Hindawi
Complexity
Volume 2021, Article ID 5526412, 13 pages
https://doi.org/10.1155/2021/5526412

Research Article

Anonymous Authentication and Key Agreement Scheme Combining the Group Key for Vehicular Ad Hoc Networks

Mei Sun,[1,2] **Yuyan Guo**,[2] **Dongbing Zhang**,[2] **and MingMing Jiang**[2]

[1]*School of Information and Control Engineering, China University of Mining and Technology, Xuzhou 221116, China*
[2]*School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, China*

Correspondence should be addressed to Mei Sun; sunmei109@163.com

Received 24 January 2021; Revised 25 March 2021; Accepted 20 April 2021; Published 4 May 2021

Academic Editor: Jia Wu

Vehicular ad hoc network (VANET) is a multihop mobile wireless communication network that can realize many vehicle-related applications through multitop communication. In the open wireless communication environment, security and privacy protection are important contents of VANET research. The most basic method of VANET privacy protection is anonymous authentication. Even through, there are many existing schemes to provide anonymous authentication for VANETs. Many existing schemes suffer from high computational cost by using bilinear pairing operation or need the assistance of the trust authorities (TAs) during the authentication process or rely on an ideal tamper-proof device (TPD), which requires very strong security assumption. In this study, an anonymous authentication and key negotiation scheme by using private key and group key is proposed, which is based on pseudonym using the nonsingular elliptic curve. In this scheme, there is no third party trust center to participate in the authentication, there is no need to query the database, and there is no need of the local database to save the identity information of many vehicles, which reduce the storage space and the authentication time compared with other schemes. The proposed scheme only needs realistic TPDs. In the proposed scheme, TPDs do not need to preinstall the system key as many other schemes do; hence, the failure of a single TPD does not affect the security of the entire system. The security of the scheme is proved under the random oracle model. Compared with the related schemes using bilinear pairings, the computational cost and communication cost of the proposed scheme are reduced by 82% and 50%, respectively.

1. Introduction

With the development of network technology, there are many forms of network and new technologies [1, 2]. Vehicular ad hoc network (VANET) is a highly mobile self-organizing wireless communication network. By using VANET, vehicles in front can in a timely manner report the road condition information to the rear vehicles; this can improve the travel efficiency and reduce road congestion and traffic accidents. VANET plays a significant role in traffic optimization and safety [3]. Since VANET mainly adopts a wireless communication mode, messages are vulnerable to various attacks, such as counterfeiting, interception, tampering, tracking, and other attacks [4, 5]. These attacks seriously threaten the safety of vehicles and the privacy of users. Therefore, security authentication and privacy protection are important research directions of VANET. VANET generally has the following main components: road side unit (RSU), trust agency (TA), and on-board unit (OBU) [6]. OBU is installed in the vehicle and can realize the communication between the vehicle and RSU or other vehicles. The communication between OBU and RSU adopts dedicated short range communication (DSRC) [7]. The communication with vehicles requires authenticating one another and negotiating the communication key to prevent attacks such as tracking, privacy exposure, and message counterfeiting. Authentication and key agreement in VANETs are anonymous. Hence, even if an attacker intercepts the message, the specific source of the message cannot be determined. Additionally, the authority of

VANET can identify every message sent by vehicles, and this can prevent vehicles from sending false messages maliciously.

1.1. Related Works. In recent years, some authentication protocols based on public key infrastructure (PKI) [8–10] have been proposed. In these works, some anonymous authentication and key agreement schemes are proposed, in which a large number of certificates are assigned to vehicles. However, these schemes require vehicles to be equipped with many anonymous certificates in advance; this leads to many problems such as certificate storage and certificate management. Lu et al. [11] proposed a key agreement and authentication scheme for generating a short-term key and certificate between the vehicle and RSU. However, the communication efficiency of the scheme is low due to the frequent interaction between the vehicle and RSU for changing the authenticated group. Rajput et al. [12] proposed an anonymous authentication scheme with hierarchical privacy protection to solve the defects based on PKI. This protocol does not need to manage the certificate revocation list (CRL), and each vehicle uses two pseudonyms to complete anonymous authentication, but once the pseudonym expires, the vehicle needs to acquire the pseudonym from TA or RSU again; this increased the number of communications. Wang [13] proposed a local identity-based anonymous authentication protocol for VANET (LIAP). In this method, each vehicle and RSU are assigned a unique long-term certificate from the certification authority (CA) in the registration phase. The vehicle and RSU complete mutual authentication through certificates. After successful authentication, RSU distributes a local-master key to the vehicle. The vehicle randomly generates a pseudonym to communicate with the RSU through the local-master key. The use of the local-master key improves the communication efficiency and system security. But this scheme needs to manage CRL.

The storage and management of certificates restrict the development of authentication schemes based on PKI. To overcome the problems caused by authentication certificates, some identity-based public key cryptosystems are introduced into authentication of VANET [4, 14–19]. In 1984, Miller first proposed an identity cryptosystem [14]. In this cryptosystem, the user's public key is calculated by the user's identity, and the user's private key is generated by the authentication center through the system key according to the user's identity. In 2008, Zhang et al. [15] proposed an authentication protocol for VANET using the identity of the vehicle user, solving the certificate storage and management problem and supporting batch authentication. In 2011, Huang [16] proposed an anonymous batch authenticated and key agreement scheme based on identity authentication for VANET. Shim et al. [17] noted that the scheme [15] was vulnerable to replay attack and did not achieve the nonrepudiation of signature and proposed a vehicle-to-infrastructure (V2I) authentication scheme. However, the scheme is vulnerable to tampering attacks [18] and cannot satisfy its claimed chosen message attack resistance [17]. Wang et al. [20] mentioned that Huang et al. [16] could not resist a collusion attack, and therefore, they proposed an improved scheme. And, in [20], it is indicated that the scheme [18] cannot resist replay attacks and cannot track the real identity of the message sender. In 2016, Azees and Vijayakumar [21] proposed a novel key distribution scheme for secure group communication using Lagrange polynomials. The limitation of the scheme is that it only provides one-way authentication from vehicle to TA. Then, Vijayakumar et al. [22] proposed a privacy-preserving anonymous mutual and batch authentication scheme for vehicle-to-vehicle. This scheme implements the authentication of message source and message integrity and has the mechanism of tracking and revoking vehicles. In 2017, Azees et al. [23] proposed an anonymous authentication scheme to avoid malicious vehicles into the VANET based on bilinear pairing. Each user computes multiple temporary short time certificates to realize anonymous authentication in the scheme. The scheme has high computing performance and security. However, the dummy identity (DIU_{ui}) in each certificate is the same, and the scheme does not consider the unlinkability of different sessions. In 2018, Pournaghi et al. [24]. proposed an anonymous authentication and key agreement scheme combining TPD and RSU. The scheme saves the system master key in the TPD of RSU instead of the TPD of each vehicle, which improves the security and authentication efficiency of the system. In 2019, Ikram et al. [25] proposed a conditional privacy-preserving authentication scheme for V2I. This scheme uses general one-way hash functions instead of map-to-point hash functions to achieve high efficiency.

The identity-based authentication schemes for VANET address the problems presented by the schemes based on PKI. The existing schemes [21–25] are novel in design and have good security. However, the bilinear pairing operations of elliptic curve are used, and the computational efficiency of bilinear pairing operation is low. The works [26–28] based on pseudonym on elliptic curve, which do not use bilinear pairing operation and have achieved high computational efficiency. However, TA is required to participate in authentication, this increases communication times and communication burden. He et al. [29] proposed a privacy protection authentication scheme based on identity. This scheme also uses elliptic curve instead of bilinear pairing operations and achieves satisfactory performance in both computation and communication. However, the scheme is based on ideal TPD, and the master key is stored on the TPD of each vehicle. Islam et al. [30] proposed a conditional privacy-preserving authentication scheme based on hash function. And the scheme offers group-key generation, user leaving, user join, and password change facilities. The scheme does not need bilinear pairing mapping or elliptic curve operation and is lightweight in terms computation and communication. However, TA is required to participate in each authentication between the vehicle and RSU. Wu et al. [6] proposed an effective location-based conditional secret authentication scheme. The scheme does not require bilinear pairing operations or TPDs. However, when RSU is certified by vehicle, TA needs to query the database and return the

