Hindawi
Security and Communication Networks
Volume 2022, Article ID 3116682, 13 pages
https://doi.org/10.1155/2022/3116682

Research Article

An Authentication and Key Agreement Scheme Based on Roadside Unit Cache for VANET

Sun Mei,[1,2] **Guo Yuyan**,[1] **Zhang Juan**,[1] **and Jiang Mingming**[1]

[1]*School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, China*
[2]*School of Information and Control Engineering, China University of Mining and Technology, Xuzhou 221008, China*

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

Received 22 March 2022; Revised 24 June 2022; Accepted 6 July 2022; Published 8 August 2022

Academic Editor: M. Azees

Vehicular Ad Hoc Network (VANET) is a wireless Mobile Ad Hoc Network that is used for communication between vehicles, vehicles and fixed access points, and vehicles and pedestrians. However, because of the use of open wireless channels, VANET is more vulnerable. Therefore, VANET security is critical for safe driving and user privacy protection. Authentication and key agreement are crucial for ensuring security. Numerous authentication schemes have been proposed between vehicles and roadside units (RSUs). Many solutions are authentication and key negotiation between the vehicle and a single RSU. The vehicle passing through a region needs to complete authentication and key agreement with multiple RSUs separately, which brings a great burden to the vehicle. In order to simplify the authentication process of vehicles and multiple RSUs and improve the efficiency of authentication and key agreement, an efficient authentication and key agreement scheme based on RSU cache is proposed when the vehicle moves from one RSU to another RSU region. In the proposed scheme, RSUs are divided into regions, and each region has a RSU cluster head. When the vehicle enters a certain region and authenticates with a RSU successfully, the RSU submits the authentication information to the RSU cluster head. The RSU cluster head shares the authentication information with other RSUs in the region using the shared key. Other RSUs record the authentication information in the cache. When the vehicle communicates with other RSUs, the authentication is not necessary; the session key can be negotiated by simply exchanging information. After using the cache, the calculation and communication cost of the authentication and key negotiation between the vehicle and other RSU can be significantly saved, the calculation cost is reduced by 37%, and the traffic is reduced by 35%. The random oracle model is used to prove the security of the scheme. The results revealed that the authentication overhead of the proposed scheme is considerably lower than those of other schemes. Compared with the related schemes, the computational cost of the proposed scheme is reduced by 34% on average; the communication cost is close to other related schemes. Moreover, the security analysis shows that the proposed scheme provides better security compared to other related schemes.

1. Introduction

VANETs can be used to obtain timely report road condition information, query road condition information, plan travel routes, improve travel efficiency, and reduce road congestion and traffic accidents. VANETs can facilitate traffic optimization and safe transportation. VANET security is critical because security messages contain life-critical information. Using open wireless modules, VANETs are vulnerable to various types of attacks. These attacks may not only affect the use of network communication and network services but also pose a threat to people's lives and property. The main components of VANET are roadside units (RSUs), a trust agency (TA), onboard units (OBUs), and application servers (ASs) [1]. The TA is responsible for system initialization and providing system parameters, including the private-public key pair; RSUs are placed on both sides of the road to function as vehicle routers or Internet access points; OBU is a microwave device which is installed on the vehicle to realize vehicle-to-RSU or vehicle-to-vehicle communication. Data storage and various application services of VANET are realized by ASs. IEEE802.11p is a short range communication protocol (DSRC) [2] to achieve vehicle-to-RSU and vehicle-to-vehicle communication.

1.1. Related Works. To address the security problems, such as message integrity and privacy protection of VANET, authentication and key agreement have been introduced into VANET. Some logic operations and hash functions are generally used in lightweight protocols to complete authentication and key agreement. Computation is considerably lower than those of the bilinear pairing and elliptic-curve-based authentication schemes. Wazid et al. [3] designed a lightweight no-center service authentication and key negotiation protocol for VANET in which similar vehicles are aggregated into a cluster to realize authentication types, such as vehicle-to-vehicle, vehicle-to-cluster head, and cluster head-to-RSU communication. However, all vehicles and RSUs prestore the same keys x and x', which cannot provide satisfactory defense against internal node attacks. Vijayakumar et al. [4] proposed a lightweight authentication and group key agreement protocol using a symmetric cryptosystem. The scheme is used to realize the authentication of a vehicle and RSUs through the shared key between the vehicle and TA and the shared key between RSU and TA. After successful authentication, the vehicle signs the message using the authentication code encrypted by group and TA private keys. This scheme involves limited calculation and exhibits high authentication efficiency. However, TA needs to query the key list of all vehicles or RSUs during the authentication. Zhong et al. [5] proposed an authentication and key negotiation scheme based on hash function and registration list. In this scheme, the vehicle and TA, RSU and TA have shared keys, and the authentication and key negotiation between the vehicle and RSU are completed through TA. The computational overhead of this scheme is considerably lower than other schemes. Although this scheme requires TPD support, strong security assumptions are not required. Islam et al. [1] proposed a lightweight authentication scheme combining passwords with group keys. Paliwal et al. [6] proposed a lightweight vehicle-to-RSU authentication scheme based on dynamic password; however "$publicidentifier_{OBU}$" is unchanged in the authentication process. Cui et al. [2] proposed a scheme based on hash function and group key negotiation, which exhibits high computational efficiency. Zhang and Wen [7] also proposed a lightweight authentication and key negotiation scheme based on XOR and hash functions. Schemes based on [1, 2, 6, 7] require TA to participate in the authentication, and they cannot satisfy the unlinkability of authentication in VANET. Li et al. [8] proposed a lightweight authentication and key agreement protocol based on hash function and XOR operation. However, the authentication between vehicle and RSU should be completed through TA, which requires TAs to continuously generate pseudonyms for vehicles. A study [9] revealed that the scheme proposed by Li et al. cannot resist RSU counterfeiting attacks. And, the anonymity and untraceability of vehicles are not guaranteed. Alfadhli et al. [10] proposed a lightweight vehicle and RSU authentication scheme using general hash function. However, "CR_i" [10] of the vehicle remains unchanged during every authentication in the scheme. Therefore, the vehicle is easy to be tracked. Lee et al. [11] proposed a lightweight authentication and key agreement protocol for cloud computing of Internet of vehicles. However, the HID_i [11] of the vehicle remains unchanged during the authentication process, and the vehicle can be easily tracked. In [12], a lightweight VANET authentication and key agreement scheme was proposed. In the scheme, the CA is distributed in multiple regions, and the shared key in one region is obtained through vehicle and CA authentication. However, the authentication between vehicle and RSU is not considered. In a study [13], an authentication protocol for hiding path information from TA was proposed. After successful authentication, the vehicle obtains the keys from TA. The keys are shared between the vehicle and multi-RSU. In this scheme, the path information of the vehicle is hidden by the matrix transformation to protect the vehicle privacy. However, the calculation cost of the scheme is large. Lightweight authentication and key agreement schemes for VANET exhibit excellent computing performance. However, the centralized authentication of TA or CA is required, which is not suitable for large-scale VANETs. Such schemes cannot satisfy high security requirements. Recently, researchers have proposed schemes using public key cryptosystems for VANET authentication and key agreement. Li et al. [14] proposed an authentication and key agreement scheme between vehicles using the private key. In this scheme, bilinear pairing operation is not required. It has high protocol efficiency. However, the scheme cannot satisfy the authentication anonymity of VANETs because the vehicle identification is directly transmitted. In [15, 16], V2V authentication and key agreement schemes based on identity are proposed. The session key is obtained from the vehicles through the private key. However, the communication unlinkability of VANETs is not considered in these schemes. Bayat et al. [17] proposed a public key authentication scheme based on RSU to realize the authentication and key negotiation between the vehicle and RSU. In the scheme, the system key is preinstalled in the TPD of the RSU, the vehicle encrypts and transmits the real name to the RSU using the system public key, and the RSU decrypts the real name of the vehicle using the system key. After verifying that the real name is legal, multiple private keys and shared keys are generated by the RSU for the vehicle. However, in this scheme, bilinear pair operation is required, and considerable authentication calculation is involved. Alazzawi et al. [18] proposed an authentication and key agreement scheme between the vehicle and RSUs. TA prestores the system key in the TPD of RSU. After the vehicle is successfully authenticated, the system key is used in RSAs to generate the private key "sk" for the vehicle. When the vehicle communicates with other RSUs, only "sk" needs to be updated without further authentication. The scheme is implemented using an elliptic curve without bilinear pair operation, and the computational performance is considerably improved. However, system key "s" can be calculated from the key "sk" in the OBU; if the system key "s" is leaked, the scheme security is compromised. Currently, the authentication and key agreement of V2I in VANETs mainly solve the authentication and key agreement from vehicle to RSU. When the vehicle passes through each RSU, numerous authentications and key negotiations are required. TA can perform

