Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 569526, 11 pages
http://dx.doi.org/10.1155/2015/569526

Research Article

Message Authentication Mechanism and Privacy Protection in the Context of Vehicular Ad Hoc Networks

Hsin-Te Wu,[1] Alan Dahgwo Yein,[2] and Wen-Shyong Hsieh[3,4]

[1]*Department of Information Management, Fortune Institute of Technology, Kaohsiung, Taiwan*
[2]*Department of Information Management, Shu-Te University, Kaohsiung, Taiwan*
[3]*Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan*
[4]*Department of Computer and Communication, Shu-Te University, Kaohsiung, Taiwan*

Correspondence should be addressed to Hsin-Te Wu; wuhsinte@fotech.edu.tw

Received 14 September 2014; Accepted 10 December 2014

Academic Editor: Mo Li

Vehicular ad hoc networks (VANETs) have been widely researched in recent years. VANETs are used mostly for road safety and traffic efficiency; therefore, it is imperative that the communication between vehicles is rapid and secure in a VANET environment. In the present study, bilinear pairings were used to construct a complete message authentication scheme. This scheme provided the following features: (1) vehicle or roadside unit (RSU) parameters were determined via a hierarchical protocol, which prevented potentially a large computational overhead for a single node; (2) message broadcasts and private communications between vehicles in the transmission range of the same RSU were enabled; (3) message broadcasts and private communications between vehicles in the transmission ranges of different RSUs were enabled; (4) a fast handoff mechanism was established for vehicles in the transmission ranges of different RSUs; and (5) mechanisms for message broadcasts and private communication were established for vehicles in areas where RSUs were sparsely located. Based on the experimental results, our scheme was confirmed to be superior to previous schemes. In terms of security, our scheme offered the following features: confidentiality, message integrity, nonrepudiation, conditional anonymity, and conditional untraceability.

1. Introduction

Vehicular ad hoc networks (VANETs) have been widely researched in recent years. VANETs are mobile networks in which vehicles equipped with on-board units (OBUs) communicate with each other or roadside units (RSUs) [1, 2]. Vehicles can broadcast traffic information to one another over VANETs [3]. In addition, passengers can communicate with passengers in other vehicles or send electronic mail using hand-held devices over VANETs [4]. VANETs have drawn special attention for traffic safety and management [5, 6]. The information exchanged between vehicles over VANETs enhances road safety and improves traffic efficiency. Generally, there are two different modes in VANETs for sending messages: the message broadcast mode, in which neighboring vehicles may provide one another with up-to-date proximal vehicle state information via message broadcasts, and the one-hop broadcast mode, in which a vehicle can send messages to one other specific vehicle. One-hop broadcasts are mainly used for private communication between vehicles.

There are two vehicular communication modes in VANETs [7], vehicle-to-vehicle communication (IVC) and RSU-to-vehicle communication (RVC). IVC allows each vehicle to broadcast information to other vehicles or send information to one specific vehicle via others. RVC allows vehicles to exchange information with one another within the broadcast range or communicate with and obtain information from other vehicles via wireless-device equipped RSUs. VANETs enable vehicles to exchange up-to-date traffic information, which improves the flow of traffic and driving safety. However, if the information is modified or falsified by a malicious vehicle user, serious consequences such as traffic congestion and even a traffic accident can occur. A scheme for ensuring information security is proposed in the present study.

A message authentication scheme for VANETs should take the following problems into consideration: (1) the exchange of information between vehicles in VANETs is accomplished through wireless communication. Therefore, to be timely, the volume of information cannot be excessively high nor can the method for message authentication be excessively complicated. (2) Vehicles should be able to not only broadcast information but additionally communicate privately with other devices. (3) Vehicles use a short-range wireless communication technique to communicate with RSUs and are usually moving at high speeds, requiring frequent handoffs with RSUs. Handoff schemes with long computation times adversely affect the communication quality. (4) RSUs may be available only on main roads and not on minor ones.

In the present study, a complete message authentication scheme is constructed using the bilinear pairings technique. The encryption scheme from bilinear pairings is appropriate for VANETs. The parameters for each node in this study are generated in a hierarchical way. The long-term parameters for each vehicle are generated by the trusted authority (TA). Vehicles use their long-term parameters to perform identity (ID) authentication with RSUs and then gain trust from them. RSUs then produce short-term parameters for the vehicles that allow them to broadcast information and conduct private communications. When the vehicles are not within the transmission range of any RSUs, they can use their long-term parameters to broadcast information and communicate privately with one another. The trust gained from one RSU enables the vehicle to perform handoffs with other RSUs. Based on the experimental results, the scheme proposed in this study shows excellent performance and is superior to other schemes in the literature.

2. Related Works

The conventional public key infrastructure (PKI) scheme was used in [8]. Assuming that a certificate authority (CA) provides each vehicle with a digital certificate of identity, that is, a private key together with its associated public key, the vehicle can then use the asymmetric key for signing and verifying a message. However, the computational complexity increases when a vehicle uses the PKI for message signature and verification, resulting in communication overhead. In addition, for the purposes of privacy and untraceability, a vehicle must constantly change its certificate, which adversely affects the CA overhead.

A solution is defined in [9] in which vehicles can generate public/private key pairs on their own. The benefits lie in the fact that a vehicle uses a different key each time it sends a message and that the vehicle is not required to update the related parameters with the CA. Assuming that there is a cryptographic device, or black box, installed in each vehicle and in each black box there are an asymmetric key and a certificate issued by the CA, the black box generates the public/private key pair for the vehicle. However, the public/private key pair is the continuous product of two values, resulting in each key pair having a long message length. This long message length may result in communication overhead when the vehicle is sending messages.

The scheme for vehicular communications used in [10] was constructed with a hierarchy in which the keys were generated in a top-to-bottom manner. The hierarchical method allows vehicles to generate parameters such as their IDs through RSUs, which mitigates the key escrow problem in the CA. The generated keys are reliable and nonforgeable. However, this scheme requires the use of vehicle certificates. Thus, the information exchanged between vehicles is verified via the contents of the certificates. The requirement for a certificate with each message may nevertheless result in data packet overhead. In addition, message encryption based on bilinear pairings may result in computation overhead.

In [11], to provide network access services, a vehicle must establish a common key with the recipient vehicle via a broadcast message. The common key ensures the security of the subsequent information exchange, authentication, message integrity, and nonrepudiation. However, the common key is established using the identity-based cryptography (IBC) scheme, which is based on bilinear pairings. The establishment of a shared common key with each vehicle may result in vehicle computation overhead. The authors in [11] did not discuss the problems of rekeying and pseudonym changes. These problems are significant in vehicle networks, warranting resolution. A dynamic, privacy-preserving key management scheme for location-based services in VANETs was proposed in [12]. This scheme ensures the anonymous authentication of a vehicle and enables double-registration detection. In addition, each vehicle can use a one-way hash function to update the vehicles new session key. However, the computations for message signature and verification presented in [12] are complicated, and the author did not investigate a private communication scheme.

In [13], an elliptic curve digital signature algorithm (ECDSA) was used for message authentication. The current position information is used together with the ECDSA for signing messages from anonymous IDs. Other vehicles do not require a third-party public key certificate for message authentication. However, the authors did not discuss the problems of rekeying and private communication.

The delay in long-term verification of centralized AAA architecture in literature [14] has been alleviated. In this paper, a set of network security approaches based on bilinear Diffie-Hellman (BDH) problem are proposed to protect the privacy of vehicles and network security of portable electronic currency in VANETs environment. However, the proposed method requires a key to be generated at regular intervals on each vehicle in advance for privacy, which is a big burden for the vehicle.

In literature [15], a set of network security mechanisms based on chameleon hashing was proposed to ensure vehicle privacy and network communications security in VANETs. However, owing to computational complexity and packet length of chameleon hashing, it constitutes a big burden for VANETs.

In literature [16], a set of network security mechanisms based on bilinear pairing was proposed. Although it can ensure network communications security of vehicles in VANETs, it does not provide private communications between vehicles. Besides, the changes of relevant parameters

for vehicles involved have to be updated via TA. Therefore, it has a centralized authentication issue.

3. Background

This section will introduce the technologies used in the method developed in this study. Section 3.1 introduces bilinear pairing and hard problems, Section 3.2 discusses Boneh and Franklins ID-based encryption, Section 3.3 discusses Shamirs ID-based cryptosystem, and Section 3.4 covers bilinear Diffie-Hellman message authentication.