results. Cui et al. [31] proposed a scheme without relying on any special hardware such as TPD. The scheme is based on elliptic discrete logarithm and has high computational performance. The cuckoo filter and binary tree search method are used to achieve a higher success rate in batch authentication. However, TA is required to generate communication key for the vehicle and RSU. Zhong et al. [32] proposed an authentication and key agreement scheme based on hash function and registration list. And the scheme does not require the strong security assumptions of TPD. Xiong Li et al. [33] proposed a lightweight authentication scheme for VANETs with only hash functions and exclusive-OR operations. Compared with previous schemes, the computational cost of the schemes [32, 33] has been greatly improved. However, the schemes also need TA to participate in the authentication. In recent years, there are some authentication schemes using group key, which can reduce the authentication burden of TA. The works [34, 35] introduce group key management schemes based on Chinese remainder theorem, which reduces computation complexity of the key server. In 2019, Jing Zhang et al. [36] proposed a message authentication scheme based on the group key using Chinese remainder theorem. The TPD of the vehicle only save the real identity and the group key. So the proposed scheme only requires realistic TPDs and ensures higher security for the entire system. In 2020, Wei et al. [37] proposed tow privacy-preserving multimodal implicit authentication protocols for Internet of connected vehicles. The proposed protocols use the password and vehicle owner's behavior features as the authentication factors skillfully and do not reveal any information about vehicle owner's behavior. The protocols have advantages in computational cost and accuracy. However, the protocols do not consider the unlinkability of sessions. Vinoth et al. [38] proposed a multifactor authenticated key agreement scheme for industrial Internet of things (IoT). The scheme implements authentication and key agreement between the user and multiple sensing devices at the same time. The scheme only used hash function, bit-wise XOR operation, and symmetric cryptography. It has less communication cost and computational cost compared with other correlative schemes. However, the scheme does not consider internal attack.

1.2. Our Contributions. In this study, an anonymous authentication and key agreement scheme based on elliptic curve for VANET is proposed. Each vehicle is equipped with a TPD. The TPD saves the private key of the vehicle and the group key for multivehicle communication. The vehicle can authenticate with RSU anonymously by combining a private key with a group key. After successful authentication, the session key can be negotiated for both parties. The scheme can also implement message signature and anonymous verification. In this scheme, the TPD only saves the private key of the vehicle and the group key instead of the system key. The attack on the TPD will not affect other nodes in VANET. So, we only need realistic TPD instead of ideal TPD. There is no need for the third party to participate in the authentication and key agreement between vehicle and RSU compared with the works [6, 30–33], and there is no need to query the database in the scheme. In addition, the use of group key in this scheme can help RSU resist certain denial of service (DoS) attacks.

The main contributions of this study are summarized as follows.

(1) In order to optimize the computational cost and key management, we present an efficient anonymous authentication and key agreement scheme for RSUs and vehicles using the private key of the vehicle and the group key

(2) In order to reduce the communication time and storage space, we implement independent authentication and key agreement between vehicle and RSU, and RSU does not need to save vehicle information or query database.

(3) In this scheme, we also implement anonymous signature and verification of messages

(4) In this scheme, we use realistic TPDs instead of ideal TPDs, which is more suitable for VANET

1.3. Organization of This Article. The rest of the study is structured as follows: Section 2 describes the preliminaries of the proposed scheme, Section 3 gives the working of the proposed scheme, Sections 4 and 5 present a security analysis and a performance analysis, respectively. Our study is concluded in Section 6.

2. Preliminaries

In this section, we introduce the related background information of VANET and the proposed scheme.

2.1. Network Model. As shown in Figure 1, the network model of VANET mainly includes TA, RSU, OBU, TPD, and application server (AS). TA is a trusted service center. It is responsible for generating the private and public keys for RSU and vehicle and the group key for multivehicle communication. TA is an entity with the highest level of security protection and is completely trusted. RSU is the communication equipment installed on both sides of the road, with high security, thus providing access service for vehicles. The RSU communicates with the vehicle using DSRC protocol. Each vehicle is equipped with an OBU. The OBU of the vehicle realizes short distance communication with RSU and OBUs of other vehicles. TA allocates a TPD to each vehicle. TPD has high security, and other attackers cannot obtain sensitive information from the device [39]. AS is an application server and provides data service for TA. AS has high security and is credible.

2.2. Elliptic Curve. Suppose that F_P denotes a finite field of order p, where p is a large prime number. E denotes an elliptic curve over F_P. The curve E is defined as $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$. The group G is a

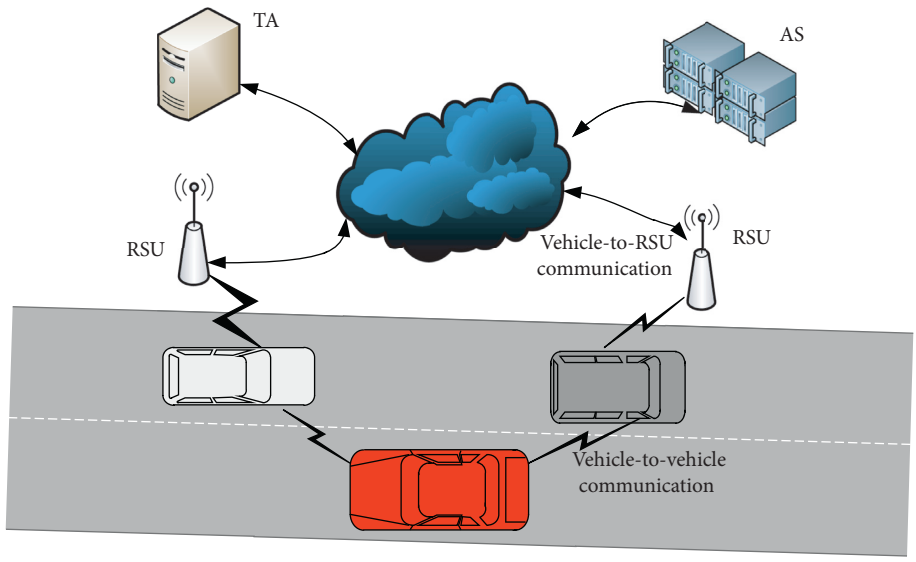

Figure 1: VANET network model.

cyclic additive group of order q on E, and P is the generator and O is the infinite point.

The group G has the following properties:

(1) Additive (±). For $P, Q \in G$, if $P \neq Q$, $R = P + Q$, then R is the intersection point of the straight line passing through P and Q with E; if $P = Q$, $R = P + Q$, then R is the tangent intersection point of P and Q with E; if $P = -Q$, then $P + Q = P - P = O$.

(2) Scalar multiplication (.). Let $m \in Z_q^*$, scalar point multiplication in G is defined as $m.P = P + P + \ldots + P$ (m times).

Two difficult problems are defined as follows:

Definition 1. Elliptic curve discrete logarithm problem (ECDLP). Let Q be a random point on G and calculate a solution x which satisfies $Q = xP$, where $x \in Z_q^*$.

Definition 2. Elliptic curve computational Diffie–Hellman problem (ECCDH). Assume a generator P of G, $aP, bP \in G$, where $a, b \in Z_q^*$ are unknown. The ECCDH problem is to compute $abP \in G$.

If ECDLP or ECCDH on a group G cannot be solved with nonnegligible probability ε in time t, then ECDLP or ECCDH is said to be a difficult problem on elliptic curve.

2.3. Security Requirements. The open multihop wireless network is vulnerable to various attacks. Therefore, the authentication and key agreement for VANET need to meet the following security requirements [29, 39]:

(1) Authentication and integrity. After receiving the message, VANET needs to determine whether the source of the message is reliable and whether the message has been tampered by others

(2) Privacy protection. When users are communicating, VANET should protect the confidential information such as user's identity, session record, location, and driving path. VANET provides privacy protection by imparting anonymity.

(3) Session key agreement. When the vehicle transmits data with RSU, the session key should be used to encrypt the data to protect the session privacy

(4) Traceability. To prevent malicious users from sending false messages by anonymity, the authentication scheme should trace the real identity of the sender when the message is in dispute

(5) Resistance to attacks. VANET is vulnerable to various attacks, such as replay attacks and forgery attacks. Authentication and key agreement of VANET needs to be able to resist all kinds of attacks to ensure the security and reliability of the scheme.

(6) Unlinkability. In order to protect privacy, attackers or other vehicles cannot link different sessions of the same vehicle via the public channel.

3. Proposed Authentication Scheme for VANET

Our scheme includes the following phases: initialization, RSU and vehicle registration, authentication and communication key agreement, message signing, signature verification, identity extraction, and updating the group key. The mutual authentication and the key agreement process between RSU and the vehicle is shown in Figure 2. The main notations used in the scheme are given in Table 1.