limited authentications, which can easily result in authentication bottlenecks. To improve V2I authentication efficiency, Xie et al. [19] proposed an authentication and key agreement scheme for VANETs with multiserver architectures. In the scheme, a server cluster is constructed on VANETs, and information is shared between servers. One-time server authentication is required, and the session key is negotiated after successful authentication. Although this scheme has high authentication efficiency, strong TPD security assumptions are required. In [20], an authentication and key agreement protocol was proposed for VANET roaming. In the protocol, there are local and foreign areas, and the tow proxy servers are set in both areas, respectively. The vehicle and the local agent as well as the local agent and the foreign agent are preinstalled with shared keys. When a vehicle enters a foreign area, authentication information is transmitted to the local agent through the foreign agent for authentication. The authentication is completed using the local agent. The proposed protocol is insecure against a MITM attack, impersonation attack, and KCI attack [21]. Centralized authentication and key agreement through cloud server are realized in a few schemes [19, 20]. However, when the server is far from the vehicle and many instantaneous vehicles are present, authentication delay may occur. To address this challenge, Ma et al. [22] proposed an authentication and key agreement scheme for VANET based on fog computing, in which some network services are dispersed to the fog server of the network edge. In the scheme, the authentication between vehicle and fog server is completed using cloud computing servers. However, communication between vehicles and RSUs is not considered.

At present, many scholars have proposed some other new authentication and key agreement schemes for VANET. Li et al. [23] proposed a VANET authentication key agreement scheme combined with blockchain, which meets the requirements of anticollusion attack and unlinkability of VANET. In [24], a many-to-many authentication and key negotiation scheme between vehicles and cloud servers is proposed. Zhang et al. [25] proposed a drone-assisted authentication and key agreement scheme between vehicle and control center. In [26], a cache-based access control scheme for vehicle and cloud services based on SDN is proposed.

The RSU is closest to the vehicle, and it can provide timely and fast services to the vehicle. However, the authentication and communication of vehicles and RSUs are not considered in much literature. In many proposed authentication and key agreement schemes between vehicles and RSUs, the authentication and key agreement between the vehicle and a single RSU are only considered; the vehicle passing through a region needs to complete authentication and key negotiation with multiple RSUs separately, which brings a great burden to the vehicle, which considerably increases communication and computing burden. In this study, an efficient authentication and key agreement scheme between vehicle and multiple RSUs based on RSU cache is proposed when the vehicle moves from one RSU to another RSU region. RSUs are divided into numerous regions. Each region has a cluster head. The cluster head has high security and can be completed by the sub-TA. The cluster head forms a group with RSUs in the region. When a vehicle enters an area, authentication and negotiation can be performed with any RSU. After successful authentication, part of the authentication information is shared among RSUs in the area through the cluster head. Each RSU sets the security cache to store the authentication information between the vehicle and the RSU, and the authentication information has the survival time. In the survival time, authentication is not required when the vehicle moves from one RSU to another RSU region. The vehicle can negotiate session keys directly with other RSUs. This solution not only solves the problem of repeated authentication and key agreement between vehicles and RSUs but also avoids the problem that vehicles can only authenticate with cloud services.

1.2. Our Contributions. In this study, a temporary cache method was constructed to optimize the authentication scheme of vehicles and RSUs. After using the cache, the calculation and communication cost of the authentication and key negotiation between the vehicle and other RSU can be significantly saved, the calculation cost is reduced by 37%, and the traffic is reduced by 35%. In terms of security performance, this scheme does not require strong security support of TPD, and querying the database during authentication and key agreement is not required.

The main contributions of this study are as follows.

(1) We simplify the authentication and key negotiation process between vehicles and multiple RSUs by establishing a group for RSUs and sharing authentication information securely within the group.

(2) In negotiation, the efficiency of key agreement is improved by using secure cache in RSU.

(3) The vehicle and RSU authenticate anonymously through their private keys. We avoid saving the system key in the TPD of RSUs and vehicles. In this study, the strong security of the TPD is not required to support the storage of the system key.

(4) Dual-system keys s_1 and s_2 are used in this study. Different keys are used in different occasions. If a single key is cracked, the security of other occasions will not be affected and the overall security of the system will be enhanced.

2. Background Knowledge

2.1. Elliptic Curve. Let F_p represent a finite field of order p and E be an elliptic curve E: $y^2 = x^3 + ax + b \bmod p$. Let G be a finite cyclic group with order q on E, and P be the generator, and O be an infinite point.

G has the following properties:

(1) Addition ($\pm$). P, Q are two points on G; if $P \neq Q$, $R = P + Q$, then R is the intersection of the straight line passing through P and Q; if $P = Q$, $R = P + Q$, then R is the tangent intersection of E and P, Q; if $P = -Q$, then $P + Q = P - P = O$.

(2) Scalar multiplication (.). Let $m \in Z_q^*$; then the scalar multiplication of P is $m.P = P + P + \cdots P$ (m times in total).

Two difficult problems are defined as follows:

Define 1 elliptic curve discrete logarithm problem (ECDLP); let Q be a random point on G; the ECDLP problem is to calculate x satisfying $Q = xP$, where $x \in Z_q^*$.

Define 2 elliptic curve calculation Diffie-Hellman problem (ECCDH), for $P, aP, bP \in G$, where $a, b \in Z_q^*$ are unknown. The ECCDH problem is to calculate abP.

If ECDLP or ECCDH on group G cannot be solved with nonnegligible probability in time t, ECDLP or ECCDH is difficult problem on the elliptic curve.

2.2. Network Model. In the network model in this study, as shown in Figure 1, TA is a trusted service center with strong security. RSUs are installed on both sides of the road to provide access services for vehicles. Each vehicle is equipped with an OBU to communicate with RSUs or other vehicles. OBUs communicate wirelessly with RSUs through DSRC protocol. TA establishes system parameters, and it is the registration of RSUs and vehicles and generates private-public key pairs for RSUs and vehicles; TA establishes clusters for RSUs and specifies a cluster head for each cluster. The security of the cluster head is higher than that of other RSUs. RSUs in the cluster form a communication group. When the vehicle releases messages to the VANET or receives various services provided by the VANET, the vehicle and RSU first complete authentication and key negotiation.

3. Proposed Scheme

The scheme includes system initialization, RSU and vehicle registration, RSU group establishment, vehicle and RSU authentication and key negotiation, and vehicle and other RSU key negotiations. The main notations used are shown as Table 1.

3.1. System Initialization. In TA, two random numbers s_1, s_2 are selected as the system keys, and system public keys $P_{\text{pub1}} = s_1 P, P_{\text{pub2}} = s_2 P \in G$ are computed, and TA selects seven secure hash functions: $h_0: \{0,1\}^* \times G \longrightarrow Z_q^*$, $h_1: \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \times \{0,1\}^* \longrightarrow Z_q^*$, $h_2: \{0,1\}^* \times G \times \{0,1\}^* \longrightarrow Z_q^*$, $h_3: \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \longrightarrow Z_q^*$, $h_4: \{0,1\}^* \times \{0,1\}^* \times G \times G \times \{0,1\}^* \longrightarrow Z_q^*$, $h_5: \{0,1\}^* \times \{0,1\}^* \times G \longrightarrow Z_q^*, h_6: G \times G \times \{0,1\}^* \longrightarrow Z_q^*$. TA divides RSUs into an RSU group and assigns a cluster head to each group. The cluster head has strong security. TA assigns TPD to each cluster head and preinstalls the system key s_2, the group key g, group identification ID_g, and system parameters in the TPD of the cluster head.

