Hindawi
Mobile Information Systems
Volume 2019, Article ID 3109238, 9 pages
https://doi.org/10.1155/2019/3109238

Research Article

Mix-Context-Based Pseudonym Changing Privacy Preserving Authentication in VANETs

Mengjia Zeng [1,2] **and Huibin Xu** [1]

[1]*School of Information Engineering, Huzhou University, Huzhou, Zhejiang 313000, China*
[2]*Qiuzhen School of Huzhou Teachers College, Huzhou, Zhejiang 313000, China*

Correspondence should be addressed to Huibin Xu; 02623@zjhu.edu.cn

Received 15 January 2019; Revised 1 April 2019; Accepted 2 April 2019; Published 2 June 2019

Academic Editor: Yuh-Shyan Chen

Vehicular ad hoc networks (VANETs) have attracted significant attention in academia insofar as they can provide reliable and secure communication between vehicles. It is thus essential to ensure security and preserve privacy. In this paper, we propose mix-context-based pseudonym changing privacy-preserving authentication (MPCPA). MPCPA introduces privacy protection through a mutual authentication mechanism to prevent attack-vehicles from sneaking into a VANET system. Moreover, it preserves the integrity of transmitted messages with an anonymous authentication mechanism. In addition, MPCPA adopts a mix-context-based pseudonym changing strategy to prevent vehicle tracking. A performance analysis demonstrates that MPCPA incurs low computational costs and offers a privacy-preserving scheme that is more secure than existing authentication schemes.

1. Introduction

Vehicular ad hoc networks (VANETs) have gained momentum recently due to the emergence of intelligent transportation systems (ITSs). 5G is the next-generation mobile communication system, which is being developed for the expected demand of VANETs [1]. Most ITS research is dedicated to VANETs, offering extensive improvements to the safety and efficiency of transportation networks [2]. Wireless communication permits vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication, as shown in Figure 1. As such, VANETs can improve road safety and offer value-added services to drivers on the road. Here, the infrastructure mainly refers to roadside units (RSUs). Furthermore, through V2V and V2I communication, VANETs can deliver safety-related messages (e.g., emergency reporting, collision warnings, and lane-change assistance) as well as traffic management and infotainment messages [3].

Although the feasible benefits for building up traffic safety and efficiency are conceptually attractive, there are some security and privacy challenges that need to be addressed in order to deploy VANETs [4, 5]. For instance, to prove that the sender is a genuine vehicle, messages broadcasted by the sender need to be signed. Neighboring vehicles are then able to verify the integrity of the message and the authenticity of the sender.

However, unlike mobile ad hoc networks, VANETs have distinct characteristics that require specific technology to authenticate messages, identify attackers, and protect the privacy and security of the driver's information.

Several privacy requirements for VANETs are identified in the literature. Anonymity is essential among these [6]. Messages must be authenticated without revealing the senders' identifiers. In order to meet this requirement, many pseudonymous authentication schemes have been proposed.

A pseudonym is an anonymous certificate that does not reveal any information about the real identifier of the vehicle. Pseudonyms can be generated or pregenerated on demand [7, 8]. If they are pregenerated, the pseudonyms are stored in the vehicle's on-board unit [9]. However, research has revealed that the position of a vehicle can be tracked even when pseudonyms are used, as a result of a pseudonym linking attack [10]. An attacker can excavate the relationship

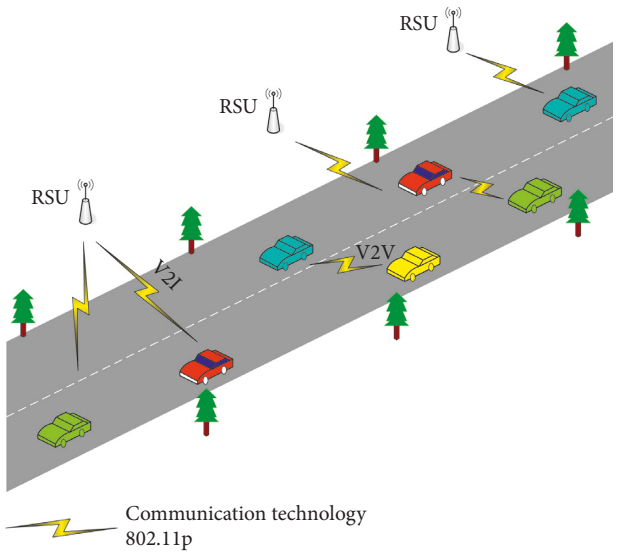

Figure 1: Schematic diagram of vehicle communication.

between pseudonyms and the real identification of the vehicle. Then, the attacker can steal the vehicles' real identification.