3.1. Bilinear Pairings and Hard Problems. Let G_1 and G_2 denote an additive and a multiplicative group and both of them with prime order q. Let P be generator of G_1 and let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear mapping with the following properties.

(1) Bilinear:

$$e = (aP, bP) = e(P, P)^{ab}$$
$$e(a \cdot P + b \cdot P, P) = e(a \cdot P, P)\, e(b \cdot P, P), \quad \forall P \in G_1, \quad a, b \in Z_q^*. \tag{1}$$

(2) Nondegeneracy: $\exists P \in G_1$ such that $\hat{e}(P, P) \neq 1$. That is, the mapping does not send all pairs in $G_1 \times G_1$ to the identity in G_2.

(3) Computable: there exists an efficient algorithm to compute $e(P, P)$ for all $P \in G_1$.

The bilinear map e can be implemented using the Weil [9] and Tate [10] pairings on elliptic curves. We consider the implementation of a Tate pairing on a Miyaji–Nakabayashi–Takano (MNT) curve [11] with embedding degree 6, where G_1 is represented by 161 bits and the order q is represented by 160 bits.

The following part will define and specify various relevant mathematical problems [12] which will be applied in the essay subsequently.

Bilinear Diffie-Hellman problem:

Given $(P, aP, bP, cP) \in G_1$, where $a, b, c \in Z_q^*$, compute $e = (P, P)^{abc}$.

Elliptic curve discrete logarithm problem (ECDLP):

Given two elements $P, Q \in G_1$, find an integer $a \in Z_q^*$, such that $Q = aP$.

3.2. ID-Based Encryption. We used ID-based encryption [17] to encrypt and decrypt messages. A private key generator (PKG) chooses a random number $g_{\mathrm{PKG}} \in Z_q^*$ as its master key and selects two distinct hash functions, $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : G_2 \rightarrow \{0,1\}^*$. Given a user i with an identity $\mathrm{ID}_i \in \{0,1\}^*$, any party can obtain the user's public key $\mathrm{PU}_{\mathrm{ID}_i} = H_1(\mathrm{ID}_i)$. The PKG sets the user's private key $\mathrm{PR}_{\mathrm{ID}_i} = g_{\mathrm{PKG}} \cdot H_1(\mathrm{ID}_i)$. User i chooses $s_{\mathrm{ID}_i} \in Z_q^*$ as her/his own secret value and sets $D_{\mathrm{ID}_i} = s_{\mathrm{ID}_i} \cdot P$. In the final step, the PKG publishes the system parameters $(q, G_1, G_2, \hat{e}, P, D_{\mathrm{ID}_i}, \mathrm{ID}_i, H_1, H_2)$ and withholds s_{ID_i}.

Encrypt. To encrypt a message $M \in \{0,1\}^*$ for the user with identity ID_i is as follows.

(1) Choose a random number $r \in Z_P^*$.

(2) Set the cipher text C to be

$$C = E_{\mathrm{IBC}}\left(r, M, \mathrm{PU}_{\mathrm{ID}_i}, D_{\mathrm{ID}_i}\right) = \left\{r \cdot P, M \oplus H_2\left(e\left(\mathrm{PU}_{\mathrm{ID}_i}, D_{\mathrm{ID}_i}\right)^r\right)\right\}. \tag{2}$$

Decryption. Let $C = \langle U, V \rangle$. To decrypt C using the secret value s_{ID_i}, compute $D_{\mathrm{IBC}}(s_{\mathrm{ID}_i}, C) = V \oplus H_2(e(s_{\mathrm{ID}_i}\mathrm{PU}_{\mathrm{ID}_i}, U)) = M$, where

$$\begin{aligned} & V \oplus H_2\left(e\left(s_{\mathrm{ID}_i}\mathrm{PU}_{\mathrm{ID}_i}, U\right)\right) \\ &= M \oplus H_2\left(\hat{e}\left(\mathrm{PU}_{\mathrm{ID}_i}, rD_{\mathrm{ID}_i}\right)\right) \oplus H_2\left(\hat{e}\left(s_{\mathrm{ID}_i}\mathrm{PU}_{\mathrm{ID}_i}, rP\right)\right) \\ &= M \oplus H_2\left(\hat{e}\left(\mathrm{PU}_{\mathrm{ID}_i}, rs_{\mathrm{ID}_i}P\right)\right) \oplus H_2\left(\hat{e}\left(s_{\mathrm{ID}_i}\mathrm{PU}_{\mathrm{ID}_i}, rP\right)\right) \\ &= M \oplus H_2\left(\hat{e}\left(\mathrm{PU}_{\mathrm{ID}_i}, rs_{\mathrm{ID}_i}P\right)\right) \oplus H_2\left(\hat{e}\left(\mathrm{PU}_{\mathrm{ID}_i}, rs_{\mathrm{ID}_i}P\right)\right) \\ &= M. \end{aligned} \tag{3}$$

3.3. ID-Based Cryptosystem. The advantage of ID-based cryptosystems [17] is that public key certificates are no longer needless, and this possibly causes a saving of space requirements. Besides, it also reduces the key management cost, which is a heavy burden in conventional public key infrastructure (PKI). However, it has a serious drawback, called key escrow problem. PKG is responsible for generating a user's private key, so it can decrypt any ciphertext or forge any user's signature on any message.

3.4. Message Authentication Based on the Bilinear Hard Problems (BHD) Method. In this study, message signatures and verification are established based on the BDH method. In this scheme, user i selects a random number $h_i \in Z_q^*$ as the secret value, calculates the public value (B_i), and then broadcasts B_i to all other users. Notations of the BDH list the notation used in this study. User i broadcasts message $M_{i,j}$ by executing the following steps.

(1) User i calculates $w_{i,j} = H(M_{i,j} \parallel T_j) \bmod p$.

(2) User i calculates $h_i = y_{i,j} * w_{i,j} + r_{i,j}$, where $y_{i,j}$ represents the quotient and $r_{i,j}$ represents the remainder.

(3) User i broadcasts $\langle M_{i,j}, y_{i,j} \cdot P, \mathrm{ID}_i, T_j, \hat{e}(P, r_{i,j} \cdot P) \rangle$.

Other users can then verify the message upon receipt by executing the following steps.

(1) Calculate $w_{i,j} = H(M_{i,j} \parallel T_j) \bmod p$.

(2) Check whether $\hat{e}(w_{i,j} \cdot P, y_{i,j} \cdot P) + \hat{e}(P, r_{i,j} \cdot P) = \hat{e}(P, P)^{h_i} \stackrel{?}{=} B_i$.

If the equality in step (2) is satisfied, then this condition verifies that the user i sent the message. During the verification process, other users receive only $y_{i,j} \cdot P, \hat{e}(P, r_{i,j} \cdot P), w_{i,j}$ and B_i. Based on elliptic curves and the discrete logarithm problem (ECDLP), h_i cannot be calculated without $y_{i,j} \cdot P$ and B_i. Therefore, message security is ensured. Furthermore, because h_i belongs to the user alone, nonrepudiation of the message is also ensured.

4. Message Authentication Scheme

The scheme proposed in this study consists of five parts: (1) system initialization and RSU registration; (2) intra-RSU message authentication; (3) inter-RSU message authentication; (4) handoff; and (5) message authentication when RSUs are not available.

4.1. System Model. Figure 1 shows the system environment used in this study. We assume that the TA is a legal organization and is responsible for the security of the entire network. When there is an attack on the network infrastructure from a malicious node, the TA will broadcast the true identity of the node and take necessary action. We further assume that RSUs are installed on streetlights or traffic signs on main roads and there are no RSUs installed on minor roads. Each vehicle is equipped with an OBU. Communication between the TA and RSUs is via a wired network, whereas communication between OBUs and the TA is via an IEEE 802.11p wireless network. Notation used in this paper lists the notation used in this study.

4.2. System Initialization. Given the bilinear parameters $(q, G_1, G_2, \hat{e}, P)$ as defined in Section 3.1, the TA sets up the system by executing the following steps.

(1) The TA chooses $h_{\mathrm{ID}_{t,\mathrm{TA}}} \in Z_q^*$ as its secret value.

(2) The TA selects three hash functions: $H : \{0,1\}^* \rightarrow Z_q^*$, $H_1 : \{0,1\}^* \rightarrow G_1$, and $H_2 : G_2 \rightarrow \{0,1\}^*$.