3.2. Registration. The roadside unit RSU_j performs offline authentication with TA. After TA successfully reviews RSU_j, it is divided into corresponding groups according to the area, which is designated as ID_g, and the group key is g; furthermore, TA assigns a TPD to RSU_j. TA assigns identity ID_j to RSU_j, selects a random number r_j, computes $R_j = r_j P$, calculates the private key $s_j = s_1 h_0(ID_j, R_j) + r_j$ for RSU_j, where the public key of RSU_j is $P_j = h_0(ID_j, R_j) P_{\text{pub1}} + R_j$, and saves $s_j, g, P_j, R_j, ID_j, ID_g$, including the system parameters in the TPD of RSU_j. The cluster head can obtain the private key s_g and public key P_g through registration.

The vehicle Ve_i applies to TA for registration and TA reviews the identity, license, and other information of the vehicle. If the vehicle satisfies the requirements, TA assigns a TPD to the vehicle, selects a random number r_i, computes $R_i = r_i P$, calculates the private key $s_i = s_1 h_0(RID_i, R_i) + r_i$ for Ve_i, where the public key of Ve_i is $P_i = h_0(RID_i, R_i) P_{\text{pub1}} + R_i$, saves s_i, RID_i, R_i, P_i, and system parameters in the TPD of Ve_i, and saves the real identity RID_i, the public key P_i, and other registration information of the vehicle in the application database (AS).

3.3. Establishing the RSU Group. In the cluster head TA_g of the group where RSU_j is located, n mutually prime numbers $k_1, k_2, k_3 \cdots k_n$ are selected, $Mu = \sum_{j=1}^{n} k_j$, $Mu_j = Mu/k_j$ are calculated, and b_j is obtained so that b_j satisfies $b_j Mu_j \equiv 1 \bmod k_j$ to compute $\gamma = \sum_{j=1}^{n} b_j Mu_j$.

TA_g negotiates the session key with RSU_j.

RSU_j selects a random number u_j and computes $\sigma_j = s_j h_1(ID_j, g, U_j, ID_g, T_{s1}) + u_j$, $U_j = u_j P$ where T_{s1} is the current timestamp. RSU_j sends $(\sigma_j, ID_j, R_j, U_j, T_{s1})$ to the cluster TA_g. After receiving the message, TA_g verifies whether equation (1) is true. If the equation is true, a random number u_g is selected, TA_g computes $sk_{gj} = h_1(ID_j, g, u_g U_j, ID_g, T_{s1})$, $\sigma_g = s_g h_2(ID_g, U_g, sk_{gj}) + u_g$, $U_g = u_g P$, and sends (σ_g, U_g) to RSU_j.

TA_g obtains the session key $sk_{gj} = h_1(ID_j, g, u_g U_j, ID_g, T_{s1})$.

$$\sigma_j P = h_0\left(ID_j, R_j\right) h_1\left(ID_j, g, U_j, ID_g, T_{s1}\right) P_{\text{pub1}} + h_1\left(ID_j, g, U_j, ID_g, T_{s1}\right) R_j + U_j. \tag{1}$$

The proof of equation (1):

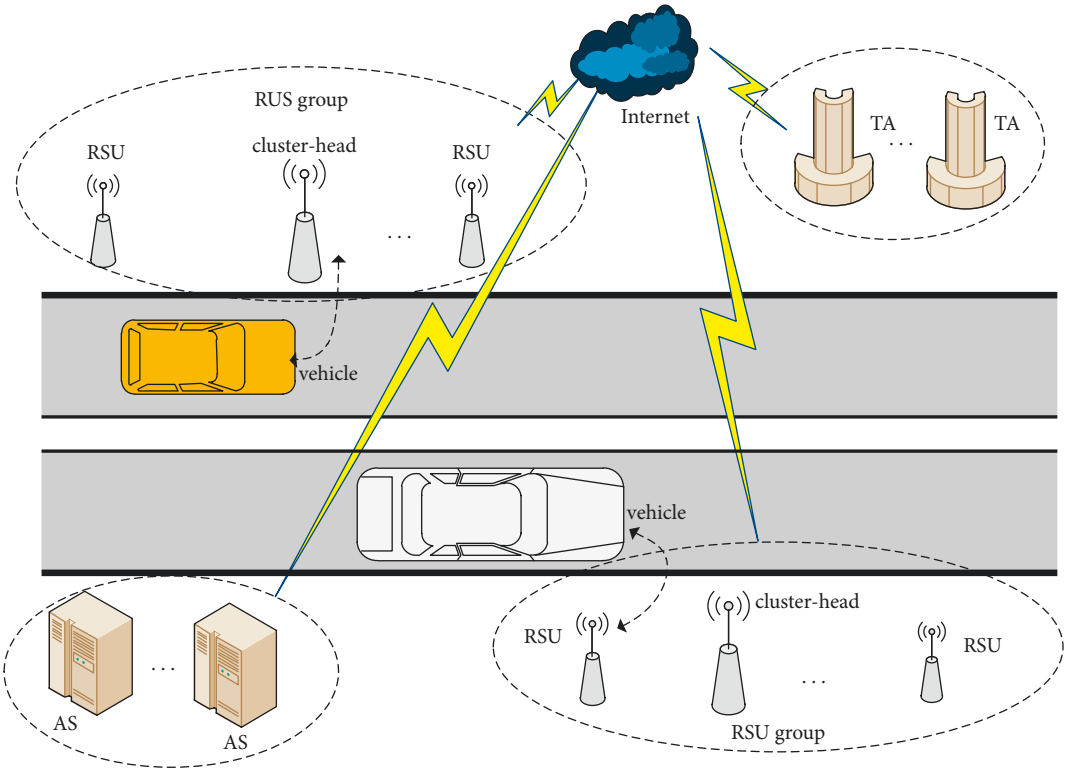

Figure 1: VANET network model.

Table 1: The notations used.

Notation	Description
E	Elliptic curve
G	A finite cyclic group with order q on E
TA_g	The cluster head
$s_1, s_2, P_{pub1}, P_{pub2}$	System private and public keys
$h_0, h_1, h_2, h_3, h_4, h_5, h_6$	Hash functions
g	The group key
ID_g	Group identification
s_j, P_j	The private key and public key of RSU
s_m, P_m	The private key and public key of other RSU
s_i, P_i	The private key and public key of the vehicle
ID_i, ID_j	The vehicle identification and RSU identification
RID_i, PID_i	Real identity and pseudonym of the vehicle
T_{s1}, T_{s2}, T_{s3}	Timestamp
sk_{gj}	The session key between the cluster head and RSU
sk_{rv}	The session key between RSU and the vehicle
sk_{im}	The session key between the vehicle and other RSU
$r_j, r_i, r_m, u_j, u_g, v_j, v_i, v_m, z_i$	The random numbers

$$\begin{aligned}\sigma_j P &= s_j h_1\left(ID_j, g, U_j, ID_g, T_{s1}\right)P + u_j P \\ &= \left(s_1 h_0\left(ID_j, R_j\right) + r_j\right)h_1\left(ID_j, g, U_j, ID_g, T_{s1}\right)P + u_j P \\ &= h_0\left(ID_j, R_j\right)h_1\left(ID_j, g, U_j, ID_g, T_{s1}\right)P_{\text{pub1}} + h_1\left(ID_j, g, U_j, ID_g, T_{s1}\right)R_j + U_j.\end{aligned} \tag{2}$$

After RSU_j receives (σ_g, U_g), $sk_{gj} = h_1(ID_j, g, u_j U_g, ID_g, T_{s1})$ is calculated to verify whether equation (3) is true, if so. RSU_j gets the session key sk_{gj}.

$$\sigma_g P = h_0\left(ID_g, R_g\right)h_2\left(ID_g, U_g, sk_{gj}\right)P_{\text{pub1}} + h_2\left(ID_g, U_g, sk_{gj}\right)R_g + U_g. \tag{3}$$

The proof of equation (3):

$$\begin{aligned}\sigma_g P &= \left(s_g h_2\left(ID_g, U_g, sk_{gj}\right) + u_g\right)P \\ &= s_g h_2\left(ID_g, U_g, sk_{gj}\right)P + u_g P \\ &= \left(s_1 h_0\left(ID_g, R_g\right) + r_g\right)h_2\left(ID_g, U_g, sk_{gj}\right)P + U_g \\ &= h_0\left(ID_g, R_g\right)h_2\left(ID_g, U_g, sk_{gj}\right)P_{\text{pub1}} + h_2\left(ID_g, U_g, sk_{gj}\right)R_g + U_g.\end{aligned} \tag{4}$$

TA_g encrypts k_j with the session key sk_{gj} and sends $E_{sk_{gj}}(k_j)$ to RSU_j. RSU_j decrypts $E_{sk_{gj}}(k_j)$ with the session key sk_{gj} to obtain k_j.