3.1. Initialization Phase. TA selects random numbers $s, x \in Z_q^*$, s is the private key of the system, x is the group key for multivehicle communication, and it can be used to compute the public key $P_{\text{pub}} = sP \in G$. Furthermore, $P_x = xP \in G$. TA selects five secure hash functions: $h_0: \{0,1\}^* \times G \longrightarrow Z_q^*$, $h_1: G \longrightarrow Z_q^*$, $h_2: \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \longrightarrow Z_q^*$, $h_3: \{0,1\}^* \times \{0,1\}^* \times G \times G \times \{0,1\}^*$, h_4

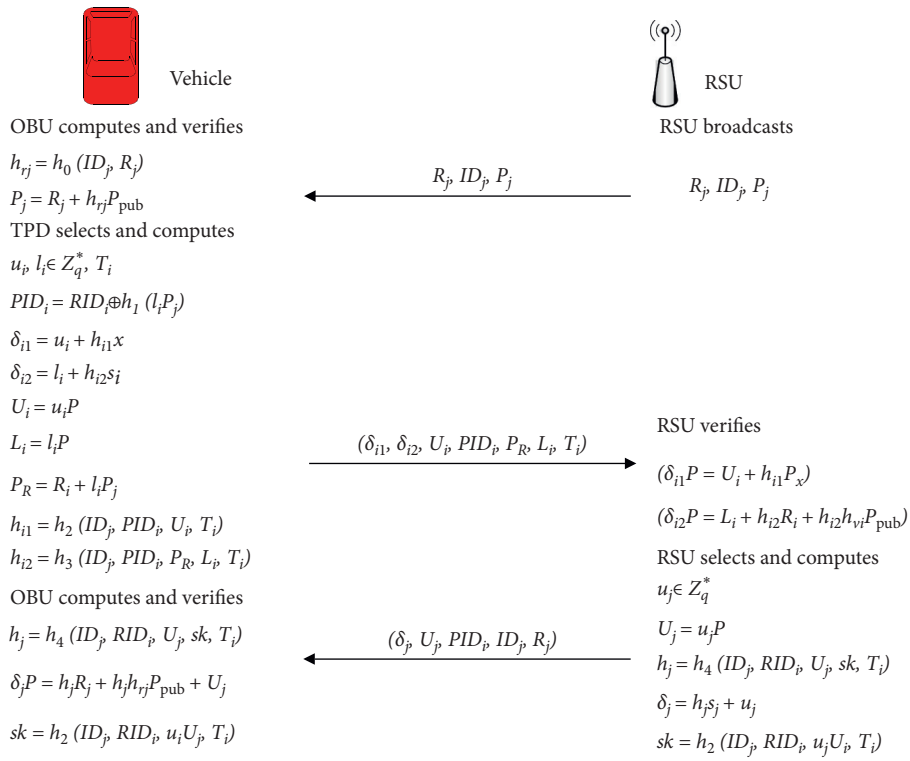

Figure 2: Mutual authentication and key agreement.

Table 1: Notations used.

Notation	Description
E	An elliptic curve
G	An additive group based on E
P	A generator of G
p, q	Large prime numbers
s, P_{pub}	Private key and public key pairs of the system
X, P_x	Group key and group public key pairs
h_0, h_1, h_2, h_3, h_4, h_5	Six secure hash functions
ID_j	Identity of the RSU
s_j, P_j	Private key and public key pairs of the RSU
s_i, P_i	Private key and public key pairs of the vehicle
RID_i	Real identities of the vehicle
PID_i	Pseudonym of the vehicle
T_i, T_m	Timestamp
sk	Session key between RSU and the vehicle
M_i	Traffic-related message

: $\{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \times \{0,1\}^* \longrightarrow Z_q^*$, and h_5: $\{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times \{0,1\}^* \longrightarrow Z_q^*$. TA also broadcasts the system parameters: Paras = $\{E, a, b, p, q, P, P_{pub}, P_x, h_0, h_1, h_2, h_3, h_4, h_5\}$.

3.2. RSU and Vehicle Registration Phase. Roadside unit RSU_j applies to TA for registration. After TA verifies the information of RSU_j successfully, it allocates the identity ID_j to RSU_j. Then, TA selects a random number r_j, computes $h_{rj} = h_0(ID_j, R_j)$ and $R_j = r_jP$. TA also generates the private key $s_j = r_j + h_{rj}s$ and then returns R_j, $s_j$to RSU_j. RSU_j computes $P_j = s_jP$ and verifies whether the following equation holds.

$$P_j = R_j + h_{rj}P_{pub}, \quad \because P_j = s_jP = r_jP + h_{rj}sP = R_j + h_{rj}P_{pub}. \tag{1}$$

If (1) holds, RSU_j broadcasts R_j, ID_j, and P_j. Otherwise, the message is rejected. After RSU broadcasts the public key P_j, the vehicle can use P_j to compute the pseudonym of the vehicle. The detailed process is shown in Section 3.3.

During the registration process, the vehicle users go to TA directly. The vehicle users submit the required information such as identification, phone number, and license, etc., to TA. TA checks whether the vehicle user is qualified. If the vehicle user is qualified, TA allocates a TPD to the vehicle V_i and assigns a unique identity RID_i to the vehicle V_i. TA allows users to set a username and password for TPD. Then, TA chooses a random number r_i and computes $R_i = r_iP$, $h_{vi} = h_0(RID_i, R_i)$, $s_i = r_i + h_{vi}s$, and $P_i = s_iP$. TA saves s_i, x, RID_i, R_i, and P_i in the TPD of the vehicle V_i. At the same time, the vehicle information such as RID_i, R_i, and P_i is saved in AS.

3.3. Authentication and Communication Key Agreement Phase. RSU_j broadcasts R_j, ID_j and P_j; the OBU of the vehicle receives them and verifies whether (1) holds. If it holds, the OBU forwards them to the TPD of the vehicle. The TPD selects the random numbers $u_i, l_i \in Z_q^*$, and the timestamp T_i. The TPD computes the pseudonym$PID_i = RID_i \oplus h_1(l_iP_j)$ and generates the signatures $\delta_{i1} = u_i + h_{i1}x$

and $\delta_{i2} = l_i + h_{i2}s_i$, where $U_i = u_iP$, $h_{i1} = h_2(ID_j, \mathrm{PID}_i, U_i, T_i)$, $L_i = l_iP$, $P_R = R_i + l_iP_j$, and $h_{i2} = h_3(\mathrm{ID}_j, \mathrm{PID}_i, P_R, L_i, T_i)$. It sends $(\delta_{i1}, \delta_{i2}, U_i, \mathrm{PID}_i, P_R, L_i, T_i)$ to RSU_j through the OBU.

RSU_j receives $(\delta_{i1}, \delta_{i2}, U_i, \mathrm{PID}_i, P_R, L_i, T_i)$, and then, it computes $h_{i1} = h_2(\mathrm{ID}_j, \mathrm{PID}_i, U_i, T_i)$ and verifies whether the following equation holds.

$$\begin{aligned} \delta_{i1}P &= U_i + h_{i1}P_x, \\ \because \delta_{i1}P &= u_iP + h_{i1}xP = U_i + h_{i1}P_x. \end{aligned} \tag{2}$$

If (2) holds, RSU_j computes $\mathrm{RID}_i = \mathrm{PID}_i \oplus h_1(s_jL_i)$, $R_i = P_R - s_jl_iP = P_R - s_jL_i$, $h_{\mathrm{vi}} = h_0(RID_i, R_i)$, and $h_{i2} = h_3(\mathrm{ID}_j, \mathrm{PID}_i, P_R, L_i, T_i)$ and verifies whether the following equation holds.

$$\begin{aligned} \delta_{i2}P &= L_i + h_{i2}R_i + h_{i2}h_{\mathrm{vi}}P_{\mathrm{pub}}, \\ \because \delta_{i2}P &= l_iP + h_{i2}(r_iP + h_{\mathrm{vi}}sP), \\ &= L_i + h_{i2}R_i + h_{i2}h_{\mathrm{vi}}P_{\mathrm{pub}}, \end{aligned} \tag{3}$$

if both (2) and (3) hold, the vehicle is legal. RSU_j chooses a random number $u_j \in Z_q^*$ and computes $U_j = u_jP$, $\mathrm{sk} = h_2(\mathrm{ID}_j, \mathrm{RID}_i, u_jU_i, T_i)$, $h_j = h_4(\mathrm{ID}_j, \mathrm{RID}_i, U_j, \mathrm{sk}, T_i)$, and $\delta_j = h_js_j + u_j$. RSU_j sends $(\delta_j, U_j, \mathrm{PID}_i, \mathrm{ID}_j, R_j)$ to the vehicle V_i.