(3) The TA calculates $B_{\mathrm{ID}_{t,\mathrm{TA}}} = \hat{e}(h_{\mathrm{ID}_{t,\mathrm{TA}}} P, P)$ as its public value.

(4) The TA sets $D_{\mathrm{ID}_{t,\mathrm{TA}}} = h_{\mathrm{ID}_{t,\mathrm{TA}}} \cdot P$.

(5) The TA sets $\mathrm{PU}_{\mathrm{ID}_{t,\mathrm{TA}}} = H_1(\mathrm{ID}_{t,\mathrm{TA}})$.

(6) The TA sets $\mathrm{PR}_{\mathrm{ID}_{t,\mathrm{TA}}} = h_{\mathrm{ID}_{t,\mathrm{TA}}} H_1(\mathrm{ID}_{t,\mathrm{TA}})$.

The TA broadcasts the parameters $(\mathrm{ID}_{t,\mathrm{TA}}, B_{\mathrm{ID}_{t,\mathrm{TA}}}, D_{\mathrm{ID}_{t,\mathrm{TA}}}, H, H_1, H_2)$, while $(\mathrm{PR}_{t,\mathrm{TA}}, h_{\mathrm{ID}_{t,\mathrm{TA}}})$ remain undisclosed. In addition, the TA sets the related parameters for each RSU by executing the following steps.

(1) The node R_R chooses $h_{\mathrm{ID}_{t,R_R}} \in Z_q^*$ as its secret value.

(2) It calculates $B_{\mathrm{ID}_{t,R_R}} = \hat{e}(h_{\mathrm{ID}_{t,R_R}} P, P)$ as its public value.

(3) It sets $D_{\mathrm{ID}_{t,R_R}} = h_{\mathrm{ID}_{t,R_R}} \cdot P$.

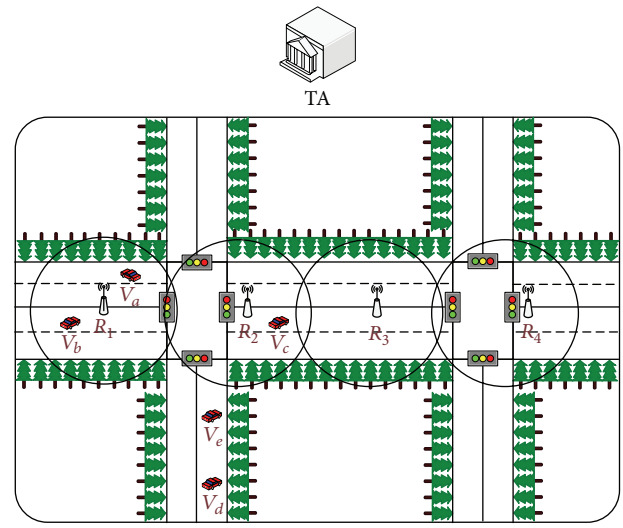

Figure 1: System environment.

(4) It sets $\mathrm{PU}_{\mathrm{ID}_{t,R_R}} = H_1(\mathrm{ID}_{t,R_R})$.

The TA sets up the system by executing the following steps.

(1) Set $\mathrm{PR}_{\mathrm{ID}_{t,R_R}} = h_{\mathrm{ID}_{t,\mathrm{TA}}} H_1(\mathrm{ID}_{t,R_R})$.

(2) Calculate $w_{\mathrm{ID}_{t,\mathrm{TA}},j} = H(H_2(B_{\mathrm{ID}_{t,R_R}}) \parallel \mathrm{ID}_{t,R_R} \parallel T_{l,\mathrm{ID}_{t,R_R}}) \bmod p$.

(3) Calculate $y_{\mathrm{ID}_{t,\mathrm{TA}},j} = h_{\mathrm{ID}_{t,\mathrm{TA}}} / w_{\mathrm{ID}_{t,\mathrm{TA}},j}$, $\hat{e}(r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, P)$.

The RSU R_R broadcasts the parameters $(\mathrm{ID}_{t,R_R}, B_{\mathrm{ID}_{t,R_R}}, D_{\mathrm{ID}_{t,R_R}}, \hat{e}(r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, P), y_{\mathrm{ID}_{t,\mathrm{TA}}} P, T_{l,\mathrm{ID}_{t,R_R}})$ and does not disclose the parameters $(h_{\mathrm{ID}_{t,R_R}}, \mathrm{PR}_{\mathrm{ID}_{t,R_R}})$. All nodes can verify the legitimacy of the ID of the RSU by executing the following steps.

(1) Calculate $w_{\mathrm{ID}_{t,\mathrm{TA}},j} = H(H_2(B_{\mathrm{ID}_{t,R_R}}) \parallel \mathrm{ID}_{t,R_R} \parallel T_{l,\mathrm{ID}_{t,R_R}}) \bmod p$.

(2) Calculate $B'_{\mathrm{ID}_{t,\mathrm{TA}}} = \hat{e}(w_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, y_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) + \hat{e}(P, r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) = \hat{e}(P, P)^{h_{\mathrm{ID}_{t,\mathrm{TA}}}}$.

(3) Check if $B_{\mathrm{ID}_{t,\mathrm{TA}}} \stackrel{?}{=} B'_{\mathrm{ID}_{t,\mathrm{TA}}}$

The TA generates the related parameters for the vehicle by executing the following steps.

(1) The node V chooses $h_{\mathrm{ID}_{i,V}} \in Z_q^*$ as its secret value.

(2) It calculates $B_{\mathrm{ID}_{i,V}} = \hat{e}(h_{\mathrm{ID}_{i,V}} P, P)$ as its public value.

(3) It sets $D_{\mathrm{ID}_{i,V}} = h_{\mathrm{ID}_{i,V}} \cdot P$.

(4) It selects an anonymous identity ID_i, and all users can obtain its public key by computing $\mathrm{PU}_{\mathrm{ID}_{i,V}} = H_1(\mathrm{ID}_{i,V})$.

The TA sets up the system by executing the following steps.

(1) Set $\mathrm{PR}_{\mathrm{ID}_{i,V}} = h_{\mathrm{ID}_{t,\mathrm{TA}}} H_1(\mathrm{ID}_{i,V})$.

(2) Calculate $w_{\mathrm{ID}_{t,\mathrm{TA}},j} = H(H_2(B_{\mathrm{ID}_{i,V}}) \parallel \mathrm{ID}_{i,V} \parallel T_{l,\mathrm{ID}_{i,V}}) \bmod p$.

(3) Calculate $y_{\mathrm{ID}_{t,\mathrm{TA}},j} = h_{\mathrm{ID}_{t,\mathrm{TA}}}/w_{\mathrm{ID}_{t,\mathrm{TA}},j}$, $\hat{e}(r_{\mathrm{ID}_{i,\mathrm{TA}},j} \cdot P, P)$.

Each vehicle broadcasts the parameters $(\mathrm{ID}_{i,V}, B_{\mathrm{ID}_{i,V}}, D_{\mathrm{ID}_{i,V}}, \hat{e}(r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, P), y_{\mathrm{ID}_{t,\mathrm{TA}},j}P, T_{l,\mathrm{ID}_{i,V}})$ and does not disclose the parameters $(h_{\mathrm{ID}_{i,V}}, \mathrm{PR}_{\mathrm{ID}_{i,V}})$. The TA records the parameters $(\mathrm{ID}_{t,V}, \mathrm{ID}_{i,V}, B_{\mathrm{ID}_{i,V}}, D_{\mathrm{ID}_{i,V}}, T_{\mathrm{ID}_{i,V},j})$ for each vehicle.

Each vehicle or RSU can verify the legitimacy of the vehicle ID by executing the following steps.

(1) Calculate $w_{\mathrm{ID}_{t,\mathrm{TA}},j} = H(H_2(B_{\mathrm{ID}_{i,V}}) \parallel \mathrm{ID}_{i,V} \parallel T_{l,\mathrm{ID}_{i,V}}) \bmod p$.

(2) Calculate $B'_{\mathrm{ID}_{t,\mathrm{TA}}} = \hat{e}(w_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, y_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) + \hat{e}(P, r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) = \hat{e}(P,P)^{h_{\mathrm{ID}_{t,\mathrm{TA}}}}$.

(3) Check if $B_{\mathrm{ID}_{t,\mathrm{TA}}} \stackrel{?}{=} B'_{\mathrm{ID}_{t,\mathrm{TA}}}$. If the equality is satisfied, then the user is legal.