3.4. Authentication and Session Key Negotiation between Vehicle and RSU. RSU_j selects a random number v_j and calculates $\mu_j = s_j h_3(ID_j, ID_g, V_j, T_{s2}) + v_j$, $V_j = v_j P$. RSU_j broadcasts message $(\mu_j, P_j, ID_j, ID_g, R_j, V_j, T_{s2})$ in the coverage area, where T_{s2} indicates the current timestamp.

After the vehicle Ve_i receives the message, it checks whether the time stamp of $RSU_j T_{s2}$ has expired; if not, it verifies whether the following equation holds.

$$\mu_j P = h_0\left(ID_j, R_j\right)h_3\left(ID_j, ID_g, V_j, T_{s2}\right)P_{\text{pub1}} + h_3\left(ID_j, ID_g, V_j, T_{s2}\right)R_j + V_j. \tag{5}$$

The proof of equation (5):

$$\begin{aligned}\mu_j P &= \left(s_j h_3\left(ID_j, ID_g, V_j, T_{s2}\right) + v_j\right)P \\ &= s_j h_3\left(ID_j, ID_g, V_j, T_{s2}\right)P + v_j P \\ &= \left(s_1 h_0\left(ID_j, R_j\right) + r_j\right)h_3\left(ID_j, ID_g, V_j, T_{s2}\right)P + V_j \\ &= h_0\left(ID_j, R_j\right)h_3\left(ID_j, ID_g, V_j, T_{s2}\right)P_{\text{pub1}} + h_3\left(ID_j, ID_g, V_j, T_{s2}\right)R_j + V_j.\end{aligned} \tag{6}$$

If true, the vehicle Ve_i selects a random number v_i, calculates pseudonym $PID_i = RID_i \oplus h_0(T_{s2}, v_i P_{\text{pub2}})$, calculates $V_i = v_i P$, $sk_{rv} = h_3(ID_j, PID_i, v_i V_j, T_{s2})$, $P_R = R_i + v_i P_{\text{pub2}}$, $\mu_i = h_4(ID_j, PID_i, V_i, P_R, sk_{rv})s_i + v_i$, and sends $(PID_i, P_R, V_i, \mu_i, T_{s2})$ to RSU_j.

After RSU_j receives the message, it checks whether timestamp T_{s2} has expired. If it has not expired, RSU_j sends $E_{sk_{gj}}(PID_i, P_R, V_i, T_{s2})$ to TA_g, where $E_{sk_{gj}}$ represents a function for symmetric encryption using the shared key sk_{gj} of TA_g and RSU_j.

After TA_g receives the message, it checks whether timestamp T_{s2} has expired. If not, the following calculation is performed: $RID_i = PID_i \oplus h_0(T_{s2}, v_i P_{\text{pub2}})$, $R_i = P_R - s_2 V_i$, $P_i = h_0(RID_i, R_i)P_{\text{pub1}} + R_i$, then $E_{sk_{gj}}(P_i, T_{s2})$ is sent to RSU_j, RSU_j decrypts $E_{sk_{gj}}(P_i, T_{s2})$ to obtain (P_i, T_{s2}), and RSU_j calculates $sk_{rv} = h_3(ID_j, PID_i, v_j V_i, T_{s2})$ and verifies whether equation (7) holds.

$$\mu_i P = h_4\left(ID_j, PID_i, V_i, P_R, sk_{rv}\right)P_i + V_i. \tag{7}$$

If equation (7) holds, RSU_j sends $E_{sk_{gj}}(PID_i, T_{s2})$ to TA_g.

The proof of equation (7):

$$\begin{aligned}\mu_i P &= \left(h_4\left(ID_j, PID_i, V_i, P_R, sk_{rv}\right)s_i + v_i\right)P \\ &= h_4\left(ID_j, PID_i, V_i, P_R, sk_{rv}\right)s_i P + V_i \\ &= h_4\left(ID_j, PID_i, V_i, P_R, sk_{rv}\right)P_i + V_i.\end{aligned} \tag{8}$$

After receiving the message, TA_g selects a random number w_c and calculates $w_c\gamma$, and TA_g broadcasts $w_c\gamma$, $E_{w_c}(h_5(RID_i, T_{s2}, P_i), T_{s2}, P_i)$ in the RSU group. Another RSU node RSU_i uses k_i to calculate $w_c = w_c\gamma \bmod k_i$. Furthermore, RSU_i decrypts $E_{w_c}(h_5(RID_i, T_{s2}, P_i), T_{s2}, P_i)$ with w_c to obtain $(h_5(RID_i, T_{s2}, P_i), T_{s2}, P_i)$ and records it in RSU_i cache. RSU cache is shown as Table 2.

The vehicle Ve_i obtains the shared key $sk_{rv} = h_3(ID_j, PID_i, v_i V_j, T_{s2})$ and records (ID_g, T_{s2}, ID_j) in secure cache.

Table 2: RSU cache.

Part certification information of vehicles	Expiration time
$(h_5(RID_{i1}, T_{s2}, P_{i1}), T_{s2}, P_{i1})$	T_{ex1}
$(h_5(RID_{i2}, T_{s2}, P_{i2}), T_{s2}, P_{i2})$	T_{ex2}
...	...
$(h_5(RID_{im}, T_{s2}, P_{im}), T_{s2}, P_{im})$	T_{exm}

RSU_j obtains the shared key $sk_{rv} = h_3(ID_j, PID_i, v_j V_i, T_{s2})$ with Ve_i.

The authentication and key negotiation between the vehicle and RSU are shown in Figure 2.

3.5. Key Negotiation between Vehicle and Other RSUs. When the vehicle Ve_i reaches the region of RSU_m $(1 \le m \le n)$, RSU_m broadcasts signature information and public key information $(\mu_m, P_m, ID_m, ID_g, R_m, V_m, T_{s3})$ in this region, where $\mu_m = s_m h_3(ID_m, ID_g, V_m, T_{s3}) + v_m$, $V_m = v_m P$, v_m is the random number selected by RSU_m, ID_m is the unique identity of RSU_m, ID_g is the group ID of RSU_m, and (P_m, R_m) is the public key of RSU_m.

After Ve_i receives the message, it checks whether timestamp T_{s3} has expired. If not, it checks whether records of ID_g are present in the cache; if not, it is authenticated according to the process in Section 3.4. If yes, it indicates that the vehicle has been authenticated and key negotiated in this area; the vehicle verifies whether equation (9) is true. If so, Ve_i selects a random number z_i and calculates $PID_i = h_5(RID_i, T_{s2}, P_i) \oplus h_6(z_i P_m, V_m, T_{s3})$, $Z_i = z_i P$. Then, Ve_i sends $(PID_i, ID_m, Z_i, T_{s3})$ to RSU_m.

$$P_m = h_0(ID_m, R_m) P_{pub1} + R_m. \tag{9}$$

After RSU_m receives the message, it calculates $h_5(RID_i, T_{s2}, P_i) = PID_i \oplus h_6(s_m Z_i, V_m, T_{s3})$; RSU_m looks up whether a value is equal to $h_5(RID_i, T_{s2}, P_i)$ in the cache. If so, RSU_m calculates $sk_{im} = h_4(PID_i, ID_m, s_m Z_i, v_m P_i, T_{s3})$, $\lambda_m = h_6(v_m P_i, V_m, sk_{im})$, and RSU_m sends $(PID_i, \lambda_m, T_{s3})$ to Ve_i. After receiving the message, the vehicle calculates $sk_{im} = h_4(PID_i, ID_m, z_i P_m, s_i V_m, T_{s3})$ and verifies whether the equation $\lambda_m = h_6(s_i V_m, V_m, sk_{im})$ is true. If so, the vehicle Ve_i obtains the shared key $sk_{im} = h_4(PID_i, ID_m, z_i P_m, s_i V_m, T_{s3})$.

RSU_m obtains the shared key $k_{im} = h_4(PID_i, ID_m, s_m Z_i, v_m P_i, T_{s3})$.

The key negotiation between the vehicle and other RSUs is shown in Figure 3.

