Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 231976, 13 pages
http://dx.doi.org/10.1155/2014/231976

Research Article

Using BDH for the Message Authentication in VANET

Mei-Wen Huang,[1] Hsin-Te Wu,[2] Gwo-Jiun Horng,[3] and Wen-Shyong Hsieh[1,4]

[1] *Department of Computer Science and Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan*
[2] *Department of Information Management, Fortune Institute of Technology, Kaohsiung, Taiwan*
[3] *Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Tainan, 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 9 June 2014; Accepted 29 August 2014; Published 25 September 2014

Academic Editor: Teen-Hang Meen

The transport message security provided by vehicles in VANETs is quite important; vehicle message should be real-time and it will be not complicated to validate message calculation. The method proposed in the essay is mainly to validate the identity by means of Bilinear Diffie-Hellman method, and make vehicles validate the authenticity of RSU and TA's identity and the effectiveness of key. RSU and TA only need to validate vehicle identity, without helping vehicles produce any key. When vehicle identity validation is completed, vehicles will produce public value and transmit it to other RSU and vehicles, while other vehicles could validate the identity through the message from the sender and public value from RSU. The advantages of the method proposed in this essay are listed as follows. (1) Vehicles, RSU, and TA can validate mutual identities and the effectiveness of keys. (2) Vehicles can produce public value functions automatically, thus reducing key control risks. (3) Vehicles do not need to show certificates to validate their identities, preventing the certificates from attacking because of long-term exposure. (4) Vehicles adopt a pseudonym ID challenge to validate their own identities during the process of handoff. (5) Vehicle messages can be validated using the Bilinear Diffie-Hellman (BDH) method without waiting for the RSU to validate messages, thus improving the instantaneity of messaging. The method proposed in the essay can satisfy source authentication, message integrity, nonrepudiation, privacy, and conditional untraceability requirements.

1. Introduction

Especially VANET receives special attention in terms of traffic security and traffic management [1, 2]. In order to reach the demand of vehicle security, vehicles often broadcast traffic related message among themselves (vehicle position, speed, traffic accidents, and so on) and other services [3], which could reduce traffic jams and dangerous road sections and improve the driving security. VANET usually has two message transmission modes: (1) message broadcast mode, through which vehicles could make other vehicles nearby know the traffic condition in the neighborhood; (2) one hop message transmission, through which vehicles could transmit message to the designated vehicle and which is mainly used for private communication among vehicles.

The essay mainly investigates message security and integral security system layout in VANET, which aims at vehicles' safety on road. Each vehicle could use broadcast mode and inform other vehicles of the traffic condition nearby, so as to avoid traffic jam and improve driving efficiency. They could also use private communication and RSU or TA (trusted authority) for updating. Assume this message was maliciously attacked or forged, it would cause vehicle collision or traffic jam; so message integrity and source authentication is the important key.

The method proposed in the essay is based on RSU. Suppose that each main road was provided with RSU and secondary roads were not. In the whole system framework, TA utilizes Bilinear Diffie-Hellman to generate public/private key and other parameters of its own and RSU, where the

effective time of key is added, so TA and RSU is forced to change key regularly and improve system security and all vehicles could validate the legality of RSU through public key and other parameters of RSU and by means of Bilinear Diffie-Hellman.

We adopt two-level pseudonym method; that is to say, vehicles have the first-level pseudonym ID in TA and the second-level pseudonym ID in RSU. There is no relationship between the two levels of pseudonym ID in terms of original generation modes, which avoids RSU maliciously conspiring and tracing vehicles. TA and RSU are only responsible for validating vehicle identity, not for the vehicle broadcast message. After the identity authentication of vehicles and RSU, vehicles would transmit public value to RSU, which will then send the public value to each RSU and vehicle, so when a vehicle is broadcasting message, all vehicles could validate the message integrity through the method of Bilinear Diffie-Hellman, without using RSU. Meanwhile, the calculation of Bilinear Diffie-Hellman signatures is not very complicated and the key of Bilinear Diffie-Hellman signatures for vehicles is different each time, so it is unable to get forged and attacked.

During the process of handoff, vehicles adopt pseudonym ID challenge method to validate their own identities, which only need communicate pseudonym generation mode with the next RSU. As only vehicles and RSU know the pseudonym generation mode, if the challenge is successful, the identities could be validated mutually, so as to reduce the identity validation time when vehicles are handoff. Meanwhile, vehicles have different public values and pseudonym ID in each RSU.

2. Related Works

Public key infrastructure (PKI) method is used in [9]. Suppose that TA issues certificates; each vehicle has private key and certificates have public key relative to private key; when vehicle a is about to communicate with another vehicle b, a will use the public key in b's certificates to encrypt the message, then a transmits the encrypted message to b, and b decrypts the message through private key. As the certificates are issued by TA, so they are reliable. Provided that b could decrypt the message, the message integrity could be confirmed. Vehicles utilizing PKI for message encrypting and decrypting would improve the calculation complexity and bring great calculation burden during the communication process. In order to protect privacy and not to be traced, certificates must be changed frequently, which will cause burden on TA.

A dynamic privacy-preserving key management scheme for location-based services in VANETs was proposed in [4]. 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 [4] are complicated, and the author did not investigate a private communication scheme.

In [5], when vehicles are able to get some network access services from RSU, they must broadcast a message and establish common key with vehicles receiving the message, and then this common key could be utilized to guarantee the security while communicating the message. However, the establishment of common key is got through pairing computation of identity-based cryptography (IBC) [10], whose calculation is much more complicated than normal computation, and the calculation burden is quite great. The essay does not discuss the problems when vehicles rekey or change pseudonym ID, which is quite important to VANETs, so it is necessary to propose the solutions.

In [6], 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 literature [7] proposed that a driver can check the status of a road through VANET, the transmission process that utilizes bilinear technology to ensure information security and vehicle privacy. Either a vehicle or an RSU must have identity verification with TA and related key generation. Identity verification utilizes bilinear technology to ensure information security and nonrepudiation. Traditional asymmetric encryption, symmetric encryption, and signature are used for messaging of any unit (vehicle, RSU, or TA). In the literature [7] TA must constantly change the master secret key of a vehicle or RSU, which results in a heavy computational load of TA, and the messaging using asymmetric encryption will cause the same problem during decryption.

The literature [8] proposed message batch verification and group message signing and verification for vehicle privacy and information security. Vehicles form a group and each group has a related key for message encryption and decryption. Because the message is sent by a group, it cannot be traced back to a specific vehicle. If a vehicle in the group sends a malicious message, however, it may also be difficult to track down and batch verification will delay real-time messaging.

The literature [11] primarily involves group message signing improvement. This paper has improved the group message signing performance, but has not discussed private communications between vehicles or the replacement of relevant vehicle parameters. A vehicle is vulnerable to tracking if the relevant parameters are not replaced regularly.

3. Background

3.1. Bilinear Pairings and Hard Problems. Let G_1 and G_2 denote an additive and a multiplicative group, and both of them are 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 [12] and Tate [13] pairings on elliptic curves. We consider the implementation of a Tate pairing on a Miyaji-Nakabayashi-Takano (MNT) curve [14] 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 [15] which will be applied in the essay subsequently.

Bilinear Diffie-Hellman (BDH) 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. Boneh and Franklin's ID-Based Encryption. We use Boneh and Franklin's ID-Based Encryption [13] to encrypt and decrypt message. Let k be the system security parameter. Then PKG selects two groups G_1 and G_2 of prime order q, a bilinear mapping $e = G_1 \times G_1 \rightarrow G_2$, and a generator P of group G_1. PKG also picks a random number $s \in Z_q^*$ as its master key and then selects two distinct hash functions: $H_1 : \{0,1\}^* \rightarrow G_1^*$, $H_2 : G_2 \rightarrow \{0,1\}^*$. At last, PKG publishes the system parameters $(q, G_1, G_2, e, P, H_1, H_2)$ and keeps g secretly.