4.3. Registration. When a vehicle V_a is within the transmission range of RSU R_1, the vehicle V_a and R_1 will send an ID verification request to each other. After successful verification, RSU R_1 will then generate the short-term parameters for V_a. Vehicle V_a can retain its anonymity and security using the short-term parameters by executing the following steps.

(1) Use the identity-based cryptography (IBC) technique to generatethe common session key for RSU R_1 and vehicle V_a. Vehicle V_a uses its own private key and the public key of RSU R_1 to generate the common session key. The public key of RSU R_1 is calculated from the true ID of RSU R_1. Therefore, vehicle V_a does not require the public key of RSU R_1. The calculation is as follows:

$$\begin{aligned}\mathrm{SK}_{V_a-R_1} &= \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{i,V_a}}, \mathrm{PU}_{\mathrm{ID}_{t,R_1}}\right) \\ &= \hat{e}\left(\mathrm{PU}_{\mathrm{ID}_{i,V_a}}, h_{\mathrm{ID}_{t,\mathrm{TA}}}\mathrm{PU}_{\mathrm{ID}_{t,R_1}}\right) = \mathrm{SK}_{R_1-V_a}.\end{aligned} \tag{4}$$

Because the TA generates the private keys for both RSU R_1 and vehicle V_a, the common session keys generated from RSU R_1 and vehicle V_a are the same. Therefore, RSU R_1 and vehicle V_a can communicate with each other privately.

(2) V_a generates the short-term parameters $\mathrm{ID}_{p,V_t}, B_{\mathrm{ID}_{p,V_t}}$, and $D_{\mathrm{ID}_{p,V_t}}$ and uses symmetric encryption to encrypt the common session key $(\mathrm{SK}_{V_a-R_1})$ as a security key. The encryption is supplemented by the plain-text parameters $(\mathrm{ID}_{i,V_a}, B_{\mathrm{ID}_{i,V_a}}, \hat{e}(r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, P), y_{\mathrm{ID}_{t,\mathrm{TA}},j}P, T_{l,\mathrm{ID}_{i,V_a}})$. The calculation is as follows:

$$C = \mathrm{SE}\left(\mathrm{ID}_{p,V_t} \parallel B_{\mathrm{ID}_{p,V_t}} \parallel D_{\mathrm{ID}_{p,V_t}} \parallel T_j\right)_{\mathrm{SK}_{V_a-R_1}}. \tag{5}$$

Vehicle V_a sends the message $C \parallel \mathrm{ID}_{i,V_a} \parallel B_{\mathrm{ID}_{i,V_a}} \parallel \hat{e}(r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, P) \parallel y_{\mathrm{ID}_{t,\mathrm{TA}},j}P \parallel T_{l,\mathrm{ID}_{i,V_a}}$ to R_1.

(3) When RSU R_1 receives the message, R_1 first verifies whether the parameters of vehicle V_a are within the valid limits through the following steps.

(3.1) Calculate $w_{\mathrm{ID}_{t,\mathrm{TA}},j} = H(H_2(B_{\mathrm{ID}_{i,V_a}}) \parallel \mathrm{ID}_{i,V_a} \parallel T_{l,\mathrm{ID}_{i,V_a}}) \bmod p$.

(3.2) Calculate $B'_{\mathrm{ID}_{t,\mathrm{TA}}} = \hat{e}(w_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, y_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) + \hat{e}(P, r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) = \hat{e}(P,P)^{h_{\mathrm{ID}_{t,\mathrm{TA}}}}$.

(3.3) Check if $B_{\mathrm{ID}_{t,\mathrm{TA}}} \stackrel{?}{=} B'_{\mathrm{ID}_{t,\mathrm{TA}}}$. If the equality is satisfied, then the user is legal.

(4) To decrypt the encrypted message, RSU R_1 first calculates the common session key shared with vehicle V_a. Then, RSU R_1 uses the common session key to decrypt the message. The calculation is as follows:

$$\begin{aligned}\mathrm{SK}_{R_1-V_a} &= \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{t,R_1}}, \mathrm{PU}_{\mathrm{ID}_{i,V_a}}\right) \\ &= \hat{e}\left(\mathrm{PU}_{\mathrm{ID}_{t,R_1}}, h_{\mathrm{ID}_{t,\mathrm{TA}}}\mathrm{PU}_{\mathrm{ID}_{i,V_a}}\right) = \mathrm{SK}_{V_a-R_1}.\end{aligned} \tag{6}$$

(5) RSU R_1 calculates the private key, the common secret key, and the signature of V_a. The calculations are as follows.

(5.1) R_1 calculates $\mathrm{PR}_{\mathrm{ID}_{p,V_a}}$ as its private key.

(5.2) R_1 chooses $C_{\mathrm{ID}_{p,V_a}} \in Z_q^*$ as its common secret key.

(5.3) R_1 calculates $y_{\mathrm{ID}_{t,R_1},j} = h_{\mathrm{ID}_{t,R_1}}/w_{\mathrm{ID}_{t,R_1},j}$, $\hat{e}(r_{\mathrm{ID}_{t,R_1},j} \cdot P, P)$, $w_{\mathrm{ID}_{t,R_2},j} = H(H_2(B_{\mathrm{ID}_{p,V_a}}) \parallel \mathrm{ID}_{p,V_a} \parallel T_{l,\mathrm{ID}_{p,V_a}}) \bmod p$.

(6) RSU R_1 encrypts the parameters $(\mathrm{PR}_{\mathrm{ID}_{p,V_a}}, C_{\mathrm{ID}_{p,V_a}})$ using the common session key. The calculation is as follows:

$$C = \mathrm{SE}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_a}} \parallel C_{\mathrm{ID}_{p,V_a}} \parallel T_j\right)_{\mathrm{SK}_{R_1-V_a}}. \tag{7}$$

RSU R_1 sends the message $C \parallel \mathrm{ID}_{i,V_a} \parallel \hat{e}(r_{\mathrm{ID}_{t,R_1},j} \cdot P, P) \parallel y_{\mathrm{ID}_{t,R_1},j}P \parallel T_{l,\mathrm{ID}_{p,V_a}}$ to vehicle V_a.

(7) When vehicle V_a receives the message, the vehicle uses the common session key to decrypt the message.

(8) R_1 records $(\mathrm{ID}_{i,V_a}, \mathrm{ID}_{p,V_a}, B_{\mathrm{ID}_{p,V_a}}, D_{\mathrm{ID}_{p,V_a}}, C_{\mathrm{ID}_{t,R_1},j}, T_{l,\mathrm{ID}_{p,V_a}})$ and publishes $(\mathrm{ID}_{p,V_a}, B_{\mathrm{ID}_{p,V_a}}, D_{\mathrm{ID}_{p,V_a}}, \hat{e}(r_{\mathrm{ID}_{t,R_1},j} \cdot P, P), y_{\mathrm{ID}_{t,R_1},j}P, T_{l,\mathrm{ID}_{p,V_a}})$ to all vehicles in its domain.

To improve the efficiency of the handoff process, RSU R_1 generates a common secret key for vehicle V_a and each RSU. RSU R_1 uses a one-way hash chain [13] to generate m keys

Table 1: RID-key table.

ID of RSU	New ID of vehicle (handoff)	ID of vehicle (RSU generate)	ID of vehicle (TA generate)	Common secret key	Expire time of common secret key	BDH value of vehicle	Data key of vehicle	Expire time of key
R_1	ID'_{p,V_a}	ID_{p,V_a}	ID_{i,V_a}	$k_{\mathrm{ID}_{p,V_a},R_1}$	$T_{l,\mathrm{ID}'_{p,V_a}}$	$B_{\mathrm{ID}_{p,V_a}}$	$D_{\mathrm{ID}_{p,V_a}}$	$T_{l,\mathrm{ID}_{p,V_a}}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
R_m	ID''_{p,V_a}	ID_{p,V_a}	ID_{i,V_a}	$k_{\mathrm{ID}_{p,V_a},R_m}$	$T_{l,\mathrm{ID}''_{p,V_a}}$	non	non	non
R_1	ID'_{p,V_b}	ID_{p,V_b}	ID_{i,V_b}	$k_{\mathrm{ID}_{p,V_b},R_1}$	$T_{l,\mathrm{ID}'_{p,V_b}}$	$B_{\mathrm{ID}_{p,V_b}}$	$D_{\mathrm{ID}_{p,V_b}}$	$T_{l,\mathrm{ID}_{p,V_b}}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
R_{m-1}	ID''_{p,V_b}	ID_{p,V_b}	ID_{i,V_b}	$k_{\mathrm{ID}_{p,V_b},R_m}$	$T_{l,\mathrm{ID}''_{p,V_b}}$	non	non	non
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