4. Proof of Safety

Lemma 1. *The message broadcasted by RSU cannot be forged. When ECDLP is a difficult problem, this scheme can resist the forgery attack of adaptive selection message.*

Proof. Assume an attacker who can successfully forge the request message of a vehicle in polynomial time, given the ECDLP problem instance $(P, Q = xP, P, Q \in G, x \in Z_q^*)$. Assuming a challenger C who acts as the game challenger to solve the ECDLP problem, the ECDLP problem can be solved in polynomial time.

Challenger C runs system initialization and initializes system parameters $\text{paras} = \{E_p(a,b), p, q, G, P, P_{\text{pub1}}, P_{\text{pub2}}, h_0, h_1, h_2, h_3, h_4, h_5, h_6\}$; C randomly selects the identity ID_j of a RSU as the identity of the challenger. Next, A adaptively queries the oracle machine from C, and C replies to the query of A as follows:

(1) $h_l(m_l)$: when A initiates a query with m_l, if it does not exist in the list, C selects a random number $r_l \in Z_q^*$, stores (m_l, r_l) in the list L_{hl}, and sends r_l to A. Here, $l = 0, 1, 2 \ldots, 6$.

(2) Query RSU private key.

Furthermore, C maintains the list. When A initiates the query of the oracle model, C queries list L_R. When ID_j is in the list, C returns the information s_j in the list to A; otherwise, it selects randomly $s_j, h_0 \in Z_q^*$ and makes $R_j = s_j P - h_0 P_{pub1}$. Next, (ID_j, R_j, s_j) is added to the list L_R.

(3) Query the message of vehicle certification request.

When A queries with (ID_j, T_{s2}), C randomly selects $h_0, h_3, \mu_j \in Z_q^*$ and makes $V_j = \mu_j P - h_0 h_3 P_{pub1} - h_3 R_j$. Next, C returns $(h_0, h_3, \mu_j, R_j, V_j)$ to A and A receives it. According to the bifurcation lemma [27], A selects different h_0' to output another valid signature $(h_0', h_3, \mu_j', R_j, V_j)$ in polynomial time. At this stage, the two signatures meet as follows:

$$\mu_j P = h_0 h_3 P_{\text{pub1}} + h_3 R_j + V_j, \tag{10}$$

$$\mu_j' P = h_0' h_3 P_{pub1} + h_3 R_j + V_j. \tag{11}$$

From equations (10) and (11), we have the following:

$$(\mu_j - \mu_j') P = (h_0 h_3 - h_0' h_3) P_{\text{pub1}}, \tag{12}$$

where C is according to equation (12), and $s_1 = (\mu_j - \mu_j')(h_0 h_3 - h_0' h_3)^{-1}$ can be calculated with non-negligible probability. However, solving s_1 is an ECDLP problem. According to Definition 1, the attacker cannot solve the ECDLP problem in polynomial time. □

Lemma 2. *Authentication response message cannot be forged. When ECDLP is a difficult problem, this scheme can resist the forgery attack of adaptive selection message.*

Proof. Assume is an attacker A who can successfully forge the request message of a vehicle in polynomial time ε. Given the ECDLP problem instance $(P, Q = xP, P, Q \in G, x \in Z_q^*)$, assuming that a challenger C acts as the game challenger to solve the ECDLP problem, the ECDLP problem can be solved in polynomial time.

(1) $h_l(m_l)$. When A initiates a query with m_l, if m_l does not exist in the list, C selects a random number $r_l \in Z_q^*$, stores (m_l, r_l) in the list L_{hl}, and sends r_l to A; here, $l = 0, 1, 2 \ldots, 6$.

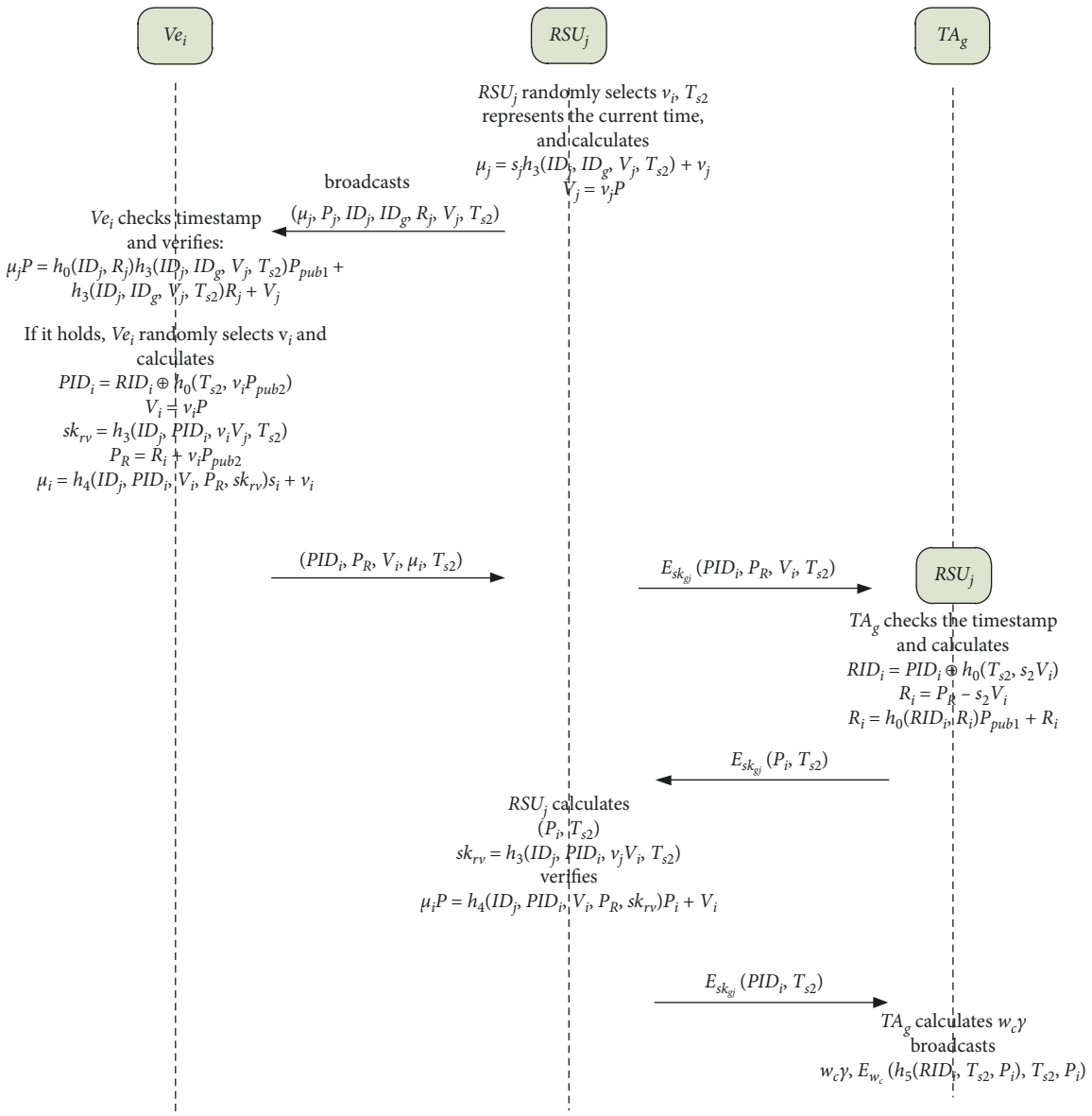

Figure 2: Authentication and session key negotiation process between vehicle Ve_i and RSU_j.

(2) Query vehicle private key.

C maintains the list $L_v = (RID_i, R_i, s_i)$. When A initiates the query of the oracle model, C queries the list $L_v = (RID_i, R_i, s_i)$. When RID_i is in the list, s_i in the list is returned to A; otherwise, C selects randomly $s_i, h_0 \in Z_q^*$ and makes $R_i = s_i P - h_0 P_{pub1}$. Next, it adds (RID_i, R_i, s_i) to the list L_v.

(3) Query vehicle authentication request message.