The vehicle V_i receives $(\delta_j, U_j, \mathrm{PID}_i, \mathrm{ID}_j, R_j)$, and then, it computes $h_{\mathrm{rj}} = h_0(\mathrm{ID}_j, R_j)$ and $h_j = h_4(\mathrm{ID}_j, \mathrm{RID}_i, U_j, \mathrm{sk}, T_i)$ and verifies whether the following equation holds.

$$\begin{aligned} \delta_jP &= h_jR_j + h_jh_{rj}P_{\mathrm{pub}} + U_j, \\ \because \delta_jP &= h_js_jP + u_jP = h_jP_j + U_j, \\ &= h_jR_j + h_jh_{rj}P_{\mathrm{pub}} + U_j. \end{aligned} \tag{4}$$

If (4) holds, the vehicle V_i computes $sk = h_2(\mathrm{ID}_j, \mathrm{RID}_i, u_iU_j, T_i)$, which is the session key between V_i and RSU_j.

The process of authentication and key agreement between vehicle and RSU is shown in Figure 2.

3.4. Message Signing Phase. When a vehicle needs to send a message M_i in the area covered by the roadside unit RSU_j, the TPD of the vehicle chooses a random number $v_i \in Z_q^*$ and the timestamp T_m and computes $V_i = v_iP$, $P_v = R_i + v_iP_j$, the pseudonym $\mathrm{PID}_i = \mathrm{RID}_i \oplus h_1(v_iP_j)$, and $\sigma_i = h_{\mathrm{rv}}h_{\mathrm{vi}}^{-1}(s_i + v_i) + h_{\mathrm{mi}}x$, where $h_{\mathrm{rv}} = h_2(M_i, \mathrm{PID}_i, R_{\mathrm{vi}}, T_m)$, $R_{\mathrm{vi}} = h_{\mathrm{vi}}^{-1}(R_i + V_i)$, and $h_{mi} = h_5(M_i, \mathrm{PID}_i, P_v, V_i, R_{\mathrm{vi}}, T_m)$. The TPD then broadcasts the signature $(\sigma_i, M_i, \mathrm{PID}_i, V_i, P_v, R_{\mathrm{vi}}, T_m)$.

3.5. Signature Verification. RSU_j receives $(\sigma_i, M_i, PID_i, V_i, P_v, R_{vi}, T_m)$, and then, it checks whether the timestamp T_m is within the valid time. If it is, RSU_j extracts the real identity of the vehicle $RID_i = PID_i \oplus h_1(s_jV_i)$and computes $R_i = P_v - s_jV_i$, $h_{vi} = h_0(RID_i, R_i)$, $R_{vi} = h_{vi}^{-1}(R_i + V_i)$, $h_{rv} = h_2(M_i, PID_i, R_{vi}, T_m)$, $h_{mi} = h_5(M_i, PID_i, P_v, V_i, R_{vi}, T_m)$, and verifies whether (5) holds.

$$\begin{aligned} h_{\mathrm{vi}}\sigma_iP &= h_{\mathrm{rv}}(R_i + V_i) + h_{\mathrm{rv}}h_{\mathrm{vi}}P_{\mathrm{pub}} + h_{\mathrm{vi}}h_{\mathrm{mi}}P_x, \\ \because h_{\mathrm{vi}}\sigma_iP &= h_{\mathrm{rv}}(s_i + v_i)P + h_{\mathrm{vi}}h_{\mathrm{mi}}xP, \\ &= h_{\mathrm{rv}}(R_i + h_{\mathrm{vi}}sP + V_i) + h_{\mathrm{vi}}h_{\mathrm{mi}}P_x \\ &= h_{\mathrm{rv}}(R_i + V_i) + h_{\mathrm{rv}}h_{\mathrm{vi}}P_{\mathrm{pub}} + h_{\mathrm{vi}}h_{\mathrm{mi}}P_x. \end{aligned} \tag{5}$$

If it holds, RSU_j accepts the message. If it does not, it means that the TPD of the vehicle is damaged. For example, suppose the attackers stole the private and group keys of the TPD, faked the identity RID_i', generated the pseudonym PID_i', forged the signature $(\sigma_i, M_i, \mathrm{PID}_i', V_i', P_v', R_{\mathrm{vi}}', T_m)$, and enabled it to satisfy (6). However, according to the TPD security assumption, this situation is extremely rare. If RSU_j detects that the TPD has been attacked, it immediately broadcasts that the signature $(\sigma_i, M_i, \mathrm{PID}_i', V_i', P_v', R_{\mathrm{vi}}', T_m)$ is not valid.

Other vehicles receive $(\sigma_i, M_i, \mathrm{PID}_i, V_i, P_v, R_{\mathrm{vi}}, T_m)$, and then, they check whether the timestamp T_m is within the valid time. If it is, the vehicles compute $h_{\mathrm{rv}} = h_2(M_i, \mathrm{PID}_i, R_{\mathrm{vi}}, T_m)$ and $h_{mi} = h_5(M_i, \mathrm{PID}_i, P_v, V_i, R_{\mathrm{vi}}, T_m)$ and verify whether the following equation holds.

$$\begin{aligned} \sigma_iP &= h_{\mathrm{rv}}R_{\mathrm{vi}} + h_{\mathrm{rv}}P_{\mathrm{pub}} + h_{\mathrm{mi}}P_x, \\ \because \sigma_iP &= h_{\mathrm{rv}}h_{\mathrm{vi}}^{-1}(s_i + v_i)P + h_{\mathrm{mi}}xP \\ &= h_{\mathrm{rv}}h_{\mathrm{vi}}^{-1}(R_i + h_{\mathrm{vi}}sP + V_i) + h_{\mathrm{mi}}P_x \\ &= h_{\mathrm{rv}}h_{\mathrm{vi}}^{-1}(R_i + V_i) + h_{\mathrm{rv}}P_{\mathrm{pub}} + h_{\mathrm{mi}}P_x \\ &= h_{\mathrm{rv}}R_{\mathrm{vi}} + h_{\mathrm{rv}}P_{\mathrm{pub}} + h_{\mathrm{mi}}P_x. \end{aligned} \tag{6}$$

If it does and the vehicles do not receive an invalid signature broadcasted by RSU_j within the specified time, the vehicles accept the message M_i.

3.6. Identity Extraction. When a valid message signature $(\sigma_i, M_i, \mathrm{PID}_i, V_i, P_v, R_{\mathrm{vi}}, T_m)$ is in dispute, it is necessary to track the real identity of a vehicle. RSU_j can extract the real identity of the vehicle through computing $\mathrm{RID}_i = \mathrm{PID}_i \oplus h_1(s_jV_i)$.

3.7. Updating the Group Key Phase. TA chooses a random number $w_i \in Z_q^*$ and the timestamp T_v and computes $W_i = xw_iP$, $\delta_t = sh_0(xw_iP, T_v) + xw_i$, $P_x = h_3(w_iP, xP, T_v)P$, where P_x is as a new group public key. TA broadcasts the signature $(\delta_t, W_i, T_v, P_x)$.

After the vehicles receive $(\delta_t, W_i, T_v, P_x)$, they compute $x^{-1}W_i$ and verify whether the following equation holds. If it does, the vehicles update the group key as $x = h_3(x^{-1}W_i, xP, T_v)$.

$$\delta_tP = h_0(W_i, T_v)P_{\mathrm{pub}} + xW_i. \tag{7}$$

4. Security Analysis

Under the random oracle model, the security model of [39] is used to prove the security of our scheme.

4.1. Proof of Safety

Lemma 1. *The authentication request message of the vehicle cannot be forged. When ECDLP is a difficult problem, our scheme can resist the forgery attack of adaptive chosen message.*

Proof. We assume that there is an attacker Ad who can successfully forge the request message of a vehicle in polynomial time ε. Given an ECDLP instance $(P, Q = xP, P, Q \in G, x \in Z_q^*)$, the challenger Ch can solve the ECDLP in polynomial time ε.