Assume there are two users a and b. User a utilizes the public key of User b to encrypt message M; the identity of User b is $\mathrm{ID}_b \in \{0,1\}^*$, with the public key, private key, and data key being $\mathrm{PU}_b = H_1(\mathrm{ID}_b)$, $\mathrm{PR}_b = s \cdot H_1(\mathrm{ID}_b)$, and $\mathrm{PD}_b = s \cdot P$, respectively, and User a selects random number $r \in Z_q^*$ randomly. The message encryption process is as follows:

$$C = \left\{ r \cdot P, M \oplus H_2\left(e\left(\mathrm{PU}_b, \mathrm{PD}_b\right)^r\right)\right\}, \tag{2}$$

where $C = \{U, V\}$ is the encrypted message, User a sends the encrypted message to User b, and then User b utilizes private key for decryption and works out message M after receiving the message, with the calculation as follows:

$$\begin{aligned} e\left(\mathrm{PR}_b, U\right) &= e\left(s \cdot \mathrm{PU}_b, r \cdot P\right) = e\left(\mathrm{PU}_b, \mathrm{PD}_b\right)^r, \\ V \oplus H_2\left(e\left(\mathrm{PR}_b, U\right)\right) &= V \oplus H_2\left(e\left(\mathrm{PU}_b, \mathrm{PD}_b\right)^r\right) = M. \end{aligned} \tag{3}$$

3.3. J. H. Cheon, Y. Kim, and H. J. Yoon's ID-Based Signature. We use J. H. Cheon, Y. Kim, and H. J. Yoon's ID-Based Signature [14] to attain message signatures and the section uses the system parameters $(q, G_1, G_2, \hat{e}, P, H_1, H_2)$ PKG publishes in Section 3.2 and keeps g secretly. Assume User b signatures message M and broadcasts it to other users, who then use the public key and data key of User b to validate the source and message integrity of signature after receiving signatures. User b selects random number $r \in Z_q^*$ at random, with the calculation as follows:

$$\begin{aligned} U &= r \cdot P, \\ h &= (M, U), \\ V &= r \cdot \mathrm{PU}_b + h \cdot \mathrm{PR}_b. \end{aligned} \tag{4}$$

When other users receive M, U, and V, they can utilize the public key and public parameter of User b to validate signatures, and the signature validation calculation is as follows:

$$e\left(\mathrm{PU}_b, U + h \cdot \mathrm{PD}_b\right) = e\left(V, P\right). \tag{5}$$

3.4. Bilinear Diffie-Hellman (BDH) Messages Authentication. The essay applies the features of bilinear pairings hard problems [15]. Though the calculation time increases, it is acceptable if the calculation is reasonable. The method we propose assumes that users select two random numbers γ_i and α_i at random, where $m_i = 1/H_4(M \| T_{\mathrm{stamp}})$; then we calculate public value as follows:

$$d = \alpha_i * \gamma_i * m_i. \tag{6}$$

Next, we apply them to bilinear pairings, with the calculation as follows:

$$D = e\left(d \cdot P, P\right) = e(P,P)^d, \tag{7}$$

$$D = e\left(\alpha_i \cdot P, m_i \cdot \gamma_i \cdot P\right) = e(P,P)^{\alpha_i m_i \gamma_i}. \tag{8}$$

If users release message M, they will first work out α_i, γ_i, and m_i through formula (6) and then issue $(D, \alpha_i \cdot P, \gamma_i \cdot P, m_i)$ to other users. Other users could validate source and message integrity through formula (8). We utilize hard problems to validate the method's security. (1) According to ECDLP, we publish $(D, \alpha_i \cdot P, \gamma_i \cdot P, m_i)$ and other users cannot get d from $D = e(P,P)^d$ and know α_i and γ_i from $\alpha_i \cdot P$ and $\gamma_i \cdot P$, so users cannot forge message maliciously; (2) according to BDH and $e(\alpha_i \cdot P, m_i * \gamma_i \cdot P) = e(P,P)^d$, DBDHP feature is utilized to validate message integrity, as shown in formula (8).

4. Proposed Scheme

This chapter would introduce the methods proposed in the essay. Section 4.2 introduces the system installation for the methods in Section 4.2. Section 4.3 introduces registration of vehicles and RSU, creation of vehicles and RSU related tables, and how vehicles carry out handoff at different RSU regions. Section 4.4 describes the message transmission between vehicles and message validation, vehicle message communication between different RSU, and private communication among TA, RSU, and vehicle. Section 4.5 introduces key updating and cancellation of identity between TA and RSU.

4.1. System Model. In system environment, as shown in Figure 1, we assume that the overall environment only has

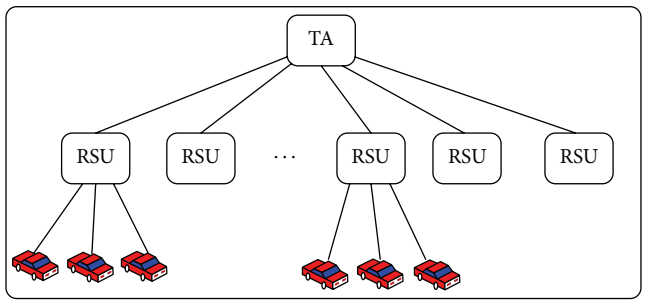

Figure 1: System environment diagram.

one TA and TA is the legally binding unit mechanism and in charge of controlling the whole network's security, which will provide the real identities of malicious nodes for legal prosecution when malicious nodes attack. On the one hand, the role of TA takes charge of validating vehicles or RSU's identities and on the other hand RSU and relevant coefficients are set by TA and RSU is set up on some common traffic facilities, such as traffic lights. TA and RSU are provided with wire/wireless communication. The communication between TA and RSU adopts wire communication, such as backbone. TA, RSU, and vehicles use short distance wireless communication equipment and the communication between RSU and vehicles adopts wireless communication. The parameters used in the method are described in the Notation section.

4.2. System Initialization. The section introduces the system installation of TA, RSU, and vehicles, which need not any certificates and could validate their own identities only by BDH messages authentication. Meanwhile, key sets the effective time, whose effectiveness could be validated any time.

4.2.1. TA System Setup. Suppose the chapter would select five distinct hash functions: $H : \{0,1\}^* \to Z_q^*$, $H_1 : \{0,1\}^* \to G_1^*$, $H_2 : G_2 \to \{0,1\}^*$, $H_3 : G_1 \to \{0,1\}^*$, and $H_4 :$ Wordseries $\to \{0,1\}^*$.

From the beginning, TA would calculate public value to solve public key, private key, and public parameter of TA as follows.

(1) Suppose $\alpha_{\mathrm{ID}_{\mathrm{TA},t}}, \gamma_{\mathrm{ID}_{\mathrm{TA},t}} \in Z_q^*$ and $m_{\mathrm{ID}_{\mathrm{TA},t}} = H_4(\mathrm{ID}_{\mathrm{TA},t} \| \mathrm{Tl}_{\mathrm{ID}_{\mathrm{TA},t}})$, where $\mathrm{Tl}_{\mathrm{ID}_{\mathrm{TA},t}}$ is the valid period of key and $\mathrm{ID}_{\mathrm{TA},t}$ is the real ID of TA.

(2) The calculation public value ($D_{\mathrm{ID}_{\mathrm{TA},t}}$) is as follows:

$$d_{\mathrm{ID}_{\mathrm{TA},t}} = \alpha_{\mathrm{ID}_{\mathrm{TA},t}} * \left(m_{\mathrm{ID}_{\mathrm{TA},t}} * \gamma_{\mathrm{ID}_{\mathrm{TA},t}}\right), \tag{9}$$

$$D_{\mathrm{ID}_{\mathrm{TA},t}} = e\left(d_{\mathrm{ID}_{\mathrm{TA},t}} P, P\right) = e(P,P)^{d_{\mathrm{ID}_{\mathrm{TA},t}}}, \tag{10}$$

$$D_{\mathrm{ID}_{\mathrm{TA},t}} = e\left(\alpha_{\mathrm{ID}_{\mathrm{TA},t}} P, m_{\mathrm{ID}_{\mathrm{TA},t}} * \gamma_{\mathrm{ID}_{\mathrm{TA},t}} P\right). \tag{11}$$

(3) Set public key $\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}} = H_1(\mathrm{ID}_{\mathrm{TA},t}) \in G_1^*$.

(4) Set private key $\mathrm{PR}_{\mathrm{ID}_{\mathrm{TA},t}} = \alpha_{\mathrm{ID}_{\mathrm{TA},t}} \mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}$.

(5) Set data key $\mathrm{PD}_{\mathrm{ID}_{\mathrm{TA},t}} = \alpha_{\mathrm{ID}_{\mathrm{TA},t}} \cdot P$.

