_i\right) \cdot P_{\mathrm{pub}} + \sum_{i=1}^{n} v_i \cdot Y_i \cdot R_i. \tag{5}$$

7. Security Analysis and Comparison

7.1. Security Analysis. Based on the hard problems introduced in Section 3.2, we prove that our scheme is secure by a game played between an adversary $\mathscr{A}$ and a challenger $\mathscr{C}$ using random oracle model.

Theorem 1. *The proposed scheme for VANETs is secure under the random oracle model in the adaptive chosen-message attack with an assumption that the ECDL problem is hard.*

Proof. Suppose an adversary $\mathscr{A}$ could forge a message $\{M_i, \sigma_i, \mathrm{PID}_i, R_i, W_i, T_i\}$, and a challenger $\mathscr{C}$ could tackle the ECDL problem with a nonnegligible probability by running $\mathscr{A}$ as a subroutine. The details are as follows:

Setup phase: $\mathscr{C}$ initializes public system parameters $\psi = \{a, b, p, q, P, H_0, H_1, H_2, H_3, H_4, P_{\mathrm{pub}}\}$ and delivers them to $\mathscr{A}$. Note that $P_{\mathrm{pub}} = s_T \cdot P$, where $s_T \in Z_q^*$ is randomly selected by TA.

Query phase: in each random oracle, the adversary $\mathscr{A}$ initiates an inquiry to the challenger $\mathscr{C}$, and $\mathscr{C}$ returns the result of the inquiry to $\mathscr{A}$ from the list. Suppose list_{h1} and list_{h2} are the lists maintained by $\mathscr{C}$ and are initially empty.

$\mathbf{H}_1$-Oracle: if $\mathscr{A}$ launches an inquiry on $\{\mathrm{PID}_i, W_i\}$, $\mathscr{C}$ will check whether $\{\mathrm{PID}_i, W_i, \rho_{h1}\}$ exists in list_{h1}. If does exist, $\mathscr{C}$ delivers ρ_{h1} to $\mathscr{A}$; otherwise, $\mathscr{C}$ sets $\rho_{h1} = H_1(\mathrm{PID}_i \| W_i)$ and adds $\{\mathrm{PID}_i, W_i, \rho_{h1}\}$ into list_{h1}. Finally, $\mathscr{C}$ sends ρ_{h1} to $\mathscr{A}$.

$\mathbf{H}_2$-Oracle: if $\mathscr{A}$ initiates an inquiry on $\{M_i, \mathrm{PID}_i, R_i, T_i\}$, $\mathscr{C}$ will check whether $\{M_i, \mathrm{PID}_i, R_i, T_i, \rho_{h2}\}$ exists in list_{h2}. If does exist, $\mathscr{C}$ delivers ρ_{h2} to $\mathscr{A}$; else, $\mathscr{C}$ sets $\rho_{h2} = H_2(M_i \| \mathrm{PID}_i \| R_i \| T_i)$ and adds $\{M_i, \mathrm{PID}_i, R_i, T_i, \rho_{h2}\}$ to list_{h2}. Finally, $\mathscr{C}$ sends ρ_{h2} to $\mathscr{A}$.

Sign-Oracle: after $\mathscr{C}$ obtains the query on the message M_i from $\mathscr{A}$, it randomly generates three integers $\sigma_i, X_i, Y_i \in Z_q^*$ and then adds $\{\mathrm{PID}_i, W_i, X_i\}$ into list_{h1} and adds $\{M_i, \mathrm{PID}_i, R_i, T_i, Y_i\}$ into list_{h2}. Finally, $\mathscr{C}$ sends the messages $\{M_i, \mathrm{PID}_i, R_i, W_i, T_i, \sigma_i\}$ to $\mathscr{A}$. It is obvious that the equation $\sigma_i \cdot \mathrm{PID}_{i,1} = W_i + X_i \cdot P_{\mathrm{pub}} + Y_i \cdot R_i$ holds.