$k_{\mathrm{ID}_{p,V_a},R_m}, k_{\mathrm{ID}_{p,V_a},R_{m-1}}, \ldots, k_{\mathrm{ID}_{p,V_a},R_1}$. The method for generating the keys is as follows:

$$\begin{aligned} F\left(C_{\mathrm{ID}_{p,V_a}} \parallel \mathrm{PR}_{\mathrm{ID}_{p,V_a}}\right) &= k_{\mathrm{ID}_{p,V_a},R_m}, \\ F\left(k_{\mathrm{ID}_{p,V_a},R_m} \parallel \mathrm{PR}_{\mathrm{ID}_{p,V_a}}\right) &= k_{\mathrm{ID}_{p,V_a},R_{m-1}}, \ldots, \\ F\left(k_{\mathrm{ID}_{p,V_a},R_2} \parallel \mathrm{PR}_{\mathrm{ID}_{p,V_a}}\right) &= k_{\mathrm{ID}_{p,V_a},R_1}. \end{aligned} \tag{8}$$

RSU R_1 uses a one-way hash chain [13] to generate m anonymous IDs $\mathrm{ID}'_{p,V_a}, \mathrm{ID}''_{p,V_a}, \ldots, \mathrm{ID}'''_{p,V_a}$. The method for generating the IDs is as follows:

$$\begin{aligned} F\left(\mathrm{ID}_{p,Va} \parallel \mathrm{PR}_{\mathrm{ID}_{p,V_a}}\right) &= \mathrm{ID}'_{p,V_a}, \\ F\left(\mathrm{ID}'_{p,V_a} \parallel \mathrm{PR}_{\mathrm{ID}_{p,V_a}}\right) &= \mathrm{ID}''_{p,V_a}, \ldots, \\ F\left(\mathrm{ID}''_{p,V_a} \parallel \mathrm{PR}_{\mathrm{ID}_{p,V_a}}\right) &= \mathrm{ID}'''_{p,V_a}. \end{aligned} \tag{9}$$

Each RSU has two tables, an RID-key table and an SID-key table. The RID-key table is used to store the related parameters generated by RSU (Table 1). RSU R_1 uses the common session key that it shares with each RSU to encrypt the common secret key that vehicle V_a has with each RSU and the anonymous ID. RSU R_1 then sends the encrypted message to other RSUs. When another RSU receives the encrypted message, that RSU first uses the common session key that it shares with RSU R_1 to decrypt the message and then stores the parameters for vehicle V_a in the table (Table 2). Because vehicle V_a has the related parameters $(\mathrm{PR}_{\mathrm{ID}_{p,V_a}}, \mathrm{ID}_{p,V_a}, C_{\mathrm{ID}_{p,V_a}})$, it can generate a common secret key shared with each RSU and an anonymous ID on its own. The parameters are stored in the table (Table 3). The parameters for vehicle V_a do not permit any one RSU to obtain the parameters that vehicle V_a shares with other RSUs. Because other RSUs cannot obtain the private key and the common secret key of vehicle V_a, the security of vehicle V_a is ensured.

4.4. Intra-RSU Message Authentication. Vehicle V_a broadcasts messages to other vehicles within the transmission range of an RSU. The calculations are as follows.

(1) Vehicle V_a uses the BDH method to authorize a message signature. The calculations are as follows.

(1.1) Vehicle V_a calculates $w_{\mathrm{ID}_{p,V_a},j} = H(M_{\mathrm{ID}_{p,V_a},j} \parallel \mathrm{ID}_{p,V_a} \parallel T_j) \bmod p$.

(1.2) Vehicle V_a calculates $y_{\mathrm{ID}_{p,V_a},j} = h_{\mathrm{ID}_{p,V_a},j}/w_{\mathrm{ID}_{p,V_a},j}$, $\widehat{e}(r_{\mathrm{ID}_{p,V_a},j} \cdot P, P)^{\circ}$.

(1.3) Vehicle V_a broadcasts the message $\langle M_{\mathrm{ID}_{p,V_a},j}, B_{\mathrm{ID}_{p,V_a}}, D_{\mathrm{ID}_{p,V_a}}, \widehat{e}(r_{\mathrm{ID}_{p,V_a},j} \cdot P, P), y_{\mathrm{ID}_{p,V_a},j} P, \mathrm{ID}_{p,V_a}, T_j \rangle$ to other vehicles within range.

(2) When other vehicles receive the message, they can verify the authenticity of the message. The calculations are as follows.

(2.1) Calculate $w_{\mathrm{ID}_{p,V_a},j} = H(M_{\mathrm{ID}_{p,V_a},j} \parallel \mathrm{ID}_{p,V_a} \parallel T_j) \bmod p^{\circ}$.

(2.2) Calculate $B'_{\mathrm{ID}_{p,V_a}} = \widehat{e}(w_{\mathrm{ID}_{p,V_a},j} \cdot P, y_{\mathrm{ID}_{p,V_a},j} \cdot P) + \widehat{e}(r_{\mathrm{ID}_{p,V_a},j} \cdot P, P) = \widehat{e}(P,P)^{h_{\mathrm{ID}_{t,\mathrm{TA}}}}$.

(2.3) Check if $B_{\mathrm{ID}_{p,V_a}} \stackrel{?}{=} B'_{\mathrm{ID}_{p,V_a}}$. If the equality is satisfied, then vehicle V_a sent the message.

Assuming that two vehicles within the transmission range of a given RSU want to send private messages to each other (Figure 1), vehicle V_a and vehicle V_b will calculate their common key. The calculation is as follows:

$$\begin{aligned} \mathrm{SK}_{V_a-V_b} &= \widehat{e}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_a}}, \mathrm{PU}_{\mathrm{ID}_{p,V_b}}\right) \\ &= \widehat{e}\left(\mathrm{PU}_{\mathrm{ID}_{p,V_a}}, h_{\mathrm{ID}_{t,R_R}} \mathrm{PU}_{\mathrm{ID}_{p,V_b}}\right) = \mathrm{SK}_{V_b-V_a}. \end{aligned} \tag{10}$$

Then, vehicle V_a uses the common session key $(\mathrm{SK}_{V_a-V_b})$ to first encrypt the message and then send it to vehicle V_a. When V_b receives the encrypted message, the vehicle uses the common session key $(\mathrm{SK}_{V_b-V_a})$ to decrypt the message and then obtain the contents of the message. The benefits of using IBC lie in the fact that the other vehicle's public key can be easily calculated based on its ID and that the common session key can be calculated based on the other vehicle's public key

Table 2: SID-key table.

New ID of vehicle (handoff)	Informed by RSU	Common secret key	Expire time of common secret key	BDH value of vehicle	Data key of vehicle	Expire time of key
ID'_{p,V_t}	R_7	$k_{\mathrm{ID}_{p,V_t},R_1}$	$T_{l,\mathrm{ID}'_{p,V_t}}$	non	non	non
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$\mathrm{ID}''_{p,V_{t-7}}$	R_m	$k_{\mathrm{ID}_{p,V_{t-7}},R_1}$	$T_{l,\mathrm{ID}''_{p,V_{t-7}}}$	non	non	non
ID'_{p,V_c}	R_{m-2}	$k_{\mathrm{ID}_{p,V_c},R_1}$	$T_{l,\mathrm{ID}'_{p,V_c}}$	$B_{\mathrm{ID}_{p,V_c}}$	$D_{\mathrm{ID}_{p,V_c}}$	$T_{l,\mathrm{ID}_{p,V_c}}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
ID''_{p,V_d}	R_7	$k_{\mathrm{ID}_{p,V_d},R_1}$	$T_{l,\mathrm{ID}''_{p,V_d}}$	$B_{\mathrm{ID}_{p,V_d}}$	$D_{\mathrm{ID}_{p,V_d}}$	$T_{l,\mathrm{ID}_{p,V_d}}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Table 3: SID issue table.

ID of RSU	New ID of vehicle (handoff)	ID of vehicle (RSU generate)	ID of vehicle (TA generate)	Common secret key	Private key (RSU)	Secret value	Expire time of key
R_1	ID'_{p,V_a}	ID_{p,V_a}	ID_{i,V_a}	$k_{\mathrm{ID}_{p,V_a},R_1}$	$\mathrm{PR}_{\mathrm{ID}_{p,V_a}}$	$h_{\mathrm{ID}_{p,V_a}}$	$T_{l,\mathrm{ID}_{p,V_a}}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
R_m	ID''_{p,V_a}	ID_{p,V_a}	ID_{i,V_a}	$k_{\mathrm{ID}_{p,V_a},R_m}$	non	non	non

and its own private key. Conversely, the other vehicle can also calculate the common session key because the secret value of the common session key is the same.