TA would store $d_{\mathrm{ID}_{\mathrm{TA},t}}$ and provide it for TA or RSU changing public key and other parameters in the future, which would also make the following parameters (q, G_1, G_2, e, P, H, H_1, H_2, H_3, H_4, $D_{\mathrm{ID}_{\mathrm{TA},t}}$, $\mathrm{ID}_{\mathrm{TA},t}$, $\mathrm{PD}_{\mathrm{ID}_{\mathrm{TA},t}}$, $\gamma_{\mathrm{ID}_{\mathrm{TA},t}} P$, and $\mathrm{Tl}_{\mathrm{ID}_{\mathrm{TA},t}}$) public. When vehicles or RSU want to communicate with TA, it will be first to validate TA's identity and key's validness. $\alpha_{\mathrm{ID}_{\mathrm{TA},t}}$, $\gamma_{\mathrm{ID}_{\mathrm{TA},t}}$, and $d_{\mathrm{ID}_{\mathrm{TA},t}}$ cannot be known from the above public parameters. Therefore, malicious attackers couldn't forge TA and TA does not need any certificates to validate its own identity.

4.2.2. RSU System Setup. TA utilizes $\alpha_{\mathrm{ID}_{\mathrm{TA},t}}$ to set public key, private key, and other parameters of each RSU and selects $y \in Z_q^*$ as the master key of private communication. Suppose the number of RSU is m and $j = 1$ to m; then the calculation of TA is as follows.

(1) TA selects $x_{\mathrm{ID}_{R_j,t}} \in Z_q^*$ as the master key of private communication.

(2) Calculate private communication key of R_j to be $e(y \cdot P + x_{R_j,t} \cdot P, P)$ and $e(\mathrm{PU}_{\mathrm{ID}_{R_j,t}} \cdot P + x_{\mathrm{ID}_{R_j,t}} \cdot P, P)$.

(3) Calculate public key, private key, and other parameters of R_j as follows:

$$d_{\mathrm{ID}_{\mathrm{TA},t}} = \alpha_{\mathrm{ID}_{\mathrm{TA},t}} * \left(m_{\mathrm{ID}_{\mathrm{TA},t}} * \gamma_{\mathrm{ID}_{\mathrm{TA},t}}\right), \tag{12}$$

where $m_{\mathrm{ID}_{\mathrm{TA},t}} = 1/H_4(\mathrm{ID}_{R_j,t} \| T_{\mathrm{lifetime}_{\mathrm{ID}_{R_j,t}}})$ and $\mathrm{ID}_{R_j,t}$ is the real ID of RSU.

(4) Set public key $\mathrm{PU}_{R_j,t} = H_1(\mathrm{ID}_{R_j,t})$.

(5) Set private key $\mathrm{PR}_{R_j} = \alpha_{\mathrm{ID}_{\mathrm{TA},t}} \cdot \mathrm{PU}_{R_j,t}$.

(6) Set data key $\mathrm{PD}_{R_j,t} = \alpha_{\mathrm{ID}_{\mathrm{TA},t}} P$.

TA would create a table to record RSU's ID, key's valid time, being legal or not, and RSU's common key, with the calculation method for common key proposed in Section 4.4.3.

TA will not give R_j any certificates and it can validate the identity only by BDH messages authentication. Meanwhile, each RSU's key has valid time and it could be known whether key is within the valid time only from the identity validation. Any unit could validate RSU or TA's legitimacy through the following formula, with the calculation as follows:

$$D_{\mathrm{TA}} = e\left(\mathrm{PD}_u, m_u * \gamma_u P\right), \tag{13}$$

where u represents TA or any one RSU.

4.2.3. Vehicle System Setup. TA is only in charge of validating vehicles' identities and public value and it does not produce vehicles' key, so as to avoid the risk of controlling key. Suppose the number of vehicles is m and $i = 1$ to m; then the calculation is as follows.

(1) Vehicle V_i would calculate the first-level pseudonym of it and TA's ID ($\mathrm{ID}_{V_i,i}$), where $\mathrm{ID}_{V_i,i} = H(\mathrm{ID}_{V_i,t} \| \mathrm{ID}_{\mathrm{TA},t})$ and $\mathrm{ID}_{V_i,t}$ is the real ID of the vehicle.

(2) Vehicle V_i would calculate public value of it and TA's identity validation, with the calculation as follows:

$$d_{\mathrm{ID}_{V_i,i}} = \alpha_{\mathrm{ID}_{V_i,i}} * m_{\mathrm{ID}_{V_i,i}} * \gamma_{\mathrm{ID}_{V_i,i}}. \tag{14}$$

(3) Vehicle V_i utilizes TA's public key to encrypt message M and transmit it to TA, with the calculation as follows:

$$C = \left\{ r \cdot P, M \oplus H_2\left(e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, \mathrm{PD}_{\mathrm{ID}_{\mathrm{TA},t}}\right)^r\right)\right\}, \tag{15}$$

where $r \in Z_q^*$, $M = (D_{\mathrm{ID}_{V_i,i}} \| \alpha_{\mathrm{ID}_{V_i,i}} \cdot P \| \gamma_{\mathrm{ID}_{V_i,i}} P \| \mathrm{ID}_{V_i,t} \| \mathrm{ID}_{V_i,t})$, and V_i transmits the encrypted message C to TA, with the calculation as follows:

$$\begin{aligned} e\left(\mathrm{PR}_{\mathrm{ID}_{\mathrm{TA},t}}, U\right) &= e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, \mathrm{PD}_{\mathrm{ID}_{\mathrm{TA},t}}\right)^r \\ V \oplus H_2\left(e\left(\mathrm{PR}_{\mathrm{ID}_{\mathrm{TA},t}}, U\right)\right) &= V \oplus H_2\left(e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, \mathrm{PD}_{\mathrm{ID}_{\mathrm{TA},t}}\right)^r\right) \\ &= M. \end{aligned} \tag{16}$$

TA would validate V_i's first-level pseudonym ID ($\mathrm{ID}_{V_i,i}$) and then public value, as shown in the following formula:

$$D_{\mathrm{ID}_{V_i,i}} = e\left(\alpha_{\mathrm{ID}_{V_i,i}} P, m_{\mathrm{ID}_{V_i,i}} * \gamma_{\mathrm{ID}_{V_i,i}} P\right). \tag{17}$$

4.3. Message Broadcast and Message Authentication in RSU. When a vehicle enters RSU region, the vehicle would first check if RID table has already had the message validated mutually with RSU. If there is none, what will be done is to start from Section 4.3.1 to carry out identity validation with RSU, create SPID table and RID table with RSU in Section 4.3.2, and then discuss the method of vehicles being handoff at different RSU in Section 4.3.3.

4.3.1. Registration. Suppose that when the vehicle V_i enters region R_j and V_i has not created public value related functions and identity validation with R_j, then V_i would utilize TA to validate its own identity, so RSU could believe in the second-level pseudonym ID and public value of V_i. Two ways could be adopted for TA to validate vehicle's identities: (1) challenge of vehicles' pseudonym ID; (2) validation of public value. The challenge of vehicles' pseudonym ID could be adopted for RSU validating vehicles' identities, with the calculation as follows.

(1) The calculation of vehicles validating TA identity:

(1.1) the vehicle V_i selects $k \in Z_q^*$;

(1.2) the vehicle V_i recalculates the first-level pseudonym ID as follows:

$$\begin{aligned} \mathrm{reg} &= H^k\left(\mathrm{ID}_{V_i,i}\right), \\ \mathrm{ID}'_{V_i,i} &= H\left(\mathrm{reg} \| \mathrm{ID}_{\mathrm{TA},t}\right). \end{aligned} \tag{18}$$

V_i combines the arithmetic result after experiencing k times of hash with $\mathrm{ID}_{\mathrm{TA},t}$ and then goes through one hash arithmetic to produce the first-level pseudonym ID ($\mathrm{ID}_{V_i,i}$).

(1.3) The vehicle V_i calculates $\alpha_{\mathrm{ID}_{V_i,i}}, \gamma_{\mathrm{ID}_{V_i,i}}$, and $m_{\mathrm{ID}_{V_i,i}} = 1/H_4(\mathrm{ID}'_{V_i,i})$ by formula (14).

(1.4) V_i would utilize TA's public key to encrypt message M as C, where $M = k \| \mathrm{ID}_{V_i,i} \| \mathrm{ID}_{V_i,p} \mathrm{ID}'_{V_i,i} \| \alpha_{\mathrm{ID}_{V_i,i}} \| \gamma_{\mathrm{ID}_{V_i,i}} \| T_{\mathrm{stamp}}$.