In the end, $\mathscr{A}$ outputs messages $\{M_i, \mathrm{PID}_i, R_i, W_i, T_i, \sigma_i\}$ and $\mathscr{C}$ checks whether the following equation satisfies:

$$\sigma_i \cdot \mathrm{PID}_{i,1} = W_i + X_i \cdot P_{\mathrm{pub}} + Y_i \cdot R_i. \tag{6}$$

If not, $\mathscr{C}$ terminates the game. Otherwise, according to the forgery lemma [44], if the process is executed with different H_2 – oracle once again, $\mathscr{A}$ could generate another valid messages $\{M_i, \mathrm{PID}_i, R_i, W_i, T_i, \sigma_i^*\}$. Obviously, we can get the following equation:

$$\sigma_i^* \cdot \mathrm{PID}_{i,1} = W_i + X_i \cdot P_{\mathrm{pub}} + Y_i^* \cdot R_i. \tag{7}$$

According to equations (6) and (7), $\mathscr{C}$ could compute:

$$(\sigma_i - \sigma_i^*) \cdot \mathrm{PID}_{i,1} = Y_i \cdot R_i - Y_i^* \cdot R_i. \tag{8}$$

So,

$$\sigma_i - \sigma_i^* = r_i \cdot (Y_i - Y_i^*) \bmod q. \tag{9}$$

$\mathscr{C}$ outputs $(Y_i - Y_i^*)^{-1} \cdot (\sigma_i - \sigma_i^*)$ as the result of ECDL problem which conflicts the difficulty of the ECDL problem. Consequently, our scheme for VANETs is secure under random oracle model in adaptively chosen message attack. Next, we will briefly analyze the security requirements for VANETS mentioned in Section 3.3.

(1) Message authentication: based on Theorem 1, it is known that if the ECDL problem is difficult, any polynomial adversary cannot forge a valid message signature. Thus, the verifier can inspect the integrity and validity of the messages $\{M_i, \mathrm{PID}_i, R_i, W_i, T_i, \sigma_i\}$ by checking whether the equation $\sigma_i \cdot \mathrm{PID}_{i,1} = W_i + H_1(\mathrm{PID}_i \| W_i) \cdot P_{\mathrm{pub}} + H_2(M_i \| \mathrm{PID}_i \| R_i \| T_i) \cdot R_i$ holds. Consequently, the proposed scheme for VANETs ensures the validity and integrity of the broadcast messages.

(2) Identity authentication: during the mutual authentication phase, TA authenticates the identity of the vehicle V_i by calculating $\eta_1^* = H_3(\mathrm{PID}_i \| \lambda_i \| N_v \| \alpha \cdot P)$; V_i verifies the validity of TA by computing $Q^* = H_3(\lambda_i \| \mathrm{PID}_i \| N_v \| S_i' \| \beta \cdot P \| W_i)$.

(3) Traceability: once the traffic-related message broadcast by the vehicle V_i causes an accident, TA can compute the real identity of V_i by $\mathrm{RID} = \mathrm{PID}_{i,2} \oplus H_0(s_T \cdot \mathrm{PID}_{i,1} \| \mathrm{VP}_i)$. Then, TA adds the vehicle V_i to the blacklist and deletes the information of V_i from its database. TA periodically broadcasts the blacklist to other vehicles and RSUs.

(4) Forward secrecy: the adversary cannot obtain the previous shared key between TA and V_i, even though the current shared key is exposed. In each interaction, the shared key will be updated to $\lambda_i^* = H_0(\alpha \cdot \beta \cdot P)$ with the random numbers α and β chosen by TA and V_i, respectively. The updated shared key has nothing to do with the previous key, but only related to the random numbers α and β. According to the CDH problem, it is known that the adversary cannot obtain $\alpha \cdot \beta \cdot P$ even if it intercepts $\alpha \cdot P$ and $\beta \cdot P$ from the public channel. Hence, the proposed scheme provides forward security.

(5) Replay attack: upon receiving the messages $\{M_i, \sigma_i, \mathrm{PID}_i, R_i, W_i, T_i\}$, the RSU will first verify the freshness of T_i by checking wether $T_i^* - T_i \le \Delta T$

holds. Even if T_i is fresh, it cannot satisfy the verification equation $\sigma_i \cdot \mathrm{PID}_{i,1} = W_i + X_i \cdot P_{\mathrm{pub}} + Y_i \cdot R_i$.