The challenger *Ch* sets system parameters paras $= \{E_p(a,b), p, q, G, P, P_{\text{pub}}, P_x, h_0, h_1, h_2, h_3, h_4, h_5\}$. Ch randomly chooses RID_i of a vehicle as the identity of the challenger Ch. Ch builds and maintains six hash lists: L_{hl}, where $l = 0, 1, 2, \ldots, 5$. Finally, Ch sends params to Ad.

h_1- *Oracle*. When Ad makes a query with θ, Ch checks whether the tuple (θ, τ_{h1}) is already in L_{h1} or not. If it is, Ch sends τ_{h1} to Ad. Otherwise, Ch randomly selects $\tau_{h1} \in Z_q^*$ and adds $(\theta, \tau_{h1})$to L_{h1}. Finally, Ch sends $\tau_{h1} = h_1(\theta)$ to Ad.

h_2- *Oracle*. When Ad makes a query with $(\text{ID}_j, \text{PID}_i, U_i, T_i)$, Ch checks whether the tuple $(\text{ID}_j, \text{PID}_i, U_i, T_i, \tau_{h2})$ is already in L_{h2} or not. If it is, Ch sends τ_{h2} to Ad. Otherwise, Ch randomly selects $\tau_{h2} \in Z_q^*$ and adds $(\text{ID}_j, \text{PID}_i, U_i, T_i, \tau_{h2})$to L_{h2}. Finally, Ch sends $\tau_{h2} = h_2(\text{ID}_j, \text{PID}_i, U_i, T_i)$ to Ad.

h_3- *Oracle*. When Ad makes a query with $(\text{ID}_j, \text{PID}_i, P_R, L_i, T_i)$, Ch checks whether the tuple $(\text{ID}_j, \text{PID}_i, P_R, L_i, T_i, \tau_{h3})$ is already in L_{h3} or not. If it is, Ch sends τ_{h3} to Ad. Otherwise, Ch randomly selects$\tau_{h3} \in Z_{q^*}$ and adds $(\text{ID}_j, \text{PID}_i, P_R, L_i, T_i, \tau_{h3})$ to L_{h3}. Finally, Ch sends $\tau_{h3} = h_3(\text{ID}_j, \text{PID}_i, P_R, L_i, T_i)$ to Ad.

Extract (RID_i). Ch builds and maintains the list $L_v = (\text{RID}_i, R_i, s_i)$. When Ad makes a query with RID_i and R_i, Ch checks whether the tuple (RID_i, R_i, s_i) is in L_v. If it is, Ch sends $s_i$to Ad. Otherwise, Ch randomly selects $s_i, h_{vi} \in Z_q^*$, lets $R_i = s_iP - h_{vi}P$, and adds them to L_v. Finally, Ch sends $L_v = (\text{RID}_i, R_i, s_i)$ to Ad.

Sign-Oracle. When Ad makes a query with (PID_i, T_i), Ch randomly selects $h_{i1}, h_{i2}, h_{vi}, \delta_{i1}, \delta_{i2} \in Z_q^*$ and sets $U_i = \delta_{i1}P - h_{i1}P_x$, $R_i = s_iP - h_{\text{vi}}P$, $L_i = \delta_{i2}P - h_{i2}R_i - h_{i2}h_{vi}P_{\text{pub}}$, and $P_R = R_i + s_jL_i$. Finally, Ch sends $(\delta_{i1}, \delta_{i2}, U_i, \text{PID}_i, P_R, L_i, T_i)$ to Ad.

Output. Finally, Ad outputs an authentication request message $(\delta_{i1}, \delta_{i2}, U_i, \text{PID}_i, P_R, L_i, T_i)$ with nonnegligible probability. According to the forgery lemma [40],.Ad chooses different h_{i1}' andh_{vi}' and generates another valid authentication request message $(\delta_{i1}', \delta_{i2}', U_i, \text{PID}_i, P_R, L_i, T_i)$ in polynomial time. At this time, the two authentication request messages satisfy the following:

$$\delta_{i1}P = U_i + h_{i1}P_x, \tag{8}$$

$$\delta_{i1}'P = U_i + h_{i1}'P_x, \tag{9}$$

$$\delta_{i2}P = h_{i2}R_i + h_{i2}h_{vi}P_{\text{pub}} + L_i, \tag{10}$$

$$\delta_{i2}'P = h_{i2}R_i + h_{i2}h_{vi}'P_{\text{pub}} + L_i. \tag{11}$$

From (8)–(11), we can obtain

$$(\delta_{i1} - \delta_{i1}')P = (h_{i1} - h_{i1}')P_x, \tag{12}$$

$$(\delta_{i2} - \delta_{i2}')P = (h_{i2}h_{vi} - h_{i2}h_{vi}')P_{\text{pub}}. \tag{13}$$

Now, according to (12) and (13), Ad outputs$x = (\delta_{i1} - \delta_{i1}')(h_{i1} - h_{i2}')^{-1}$, and $s = (\delta_{i2} - \delta_{i2}')(h_{i2}h_{vi} - h_{i2}h_{vi}')^{-1}$.However, solving x or s is an ECDLP problem. Furthermore, it is impossible for an adversary to solve the ECDLP problem in polynomial time. □

Lemma 2. *The authentication response message cannot be forged. Since ECDLP is difficult to solve, our scheme can resist the forgery attack of adaptive chosen message.*

Proof. We assume that there is an attacker Ad who can successfully forge an authentication response message in polynomial time. Given an ECDLP instance $(P, Q = xP, P, Q \in G, x \in Z_q^*)$, then the challenger Ch can solve the ECDLP with nonnegligible probability. The challenger Ch sets system parameters paras $= \{E_p(a,b), p, q, G, P, P_{\text{pub}}, P_x, h_0, h_1, h_2, h_3, h_4, h_5\}$. Ch builds and maintains six lists: L_{hl}, where $l = 0, 1, 2, \ldots, 5$. Finally, Ch sends params to Ad.

h_1-*Oracle*. When Ad makes a query with θ, Ch checks whether the tuple (θ, τ_{h1}) is already in L_{h1} or not. If it is, Ch sends τ_{h1} to Ad. Otherwise, Ch randomly selects $\tau_{h1} \in Z_q^*$ and adds (θ, τ_{h1}) to L_{h1}. Finally, Ch sends $\tau_{h1} = h_1(\theta)$ to Ad.

h_2-*Oracle*. When Ad makes a query with $(\text{ID}_j, \text{RID}_i, u_jU_i, T_i)$, Ch checks whether the tuple $(\text{ID}_j, \text{RID}_i, u_jU_i, T_i, \tau_{h2})$ is already in L_{h2} or not. If it is, Ch sends τ_{h2} to Ad. Otherwise, Ch randomly selects $\tau_{h2} \in Z_q^*$ and adds $(\text{ID}_j, \text{RID}_i, u_jU_i, T_i, \tau_{h2})$ to h_{h22}. Finally, Ch sends $\tau_{h2} = h_2(\text{ID}_j, \text{RID}_i, u_jU_i, T_i)$ to Ad.

Extract (ID$_j$). Ch builds and maintains the list $L_R = (ID_j, R_j, s_j)$. When Ad makes a query with ID_j, Ch checks whether the tuple (ID_j, R_j, s_j) is in L_{R}. If it is, Ch sends $s_j$to Ad. Otherwise, Ch randomly selects$s_j, h_{rj} \in Z_q^*$, lets $R_j = s_jP - h_{rj}P_{\text{pub}}$, and adds $(\text{ID}_j, R_j, s_j)$to L_{R}. Finally, Ch sends $L_R = (\text{ID}_j, R_j, s_j)$ to Ad.

Sign - Oracle. When Ad makes a query with (PID_i, T_i), Ch randomly chooses $sk, h_{r_j}, h_j, \delta_j \in Z_q^*$and sets$U_j = \delta_jP - h_jR_j - h_jh_{rj}P_{\text{pub}}$. Finally, Ch sends $(\delta_j, U_j, PID_i, ID_j, R_j)$ to Ad.