(2) The calculation of RSU validating vehicles' identities:

(2.1) the vehicle V_i selects $r \in Z_q^*$;

(2.2) the vehicle V_i calculates initializing pseudonym ID to be $\mathrm{ID}_{V_i,p} = H(\mathrm{ID}_{V_i,i} \| r)$, where $\mathrm{ID}_{V_i,p}$ is the pseudonym ID of V_j within R_j range;

(2.3) the vehicle V_i calculates public value ($D_{\mathrm{ID}_{V_i,p}}$) used within R_j range;

(2.4) V_i would utilize R_j's public key to encrypt message M as $C1$, where $M = k \| \mathrm{ID}_{V_i,p} \| D_{\mathrm{ID}_{V_i,p}} \| T_{\mathrm{stamp}}$.

V_i would transmit C and $C1$ to R_j, which would use the common key ($\mathrm{SK}_{R_j,\mathrm{TA}}$) with TA to reencrypt message C by symmetric key encryption and transmit it to TA, and then TA and R_j will validate if the identities are correct, with the calculation as follows.

(1) TA validates V_i's identity as follows:

(1.1) TA utilizes private key to decrypt the encrypted message C;

(1.2) TA utilizes $\mathrm{ID}_{V_i,i}$ to search public value ($D_{\mathrm{ID}_{V_i,i}}$);

(1.3) TA utilizes k to calculate V_i's new pseudonym ID, as shown in formula (18);

(1.4) TA calculates the public value of the validated vehicles, as shown in formula (17);

(1.5) if the above is validated correctly, it shows that the identity of the vehicle V_i is correct and TA utilizes the common key ($\mathrm{SK}_{\mathrm{TA},R_j}$) with R_j to tell R_j that the vehicle V_i is legal;

(1.6) TA restores V_i's $\mathrm{ID}_{V_i,i} = \mathrm{ID}'_{V_i,i}$ and $\mathrm{ID}_{V_i,p}$ in table.

(2) RSU validates V_i's identity as follows:

(2.1) R_j receives the message from TA that V_i is legal and R_j utilizes private key to decrypt the encrypted message $C1$;

(2.2) R_j calculates V_i's private communication key as follows:

$$\frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}} + x_{\mathrm{ID}_{R_j,t}} \cdot P\right) \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,t}} + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right) e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)}, \tag{19}$$

where $Z_{\mathrm{ID}_{V_i,p}}$ is the random number selected by V_i;

(2.3) R_j provides signatures to V_i, with the calculation as follows: $r \in Z_q^*$, $U = r \cdot P$, $h = (M, U)$, $V = r \cdot \mathrm{PU}_{\mathrm{ID}_{R_j,t}} + h \cdot \mathrm{PR}_{\mathrm{ID}_{R_j,t}}$, message $M = (D_{\mathrm{ID}_{V_i,p}} \| \mathrm{Tl}_{\mathrm{ID}_{V_i,p}} \| \mathrm{ID}_{V_i,p} \| \mathrm{PD}_{\mathrm{ID}_{R_j,t}} \| \mathrm{PU}_{\mathrm{ID}_{R_j,t}} \| \mathrm{ID}_{R_j,t} \| \mathrm{Tl}_{\mathrm{ID}_{R_j,t}} \| \gamma_{\mathrm{ID}_{R_j,t}})$, and the message after signing is $\mathrm{Sign}_{R_j,V_i} = (U \| V \| M)$;

(2.4) R_j utilizes k as the key of symmetric encryption and transmits V_i's private communication key and R_j's signature Sign_{R_j,V_i} to V_i.

R_j would sign public value, pseudonym ID, and key's validness of the vehicles within the range at the fixed time and transmit the signature to each vehicle within the range. The signature is $\mathrm{Sign}_{R_j,V} = (\mathrm{ID}_{V_i,p} \| D_{\mathrm{ID}_{V_i,p}} \| \mathrm{Tl}_{\mathrm{ID}_{V_i,p}} \| \cdots \| \mathrm{ID}_{V_m,p} \| D_{\mathrm{ID}_{V_m,p}} \| T_{\mathrm{stamp}})$, so each vehicle only needs to validate the signature after receiving the signature message and then the public value of each vehicle could be known, with the calculation of signature validation as follows:

$$e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, U + h \cdot \mathrm{PD}_{\mathrm{ID}_{R_j,t}}\right) = e(V, P). \tag{20}$$

Each vehicle would store the message in the vehicle message table (see Table 1).

During the process, only V_i and TA know $\mathrm{ID}_{V_i,i}$ and RSU cannot know $\mathrm{ID}_{V_i,i}$, so pseudonym and privacy could be attained. After knowing $\mathrm{ID}_{V_i,i}$, TA could validate V_i's identity. If V_i is a legal vehicle, RSU would also accept V_i's second-level initializing pseudonym ID and public value and assist V_i to create RID-key table.

4.3.2. Table Establishment. Each vehicle would have RID-key table (see Table 2) and vehicle message table (see Table 1); RID-key table is for storing public value and relevant parameters which vehicles establish for RSU and vehicle message table is for storing public value and relevant parameters of other vehicles. Each RSU has SPID-key for storing vehicles' public value and relevant parameters and RSU message table (see Table 3) is used for storing the key of private communication between RSU and relevant parameters.

After the vehicle V_i and R_j create public value and relevant parameters, V_i begins to produce public value and pseudonym ID close to RSU, with the calculation as follows.

(1) V_i selects $k \in Z_q^*$ at random.

(2) Calculate each RSU's pseudonym ID as follows:

$$\mathrm{reg} = H^k\left(\mathrm{ID}_{V_i,p}\right), \tag{21}$$

$$\mathrm{ID}'_{V_i,p} = H\left(\mathrm{reg} \| \mathrm{ID}_{R_R}\right). \tag{22}$$

(3) Calculate each RSU's public value ($D_{\mathrm{ID}_{V_i,p}}$).

(4) V_i would calculate the common key with R_j as the key of symmetrical encryption, encrypt message M, and transmit it to R_j. The message content comprises each RSU's public value, random numbers $k \in Z_q^*$ and $\mathrm{ID}_{V_i,p}$, $M = D'_{\mathrm{ID}_{V_i,p}} \| k \| \mathrm{ID}_{V_i,p} \| \cdots \| D'''_{\mathrm{ID}_{V_i,p}} \| k''' \| \mathrm{ID}_{V_i,p} \| T_{\mathrm{stamp}}$, and common key, with the calculation as formula (31).

(5) Then, the vehicle stores relevant parameters in RID table.

After receiving the encrypted message of V_i, R_j would calculate the common key with V_i and only R_j and V_i know the common key, so the message source and integrity could be confirmed. Then, after decrypting message C, R_j would encrypt individual public value, pseudonym ID and random numbers of V_i, and each RSU and transmit them to each RSU. Each RSU receives the message and stores V_i's public value, pseudonym ID, and random numbers in SPID table, as shown in Table 4. Meanwhile, each RSU would calculate V_i's pseudonym ID, as shown in formula (18) and R_j would also report illegal RSU and valid time close to RSU to the vehicle V_i, so as to avoid malicious attack.

4.3.3. Handoff Problem. VANET Standard 802.11P [16] is focused on the dedicated short-range communication (DSRC) protocol, which applies to short-range communications. As a result, vehicles use different RSUs to perform handoff when moving at high speed. A problem would be caused; that is, vehicles must revalidate identities mutually with TA and RSU and reestablish a new key. Suppose vehicles establish trusting relationship with each RSU from the beginning; they could know if other RSUs are legal or not and the validity of RSU related key through the trusted RSU and transmit vehicles' public value and other parameters to other RSUs via the trusted RSU.

Suppose the vehicle V_i has already created RID-key table; when V_i is about to enter R_b, it would first check if Table R_b is legal and valid. If it is confirmed legal and valid, V_i would transmit pseudonym ID ($\mathrm{ID}_{V_i,p}$) and public value ($D_{\mathrm{ID}_{V_i,p}}$) to R_b, which would utilize $\mathrm{ID}_{V_i,p}$ to check if V_i is within the valid time and if it is the legal user in SPID table after receiving the message. If it is legal, R_b would calculate V_i's private communication key and sign to V_i and V_i's private communication key is calculated as follows:

$$\frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}} + x_{\mathrm{ID}_{R_b,p}} \cdot P + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_b,p}} \cdot P, P\right) e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)}. \tag{23}$$

Use $Z_{\mathrm{ID}_{V_i,p}} = k$ as the symmetrical encryption and transmit private communication key and signature to V_i.

Only V_i and R_b know k. If the message could be unlocked and represent V_i itself, the identities of both sides could be validated by means of pseudonym ID challenge. If it is validated correctly, R_b would periodically broadcast V_i's pseudonym ID, public value, and validity by means of signature.