(6) Impersonation attack: according to Theorem 1, it is not possible for an adversary to imitate other valid vehicles to successfully broadcast the signatures of messages. Because once the RSU receives the messages $\{M_i, \sigma_i, \mathrm{PID}_i, R_i, W_i, T_i\}$, it will first check the validity of the verification equation $\sigma_i \cdot \mathrm{PID}_{i,1} = W_i + X_i \cdot P_{\mathrm{pub}} + Y_i \cdot R_i$. Hence, the impersonation attack can be resisted in our scheme.

(7) Forgery attack: according to Theorem 1, any adversary cannot forge a valid messages $\{M_i, \sigma_i, \mathrm{PID}_i, R_i, W_i, T_i\}$ because this attack can be detected by the verifier through checking whether the equation $\sigma_i \cdot \mathrm{PID}_{i,1} = W_i + X_i \cdot P_{\mathrm{pub}} + Y_i \cdot R_i$ holds. So, our scheme is resistant of the forgery attack.

(8) Known key secrecy attack: even though the previous shared key between TA and V_i is stolen, the adversary cannot generate the current shared key. This is because the shared key will be replaced as $\lambda_i^* = H_0(\alpha \cdot \beta \cdot P)$ in each round. It is just associated with the random numbers α and β, which are selected, respectively, by the vehicle and TA for each session. The adversary cannot obtain $\alpha \cdot \beta \cdot P$ from $\alpha \cdot P$ and $\beta \cdot P$ unless it could solve CDH problem. The CDH problem is recognized as hard; hence, the proposed scheme can withstand known key secrecy attack. □

7.2. Security Comparison. We compare the security of our scheme with three related schemes [6, 37, 38] for VANETs. Suppose S1, S2, S3, S4, S5, S6, S7, and S8, respectively, denote message authentication, identity authentication, traceability, forward secrecy, resistance against replay attack, impersonation attack, forgery attack, and known key secrecy attack. The result of security comparison is shown in Table 3.

From Table 3, we can see that all the four schemes can satisfy the security requirements of message authentication, traceability, and resistance against replay attack. Identity authentication is only met in our scheme and the scheme [6]. Our scheme is the only one that can provide forward secrecy and resist known key secrecy attack. In summary, our scheme provides better security property compared with the recent proposed schemes.

8. Performance Analysis

In this part, we present the performance analysis with respect to the computational and communication overhead of our scheme and the schemes proposed by Ali and Li [38], Zhong et al. [37], and Cui et al. [6].

8.1. Computation Cost Analysis. To estimate the computational cost of our scheme and other related schemes [6, 37, 38], we adapt the Java Pairing-Based Cryptography (JPBC) library. In terms of the bilinear map e: $G \times G \longrightarrow G_T$, we choose the Type A pairing for schemes [37, 38]. It is constructed on the elliptic curve $y^2 = x^3 + x$:mod$p$ over the field F_q, where p and the order of group G_1 are, respectively, 512 bits and 160 bits. While in the proposed scheme using the elliptic curve, the group G_2 is generated by the elliptic curve $y^2 = x^3 + a \cdot x + b$:mod$p$, where the order of G_2 and the prime p are both 160 bits. The experiment is conducted on a Laptop running Intel I5–8250U, 4 GB memory, 1.8 GHz processor with Windows 10 operating system. In our simulation experiment, we only consider the cryptographic operations which have a major impact on efficiency and ignore the execution time of addition operation. Table 4 shows the notations and the execution time of several cryptographic-related operations.

Table 5 lists the total computation overhead about message signing, single signature verification, and n signatures' verification. In the process of message signing, our scheme requires one multiplication operation based on ECC and one hash function operation. Accordingly, the computation overhead of this process is $T_{\mathrm{mp-ECC}} + T_h \approx 13.1$ ms. In Ali and Li's scheme [38], the computation overhead of message signing is $3T_{\mathrm{mp-ECC}} + 2T_h \approx 38.6$ ms. The cost of generating a signature is $3T_{\mathrm{mp-ECC}} + T_{\mathrm{mtp}} + T_h \approx 68.5$ ms in Zhong et al.'s scheme [37]. In Cui et al.'s scheme [6], the computation overhead of generating a signature is $2T_{\mathrm{mp-ECC}} + 2T_h \approx 26.2$ ms.