When A queries PID_i, T_{s2}, C randomly selects $h_0, h_4, \mu_i \in Z_q^*$ and makes $R_i = s_i P - h_0 P_{pub1}$, $P_i = h_0 P_{pub1} + R_i$, $V_i = \mu_i P - h_4 R_i - h_0 h_4 P_{pub}$. Then, C returns (μ_i, V_i, PID_i) to A and A receives it. According to the bifurcation lemma [27], A selects different h_0' to generate another valid signature (μ_i', V_i, PID_i) in polynomial time. At this time, the two signatures meet as follows:

$$\mu_i P = h_4 P_i + V_i = h_4 R_i + h_0 h_4 P_{\text{pub1}} + V_i, \tag{13}$$

$$\mu_i' P = h_4 P_i + V_i = h_4 R_i + h_0' h_4 P_{\text{pub1}} + V_i. \tag{14}$$

From equations (13) and (14):

$$(\mu_i - \mu_i')P = (h_0 h_4 - h_0' h_4) P_{\text{pub1}}, \tag{15}$$

$s_1 = (\mu_i - \mu_i')(h_0 h_4 - h_0' h_4)^{-1}$ can be calculated according to equation (15). However, solving s_1 is an ECDLP problem. According to Definition 1, it is impossible for an enemy to solve the ECDLP problem in polynomial time. □

Theorem 1. *Lemmas 1 and 2 reveal that when the ECDLP problem is difficult, the opponent cannot forge the authentication request message and response message. Thus, the*

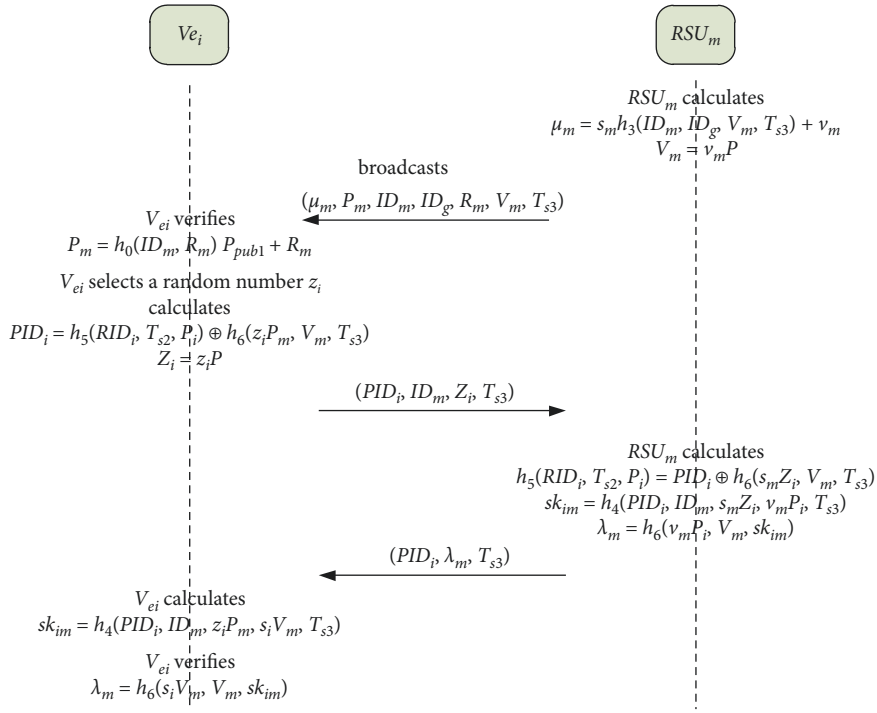

Figure 3: Session key negotiation process between vehicle Ve_i and other RSU_m.

authentication scheme can resist the adaptive selection message forgery attack.

Theorem 2. *The key agreement of this scheme is to secure under the ECCDH problem.*

Proof. Given an ECCDH problem instance $(Q_1 = x_1 P, Q_2 = x_2 P, Q_3 = x_1 x_2 P)$, where $x_1, x_2 \in Z_q^*$, in the key agreement between vehicle Ve_i and RSU_j in this paper, let $Q_1 \leftarrow V_i = \nu_i P$, $Q_2 \leftarrow V_j = \nu_j P$, $Q_3 \leftarrow \nu_i \nu_j P$. If attacker A can calculate $\nu_i \nu_j P$ according to V_i, V_j, the attacker can obtain the key negotiated between the vehicle and RSU. According to Definition 2, the enemy cannot solve the ECCDH problem in polynomial time; that is, the key negotiation between vehicle Ve_i and RSU_j is secure. □

Theorem 3. *Under the random oracle model, this scheme can realize anonymity and identity tracking.*

Proof. In this scheme, the pseudonym $PID_i = RID_i \oplus h_0(T_{s2}, \nu_i P_{\text{pub2}})$ is used for authentication and key negotiation between vehicle Ve_i and RSU_j; the authentication response sent is $(PID_i, P_R, V_i, \mu_i, T_{s2})$, $P_R = R_i + \nu_i P_{\text{pub2}}$, $V_i = \nu_i P$, $\mu_i = h_4(ID_j, PID_i, V_i, P_R, sk_{rv}) s_i + \nu_i$, and $sk_{rv} = h_3(ID_j, PID_i, \nu_i V_j, T_{s2})$, where $P_{pub2} = s_2 P$, $\nu_i P_{pub2} = \nu_i s_2 P$; if the attacker wants to obtain the real identity RID_i of the vehicle, $\nu_i s_2 P$ should be solved according to $V_i = \nu_i P$ and $P_{pub2} = s_2 P$, that is, to solve the ECCDH problem. In the authentication response sent by the vehicle, ν_i is a random number. The response message generated in the communication between the vehicle and RSU each time contains unrelated pseudonym and different random number. Similarly, when the vehicle negotiates with other RSUs, the pseudonym $PID_i = h_5(RID_i, T_{s2}, P_i) \oplus h_6(z_i P_m, V_m, T_{s3})$ is used, and the authentication response sent is $(PID_i, ID_m, Z_i, V_m, T_{s3})$, $Z_i = z_i P$; here, z_i is a random number. The attacker solves $z_i s_m P$ according to the known $Z_i = z_i P$ and $P_m = s_m P$, that is, to solve ECCDH problem. According to Definition 2, an opponent cannot solve the ECCDH problem in polynomial time. The messages generated by the vehicle each time are irrelevant pseudonyms and different random numbers. Therefore, the authentication and key agreement of this scheme can realize the anonymity of vehicles under the ECCDH problem. Furthermore, the scheme can realize the traceability of real identity. In this study, the pseudonym used for the first authentication between the vehicle and a RSU is $PID_i = RID_i \oplus h_0(\nu_i P_{\text{pub2}}, T_{s2})$. The cluster head in this area can calculate the real identity $RID_i = PID_i \oplus h_0(s_2 V_i, T_{s2})$ of the vehicle through the system key s_2. The pseudonym used for the authentication between the vehicle and other RSUs in this area is $PID_i = h_5(RID_i, T_{s2}, P_i) \oplus h_6(z_i P_m, V_m, T_{s3})$. If a dispute occurs, the RSU can calculate $h_5(RID_i, T_{s2}, P_i) = PID_i \oplus h_6(s_m Z_i, V_m, T_{s3})$ through the private key and sends $(h_5(RID_i, T_{s2}, P_i), T_{s2})$ to TA, which can recover the real identity RID_i of the vehicle by querying the vehicle information database. Therefore, this scheme can realize identity traceability. □

4.1. Other Safety Analyses. Theorems 1 and 2 suggest that, under the random oracle model, the authentication and key agreement in this study can resist the adaptive selection message forgery attack. Therefore, the proposed scheme can

Table 3: Safety comparison.

Schemes	Anti-forgery attack	Traceability	Strong security of TPD	Resist replay attacks	Anti-internal attack	Require database support
Literature [17]	Yes	Yes	Yes	Yes	Yes	Yes
Literature [19]	Yes	Yes	Yes	Yes	Yes	No
Literature [20]	No	Yes	No	Yes	Yes	Yes
Literature [22]	Yes	Yes	No	Yes	Yes	No
Our scheme	Yes	Yes	No	Yes	Yes	No

resist attacks, such as the impersonation attack, tampering attack, and man-in-the-middle attack. When the vehicle is certified with RSU for the first time, querying the certification form is not necessary. When the vehicle conducts key negotiation with other RSUs, the authentication and signature use time stamps, so the authentication and key negotiation scheme proposed herein can resist replay attacks. When the vehicle authenticates the RSU group for the first time, the private key of the vehicle and RSU is used to sign the message in the authentication. When the vehicle authenticates other RSUs, it queries the RSU cache, even if the cache is intercepted by an internal attacker. An internal attacker cannot forge a vehicle for key negotiation with RSU because calculating the session key $sk_{im} = h_4(PID_i, ID_m, z_i P_m, s_i V_m, T_{s3})$ requires the private keys of the vehicle and the RSU. Given the public keys of the vehicle and RSU, solving the private keys of the vehicle and RSU requires solving the ECDLP problem. According to Definition 1, an opponent cannot solve the ECDLP problem in polynomial time. Therefore, the proposed authentication scheme can resist internal attacks. In this scheme, when updating the RSU cache, the cluster head uses the group key to encrypt and calculate $E_{w_c}(h_5(RID_i, T_{s2}, P_i), T_{s2}, P_i)$ and then broadcasts in the RSU area. After receiving the key, other RSU nodes decrypt it to get $(h_5(RID_i, T_{s2}, P_i), T_{s2}, P_i)$ and then update the local RSU cache. The group key is updated every time, which can effectively avoid other malicious nodes forging the cluster head and issuing false authentication information. Furthermore, spoofing attacks in other caches, such as ARP spoofing attacks, can be avoided.