4.4. Message Transmission and Validation. This section mainly discusses vehicles' message broadcasting and validation within RSU range in Section 4.4.1, that is, between different RSUs in Section 4.4.2 and the private communication from TA to RSU, from RSU to vehicles, and from vehicle to vehicle in Section 4.4.3.

Table 1: Vehicle message table.

Vehicle's ID	Public value	Valid time	Being legal or not
$\mathrm{ID}_{V_1,p}$	$D_{\mathrm{ID}_{V_1,p}}$	$\mathrm{Tl}_{\mathrm{ID}_{V_1,p}}$	True
...	...	...	...
$\mathrm{ID}_{V_{m-1},p}$	$D_{\mathrm{ID}_{V_{m-1},p}}$	$\mathrm{Tl}_{\mathrm{ID}_{V_{m-1},p}}$	True
$\mathrm{ID}_{V_m,p}$	$D_{\mathrm{ID}_{V_m,p}}$	$\mathrm{Tl}_{\mathrm{ID}_{V_m,p}}$	True

Table 2: RID-key table.

ID of RSU	Public value	Pseudonym ID	Random number	Valid time	Being legal or not
R_1	$D'_{\mathrm{ID}_{V_i,p}}$	$\mathrm{ID}'_{V_i,p}$	k'	$\mathrm{Tl}'_{\mathrm{ID}_{V_i,p}}$	True
...	...	...			
R_{j+2}	$D''_{\mathrm{ID}_{V_i,p}}$	$\mathrm{ID}''_{V_i,p}$	k''	$\mathrm{Tl}''_{\mathrm{ID}_{V_i,p}}$	True
...	...	...			
R_m	$D'''_{\mathrm{ID}_{V_i,p}}$	$\mathrm{ID}'''_{V_i,p}$	k'''	$\mathrm{Tl}'''_{\mathrm{ID}_{V_i,p}}$	True

4.4.1. Message Transmission and Validation within RSU Range. When V_i is about to broadcast one message M within R_j communication range, V_i would perform the calculation as follows:

$$e(P,P)^{d_{\mathrm{ID}_{V_i},p}} = e\left(\alpha_{\mathrm{ID}_{V_i,p}} \cdot P, \frac{1}{H_4\left(\mathrm{ID}_{V_i,p} \| M \| T_{\mathrm{stamp}}\right)} \cdot \gamma_{\mathrm{ID}_{V_i,p}} \cdot P\right). \tag{24}$$

V_i would broadcast $\alpha_{\mathrm{ID}_{V_i,p}} \cdot P$, $\mathrm{ID}_{V_i,p}$, $\gamma_{\mathrm{ID}_{V_i,p}} \cdot P$, T_{stamp}, and M to the vehicles within the communication range. After receiving the message, other vehicles would check if there is $\mathrm{ID}_{V_i,p}$'s public value in their own vehicle message table and if they know V_i's public value, they could validate the message source and integrity through formula (24).

Assuming that after vehicle V_j receives a message from V_i, V_j can judge whether message V_i is correct. As the public value of $V_i(e(P,P)^{d_{\mathrm{ID}_{V_i},p}})$ is public, then V_j can determine whether $\alpha_{\mathrm{ID}_{V_i,p}} \cdot P$, $\mathrm{ID}_{V_i,p}$, $\gamma_{\mathrm{ID}_{V_i,p}} \cdot P$, T_{stamp}, and M are the message sent by V_i. First calculate $1/H_4(\mathrm{ID}_{V_i,p} \| M \| T_{\mathrm{stamp}})$ and then calculate whether $e(\alpha_{\mathrm{ID}_{V_i,p}} \cdot P, (1/H_4(\mathrm{ID}_{V_i,p} \| M \| T_{\mathrm{stamp}})) \cdot \gamma_{\mathrm{ID}_{V_i,p}} \cdot P) = e(P,P)^{d_{\mathrm{ID}_{V_i},p}}$ is correct. If it is correct, it indicates that the message is issued by V_i; otherwise it will be discarded. Since only V_i knows $d_{\mathrm{ID}_{V_i},p}$ and $e(P,P)^{d_{\mathrm{ID}_{V_i},p}}$ is a problem, it cannot be forged by other vehicles.

4.4.2. Communication between Different RSUs. Two vehicles cannot communicate with each other between different RSUs; the reason lies in that the vehicle's public value and pseudonym ID are different in different RSUs and vehicles' public value in each RSU cannot be known between RSUs. Therefore, it is unable to assist vehicles to validate the correctness of the message transmitted from other RSUs. As shown in Figure 2, V_i and V_j are R_a and R_b, respectively,

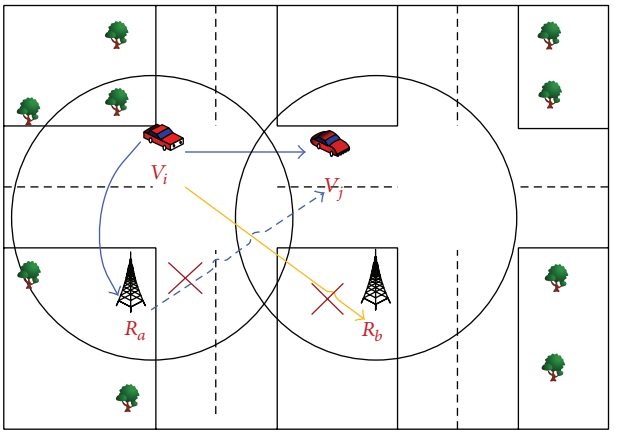

Figure 2: The communication problem between two vehicles in the different RSU.

in two different RSUs. When V_i broadcasts a message to V_j, though V_j receives the message, it does not know if public value is owned by itself and it cannot confirm if it is the legal user. In order to resolve the above problem, as shown in Figure 3, (1) V_j first transmits the message to V_i, the message content is request message: $R_b \| \mathrm{ID}_{V_j,p} \| T_{\mathrm{stamp}}$, and V_j informs us within different RSUs; (2) after the successful entry of R_a identity validation, V_i transmits one signature to V_i and the signature is $\mathrm{Sign}_{R_a \to V_i} = (U \| V \| M)$, where $M = (D_{\mathrm{ID}_{V_i,p}} \| \mathrm{Tl}_{\mathrm{ID}_{V_i,p}} \| \mathrm{ID}_{V_i,p} \| \mathrm{PD}_{\mathrm{ID}_{R_a,t}} \| \mathrm{PU}_{\mathrm{ID}_{R_a,t}} \| \mathrm{ID}_{R_a,t} \| \mathrm{Tl}_{\mathrm{ID}_{R_a,t}} \| \gamma_{\mathrm{ID}_{R_a,t}})$. V_i would broadcast signatures to V_j, then V_j could know R_a's public key and public parameters and validate signatures and R_a's validity. After the success of validation, V_j could know V_i's public value and validate the message source and integrity.

4.4.3. Private Communication. In the following part we will discuss five cases of private communication: Case 1: private communication between TA and RSU, Case 2: private

Table 3: RSU message.

ID of RSU	Public key	Public parameter	Valid time	Legal or illegal	Private communication key
R_1	$\mathrm{PU}_{\mathrm{ID}_{R_1},t}$	$\mathrm{PD}'_{\mathrm{ID}_{R_1},t}$ $\gamma_{\mathrm{ID}_{R_1},t}$	$\mathrm{Tl}_{\mathrm{ID}_{R_1},t}$	True	$\mathrm{SK}_{R_1,R_j} = \dfrac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_1},t}, P\right)}{e(P,P)^y}$
…	…	…	…	…	…
R_m	$\mathrm{PU}_{\mathrm{ID}_{R_m},t}$	$\mathrm{PD}'_{\mathrm{ID}_{R_m},t}$ $\gamma_{\mathrm{ID}_{R_m},t}$	$\mathrm{Tl}_{\mathrm{ID}_{R_m},t}$	True	$\mathrm{SK}_{R_m,R_j} = \dfrac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_m},t}, P\right)}{e(P,P)^y}$
…	…	…	…	…	…

Table 4: SPID-key table.