During the message verification phase, in our scheme, the verifier takes three multiplication operations based on ECC and two hash function operations for single message verification, $2n + 1$ multiplication operations based on ECC, and $2n$ hash function operations for n signatures verification. Therefore, the computation cost of verifying a single signature and n signatures are $3T_{mp-ECC} + 2T_h \approx 38.6$ ms and $(2n + 1)T_{\mathrm{mp-ECC}} + 2nT_h \approx (12.4 + 26.2n)$ ms, respectively. In the scheme of Ali and Li [38], the computation overhead of single signature verification and batch verification are $T_p + T_{\mathrm{mp-ECC}} + T_h \approx 35.5$ ms and $T_p + nT_{\mathrm{mp-ECC}} + nT_h \approx (22.4 + 13.1n)$ ms, respectively. In the scheme of Zhong et al. [37], $3T_p + T_{\mathrm{mtp}} + 2T_{\mathrm{mp-ECC}} + T_{\mathrm{mp}-p} + T_h \approx 126.4$ ms and $3T_p + nT_{\mathrm{mtp}} + 2nT_{\mathrm{mp-ECC}} + nT_h + T_{\mathrm{mp}-p} \approx (70.3 + 56.1n)$ms are, respectively, spent on the phase of single verification and batch verification. In Cui et al.'s scheme [6], the verifier spends $T_h \approx 0.7$ ms and $nT_h \approx (0.7n)$ms on verifying a single signature and n signatures, respectively.

From Figures 2–4, compared with the three recently proposed schemes [6, 37, 38], we can more intuitively and clearly find that our scheme has the least computation overhead in the message signing step. During the single verification and batch verification phases, although the computation overhead of Cui et al.'s scheme [6] is negligible, their scheme is subject to some security attacks such as impersonation attack and forgery attack; the computation overhead of our scheme is far lower than that of Zhong et al. [37] and slightly higher than that of Ali and Li [38]. However, our scheme has better security performance such as supporting identity authentication and forward secrecy, withstanding known key secrecy attack. On the whole, our

Table 3: The result of security comparison.

Schemes	S1	S2	S3	S4	S5	S6	S7	S8
Ali and Li [38]	√	×	√	×	√	√	√	×
Zhong et al. [37]	√	×	√	×	√	√	√	×
Cui et al. [6]	√	√	√	×	√	×	×	×
Our scheme	√	√	√	√	√	√	√	√

Table 4: The execution time of cryptographic operations.

Cryptographic operations	The notations of cryptographic operations	Execution time (ms)
T_p	The execution time of the bilinear pairing operation	22.4
$T_{\text{mp}-p}$	The execution time of multiplication operation based on bilinear pairing	3.1
$T_{\text{mp}-\text{ECC}}$	The execution time of multiplication operation based on the elliptic curve	12.4
T_{mtp}	The execution time of the map-to-point operation	30.6
T_h	The execution time of hash function	0.7

Table 5: The comparison of computation costs.

Schemes	Message signing	Single message verification	Multiple messages verification
Ali and Li [38]	$3T_{\text{mp}-\text{ECC}} + 2T_h$	$T_p + T_{\text{mp}-\text{ECC}} + T_h$	$T_p + nT_{\text{mp}-\text{ECC}} + nT_h$
Zhong et al. [37]	$3T_{\text{mp}-\text{ECC}} + T_{\text{mtp}} + T_h$	$3T_p + T_{\text{mtp}} + 2T_{\text{mp}-\text{ECC}} + T_{\text{mp}-p} + T_h$	$3T_p + nT_{\text{mtp}} + 2nT_{\text{mp}-\text{ECC}} + T_{\text{mp}-p} + nT_h$
Cui et al. [6]	$2T_{\text{mp}-\text{ECC}} + 2T_h$	T_h	nT_h
Our scheme	$T_{\text{mp}-\text{ECC}} + T_h$	$3T_{\text{mp}-\text{ECC}} + 2T_h$	$(2n+1)T_{\text{mp}-\text{ECC}} + 2nT_h$