In [17], each RSU requires TPD to save the system key. When the system key is leaked, attacks such as forgery and internal impersonation attacks can occur. Therefore, TPD should ideally possess strong security. During authentication and key negotiation, RSU must extract the real identity of the vehicle using the system key according to the pseudonym of the vehicle and verify the legitimacy of the real identity of the vehicle according to the database. In [19], saving the system key in the TPD of the vehicle is necessary, and TPD should have ideal strong security. According to [20], when the vehicle and the external server agent as well as the vehicle and the local server agent authenticate and negotiate the key, the external server agent and the local server agent query the vehicle's public key Q_i using the database. In [22], the authentication and key negotiation of vehicle and fog node are realized using a cloud server. In the negotiation, both vehicle and fog node authenticate through their private keys, and TPD support is not required for authentication. In our scheme, the vehicle and RSU authenticate each other through their own private key. In this scheme, the dual-system keys s_1 and s_2 are used, and s_1 is saved in TA with high security, it is used to calculate the private keys of vehicles and RSUs, and s_2 is saved in the cluster head to help RSU calculate the public key of the vehicle. Even if s_2 is cracked, the attacker can only calculate the public key of the vehicle according to s_2, but the public key of the vehicle is not transmitted in plaintext during the authentication and key negotiation between the vehicle and RSU. Thus, the attacker cannot track the vehicle according to the public key or negotiate the communication key using the public key. Therefore, the vehicle does not require strong TPD security to support the system key storage. The schemes proposed in [17, 19, 22] and that proposed in this study can resist forgery, replay, and internal attacks. When the vehicle falls into a dispute, the real identity of the vehicle can be restored through TA. Table 3 lists the safety comparison of various schemes.

Table 4: Execution time of main cryptographic operations.

Execution time	Value (ms)
T_{bp}	7.272
T_{bm}	1.211
T_{ba}	0.039
T_{em}	0.652
T_{ea}	0.006
T_{H}	2.543
E_{ed}	0.004

5. Performance Analysis

Two critical indicators to measure VANET authentication protocol are computing overhead and communication overhead. We mainly analyze computing overhead and communication overhead of the proposed scheme.

5.1. Calculation Overhead. In [19, 20, 22], nonsingular elliptic curve cryptography was used, and in [17] bilinear pair construction scheme was used. At the same security level, we constructed two cryptographic operation schemes with 80-bit security level. The bilinear pairing scheme is set as follows: e: $G_1 \times G_1 \longrightarrow G_2$. Here, the generator of the additive group G_1 is $\overline{P}$, the order is $\overline{q}$, and $\overline{P}$ is the point on the hypersingular curve $\overline{E}$: $y^2 = x^3 + ax + b \bmod \overline{p}$ with degree 2, and $\overline{p}$ is a 512-bit prime. The elliptic curve cryptography with the same security level is set as follows: the nonsingular elliptic curve is E: $y^2 = x^3 + ax + b \bmod p$, G is the addition group on E, P is the generator of G, and the order of G is q,

Table 5: Calculation cost of authentication and session key negotiation of various schemes.

Schemes	User (ms)	RSU (ms) or proxy node	TA or server (ms)	Total (ms)
Literature [17]	$1T_{bp} + 3\ T_{bm} + 1T_H + 1E_{ed}$	$3\ T_{bm} + 1E_{ed}$	No	$1T_{bp} + 6\ T_{bm} + 1T_H + 2E_{ed} \approx 17.09$
Literature [19]	$7\ T_{em} + 2T_{ea}$	No	$5\ T_{em} + 2T_{ea}$	$12T_{em} + 4T_{ea} \approx 7.85$
Literature [20]	$6\ T_{em} + 2T_{ea}$	$7\ T_{em} + 2T_{ea}$	$4\ T_{em} + 2T_{ea}$	$17\ T_{em} + 6T_{ea} \approx 11.12$
Literature [22]	$3T_{em}$	$4T_{em}$	$10\ T_{em}$	$17\ T_{em} \approx 11.08$
Our scheme	$6T_{em} + 3T_{ea}$	$3\ T_{em} + 1T_{ea} + 3E_{ed}$	$2\ T_{em} + 2T_{ea} + 3E_{ed}$	$11\ T_{em} + 6T_{ea} + 6E_{ed} \approx 7.23$

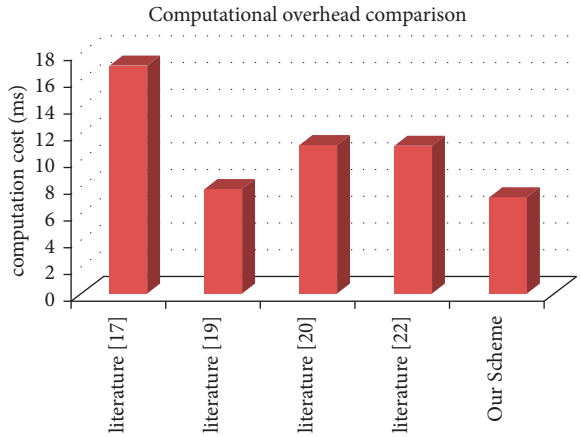

Figure 4: Comparison of calculation cost.

Table 6: Comparison of communication overhead.

Schemes	User (byte)	RSU (byte) or proxy node	TA or server (byte)	Total (byte)
Literature [17]	$1\|G_1\| + 1\|\ Z_q^*\|$	$2\|G_1\| + 2\|\ Z_q^*\| + \|T\|$		$3\|G_1\| + 3\|Z_q^*\| + \|T\| = 448$
Literature [19]	$2\|G\| + 3\|Z_q^*\| + \|T\|$		$\|G\| + 3\|Z_q^*\|$	$3\|G\| + 6\|Z_q^*\| + \|T\| = 244$
Literature [20]	$1\|G\| + 3\|\ Z_q^*\| + \|T\|$	$3\|G\| + 5\|\ Z_q^*\| + 2\|T\|$	$\|Z_q^*\| + \|T\|$	$4\|G\| + 9\|Z_q^*\| + 4\|T\| = 356$
Literature [22]	$1\|G\| + 4\|Z_q^*\| + \|T\|$	$6\|G\| + 6\|\ Z_q^*\| + 3\|T\|$	$3\|G\| + 4\|\ Z_q^*\| + \|T\|$	$10\|G\| + 14\|Z_q^*\| + 5\|T\| = 700$
Our scheme	$2\|G\| + 2\|Z_q^*\| + \|T\|$	$5\|G\| + 5\|Z_q^*\| + 3\|T\|$	$1\|G\| + \|T\|$	$8\|G\| + 7\|Z_q^*\| + 5\|T\| = 480$

and p and q are 160 bit primes, $a, b \in Z_q^*$. Let T_{bp}, T_{bm}, and T_{ba} represent the bilinear pairing operation, scalar multiplication operation, and scalar addition operation time of the bilinear pair, respectively, T_{em} and T_{ea} represent the scalar multiplication and scalar addition operation time of elliptic curve cryptography, and T_H represents the hash operation time of map to point. Let E_{ed} represent symmetric encryption or decryption operation time. For performing the abovementioned operations on $\overline{E}, E$, we use the functions defined in MIRACL cryptographic library on a 1.8-GHz machine with 8 GB memory. The running environment is Visual Studio 2012 on Windows 10. The experimental method is similar to [28]. Table 4 presents the average execution time of cryptographic operations.