Output. Finally, Ad outputs an authentication request message $(\delta_j, U_j, PID_i, ID_j, R_j)$ with nonnegligible probability. According to the forgery lemma [40].Ad chooses different h_{rj}' and generates another valid authentication request message $(\delta_j', U_j, PID_i, ID_j, R_j)$ in polynomial time. Now, the two authentication request messages satisfy the following:

$$\delta_j P = h_j R_j + h_j h_{rj} P_{\text{pub}} + U_j, \tag{14}$$

$$\delta'_j P = h_j R_j + h_j h'_{rj} P_{\text{pub}} + U_j. \tag{15}$$

From (14) and (15), we can deduce the following expression:

$$\left(\delta_j - \delta'_j\right) P = h_j \left(h_{rj} - h'_{rj}\right) P_{\text{pub}}. \tag{16}$$

Next, Ch can output $s = (\delta_j - \delta'_j)(h_j(h_{rj} - h'_{rj}))^{-1} \bmod q$. However, solving s is an ECDLP, which is impossible for an adversary to solve in polynomial time. □

Theorem 1. *From Lemma 1 and Lemma 2, we know that when the ECDLP problem is difficult to solve, and the adversary cannot forge the authentication request message and response message, that is, our authentication scheme can resist adaptive chosen message forgery attack.*

Theorem 2. *The message signature cannot be forged. Since ECDLP is hard to solve, our scheme can resist the forgery attack of adaptive chosen message attack.*

Proof. We assume that there is an attacker Ad who can successfully forge an authentication response message in polynomial time. Given an ECDLP instance $(P, Q = xP, P, Q \in G, x \in Z_q^*)$, the challenger Ch can solve the ECDLP in polynomial time ε.

The challenger Ch sets system parameters paras $= \left\{E_p(a,b), p, q, G, P, P_{\text{pub}}, P_x, h_0, h_1, h_2, h_3, h_4, h_5\right\}$. Ch randomly chooses ID_j as the identity of the challenger Ch. Ch builds and maintains six lists: L_{hl}, where $l = 0, 1, 2, \ldots, 5$. Then, Ad adaptively queries the oracle machine to Ch, and Ch replies to Ad in the following way.

When Ad makes a query with (PID_i, M_i, T_m), Ch randomly chooses $h_{rv}, h_{mi}, \sigma_i \in Z_q^*$, and $V_i, P_v \in G$; furthermore, it sets $R_{\text{vi}} = h_{rv}^{-1}(\sigma_i P - h_{rv} P_{\text{pub}} - h_{mi} P_x)$. Finally, Ch sends $(\sigma_i, M_i, V_i, P_v, R_{vi}, T_m)$ to Ad.

Subsequently, Ad outputs a valid signature $(\sigma_i, M_i, V_i, P_v, R_{vi}, T_m)$ with a nonnegligible probability. According to the forgery lemma [40], Ad chooses different $h_{\text{mi}}{}'$ and generates another valid signature $(\sigma'_i, M_i, V_i, P_v, R_{vi}, T_m)$ in polynomial time. At this time, the two signatures satisfy the following relationships:

$$\sigma_i P = h_{\text{rv}} R_{\text{vi}} + h_{\text{rv}} P_{\text{pub}} + h_{\text{mi}} P_x, \tag{17}$$

$$\sigma'_i P = h_{\text{rv}} R_{\text{vi}} + h_{rv} P_{\text{pub}} + h'_{\text{mi}} P_x. \tag{18}$$

From (17) and (18), we can obtain the following equation:

$$(\sigma_i - \sigma'_i) P = (h_{mi} - h'_{mi}) P_x. \tag{19}$$

Now, according to (19), Ch can output $x = (\sigma_i - \sigma'_i)(h_{mi} - h'_{mi})^{-1} \bmod q$. However, solving for x is an ECDLP problem, which is impossible for an adversary to solve in polynomial time. Thus, our proposed signature scheme under the random oracle model is resistant against a chosen adaptive message attack. □

Theorem 3. *The key agreement of our scheme is secure under the ECCDH problem.*

Proof. Given an ECCDH instance, $Q_1 = x_1 P, Q_2 = x_2 P$, and $Q_3 = x_1 x_2 P$, where $x_1, x_2 \in Z_q^*$. In our key agreement, we let $Q_1 \longleftarrow U_i = u_i P$, $Q_2 \longleftarrow U_j = u_j P$, $Q_3 \longleftarrow u_i u_j P$. In this method, if the attacker Ad gets $u_i u_j P$ according to U_i, U_j, the key negotiated between the vehicle and RSU can be obtained. However, it is impossible for the adversary to solve the ECCDH problem in polynomial time, implying that the key agreement proposed in this study is secure. □

Theorem 4. *In the random oracle model, we can achieve conditional anonymity and traceability.*

Proof. In the proposed scheme, the authentication request message uses the pseudonym $\text{PID}_i = \text{RID}_i \oplus h_1(l_i P_j)$, where $L_i = l_i P$, $l_i \in Z_q^*$. According to ECDLP, it is not feasible for the adversary to solve $l_i P_j$ without knowing l_i. The request authentication signatures are $\delta_{i1} = u_i + h_{i1} x$ and $\delta_{i2} = h_{i2} s_i + l_i$, where $h_{i1} = h_2(\text{ID}_j, \text{PID}_i, U_i, T_i)$, $h_{i2} = h_3(\text{ID}_j, \text{PID}_i, P_R, L_i, T_i)$, and $u_i, l_i \in z_q^*$ are the random numbers. Every time a vehicle is certified, it can produce unrelated pseudonyms and different authentication requests. Similarly, the pseudonym is also used in message signature $\text{PID}_i = \text{RID}_i \oplus h(v_i P_j)$, $V_i = v_i P$. The message signature is $(\sigma_i, M_i, V_i, P_v, R_{vi}, T_m)$, $\sigma_i = h_{rv}(h_{vi}^{-1}(s_i + v_i)) + h_{mi} x$, $h_{\text{rv}} = h_2(M_i, \text{PID}_i, R_{\text{vi}}, T_m)$, and $h_{\text{mi}} = h_5(M_i, \text{PID}_i, P_v, V_i, R_{\text{vi}}, T_m)$. The pseudonym used in the signature is different every time. Therefore, the scheme can provide anonymity for vehicle users in authentication and message signature. In addition, this scheme can also realize the traceability of the real identity; RSU can calculate the real identity of the vehicle $\text{RID}_i = \text{PID}_i \oplus h_1(s_j L_i)$ through the private key. Similarly, through pseudonym of signature message $\text{PID}_i = \text{RID}_i \oplus h(v_i P_j)$, RSU can also calculate $\text{RID}_i = \text{PID}_i \oplus h_1(s_j V_i)$ using the private key. Therefore, this scheme can realize the traceability of identity. □

Theorem 5. *In the proposed scheme, we can achieve unlinkability.*

Proof. In our scheme, the authentication request message of the vehicle $(\delta_{i1}, \delta_{i2}, U_i, \text{PID}_i, P_R, L_i, T_i)$ is different for each session. Meanwhile, the signature message $(\sigma_i, M_i, \text{PID}_i, V_i, P_v, R_{\text{vi}}, T_m)$ is also different for each message. Therefore, all elements from the message of the vehicle are different, and any attacker cannot tell apart if two different messages from the same vehicle. Thus, our proposed scheme supports unlinkability. □

4.2. Other Security Analysis and Feature Comparison. From Theorem 1 and Theorem 2, it is ascertained that under the random oracle model, the authentication, key agreement, and message signature can resist adaptive chosen message forgery attacks. Additionally, there is no

need for the certification table or TA to participate in the certification between vehicle and RSU. Both authentication and message signature use timestamp, which can resist replay attack. In the authentication process, RSU first checks whether the group key signature is legal, and then, it verifies the vehicle private key signature. If the group key signature is illegal, the signature is discarded directly, which can resist DoS attack to a certain extent. In this scheme, the vehicle is equipped with a TPD, which stores the private key of the vehicle and the group key. Even if a single TPD is attacked, the attacker can only intercept the group key and the private key of the vehicle. The authentication, key agreement, and message signature all need the private key of the vehicle. Thus, the attacker can only forge the signature of a single vehicle, without affecting the communication security of other VANET nodes. The schemes [13, 24] keep the system key in the TPD of each vehicle; this requires a strong TPD security assumption. If a single TPD is successfully attacked, the whole system will not be secure. Table 2 provides the features comparison with other schemes. It can be seen from Table 2 that the proposed scheme has strong advantages in security and communication efficiency.

5. Performance Analysis

In this section, we analyze the computation cost and communication cost of message authentication.