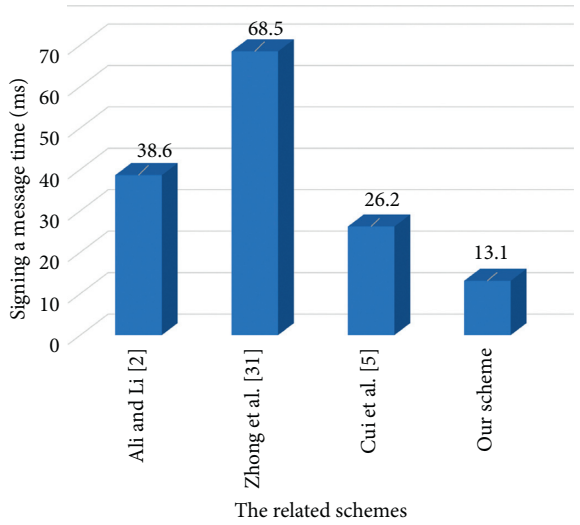

Figure 2: Message signing cost.

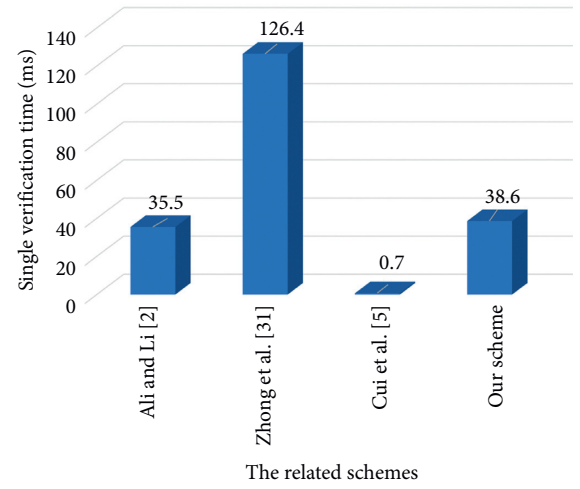

Figure 3: Single signature verification cost.

solution is suitable for VANETs in terms of security and efficiency.

8.2. Communication Cost Analysis. In this part, we analyze and compare the communication overhead between the proposed scheme and other schemes [6, 37, 38]. For the group G_1 using the bilinear pairing and the group G_2 using the ECC, the size of p is, respectively, 512 bits and 160 bits. Hence, the size of each element in group G_1 is 128 bytes and that of each element in G_2 is 40 bytes. Besides, the length of timestamp is 4 bytes; the elements in an integer group and the general hash are both considered 20 bytes. We assume that the length of all traffic-related messages is the same, so we ignore the size of traffic-related messages when calculating the communication overhead.

As shown in Table 6, in the scheme of Ali and Li [38], the vehicle V_i broadcasts a signature $\sigma_i = (A_i, B_i) \in G_1$ on the message M_i for the pseudonym identity $\text{VPID}_i = (\text{VPID}_{i,1}, \text{VPID}_{i,2})$ with the timestamp T_i to the verifier, where $\text{VPID}_{i,1} \in G_1$ and $\text{VPID}_{i,2} \in Z_q^*$. Accordingly, the total communication cost of Ali et al.' scheme is $|A_i| + |B_i| + |\text{VPID}_{i,1}| + |\text{VPID}_{i,2}| + |T_i| = 12.8 * 3 + 20 + 4 = 408$ bytes. In the scheme of Zhong et al. [37], V_i

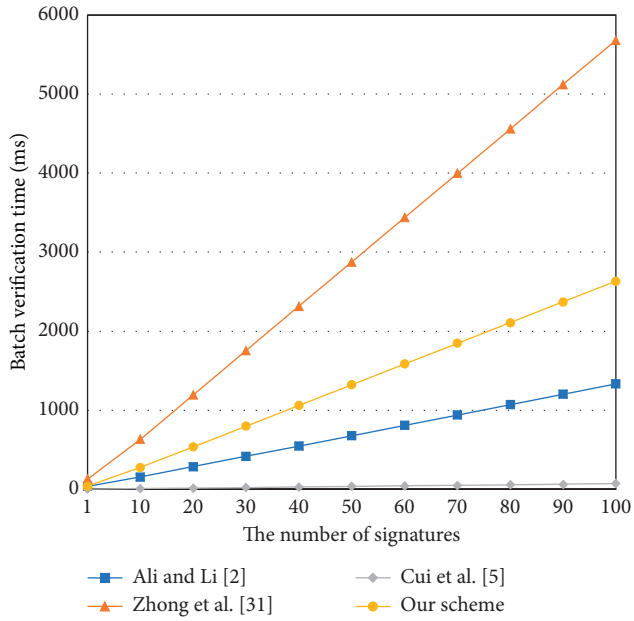

Figure 4: Multiple signatures' verification cost.