Pseudonym ID	Public value	Initializing ID	Valid time	Legal or illegal	Random number
$\mathrm{ID}'_{V_1,p}$	$D'_{\mathrm{ID}_{V_1},p}$	$\mathrm{ID}_{V_1,p}$	$\mathrm{Tl}_{\mathrm{ID}_{V_1},p}$	True	k
…	…	…	…	…	
$\mathrm{ID}''_{V_m,p}$	$D''_{\mathrm{ID}_{V_m},p}$	$\mathrm{ID}_{V_m,p}$	$\mathrm{Tl}_{\mathrm{ID}_{V_m},p}$	True	k''
…	…	…	…	…	…

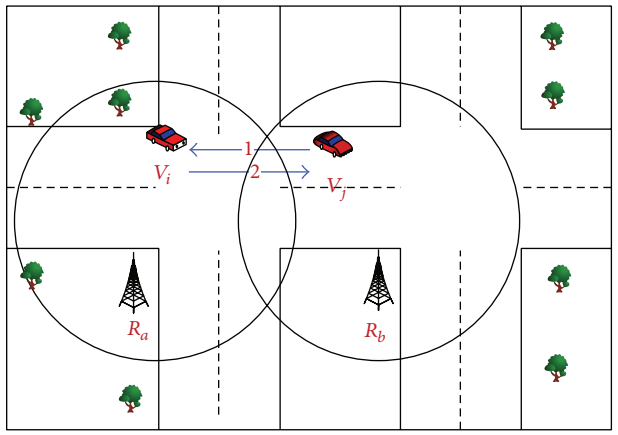

Figure 3: The solution of the communication problem.

communication between RSU and RSU, Case 3: private communication between vehicle and vehicle, Case 4: private communication between vehicle and RSU, and Case 5: private communication between TA and vehicle.

Case 1. Suppose R_j wants to perform private communication with TA; TA has already transmitted private communication key to R_j in Section 4.2.2. First, R_j and TA will validate each other's identities and key's validity and R_j would calculate the private communication with TA as follows:

$$\begin{aligned}\mathrm{SK}_{R_j,\mathrm{TA}} &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t} + x_{\mathrm{ID}_{R_j},t} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_j},t} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA}},t}, P\right) \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) e\left(x_{\mathrm{ID}_{R_j},t} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA}},t}, P\right)}{e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_j},t} \cdot P, P\right)} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA}},t}, P\right)}{e(y \cdot P, P)}.\end{aligned} \tag{25}$$

Next, TA calculates the private communication with R_j as follows:

$$\begin{aligned}\mathrm{SK}_{\mathrm{TA},R_j} &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA}},t}, P\right)}{e(y \cdot P, P)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA}},t}, P\right)}{e(y \cdot P, P)},\end{aligned} \tag{26}$$

where $\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA}},t} = H_1(\mathrm{ID}_{\mathrm{TA}})$, $\mathrm{PU}_{\mathrm{ID}_{R_j},t} = H_1(\mathrm{ID}_{R_j})$; as ID is public, it could be calculated by itself. Therefore, the common key in formulae (25) and (26) is the same and TA and R_j could perform private communication.

Case 2. Suppose R_j wants to perform private communication with R_k. First, R_j and R_k will validate each other's identities and key's validity and R_j would calculate the private communication with R_k as follows:

$$\begin{aligned}\mathrm{SK}_{R_j,R_k} &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t} + x_{\mathrm{ID}_{R_j},t} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_j},t} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{R_k},t}, P\right) \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) e\left(x_{\mathrm{ID}_{R_j},t} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_k},t}, P\right)}{e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_j},t} \cdot P, P\right)} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j},t}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_k},t}, P\right)}{e(y \cdot P, P)}.\end{aligned} \tag{27}$$

Next, R_k calculates the private communication with R_j as follows:

$$\begin{aligned}\mathrm{SK}_{R_j,R_k} &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_k,t}} + x_{\mathrm{ID}_{R_k,t}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_k,t}} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right) \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_k,t}}, P\right) e\left(x_{\mathrm{ID}_{R_k,t}} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right)}{e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_k,t}} \cdot P, P\right)} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_k,t}}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right)}{e(y \cdot P, P)},\end{aligned} \tag{28}$$

where $\mathrm{PU}_{\mathrm{ID}_{R_k,t}} = H_1(\mathrm{ID}_{R_k,t})$, $\mathrm{PU}_{\mathrm{ID}_{R_j,t}} = H_1(\mathrm{ID}_{R_j,t})$; it could be known that the private communication key is the same from the final results.

Case 3. Suppose V_i wants to perform private communication with V_j. First, V_i and V_j will validate each other's identities and key's validity and V_j would calculate the private communication with V_j as follows:

$$\begin{aligned}&\mathrm{SK}_{V_i,V_j} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}} + x_{\mathrm{ID}_{R_j,t}} \cdot P + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_j,t}} \cdot P + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{V_j,p}}, P\right) \\ &= \left(e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right)\right. \\ &\qquad \left.\times e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{V_j,p}}, P\right)\right) \\ &\quad \times \left(e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right) e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)\right)^{-1} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{V_j,p}}, P\right)}{e(y \cdot P, P)}.\end{aligned} \tag{29}$$

Next, V_j calculates the private communication with V_j as follows:

$$\begin{aligned}&\mathrm{SK}_{V_i,V_j} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_j,p}} + x_{\mathrm{ID}_{R_k,t}} \cdot P + Z_{\mathrm{ID}_{V_j,p}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_k,t}} \cdot P + Z_{\mathrm{ID}_{V_j,p}} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) \\ &= \left(e\left(\mathrm{PU}_{\mathrm{ID}_{V_j,p}}, P\right) e\left(x_{\mathrm{ID}_{R_k,t}} \cdot P, P\right)\right. \\ &\qquad \left.\times e\left(Z_{\mathrm{ID}_{V_j,p}} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right)\right) \\ &\quad \times \left(e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_k,t}} \cdot P, P\right) e\left(Z_{\mathrm{ID}_{V_j,p}} \cdot P, P\right)\right)^{-1} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_j,p}}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right)}{e(y \cdot P, P)},\end{aligned} \tag{30}$$

where $\mathrm{PU}_{\mathrm{ID}_{V_j,p}} = H_1(\mathrm{ID}_{V_j,p})$ and $\mathrm{PU}_{\mathrm{ID}_{V_i,p}} = H_1(\mathrm{ID}_{V_i,p})$ and it could be known that the private communication key is the same from the final results.

Case 4. Suppose V_i wants to perform private communication with R_j. First, V_i and R_j will validate each other's identities and key's validity and V_j would calculate the private communication with R_j as follows:

$$\begin{aligned}&\mathrm{SK}_{V_i,R_j} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}} + x_{\mathrm{ID}_{R_j,t}} \cdot P + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_j,t}} \cdot P + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right) \\ &= \left(e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right)\right. \\ &\qquad \left.\times e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right)\right) \\ &\quad \times \left(e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right) e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)\right)^{-1} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right)}{e(y \cdot P, P)}.\end{aligned} \tag{31}$$

Next, R_j calculates the private communication with V_j as follows:

$$\begin{aligned}\mathrm{SK}_{R_j,V_i} &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}} + x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right) e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right)}{e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right)} \\ &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{R_j,t}}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right)}{e(y \cdot P, P)},\end{aligned} \tag{32}$$

where $\mathrm{PU}_{\mathrm{ID}_{V_i,p}} = H_1(\mathrm{ID}_{V_i,p})$ and $\mathrm{PU}_{\mathrm{ID}_{R_j,t}} = H_1(\mathrm{ID}_{R_j,t})$; it could be known from the final results that the private communication key is the same.

Case 5. Suppose V_i wants to perform private communication with TA. First, V_i and TA will validate each other's identities

and key's validity and V_j would calculate the private communication with TA as follows:

$$\begin{aligned}
&\mathrm{SK}_{V_i,\mathrm{TA}} \\
&= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}} + x_{\mathrm{ID}_{R_j,t}} \cdot P + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)}{e\left(y \cdot P + x_{\mathrm{ID}_{R_j,t}} \cdot P + Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, P\right) \\
&= \left(e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right)\right. \\
&\qquad \left. \times e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, P\right)\right) \\
&\quad \times \left(e(y \cdot P, P)\, e\left(x_{\mathrm{ID}_{R_j,t}} \cdot P, P\right) e\left(Z_{\mathrm{ID}_{V_i,p}} \cdot P, P\right)\right)^{-1} \\
&= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, P\right)}{e(y \cdot P, P)}.
\end{aligned} \tag{33}$$

Next, TA calculates the private communication with V_j as follows:

$$\begin{aligned}
\mathrm{SK}_{\mathrm{TA},V_i} &= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, P\right)}{e(y \cdot P, P)} \cdot e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right) \\
&= \frac{e\left(\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}, P\right) e\left(\mathrm{PU}_{\mathrm{ID}_{V_i,p}}, P\right)}{e(y \cdot P, P)},
\end{aligned} \tag{34}$$

where $\mathrm{PU}_{\mathrm{ID}_{V_i,p}} = H_1(\mathrm{ID}_{V_i,p})$ and $\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}} = H_1(\mathrm{ID}_{\mathrm{TA},t})$ and it could be known from the final results that the private communication key is the same.