Statistical values of the main time-consuming operations used in the protocols of [17, 19, 20, 22], such as bilinear pairing operation, scalar multiplication operation, scalar addition operation, map-to-point hash operation, the scalar multiplication, and the addition operations of elliptic curve cryptography, were obtained. We ignored other operations with short time and simple calculation, such as the hash operation and logic operation. From Table 5 and Figure 4, the total calculation amount of authentication and session key negotiation for the first time in this paper is saved by 57.7%, 7.9%, 35.0%, and 34.7%, respectively, compared with the other four schemes. The scheme of this paper has certain advantages in terms of calculation.

Vehicle and RSU group authentication obtained for the first time is given by $11T_{em} + 6T_{ea} + 6E_{e\ d} \approx 7.23ms$. After using the cache, the vehicle and other RSU authentications and key negotiations can be given by $7T_{em} + 1T_{ea} \approx 4.57ms$, which is reduced by 37%.

5.2. Communication Overhead. According to the analysis in the previous section, $\overline{p}$ is 64 bytes and G_1 is 128 bytes, and p is 20 bytes, so G is 40 bytes. We assume that the timestamp is 4 bytes, the hash function value is 20 bytes, and the other nongroup element is 20 bytes. Let $|G_1|$ represent the length of the element in the group G_1, let $|G|$ represent the length of the group G element, let $|Z_q^*|$ represent the length of the nongroup element, and let $|T|$ represent the length of the timestamp.

According to the communication comparison in Table 6, the communication volume of this scheme before using RSU cache is 32 bytes more than that in [17], 236 bytes more than that in [19], 124 bytes more than that in [20], and 220 bytes

less than that in [22]. Table 6 reveals that the traffic volume of this paper slightly increased compared with [17, 20] and decreased compared with [22].

Before using the RSU cache, authentication and key negotiation require five interactions, but after using the RSU cache, three interactions are required. The authentication does not require the participation of cluster heads. Before using cache, the traffic is $8|G| + 7|Z_q^*| + 5|T| = 480$ bytes, while after using cache, it is $4|G| + 7|Z_q^*| + 3|T| = 312$ bytes, and the traffic is reduced by 35%.

6. Conclusion

In this paper, we proposed an efficient authentication method for the successful transfer of information when the vehicle moves from one RSU to another RSU region. The proposed scheme can resist forgery, replay, internal attacks, and traceability. The scheme in [22] exhibits the same security performance, but the computation and communication required are higher than those in the proposed scheme. The traffic volume presented in [19] is considerably better than that of the proposed scheme; however, in [19], centralized authentication of vehicles and cloud services is required. When the vehicle is far away from the cloud server, the communication delay is considerably increased, and each vehicle stores the system keys, which requires TPD to ideally have strong security. If a single TPD is attacked, the security of the whole system is compromised. Thus, the proposed scheme can overcome these problems and can be used for the development of effective authentication schemes in the future.

At present, artificial intelligence and blockchain technologies [29, 30] are widely used. How to introduce artificial intelligence or blockchain technology into the secure communication of VANET is the current research hotspot.

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 do not have any commercial or associative interest that represents the conflicts of interest in connection with the work submitted.

Acknowledgments

This work was supported in part by the Research and Development Projects Entrusted by Enterprises (no. 2021011), in part by the Natural Science Foundation of Anhui University (nos. KJ2020A0032 and KJ2021A0527), and in part by the National Natural Science Foundation of China (Grant no. 61902140).

References

[1] 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.

[2] 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.

[3] M. Wazid, A. K. Das, N. Kumar et al., "Design of lightweight authentication and key agreement protocol for vehicular Ad Hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017.

[4] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular Ad Hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.

[5] 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, 2018.

[6] S. Paliwal, A. K. Cherukuri, and X. Z. Gao, "Dynamic private Modulus based password conditional privacy preserving authentication and key-agreement protocol for VANET," *Wireless Personal Communications*, vol. 123, no. 3, pp. 2061–2088, 2022.

[7] Y. Zhang and F. Wen, "A lightweight secure and efficient authentication and key agreement protocol for VANET," *OP Conference Series: Earth and Environmental Science*, vol. 234, pp. 012069–12069, 2019.

[8] 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.

[9] S. Shamshad, M. A. Saleem, K. Mahmood, R. Muhammad, and F. Ayub, "On the security of a lightweight privacy-preserving authentication protocol for VANETs," in *Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, IEEE, Coimbatore, India, March 2021.

[10] S. A. Alfadhli, S. Lu, A. Fatani, H. Al-Fedhly, and M. Ince, "SD2PA: a fully safe driving and privacy-preserving authentication scheme for VANETs," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 38, 2020.

[11] J. Y. Lee, S. J. Yu, M. H. Kim, Y. H. Park, S. W. Lee, and B. H. Chung, "Secure key agreement and authentication protocol for message confirmation in vehicular cloud computing," *Applied Sciences*, vol. 10, no. 18, p. 6268, 2020.

[12] S. A. Alfadhli, S. Lu, K. Chen, and M. Sebai, "MFSPV: a multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs," *IEEE Access*, vol. 8, pp. 142858–142874, 2020.

[13] S. Lv and Y. Liu, "PLVA: privacy-preserving and lightweight V2I authentication protocol," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6633–6639, 2022.

[14] Q. Li, C. F. Hsu, K. K. R. Choo, and D. He, "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for vehicular Ad Hoc networks," *Security and Communication Networks*, vol. 2019, pp. 1–13, 2019.

[15] L. Deng, J. Shao, and Z. Hu, "Identity based two-party authenticated key agreement scheme for vehicular ad hoc networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2236–2247, 2021.

[16] C. L. Chen, Y. X. Chen, C. F. Lee, Y. Y. Deng, and C. H. Chen, "An efficient and secure key agreement protocol for sharing

emergency events in VANET systems," *IEEE Access*, vol. 7, pp. 148472–148484, 2019.

[17] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: a new and efficient RSU based authentication scheme for VANETs," *Wireless Networks*, vol. 26, no. 5, pp. 3083–3098, 2020.

[18] 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.

[19] Y. Xie, L. Wu, L. Zhang, and L. Ye, "Anonymous mutual authentication and key agreement protocol in multi-server Architecture for VANETS," *Journal of Computer Research and Development*, vol. 53, pp. 2323–2333, 2016.

[20] Y. Zhou, X. Long, L. Chen, and Z. Yang, "Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs," *Journal of Information Security and Applications*, vol. 47, pp. 295–301, 2019.

[21] S. ZakeriKia, R. Hajian, S. H. Erfani, and A. M. Rahmani, "Robust and anonymous handover authentication scheme without key escrow problem in vehicular sensor networks," *Wireless Networks*, vol. 27, no. 7, pp. 4997–5028, 2021.

[22] M. Ma, D. He, H. Wang, N. Kumar, and K. K. R. Choo, "An efficient and provably-secure authenticated key agreement protocol for fog-based vehicular Ad-Hoc networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, 2019.

[23] X. Li, J. Liu, M. S. Obaidat, P. Vijayakumar, Q. Jiang, and R. Amin, "An unlinkable authenticated key agreement with collusion resistant for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7992–8006, 2021.

[24] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "SMAKA: secure many-to-many authentication and key agreement scheme for vehicular networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1810–1824, 2021.

[25] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2982–2994, 2021.

[26] X. Zhang, H. Zhong, C. Fan, I. Bolodurina, and J. Cui, "CBACS: a privacy-preserving and efficient cache-based access control scheme for Software defined vehicular networks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1930–1945, 2022.

[27] D. Pointcheval and J. Stern, *Security Proofs for Signature Schemes*, pp. 387–398, Springer, Berlin Heidelberg, 1996.

[28] M. Sun, Y. Guo, D. Zhang, and M. Jiang, "Anonymous authentication and key agreement scheme combining the group key for vehicular ad hoc networks," *Complexity*, vol. 2021, pp. 1–13, 2021.

[29] A. Maria, A. S. Rajasekaran, F. Al-Turjman, C. Altrjman, and L. Mostarda, "BAIV: an efficient blockchain-based anonymous authentication and integrity Preservation scheme for secure communication in VANETs," *Electronics*, vol. 11, no. 3, p. 488, 2022.

[30] S. A. George, A. Jaekel, and I. Saini, "Secure identity management Framework for vehicular ad-hoc network using blockchain," in *Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC)*, July 2020.