5.1. Computation Performance Analysis. In this study, nonsingular elliptic curve cryptography is used, whereas bilinear pairing construction scheme is utilized in works [13, 24]. To compare at the same security level, we construct two 80 bit security level cryptographic operation schemes. Bilinear pairing cryptographic schemes are set as follows: e: $G_1 \times G_1 \longrightarrow G_2$. $\overline{E}$: $y^2 = x^3 + ax + b \bmod \overline{p}$ is a hyper singular curve with degree 2, where $\overline{p}$ is a 512 bit prime. G_1 is an additive group based on $\overline{E}$ with order $\overline{q}$ and $\overline{P}$ is the generator of G_1 with order $\overline{q}$. The elliptic curve cryptography of the same security level is set as follows: E: $y^2 = x^3 + ax + b \bmod p$ is a nonsuper singular elliptic curve, where p and q are 160 bit primes, $a, b \in Z_p^*$. G is an additive group on E. P is the generator of G with order q. Let T_{bp}, T_{bm}, and T_{ba} denote the execution time of bilinear pairing operation, scalar multiplication operation, and scalar addition operation, respectively. T_{em} and T_{ea} denote the execution time of scalar multiplication and scalar addition on elliptic curve cryptography, and T_H denotes the hash operation time of map-to-point. We use MIRACL cryptographic library, an i5-7200U processor with 2.5 GHz clock frequency and 8 GB memory in our experiment. The operating system is Windows 10. Table 3 provides the average execution time of cryptographic operations.

Next, we analyze the computation cost of the message signature and verification with the protocols given in Table 4. Message signature of LIAP [13] requires five bilinear scalar multiplication operations, one bilinear scalar addition operation, and one map-to-point operation; signature verification requires three bilinear pair operations, one bilinear scalar multiplication operation, and one map-to-point operation. Similarly, we can calculate the computation cost of message signature and signature verification for NECPPA [24], Wu et al.' scheme [6], and our scheme. As given in Table 4, the message signature cost of the vehicle is 2.475 ms in our scheme. Compared with LIAP and NECPPA, the message signature computation cost of our scheme is reduced by 74% and 87%, respectively. However, compared with Wu et al., it costs 1.65 ms more. Compared with LIAP and NECPPA, the cost of signature verification is reduced by 69% and 87%, and it is equal to Wu et al.'s scheme.

Figure 3 presents the comparisons of these computational costs graphically.

5.2. Communication Overhead. It can be seen from the analysis in the previous section that $\overline{p}$ is 64 bytes, G_1 is 128 bytes, and p is 20 bytes, G is 40 bytes. Suppose the timestamp is 4 bytes, the hash function value is 20 bytes, and the other nongroup elements have a value of 20 bytes. The signature message of the proposed method is $(\sigma_i, M_i, PID_i, V_i, P_v, R_{vi}, T_m)$, and the communication length is $20 + 20 + 20 + 40 + 40 + 40 + 4 = 184$ bytes. The signature message of LIAP is $(PID_i, M_s, PK_{Ri}, \sigma_i)$, and the communication length is $128 + 20 + 20 + 128 + 128 = 424$ bytes. The signature message of NECPPA is $(PID_i, \delta_i, M_i, ID_{RSU_j})$, and the communication length is $128 + 20 + 128 + 20 + 20 = 316$ bytes. The signature message of Wu et al.' scheme is $(m_i, PID_{vi}, T_i, T_{vi}, h_{ki}, R_i, \delta_i)$, and the communication length is $20 + 40 + 4 + 4 + 20 + 40 + 20 = 148$ bytes. Compared with LIAP and NECPPA, the proposed scheme can save 57% and 42% of the communication cost, respectively. Compared with Wu et al.' scheme, the communication length is slightly increased by 40 bytes. However, in the scheme proposed by Wu et al., RSU needs to store t pairs of the pseudonyms and local private keys (PID_{vi}, k_{vi}) [6] for each vehicle. When there are too many vehicles, it will cause a heavy burden on the memory of RSU. Similarly, each TPD also needs additional 60t bytes of storage space. The communication cost of message signature is provided in Table 5.

Figure 4 presents the comparisons graphically.

5.3. Comparison with Other Authentication Protocols. Wei et al.' protocols [37] use cosine similarity to realize the authentication for the intelligent and the authentication server. They have less computation cost and better accuracy compared with other implicit authentication schemes. The optimized computation complexity of two protocols is $3O(n^{2.3})$ and $3O(n^{2.3}) + 2Enc_p + Dec_p$, respectively, where n is the dimension of the multimodal behavior feature vector, and Enc_p and Dec_p are Pailler operations; our scheme is based on elliptic curve. Elliptic curve can achieve high security in 160-bit finite field. The complex operation used in our scheme is scalar multiplication operation. The complexity of scalar multiplication operation can be optimized to O (k), where k is the length of the coefficient, which is 160-bit in our scheme. In the process of mutual authentication

Table 2: Features comparison.

Feature	LIAP	NECPPA	Wu et al.	Our scheme
Using bilinear paring operation	Yes	Yes	No	No
Using ideal TPD	Yes	Yes	No	No
Requiring TA to participate in certification	Yes	Yes	Yes	No
Searching database	Yes	Yes	Yes	No

Table 3: Execution time of cryptographic operations.

Execution time	Value (ms)
T_{bp}	7.142
T_{bm}	1.445
T_{ba}	0.041
T_{em}	0.821
T_{ea}	0.006
T_H	2.228

Table 4: Computation cost of signature and verification of single message for various schemes.

Schemes	Message signature (ms)	Signature verification (ms)
LIAP	$5T_{bm} + 1T_{ba} + 1T_H \approx 9.494$	$3\,T_{bp} + 1\,T_{bm} + 1T_H \approx 25.099$
NECPPA	$4T_{bm} + 1T_{ba} + 1T_H \approx 8.049$	$3\,T_{bp} + 1\,T_{bm} + T_H \approx 25.099$
Wu et al.	$1T_{em} \approx 0.821$	$4T_{em} + 2T_{ea} \approx 3.296$
Our scheme	$3T_{em} + 2T_{ea} \approx 2.475$	$4T_{em} + 2T_{ea} \approx 3.296$

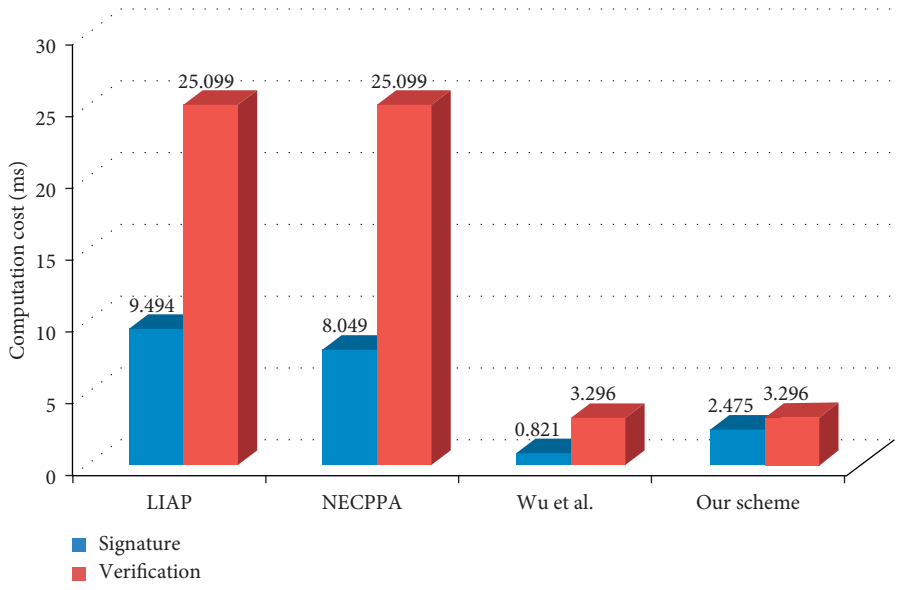

Figure 3: Comparison of computation costs.

between the vehicle and RSU, there are 15 scalar multiplication operations, and the computation complexity is 15O (160). It can be seen from the above analysis that when n is small, the work [37] has an advantage in computation cost, and when n is large, our scheme is better. In addition, in Wei et al.' protocols, the identity of the vehicle U_i is the same in different sessions, so they do not consider the unlinkability of sessions. In our scheme, we use different pseudonyms to realize unlinkability of the sessions.

Vinoth et at.' scheme [38] is a lightweight authentication and key agreement scheme, which is better than our scheme in terms of computation cost, communication cost, and storage cost. However, the scheme does not consider the internal attack. If one sensing device is attacked, the

Table 5: Communication cost of message signature in each scheme.