Table 6: The comparison of communication cost.

Schemes	Broadcasting single signature (bytes)	Broadcasting n signatures (bytes)
Ali and Li [38]	408	$408n$
Zhong et al. [37]	644	$644n$
Cui et al. [6]	100	$100n$
Our scheme	168	$168n$

transmits the messages $\{M_i, \text{VPID}_i, \text{VPK}_i, R_i, T_i, t_i\}$ to the RSU, where $\text{VPID}_i = (\text{VPID}_{i,1}, \text{VPID}_{i,2})$, t_i is the timestamp, and $\text{VPID}_{i,1}, \text{VPID}_{i,2}, \text{VPK}_i, R_i, T_i \in G_1$. Hence, the sum of communication overhead is $|\text{VPID}_{i,1}| + |\text{VPID}_{i,2}| + |\text{VPK}_i| + |R_i| + |T_i| + |T_i| = 12.8 * 5 + 4 = 644$ bytes. In Cui et al.'s scheme [6], V_i sends the messages $\{\text{PPID}_i, \text{AC}, \delta_i, R_i\}$ to the verifier, where PPID_i, AC, δ_i are all hash values, and $R_i \in G_2$. Thus, the sum of communication overhead is $|\text{PPID}_i| + |\text{AC}| + |\sigma_i| + |R_i| = 20 * 3 + 40 = 100$ bytes. Then, in our scheme, V_i transmits the messages $\{M_i, \sigma_i, \text{PID}_i, R_i, W_i, T_i\}$, where $\text{PID}_i = \{\text{PID}_{i,1}, \text{PID}_{i,2}, \text{VP}_i\}$, and $\sigma_i, \text{PID}_{i,2} \in Z_q^*$, $\text{PID}_{i,1}, R_i, W_i \in G_2$, and T_i is the timestamp. So, the whole communication overhead is $|\sigma_i| + |\text{PID}_i| + |R_i| + |W_i| + |T_i| = 20 * 2 + 40 * 3 + 4 * 2 =$ 168 bytes.

From Table 6, we can see that the total communication cost of our scheme is far less than that of the schemes [37, 38], but slightly more than that of Cui et al.'s scheme [6]. However, the scheme of Cui et al. is subject to the impersonation attack and forgery attack. In addition, our scheme can not only provide identity authentication and forward secrecy but also resist known key secrecy attack. Therefore, our scheme is appropriate for VANETs with respect to communication overhead.

9. Conclusion

In this paper, we first analyze and point out that the mutual authentication scheme of Cui et al. is subject to the impersonation attack and the forgery attack. Then, we propose an improved mutual authentication scheme with forward security for VANETs. Security proof and analysis show that our scheme can not only resist general attacks but also achieve forward secrecy and withstand known key secrecy key attack, which are not achieved in other related schemes [6, 37, 38]. In addition, our solution has relatively balanced performance.

Data Availability

No data were used to support this study.

Conflicts of Interest

All authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China under Grant no. 61932010.

References

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

[2] J. Li, K.-K. R. 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.

[3] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "Raise: an efficient rsu-aided message authentication scheme in vehicular communication networks," in *Proceedings of the 2008 IEEE International Conference on Communications*, pp. 1451–1457, IEEE, Lahore, Pakistan, May 2008.

[4] J. Zhang, W. Zhen, and M. Xu, "An efficient privacy-preserving authentication protocol in vanets," in *Proceedings of the 2013 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Networks*, pp. 272–277, IEEE, Dalian, China, December 2013.

[5] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for vanets," *IEEE Transactions on Signal and Information Processing Over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[6] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," *Vehicular Communications*, vol. 21, Article ID 100200, 2020.

[7] 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.