4.5. Inter-RSU Message Authentication. Assuming that vehicle V_a wants to broadcast a message within the transmission ranges of several RSUs and uses the BDH signature to ensure the security of the message, vehicle V_a will first send the parameters $\langle M_{\mathrm{ID}_{p,V_a},j}, \hat{e}(r_{\mathrm{ID}_{p,V_a},j} \cdot P, P), y_{\mathrm{ID}_{p,V_a},j}P, B_{\mathrm{ID}_{p,V_a}}, \mathrm{ID}_{p,V_a}, y_{\mathrm{ID}_{t,R_1},j} \cdot P, \hat{e}(r_{\mathrm{ID}_{t,R_1},j} \cdot P, P) \cdot T_{l,\mathrm{ID}_{p,V_t}}, T_j\rangle$ to nearby RSUs, and then the RSUs will relay the message to other vehicles. Then, other vehicles will first verify the legitimacy of vehicle V_a by calculating $w_{\mathrm{ID}_{t,R_1},j} = H(H_2(B_{\mathrm{ID}_{p,V_a}}) \parallel \mathrm{ID}_{p,V_a} \parallel T_{l,\mathrm{ID}_{p,V_a}}) \bmod p$ and then calculating $\hat{e}(w_{\mathrm{ID}_{t,R_1},j}P, y_{\mathrm{ID}_{t,R_1},j}P) + \hat{e}(r_{\mathrm{ID}_{t,R_1},j}P, P) = B'_{\mathrm{ID}_{\mathrm{ID}_{t,R_1}}}$. If it is the case, then it proves that vehicle V_a is the legitimate user of RSU R_1.

Other vehicles will verify the authenticity of the message from vehicle V_a by first calculating $w_{\mathrm{ID}_{p,V_a},j} = H(M_{\mathrm{ID}_{p,V_a},j} \parallel \mathrm{ID}_{p,V_a} \parallel T_j) \bmod p$ and then calculating $\hat{e}(w_{\mathrm{ID}_{p,V_a},j}P, y_{\mathrm{ID}_{p,V_a},j}P) + \hat{e}(r_{\mathrm{ID}_{p,V_a},j}P, P) = B'_{\mathrm{ID}_{p,V_a},j}$. If it is the case, then the message was sent from vehicle V_a.

In private communications, the secret private key value of each vehicle is different because there are multiple RSUs. Therefore, an ID-based encryption method should be used. Let vehicle V_a and vehicle V_c calculate their common session keys. Assuming that vehicle V_a wants to privately communicate with vehicle V_c, which is within the transmission range of a different RSU, vehicle V_c will first encrypt the message. Vehicle V_a will then calculate the public key using the anonymous ID of vehicle V_c. Upon obtaining the data key for vehicle V_c, vehicle V_a will encrypt the message using the public key and the data key of vehicle V_c. The calculation is as follows:

$$\begin{aligned} C &= E_{\mathrm{IBC}}\left(r, M, \mathrm{PU}_{\mathrm{ID}_{p,V_c}}, D_{\mathrm{ID}_{p,V_c}}\right) \\ &= \left\{r \cdot P, M \oplus H_2\left(e\left(\mathrm{PU}_{\mathrm{ID}_{p,V_c}}, D_{\mathrm{ID}_{p,V_c}}\right)^r\right)\right\}, \\ M &= \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_a}}, \mathrm{PU}_{\mathrm{ID}_{p,V_c}}\right). \end{aligned} \tag{11}$$

Subsequently, vehicle V_c uses the private key to decrypt the message. Equation (2) shows the decryption method. Vehicle V_c then uses ID-based encryption to generate an encrypted message for vehicle V_a. The calculation is as follows:

$$\begin{aligned} C &= E_{\mathrm{IBC}}\left(r, M, \mathrm{PU}_{\mathrm{ID}_{p,V_a}}, D_{\mathrm{ID}_{p,V_a}}\right) \\ &= \left\{r \cdot P, M \oplus H_2\left(e\left(\mathrm{PU}_{\mathrm{ID}_{p,V_a}}, D_{\mathrm{ID}_{p,V_a}}\right)^r\right)\right\}, \\ M &= \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_a}}, \mathrm{PU}_{\mathrm{ID}_{p,V_c}}\right) + \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_c}}, \mathrm{PU}_{\mathrm{ID}_{p,V_a}}\right). \end{aligned} \tag{12}$$

Vehicle V_a uses the private key to decrypt the message. Equation (2) shows the decryption method. When vehicle V_a receives thecommon session key that it shares with vehicle V_c, V_a can communicate with vehicle V_c privately. The common session key is

$$\begin{aligned} \mathrm{SK}_{V_a-V_c} &= \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_a}}, \mathrm{PU}_{\mathrm{ID}_{p,V_c}}\right) + \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_c}}, \mathrm{PU}_{\mathrm{ID}_{p,V_a}}\right) \\ &= \mathrm{SK}_{V_c-V_a}. \end{aligned} \tag{13}$$

4.6. Handoff Problem. When vehicle V_a comes within the transmission range of the next RSU (R_2), vehicle V_a will first inquire for the common secret key that it shares with RSU R_2 in Table 3 and then initiate the handoff. The calculation is as follows.

(1) Vehicle V_a first generates short-term parameters $B_{\mathrm{ID}_{p,V_t}}$, $D_{\mathrm{ID}_{p,V_t}}$ and uses the common secret key $(k_{\mathrm{ID}_{p,V_a},R_2})$ to encrypt the parameters. Then, vehicle V_a sends the parameters and its anonymous ID to RSU R_2.

(2) RSU R_2 inquires for the common secret key and the time of validity that it shares with vehicle V_a in Table 2 based on the anonymous ID of vehicle V_a. If the time of validity has expired, then vehicle V_a will reregister with RSU (Section 4.2). If the time of validity has not expired, R_2 will generate the short-term parameters for vehicle V_a. The calculations are as follows.

(2.1) R_2 calculates $\mathrm{PR}_{\mathrm{ID}_{p,V_a}}$ as its private key.

(2.2) R_2 calculates $w_{\mathrm{ID}_{t,R_2},j} = H(H_2(B_{\mathrm{ID}_{p,V_a}}) \parallel \mathrm{ID}_{p,V_a} \parallel T_{l,\mathrm{ID}_{p,V_a}}) \bmod p$.

(2.3) R_2 calculates $y_{\mathrm{ID}_{t,R_2},j} = h_{\mathrm{ID}_{t,R_2}}/w_{\mathrm{ID}_{t,R_2},j}, \hat{e}(r_{\mathrm{ID}_{t,R_2},j} \cdot P, P)$.

(3) RSU R_1 uses the common secret key to encrypt the parameters $(\mathrm{PR}_{\mathrm{ID}_{p,V_a}}, C_{\mathrm{ID}_{p,V_a}})$. The calculation is as follows:

$$C = \mathrm{SE}\left(\mathrm{PR}_{\mathrm{ID}_{p,V_a}} \parallel \mathrm{C}_{\mathrm{ID}_{p,V_a}} \parallel T_j\right)_{\mathrm{SK}_{R_1-V_a}}. \tag{14}$$

RSU R_1 sends the message $C \parallel \mathrm{ID}_{i,V_a} \parallel \hat{e}(r_{\mathrm{ID}_{t,R_1},j} \cdot P, P) \parallel y_{\mathrm{ID}_{t,R_1},j}P \parallel T_{l,\mathrm{ID}_{p,V_a}}$ to vehicle V_a.

(4) When vehicle V_a receives the message, the vehicle uses the common secret key to decrypt the message.

(5) R_1 records $(\mathrm{ID}_{i,V_a}, \mathrm{ID}_{p,V_a}, B_{\mathrm{ID}_{p,V_a}}, D_{\mathrm{ID}_{p,V_a}}, C_{\mathrm{ID}_{t,R_1},j}, T_{l,\mathrm{ID}_{p,V_a}})$ and publishes $(\mathrm{ID}_{p,V_a}, B_{\mathrm{ID}_{p,V_a}}, D_{\mathrm{ID}_{p,V_a}}, \hat{e}(r_{\mathrm{ID}_{t,R_1},j} \cdot P, P), y_{\mathrm{ID}_{t,R_1},j}P, T_{l,\mathrm{ID}_{p,V_a}})$ to all vehicles in its domain.