Schemes	Message signature	Communication overhead (bytes)
LIAP	$\mathrm{PID}_i, M_s, \mathrm{PK}_{\mathrm{Ri}}, \sigma_i$	424
NECPPA	$\mathrm{PID}_i, \delta_i, M_i, \mathrm{ID}_{\mathrm{RSU}_j}$	316
Wu et al.	$m_i, \mathrm{PID}_{\mathrm{vi}}, T_i, T_{\mathrm{vi}}, h_{\mathrm{ki}}, R_i, \delta_i$	148
Our scheme	$\sigma_i, M_i, \mathrm{PID}_i, V_i, P_v, R_{\mathrm{vi}}, T_m$	184

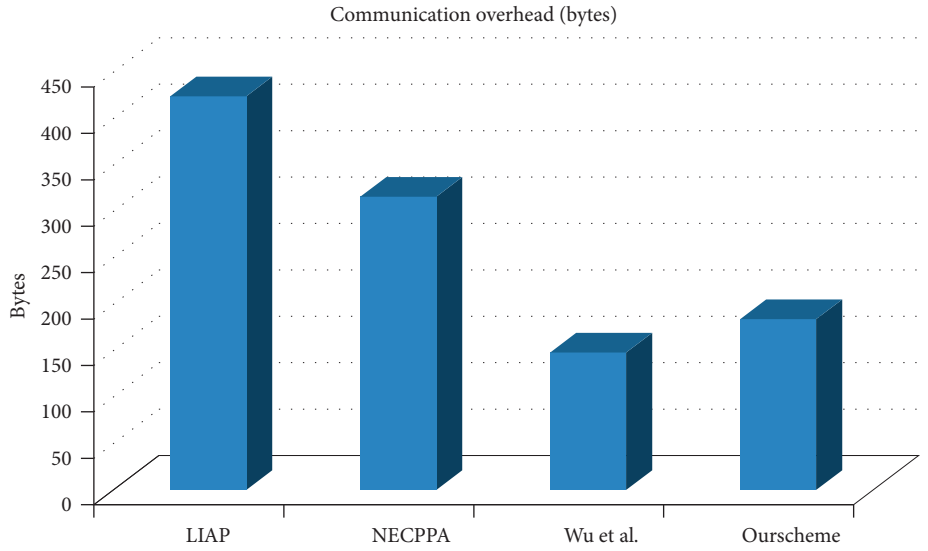

Figure 4: Comparison of communication overhead.

symmetric key $\mathrm{KEY}_{\mathrm{GWN\text{-}Ui}}$ and the session key SK can be obtained by the attacker. The attacker can monitor the communication between the user and the gateway node as well as between the user and other sensing devices. In our scheme, the vehicle is equipped with TPD, which stores the private key of the vehicle and the group key. Even if a single TPD is attacked, the attacker can only intercept the group key and the private key of the vehicle. The authentication, key agreement, and message signature all need the private key of the vehicle. Thus, the attacker can only forge the signature of a single vehicle, without affecting the communication security of other VANET nodes.

6. Conclusion

The instantaneous characteristic of VANET communication requires high efficiency in authentication and key agreement. Therefore, this study proposes an efficient anonymous authentication and key agreement scheme. The scheme includes mutual authentication and key agreement between vehicle and RSU, as well as signature and verification of the vehicle message. In the proposed scheme, an elliptic curve is used to improve the efficiency of computation and communication. Our authentication and key agreement scheme does not need to communicate with the third party authority or establish a local database, and furthermore, it avoids database query operation. It can effectively save the communication time and storage space of related nodes and is more suitable for VANET. Compared with other schemes, this scheme also has strong computing and communication advantages in message authentication. However, we do not address key negotiation and authentication between vehicles and vehicles. Lightweight and effective encryption methods to achieve anonymous authentication and communication between vehicles and vehicles is a worthy research direction. The implementation of anonymous authentication and key agreement based on channel condition is also one of the directions worthy of discussion [41, 42].

In this study, the authentication technology combined with cryptography is mainly presented. At present, deep learning and cloud computing are increasingly used in network applications. In the next step, more technologies such as deep learning [43, 44] and cloud computing can be combined into authentication and privacy protection of VANET.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Natural Science Foundation of Anhui University (KJ2018A0396,

KJ2017B015, KJ2019A0605, and KJ2020A0032), in part by the National Natural Science Foundation of China (61902140), and in part by the Anhui Provincial Natural Science Foundation (1908085QF288).

References

[1] J. Wu and Z. Cai, "Attribute weighting via differential evolution algorithm for attribute weighted naive bayes (WNB)," *Journal of Computational Information Systems*, vol. 7, no. 5, pp. 1672–1679, 2011.

[2] J. Wu, X. Zhu, C. Zhang, and P. S. Yu, "Bag constrained structure pattern mining for multi-graph classification," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 10, pp. 2382–2396, 2014.

[3] M. S. Kakkasageri and S. S. Manvi, "Information management in vehicular ad hoc networks: a review," *Journal of Network and Computer Applications*, vol. 39, pp. 334–350, 2014.

[4] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

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

[6] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, 2017.

[7] C. Cseh, "Architecture of the dedicated short-range communications(DSRC) protocol," in *Proceedings of the 1998 IEEE Conference on Vehicular Technology (VTC)*, May 1998.

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

[9] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1524–1527, 2013.

[10] C. Zhang, X. Lin, R. Lu, and P. H. Ho, "An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proceedings of IEEE International Conference on Communications*, pp. 1451–1457, Phoenix, AZ, USA, 2008.

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

[12] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

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

[14] V. S. Miller, "Use of elliptic curves in cryptography," vol. 218, pp. 417–426, in *Proceedings of CRYPTO: Conference on the Theory and Application of Cryptographic Techniques*, vol. 218, pp. 417–426, Springer, Berlin, Germany, 1986.

[15] 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 the 2008 IEEE Conference on Computer Communications*, pp. 246–250, Phoenix, AZ, USA, April 2008.

[16] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: an anonymous batch Authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.

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

[18] 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.

[19] H. Wang and Y. Zhang, "On the security of an anonymous batch authenticated and key agreement scheme for value-added services in VANETs," *Procedia Engineering*, vol. 29, no. 4, pp. 1735–1739, 2012.

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

[21] M. Azees and P. Vijayakumar, "CEKD: computationally efficient key distribution scheme for vehicular ad-hoc networks," *Australian Journal of Basic and Applied Sciences*, vol. 10, no. 2, pp. 171–175, 2016.

[22] P. Vijayakumar, V. Chang, L. Jegatha 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.

[23] M. A.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.

[24] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: a novel and efficient conditional privacy-preserving authentication scheme for VANET," *Computer Networks*, vol. 134, pp. 78–92, 2018.

[25] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs," *Vehicular Communications*, vol. 22, 2019.

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

[27] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-Hoc Network," *IEEE Access*, vol. 7, pp. 71424–71435, 2019.

[28] Y. Ming and X. Shen, "PCPA: a practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks," *Sensors*, vol. 18, no. 5, p. 1573, 2018.

[29] 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.

[30] 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.

[31] 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.

[32] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 2241–2250, 2017.

[33] 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.

[34] P. Vijayakumar, A. Bose, and A. Kannan, "Chinese remainder theorem based centralised group key management for secure multicast communication," *IET Information Security*, vol. 8, no. 3, pp. 179–187, 2014.

[35] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: a hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Vehicular Communications*, vol. 14, pp. 15–25, 2018.

[36] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "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, pp. 722–735, 2019.

[37] F. Wei, S. Zeadally, P. Vijayakumar, N. Kumar, and D. He, "An intelligent terminal based privacy-preserving multimodal implicit authentication protocol for Internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2020.

[38] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure multifactor Authenticated key agreement scheme for industrial IoT," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3801–3811, 2021.

[39] W.-B. Hsieh and J.-S. Leu, "An anonymous mobile user authentication protocol using self-certified public keys based on multi-server architectures," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 133–148, 2014.

[40] D. Pointcheval and J. Stern, "Security proofs for signature schemes," *Advances in Cryptology*, vol. 4, pp. 387–398, 1996.

[41] K. Li, W. Ni, Y. Emami et al., "Design and implementation of secret key agreement for platoon-based vehicular cyber-physical systems," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 2, 2019.

[42] K. Li, L. Lu, W. Ni, E. Tovar, and M. Guizani, "Secret key agreement for data dissemination in vehicular platoons," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9060–9073, 2019.

[43] J. Wu, S. Pan, X. Zhu, and Z. Cai, "Boosting for multi-graph classification," *IEEE Transactions on Cybernetics*, vol. 45, no. 3, pp. 416–429, 2015.

[44] F. Liu, S. Xue, J. Wu et al., "Deep learning for community detection: progress, challenges and opportunities," in *Proceedings of the 29th International Joint Conference on Artificial Intelligence (IJCAI 20)*, pp. 4981–4987, Yokohama, Japan, 2020.