[8] K. Li, W. F. Lau, and M. H. Au, "A secure and efficient privacy-preserving authentication scheme for vehicular networks with batch verification using cuckoo filter," in *Proceedings of the International Conference on Network and*

System Security, pp. 615–631, Springer, Sapporo, Japan, December 2019.

[9] N. B. Gayathri, G. Thumbur, P. V. Reddy, and M. Z. Ur Rahman, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31808–31819, 2018.

[10] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in vanets," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 807–817, 2019.

[11] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in *Proceedings of the 2006 Securecomm and Workshops*, pp. 1–5, IEEE, Baltimore, MD, USA, September 2006.

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

[13] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[14] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proceedings of the Annual International Cryptology Conference*, pp. 41–55, Springer, Santa Barbara, CA, USA, August 2004.

[15] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 1229–1237, IEEE, Phoenix, AZ, USA, April 2008.

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

[17] 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.

[18] S.-F. Zeng, 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, 2015.

[19] C. Li, X. Zhang, H. Wang, and D. Li, "An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks," *Sensors*, vol. 18, no. 1, p. 194, 2018.

[20] L. Dang, J. Xu, X. Cao et al., "Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, 2018.

[21] Q. Li, C.-F. Hsu, K.-K. Raymond Choo, and D. He, "A provably secure and lightweight identity-based two-prty authenticated key agreement protocol for vehicular ad hoc networks," *Security and Communication Networks*, vol. 2009, Article ID 7871067, , 2019.

[22] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 219, pp. 225–235, 2013.

[23] D. He, M. Tian, and J. Chen, "Insecurity of an efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 268, pp. 458–462, 2014.

[24] 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.

[25] 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.

[26] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Information Sciences*, vol. 451-452, pp. 1–15, 2018.

[27] I. A. Kamil and S. O. Ogundoyin, "An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks," *Journal of Information Security and Applications*, vol. 44, pp. 184–200, 2019.

[28] A. Malip, S.-L. Ng, and Q. Li, "A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks," *Security and Communication Networks*, vol. 7, no. 3, pp. 588–601, 2014.

[29] J. Li, H. Yuan, and Y. Zhang, "Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Networks*, vol. 317, pp. 48–66, 2015.

[30] Z. Xu, D. He, N. Kumar, and K.-K. R. Choo, "Efficient certificateless aggregate signature scheme for performing secure routing in vanets," *Security and Communication Networks*, vol. 2020, Article ID 5276813, , 2020.

[31] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[32] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in vanets," *Journal of Systems Architecture*, vol. 103, Article ID 101692, 2020.

[33] X. Hu, J. Wang, H. Xu, Y. Liu, and X. Zhang, "Secure and pairing-free identity-based batch verification scheme in vehicle ad-hoc networks," in *Proceedings of the International Conference on Intelligent Computing*, pp. 11–20, Springer, Pune, India, December 2016.

[34] C. Song, M. Zhang, Z. Jia, W. Peng, and H. Guo, "A lightweight batch anonymous authentication scheme for vanet based on pairing-free," *Computer Science and Information Systems*, vol. 15, no. 3, pp. 549–567, 2018.

[35] 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.

[36] 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.

[37] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in vanet," *Information Sciences*, vol. 476, pp. 211–221, 2019.

[38] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in vanets," *Vehicular Communications*, vol. 22, Article ID 100228, 2020.

[39] J. Zhang, J. Cui, H. Zhong, Z. Chen, L. Liu, and Pa-crt, "Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, 2021.

[40] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," *Vehicular Communications*, vol. 22, Article ID 100213, 2020.

[41] C. Xu, H. Liu, Y. Zhang, and P. Wang, "Mutual authentication for vehicular network in complex and uncertain driving," *Neural Computing and Applications*, vol. 32, no. 1, pp. 61–72, 2020.

[42] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.

[43] H. Noori and B. B. Olyaei, "A novel study on beaconing for vanet-based vehicle to vehicle communication: probability of beacon delivery in realistic large-scale urban area using 802.11 p," in *Proceedings of the 2013 International Conference on Smart Communications in Network Technologies (SaCoNeT)*, pp. 1–6, IEEE, Paris, France, June 2013.

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