From Case 1 to Case 5, it could be known that private communication could be performed among vehicles, RSU or TA, and the private communication key of any vehicle and RSU has the top secrets and their own secrets, so it is impossible to forge any vehicle or RSU, as you must know the top secrets.

Though the private communication method costs much more calculation time for the first time, which is spent in validating the other's identity and calculating the private communication key between them, the calculation time during the communication within the other's valid time is much less, as the common secret key has already been established, which will not be recalculated until the other's valid time expires. For the symmetrical encryption, the calculation time is less. For the equipment which often uses private communication, such as RSU to RSU or RSU to TA, the time which private communication spends could be reduced.

4.5. Key Updating and Identity Cancellation. When TA's key validity expires, TA would utilize formula (9) to replace $\alpha_{\mathrm{ID}_{\mathrm{TA},t}} \cdot P, \gamma_{\mathrm{ID}_{\mathrm{TA},t}} P, m_{\mathrm{ID}_{\mathrm{TA},t}}$, and $\mathrm{Tl}_{\mathrm{ID}_{\mathrm{TA},t}}$, which will not influence the communication of RSU and vehicles during the process. TA would use $\alpha_{\mathrm{ID}_{\mathrm{TA},t}} \cdot P$ as the data key ($\mathrm{PD}_{\mathrm{ID}_{\mathrm{TA},t}}$), $H_1(\mathrm{ID}_{\mathrm{TA},t}) \in G_1$ is public key ($\mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}$), $\alpha_{\mathrm{ID}_{\mathrm{TA},t}} \mathrm{PU}_{\mathrm{ID}_{\mathrm{TA},t}}$ is private key ($\mathrm{PR}_{\mathrm{ID}_{\mathrm{TA},t}}$), $\gamma_{\mathrm{ID}_{\mathrm{TA},t}} P$ is another public parameter, $\mathrm{Tl}_{\mathrm{ID}_{\mathrm{TA},t}}$ is TA's public key, private key, and valid time, and TA makes new parameters public.

At RSU's key updating part, as TA and RSU mainly perform identity validation instead of the message validation among vehicles. If R_j finds key will expire soon, R_j would calculate the common key ($\mathrm{SK}_{R_j,\mathrm{TA}}$) with TA, as shown in formula (26), and then encrypt message M and transmit to TA, $M = (\mathrm{PD}_{\mathrm{ID}_{R_j,t}} \| \mathrm{PU}_{\mathrm{ID}_{R_j,t}} \| \gamma_{\mathrm{ID}_{R_j,t}} \| \mathrm{Tl}_{\mathrm{ID}_{R_j,t}} \| T_{\mathrm{stamp}})$. After receiving the encrypted message, TA would calculate the common key ($\mathrm{SK}_{R_j,\mathrm{TA}}$) with R_j, decrypt the message, and validate R_j's identity, as shown in formula (13). Next, TA would search table to check if R_j is legal. If it is legal, TA would recalculate R_j's public key, private key, private communication key, and other parameters and then utilize $\mathrm{SK}_{\mathrm{TA},R_j}$ to encrypt the parameters and transmit them back to R_j. After receiving the message, R_j would reutilize $\mathrm{SK}_{R_j,\mathrm{TA}}$ for decryption and revalidating if the parameters are public value ($D_{\mathrm{ID}_{\mathrm{TA},t}}$), as shown in formula (13). Thus RSU key updating is completed. During the process, only the vehicle communication within the range would be influenced, and RSU requires retransmitting a new signature to each vehicle.

Suppose vehicle V_i is a malicious node; R_m would first utilize Table 5 to search V_i's initializing pseudonym ID ($\mathrm{ID}_{V_i,p}$) and then use the common key with each RSU to encrypt $\mathrm{ID}_{V_i,p}$ and transmit to each RSU. Before the receiving, each RSU would first check SPID table and see if there is initializing pseudonym ID. If there is, V_i registration would be forbidden during handoff. After receiving R_m message, TA would first validate if V_i is a malicious node. If it is, TA would search table according to $\mathrm{ID}_{V_i,p}$ and first set V_i's legality false. When TA revalidates V_i's identity via RSU (as shown in Section 4.3.1), TA would forbid V_i registration.

Suppose R_j is a malicious node; adjacent R_m would directly utilize the common key with TA to encrypt the message and inform TA that R_j is a malicious node. TA would first validate if R_j is a malicious node. If it is, TA would set R_j's legality in table false and use the common key with RSU to inform all RSUs that R_j is a malicious node, so that malicious RSU or vehicles updating KEY or communication subsequently would be stopped.

5. Security and Performance Analysis

This section mainly illustrates that the method proposed in the essay could reach (1) message source, (2) message integrity, (3) nonrepudiation, (4) pseudonym, and (5) untraceability, in terms of security analysis. As far as the performance analysis is concerned, we carry out performance analysis in [4–6] (Table 7).

5.1. Security Analysis. We discuss the security analysis from 5 aspects as follows.

(1) Confidentiality. No matter what unit (TA, RSU, and vehicles) performs private communication, the private communication with the other side could be guaranteed, as the vehicle's

Table 5: The comparison of property.

Property	Method					
	[4]	[5]	[6]	[7]	[8]	Proposed method
Security and privacy preservation	Yes	Yes	Yes	Yes	Yes	Yes
Do need the certificate	No	No	No	No	No	No
Do need the help of RSU for authentication	No	No	No	No	No	No
PKI-based system	No	No	No	Yes	No	No
Communication within different RSU	Yes	No	Yes	Yes	Yes	Yes
Privacy communicate	Yes	Yes	Yes	Yes	No	Yes

private communication key contains the vehicle, RSU, and TA's secrets. During the communication, though the vehicle and RSU's secrets could be eliminated, malicious nodes could not get TA's secret y from the private communication key or the results after elimination, so malicious nodes cannot forge other's private key or listen in.

(2) Source Authentication and Nonrepudiation. Before the communication, RSU must validate vehicles' identities. After the success of validation, RSU would utilize signature method to broadcast vehicles' pseudonym ID and public value to each vehicle, which could then know each legal vehicle's public value from the signature, so the message broadcasted by vehicles could be validated via BHD function. As the public value cannot be forged, it could represent the vehicle itself and the vehicle sending messages could reach nonrepudiation and know the source of the message.

(3) Message Integrity. As the public value $(e(P,P)^d)$ is public and the BHD function is $e(P,P)^d = e(\alpha P, (1/m)\gamma P)$, though m and P are public, α, γ, or d could not be got from P or m. Suppose the malicious node forges m and the validation result is $e(P,P)^d \neq e(\alpha P, (1/m')\gamma P)$, so malicious nodes cannot forge messages and change messages and other vehicles could validate message integrity.

(4) Pseudonym. The vehicle uses different pseudonym IDs at different RSU. Suppose RSU cannot know vehicle's real ID by collusion attack and malicious nodes cannot collect vehicle messages to calculate vehicles' read ID, as vehicle's pseudonym ID produces irregularity.

(5) Privacy. The essay adopts two-level pseudonym ID. The first level is the pseudonym ID between vehicle and TA, which is known to only TA and vehicle and not broadcasted to RSU or vehicles. The second-level pseudonym ID is produced by RSU and vehicle. Suppose RSU traces vehicles' travel path by means of collusion attack and the trace time and range are limited, as after the time slice, vehicles will be revalidated by TA and replace the first-level and second-level pseudonym ID, then the pseudonym ID produces irregularity, so the vehicles' privacy could be improved.

5.2. Performance Analysis. In this section, we compare our method with [4–8]. Table 5 shows the differences and we could know that our method has a lot of advantages from the table.

Table 6: 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
ASE	RSA encryption	0.19
ASD	RSA decryption	4.65
HMAC	HMAC	0.002
SE	AES encryption	<0.19
SD	AES decryption	<4.65

In Table 6, we propose encryption/decryption calculation time. According to [17, 18], the implementation of the bilinear mapping is provided based on the Tate pairing over a Miyaji-Nakabayashi-Takano (MNT) curve [19] with embedding degree 6 and 160-bit q.