4.7. Message Authentication When RSUs Are Not Available. When RSUs are not available, vehicles can broadcast messages and conduct private communications using the parameters generated by the TA by executing the following steps.

(1) Vehicle V_d uses the BDH signature method to authorize a message signature. The calculations are as follows.

(1.1) Vehicle V_d calculates $w_{\mathrm{ID}_{i,V_d},j} = H(M_{\mathrm{ID}_{i,V_d},j} \parallel \mathrm{ID}_{i,V_d} \parallel T_j) \bmod p$.

(1.2) Vehicle V_d calculates $y_{\mathrm{ID}_{i,V_d},j} = h_{\mathrm{ID}_{i,V_d},j}/w_{\mathrm{ID}_{i,V_d},j}, \hat{e}(r_{\mathrm{ID}_{i,V_d},j} \cdot P, P)$.

(1.3) Vehicle V_d broadcasts the message $\langle M_{\mathrm{ID}_{i,V_d},j}, B_{\mathrm{ID}_{i,V_d}}, D_{\mathrm{ID}_{i,V_d}}, \hat{e}(r_{\mathrm{ID}_{i,V_d},j} \cdot P, P), y_{\mathrm{ID}_{i,V_d},j}P, \mathrm{ID}_{i,V_d}, T_j, \hat{e}(r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, P), y_{\mathrm{ID}_{t,\mathrm{TA}},j}P\rangle$ to other vehicles.

(2) Other vehicles first verify the ID of vehicle V_d. The calculations are as follows.

(2.1) Calculate $w_{\mathrm{ID}_{t,\mathrm{TA}},j} = H(H_2(B_{\mathrm{ID}_{i,V_d}}) \parallel \mathrm{ID}_{i,V_d} \parallel T_{l,\mathrm{ID}_{i,V_d}}) \bmod p$.

(2.2) Calculate $B'_{\mathrm{ID}_{t,\mathrm{TA}}} = \hat{e}(w_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P, y_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) + \hat{e}(P, r_{\mathrm{ID}_{t,\mathrm{TA}},j} \cdot P) = \hat{e}(P,P)^{h_{\mathrm{ID}_{t,\mathrm{TA}}}}$.

(2.3) Check if $B_{\mathrm{ID}_{t,\mathrm{TA}}} \stackrel{?}{=} B'_{\mathrm{ID}_{t,\mathrm{TA}}}$. If the equality is satisfied, then the user is legal.

(3) Other vehicles then verify the authenticity of the message. The calculations are as follows.

(3.1) Calculate $w_{\mathrm{ID}_{i,V_d},j} = H(M_{\mathrm{ID}_{i,V_d},j} \parallel \mathrm{ID}_{i,V_d} \parallel T_j) \bmod p$.

(3.2) Calculate $B'_{\mathrm{ID}_{i,V_d}} = \hat{e}(w_{\mathrm{ID}_{i,V_d},j} \cdot P, y_{\mathrm{ID}_{i,V_d},j} \cdot P) + \hat{e}(r_{\mathrm{ID}_{i,V_d},j} \cdot P, P) = \hat{e}(P,P)^{h_{\mathrm{ID}_{t,\mathrm{TA}}}}$.

(3.3) Check if $B_{\mathrm{ID}_{i,V_d}} \stackrel{?}{=} B'_{\mathrm{ID}_{i,V_d}}$. Satisfaction of the equality is proof that vehicle V_d sent the message.

Assuming that two vehicles within the transmission range of the same RSU want to communicate privately with each other (Figure 1), vehicle V_d and vehicle V_e will calculate their common key. The calculation is as follows:

$$\begin{aligned}\mathrm{SK}_{V_d-V_e} &= \hat{e}\left(\mathrm{PR}_{\mathrm{ID}_{i,V_d}}, \mathrm{PU}_{\mathrm{ID}_{i,V_e}}\right) \\ &= \hat{e}\left(\mathrm{PU}_{\mathrm{ID}_{i,V_d}}, h_{\mathrm{ID}_{t,\mathrm{TA}}}\mathrm{PU}_{\mathrm{ID}_{i,V_e}}\right) = \mathrm{SK}_{V_e-V_d}.\end{aligned} \tag{15}$$

Subsequently, vehicle V_d uses the common session key $(\mathrm{SK}_{V_d-V_e})$ to encrypt the message and send the message to vehicle V_e. When vehicle V_e receives the encrypted message, it uses the common session key $(\mathrm{SK}_{V_e-V_d})$ to decrypt the message and obtain the contents of the message.

5. Security and Performance Analysis

This section gives a security analysis to demonstrate that the method developed in this study can provide confidentiality, authentication, nonrepudiation, conditional anonymity, and conditional untraceability. A performance analysis is conducted by comparing the results of the present study with those in [12–15].

5.1. Security Analysis. The following subsections discuss the specific aspects of the security analysis of the proposed method.

(1) Confidentiality. Assuming that the ID of every node is not repeated as confidential communications are occurring

Table 4: The comparison of property.

Property	Method				
	[12]	[13]	[14]	[15]	Proposed method
Security and privacy preservation	YES	YES	YES	YES	YES
Do need the certificate	NO	NO	NO	YES	NO
Do need the help of RSU for authentication	NO	NO	NO	NO	NO
PKI-based system	NO	NO	NO	NO	NO
Communication within different RSU	YES	YES	YES	YES	YES
Privacy communicate	NO	NO	NO	NO	YES

among vehicles within the range of a single RSU, the property of IBC is used to establish the common session keys. The common session key of a vehicle is calculated based on the bilinear pairings map. According to the elliptic curve discrete logarithm problem (ECDLP), the common session key of a malicious node b and node a is $SK_{b\text{-}a}$. It is difficult for node b to determine a secret value from $SK_{b\text{-}a}$, node b's private key (PR_b) and node a's public key (PU_a). Other vehicles are unable to calculate the common session key from their own private keys and the public keys of nodes a and b, and thus the security of confidential communications is ensured.

(2) Authentication and Nonrepudiation. As a vehicle registers and gains the trust of an RSU, the RSU will broadcast the vehicle's G_2 value to all vehicles within range, and that specific G_2 represents the vehicle itself. The parameters $\langle M_{\mathrm{ID},j}, B_{\mathrm{ID}}, D_{\mathrm{ID}}, y_{\mathrm{ID},j}P, \mathrm{ID}, T_j\rangle$ are broadcast as the vehicle is broadcasting messages. Other vehicles will calculate $w_{\mathrm{ID},j} = H(M_{\mathrm{ID},j} \parallel \mathrm{ID} \parallel T_{\mathrm{ID},j}) \bmod p$ upon receipt of the messages and then calculate $B'_{\mathrm{ID}} = \hat{e}(w_{\mathrm{ID},0}P, y_{\mathrm{ID},j}P) + \hat{e}(r_{\mathrm{ID},0}P, P) = \hat{e}(P,P)^{h_{\mathrm{ID}}}$. Other vehicles are unable to calculate $y_{\mathrm{ID},j}$ from $y_{\mathrm{ID},j}P$ based on the ECDLP, but $r_{\mathrm{ID},0}$, $y_{\mathrm{ID},j}$, and $w_{\mathrm{ID},j}$ can be calculated from the parameters B_{ID}, $y_{\mathrm{ID},j}P$ based on the BDH method, provided that the equality $B_{\mathrm{ID}} = B'_{\mathrm{ID}}$, which is calculated from the messages of the vehicle, is satisfied. Therefore, the vehicle sending the messages achieves undeniability, and the source of the messages is known.

(3) Conditional Anonymity. The true ID of a vehicle is known only to the TA. An anonymous ID (ID_i) is used when a vehicle registers with the TA, and this anonymous ID (ID_i) is renewed every time the vehicle registers with the TA. A vehicle will renegotiate a new anonymous ID (ID_p) within the range of every RSU. Therefore, it is difficult for another vehicle to obtain the true ID of the vehicle by tracking ID_i from ID_p because the true IDs of the vehicles are known only to the TA and the individual vehicles bearing those IDs. Every RSU knows the anonymous ID (ID_i) of each vehicle, but each vehicle has a different ID (ID_p) for every RSU, which prevents malicious RSUs from tracking the current location of the vehicle.