We utilize Table 6, to calculate the time for broadcasting messages and validating messages in [4–8]. The method proposed in the essay supposes that if a vehicle is about to broadcast messages to other vehicles within the range, the vehicle would calculate $d_{\mathrm{ID}_{V_i,p}} = \alpha_{\mathrm{ID}_{V_i,p}} * (1/H_4(\mathrm{ID}_{V_i,p} * M * T_{\mathrm{stamp}})) * \gamma_{\mathrm{ID}_{V_i,p}}$. As these calculations belong to the general integer calculation, whose calculation complexity is quite low, and the vehicle will change $\alpha_{\mathrm{ID}_{V_i,p}}$ and $\gamma_{\mathrm{ID}_{V_i,p}}$ into points, $2*T_m$ calculation time will be spent. The vehicle will broadcast the following messages to other vehicles $(M\|\alpha_{\mathrm{ID}_{V_i,p}}\|\gamma_{\mathrm{ID}_{V_i,p}}\|\mathrm{ID}_{V_i,p}\|T_{\mathrm{stamp}})$ and then calculate the message validation time. After receiving messages, other vehicles could first inquire about the vehicle's public value and the validation is $e(P,P)^{d_{\mathrm{ID}_{V_i,p}}} = e(\alpha_{\mathrm{ID}_{V_i,p}} \cdot P, (1/H_4(\mathrm{ID}_{V_i,p} * M * T_{\mathrm{stamp}})) * \gamma_{\mathrm{ID}_{V_i,p}} \cdot P)$, so the time for broadcasting and validating messages in the essay is $T_m + T_p$.

During the handoff process of vehicles in the essay, when RSU's pseudonym ID challenge is successful, RSU would assist vehicles to produce signature time, as shown in formula (4), which needs $3 * T_m$ in all. RSU produces vehicles' private communication key, as shown in formula (21), which needs $4*T_m+3*T_p$, so the total time is $7*T_m+3*T_p$. When messages are broadcast to other vehicles within different RSUs, vehicles producing message signatures need $2 * T_m$, other vehicles validating signatures, as shown in formula (22), and need

Table 7: Performance analysis.

Property	Method					
	[4]	[5]	[6]	[7]	[8]	Proposed method
The broadcast message	Signing: $5 * T_m + 3 * T_p$ Verification: $4 * T_m + 4 * T_p$	Signing $n * T_p + n *$ HMAC Verification $n * T_p + n *$ HMAC	Signing: $1 * T_p$ Verification: $3 * T_p$	Signing $T_p + T_m$ Verification $T_p + T_m$	Signing $2 * T_p + 0.19$ Verification $T_p + T_m + 0.19$	Signing $2 * T_m$ Verification $T_p + T_m$
Spending time	36.4 ms	$n * 9$ ms + $n * 0.004$ ms	18 ms	10.2 ms	9.98 ms	6.3 ms
Handoff	$3 * T_p$	$4 * T_m + T_e + 2 * T_p$	N/A	N/A	N/A	$1 *$ SE + $1 *$ SD + $3 * T_m$
Spending time	13.5 ms	11.94 ms	N/A	N/A	N/A	<5.44 ms
Communication between different RSUs	Signing: $5 * T_m + 3 * T_p$ Verification: $4 * T_m + 4 * T_p$	N/A	Signing: $1 * T_p$ Verification: $3 * T_p$	Signing $T_p + T_m$ Verification $T_p + T_m$	Signing $2 * T_p + 0.19$ Verification $T_p + T_m + 0.19$	Signing $2 * T_m$ Verification $2 * T_p + 2 * T_m$
Spending time	36.4 ms	N/A	18 ms	10.2 ms	9.98 ms	11.4 ms
Privacy communicate	N/A	Signing $T_P +$ SE Verification $T_p +$ SD	N/A	Signing ASE Verification ASD	N/A	Signing $T_m + T_P +$ SE Verification $T_m + T_P +$ SD
Spending time	N/A	<13.84 ms	N/A	4.84 ms	N/A	<15.04 ms

$T_m + T_p$, and validating vehicles' message needs $T_m + T_p$, so the total time required is $4 * T_m + 2 * T_p$.

References [4, 6] both use certificates to validate their own identities, so the broadcasting messages could validate their own identities within RSU range or outside RSU range. In [5], the concept of identity-based is utilized and vehicles establish common key with each vehicle, so when vehicles broadcast messages, they would utilize the common key with each vehicle as HMAC's key and encrypt messages and then transmit the encrypted message to the other side, as broadcasting messages requires establishing n common keys to encrypt messages and other vehicles also need establish common keys for decryption, so there is $2n * T_p$ altogether. As [5] does not discuss the communication between vehicles at different RSUs, it is unable to calculate the encryption and decryption time.

6. Conclusion

The method in the essay adopts BDH messages authentication to produce TA and RSU's public key and other parameters. Any vehicles could validate if RSU is legal through BDH messages authentication method and utilize pseudonym ID challenge method to validate RSU and vehicles' identities, which quickens handoff processing time.

It is hoped that message batch validation and how to judge vehicles are malicious nodes will be added. Though the essay proposes cancellation of users' function, it does not mention how to judge users to be malicious nodes, which will be put into the study and make the study more complete.

Notation

e: Bilinear mapping
G_1: Additive group
G_2: Multiplicative group
P: Generator of G_1
d: The user chooses a random number $d \in Z_q^*$ as its secret value
α: The α is the random number chosen by user, where $\alpha \in Z_q^*$
γ: The γ is the random number chosen by user, where $\gamma \in Z_q^*$
m: $m \in Z_q^*$ such that $m = 1/H_4(M \| T_{\text{stamp}})$
SE$(\cdot)$: A secure symmetric encryption algorithm
PU_k: Public key of node k
PR_k: Private key of node k
PD_k: Data key of node k
$\text{ID}_{k\cdot t}$: Real identity of node k
$\text{ID}_{k,i}$: Original pseudonym of node k
$\text{ID}_{k,p}$: Requested pseudonym of node k
y: Secret value of TA
x_R: Secret value of RSU
Z_V: Secret value of vehicle
Sign_{R_j,V_i}: R_j's signature to V_i
D_k: The public value of user k such that $\widehat{e}(P, P)^d$
$\text{SK}_{k\cdot j}$: The common session key between node k and node j
Z_q^*: 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 $G_2^* \rightarrow \{0, 1\}^*$

$H_3(\cdot)$: Hash function such that $G_1 \rightarrow \{0,1\}^*$
$H_4(\cdot)$: Hash function such that Word series $\rightarrow \{0,1\}^*$
T_{stamp}: Time interval j
Tl: 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.

References

[1] 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.

[2] N. Maslekar, J. Mouzna, M. Boussedjra, and H. Labiod, "CATS: an adaptive traffic signal system based on car-to-car communication," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1308–1315, 2013.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] S.-J. Horng, S.-F. Tzeng, Y. Pan et al., "B-SPECS+: batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[9] K. Zeng, "Pseudonymous PKI for ubiquitous computing," in *Proceedings of the 3rd European PKI Workshop: Theory and Practice (EuroPKI '06)*, pp. 207–222, Turin, Italy.

[10] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairings," in *Advances in Cryptology-Asiacrypt*, pp. 514–532, Springer, Berlin, Germany, 2001.

[11] J. Zhang, W. Zhen, and M. Xu, "An efficient privacy-preserving authentication protocol in VANETs," in *Proceedings of the 9th IEEE International Conference on Mobile Ad-Hoc and Sensor Networks (MSN '13)*, pp. 272–277, December 2013.

[12] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara, Calif, USA, August 2001.

[13] M. Scott, "Computing the tate pairing," in *Proceedings of the International Conference on Topics in Cryptology*, pp. 293–304, Springer, San Francisco, Calif, USA, 2005.

[14] M. Scott, "Computing the tate pairing," in *Topics in Cryptology*, pp. 293–304, Springer, Berlin, Germany, 2005.

[15] F. Bao, R. Deng, and H. Zhu, "Variations of diffie-hellman problem," in *Proceedings of the 5th International Conference (ICICS '03)*, vol. 2836 of *Lecture Notes in Computer Science*, pp. 301–312, Springer, Huhehaote, China, October 2003.

[16] Q. Wang, S. Leng, H. Fu, and Y. Zhang, "An IEEE 802.11p-based multichannel MAC scheme with channel coordination for vehicular Ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 2, pp. 449–458, 2012.

[17] M. Scott, "Implementing cryptographic pairings," in *Pairing-Based Cryptography—Pairing 2007*, vol. 4575 of *Lecture Notes in Computer Science*, pp. 177–196, 2007.

[18] S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate pairing," in *Proceedings of the 5th International Symposium (ANTS-V '02)*, vol. 2369 of *Lecture Notes in Computer Science*, pp. 324–337, Springer, Sydney, Australia, July 2002.

[19] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E84-A, no. 5, pp. 1234–1243, 2001.