(4) Conditional Untraceability. When a vehicle is involved in a criminal act, an RSU is able to trace the anonymous ID (ID_i) from the vehicle's anonymous ID (ID_p). The RSU transmits ID_i to the TA, which in turn identifies the true ID of the vehicle with the identity ID_i. Every vehicular parameter will eventually expire, therefore ensuring the validity of the anonymous ID of a vehicle.

Table 5: Bilinear pairings execution time in milliseconds.

Notations	Descriptions	Execution time (ms)
T_p	Pairing operation	≈4.5
T_m	Point multiplication	≈0.6
T_e	Field exponentiation	≈0.54

Table 6: RSA/HMAC execution time in milliseconds.

Notations	Descriptions	Execution time (ms)
ASE	RSA encryption	0.19
ASD	RSA decryption	4.65
HMAC	HMAC	0.002
SE	AES encryption	<0.19
SD	AES decryption	<4.65

Table 7: The length of the parameters.

Parameters	Length (bit)	Parameters	Length (bit)
G_1	160	AES	128
G_2	160	Variable	32
HMAC	160	Message (M)	1024
RSA	1024	Random number (r)	128

5.2. Performance Analysis. The method developed in this study was compared with those in [12–15] regarding performance, execution time, and data volume. Table 4 compares the results of the present study and those of [12–15], showing that the method developed in the present study is superior to the other methods.

To analyze efficiency, the times required for a message to be broadcast and verified in the present study and in [12–15] were calculated, and the results are listed in Tables 5–7. Table 8 shows the results of the efficiency analysis. The experimental results show that the method proposed in this paper is superior to those in other literatures regardless of computational complexity and packet length. The network security mechanisms proposed in literature [14] and this paper are both based on the use of bilinear pairing, so all the packet lengths are within a reasonable range. However, in

Table 8: Performance analysis.

Property	Method				
	[12]	[13]	[14]	[15]	Proposed method
The broadcast message	Signing: $5 * T_m + 3 * T_p$ Verification $4 * T_m + 4 * T_p$	Signing: $1 * T_p$ Verification $3 * T_p$	Signing: $5 * T_m$ Verification $6 * T_m + 1 * T_p$	Signing: $2 * T_m$ Verification $2 * T_m$	Signing $T_p + 2 * T_m$ Verification $T_p + T_m$
Spending time	36.4 ms	18 ms	11.1 ms	18 ms	10.8 ms
The length of ciphertext	1112 bits	480 bits	480 bits	$(160 * 160) + 320$ bits	480 bits
Handoff	$3 * T_p$	N/A	$4 * T_m + 2 * T_p$	$5 * T_m$	$2 * \mathrm{SE} + 2 * \mathrm{SD}$
Spending time	13.5 ms	N/A	11.4 ms	3 ms	<9.68 ms
The length of ciphertext	480 bits	N/A	1280 bits	$160 * 160 * 160$ bits	2048 bits
Communication between different RSUs	Signing: $5 * T_m + 3 * T_p$ Verification $4 * T_m + 4 * T_p$	Signing: $1 * T_p$ Verification $3 * T_p$	Signing: $5 * T_m$ Verification $6 * T_m + 1 * T_p$	Signing: $2 * T_m$ Verification $2 * T_m$	Signing $T_p + 2 * T_m$ Verification $2 * T_p + 2 * T_m$
Spending time	36.4 ms	18 ms	11.1 ms	18 ms	15.9 ms
The length of ciphertext	1112 bits	480 bits	480 bits	$(160 * 160) + 320$ bits	960 bits
Privacy communicate	N/A	N/A	N/A	N/A	Signing T_p + SE Verification T_p + SD
Spending time	N/A	N/A	N/A	N/A	<13.84 ms
The length of ciphertext	N/A	N/A	N/A	N/A	1024 bits

computational complexity, the proposed method is superior to that of literature [14]. In literature [15], there are network security mechanisms based on chameleon hashing, which employ exponential calculation. The multiplication result of three values will be huge. Although the computational complexity is not high, the transfer of large amounts of packets will affect network bandwidth and also cause packet losses in VANETs environment.

6. Conclusion

VANETs improve transportation safety and efficiency. If the information shared between vehicles is tampered with, there will be dire consequences such as vehicle collisions. The scheme proposed in this study ensures the security of the information shared between vehicles and is superior to other schemes in terms of message verification and handoff. Additionally, in terms of security, the scheme in this study ensures conditional untraceability, conditional anonymity, authentication, and nonrepudiation. Future work will include supplementing the scheme proposed in this study with revocation and trust mechanisms to corroborate the security scheme.

Notations

Notations of the BDH

h_i: The user i chooses a random number $h_i \in Z_q^*$ as its secret value
B_i: The public value of user i such that $\hat{e}(h_i P, P)$
$y_{i,j}$: The $y_{i,j}$ is the quotient
$r_{i,j}$: The $r_{i,j}$ is the remainder
$w_{i,j}$: $w_{i,j} = H(M_{i,j} \parallel T_j) \bmod p$.

Notation Used in This Paper

$\hat{e}$: Bilinear mapping
G_1: Additive group
G_2: Multiplicative group
P: Generator of G_1
SE$(\cdot)$: A secure symmetric encryption algorithm
$E_{\mathrm{IBC}}(\cdot)$: ID-based encryption
$D_{\mathrm{IBC}}(\cdot)$: ID-based decrypt
PU_k: Public key of node k
PR_k: Private key of node k
D_k: Data key of node k
$\mathrm{ID}_{t,k}$: Real identity of node k
$\mathrm{ID}_{i,k}$: Original pseudonym of node k
$\mathrm{ID}_{p,k}$: Requested pseudonym of node k
h_k: Secret value of node k
C_i: Handoff secret value
B_k: The public value of user k such that $\hat{e}(h_i P, P)$
$\mathrm{SK}_{k\text{-}j}$: The common session key between node k and node j
$k_{i\text{-}j}$: The common secret key between node i and node j
Z_q^*: Z_q^* is the finite field of mod q
$H(\cdot)$: Hash function such that $\{0,1\}^* \rightarrow Z_q^*$
$H_1(\cdot)$: Hash function such that $\{0,1\}^* \rightarrow G_1^*$
$H_2(\cdot)$: Hash function such that $G_2^* \rightarrow \{0,1\}^*$

T_j: Time interval j
$T_{l,i}$: Lifetime of the corresponding parameters
$\|$: The message concatenation operation, which appends several messages together in a special format.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This paper is the partial result of project MOST103-2632-E-366-001 and 103-2221-E-268-003. The authors would like to thank the supporting of Ministry of Science and Technology, Taiwan.

References

[1] IEEE, "Draft, amendment for wireless access in vehicular environments (WAVE)," IEEE P802.11p/D6, 2009.

[2] Dedicated Short Range Communication (DSRC), http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[3] U.S. Department of Transportation and National Highway Traffic Safety Administration, Vehicle Safety Communications Project, 2006.

[4] C. Xu, F. Zhao, J. Guan, H. Zhang, and G. M. Muntean, "QoE-driven user-centric vod services in urban multihomed P2P-based vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2273–2289, 2013.

[5] G. Marfia, M. Roccetti, A. Amoroso, and G. Pau, "Safe driving in LA: report from the greatest intervehicular accident detection test ever," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, pp. 522–535, 2013.

[6] R. Lu, X. Lin, Z. Shi, and X. S. Shen, "A lightweight conditional privacy-preservation protocol for vehicular traffic-monitoring systems," *IEEE Intelligent Systems*, vol. 28, no. 3, pp. 62–65, 2013.

[7] IEEE Trial-Use Standard, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE), Networking Services," IEEE 1609, 2006.

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

[9] G. Kounga, T. Walter, and S. Lachmund, "Proving reliability of anonymous information in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 6, pp. 2977–2989, 2009.

[10] A. Wasef, Y. Jiang, and X. Shen, "DCS: an efficient distributed-certificate-service scheme for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 533–549, 2010.

[11] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[12] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127–139, 2012.

[13] S. Biswas and J. Misic, "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, 2013.

[14] L.-Y. Yeh and J.-L. Huang, "PBS: a portable billing scheme with fine-grained access control for service-oriented vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 11, pp. 2606–2619, 2014.

[15] S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2794–2803, 2014.

[16] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Transactions on Computers*, vol. 63, no. 2, pp. 510–524, 2014.

[17] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 213–229, Springer, Berlin, Germany, 2001.