In order to address the above issues, we propose an efficient privacy preserving authentication scheme that we call mix-context-based pseudonym changing privacy-preserving authentication (MPCPA). Our main contributions are as follows:

(1) MPCPA is a privacy protecting mutual authentication mechanism that prevents attack-vehicles from sneaking into the VANET system

(2) MPCPA preserves the integrity of transmitted messages with an anonymous authentication mechanism

(3) MPCPA offers a mix-context-based pseudonym changing strategy with the capability of preventing vehicles from being tracked

(4) Experimental results show that the proposed authentication mechanism is efficient and that the pseudonym changing strategy protects against pseudonym linking attacks.

The remainder of this research is organized as follows. A brief review of related works is presented in Section 2. Our system model and the necessary preliminaries are described in Section 3. In Section 4, the efficient privacy preserving anonymous authentication scheme is discussed, and in Section 5, the pseudonym changing strategy is described in detail. Finally, we conclude the paper with a summary in Section 6.

2. Related Work

There is ample research that undertakes privacy and pseudonymity. For instance, Zhang et al. [11] proposed a novel identity-based batch verification (IBBV) algorithm, although the algorithm is vulnerable to nonrepudiation attacks. Shim [12] introduced an efficient identity- (ID-) based signature (IBS) algorithm that is able to protect against impersonation attacks. However, it is vulnerable to modification attacks. Thenmozhi et al. [13] proposed blind signature-based security and privacy. It implements a security mechanism using blind signature, where the roadside units in collaboration with the trusted authority generate the keys to be transmitted to the vehicles.

When providing safety-related messages to vehicles, only authenticated vehicles are allowed to communicate in the network and only authenticated messages can be exchanged among vehicles. Considering the privacy of vehicles, the authentication operation is done anonymously. However, existing algorithms suffer from high computational costs incurred by anonymous authentication. Thus, Vijayakumar et al. [14] proposed an efficient privacy preserving anonymous batch authentication scheme. Their scheme verifies the authenticity of a batch of vehicles when a batch of messages is received.

Islam et al. [15] designed a password-based conditional privacy preserving authentication protocol without bilinear pairing or an elliptic curve. The protocol avoids heavy computational costs and introduces a group-key generation mechanism, where vehicles can only communicate with vehicles that have the same group-key. Azees et al. [16] proposed efficient anonymous authentication in order to avoid malicious vehicles from entering into the VANET. However, their scheme still suffers from high computational costs.

In addition, a pseudonym changing approach is a common anonymous privacy protection mechanism. Freudiger et al. [17] proposed a game-theoretic solution to change pseudonyms (GSCP). Moreover, Ying et al. [18] introduced dynamic mix-zones for location privacy. However, their scheme is susceptible to semantic linking attacks. In order to avoid adversaries from making predictions, Pan et al. [19] proposed a random pseudonym changing algorithm. Moreover, Eckhoff et al. [20] proposed a mix-zone-based pseudonym changing strategy. According to the strategy, most vehicles change their pseudonym at the same time.

3. System Model and Preliminaries

3.1. System Model. VANETs consist of three types of network entities, as shown in Figure 2, viz., trusted authorities (TAs), RSUs, and vehicles.

TAs are in charge of registering vehicles and RSUs. In other words, the TA is responsible for issuing public/private key pairs and certificates [21]. It is worth mentioning that a TA is considered to be fully trusted.

An RSU is infrastructure deployed at the road side, subordinated by the TA. RSUs can connect to the Internet and communicate with vehicles within range. Furthermore, a vehicle communicates with the TA through the adjacent RSU.

Vehicles are motorized vehicles operating on the road. These vehicles mainly communicate with one another to share local traffic information. In addition, each vehicle is

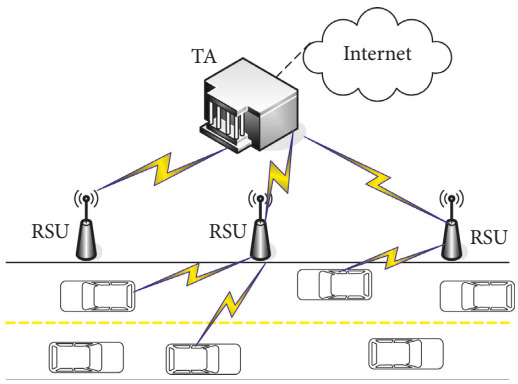

Figure 2: System model.

equipped with a tamper-proof device. This device stores the private and public keys for the vehicle. It is assumed that TAs, RSUs, and vehicles all have certain computing power. Moreover, all three communication entities adopt a consistent time mechanism.

3.2. Mathematical Model. Bilinear pairing technology was proposed by Boneh et al. in 2004 and forms the basis of our proposed authentication mechanism [22]. The mechanism is based on two additive cyclic groups and a multiplicative group. We denote the additive groups by G_1 and G_2 and the multiplicative group by G_T. The three groups have the same prime order, q. It is worth mentioning that q is a large prime. The bilinear map is $e : G_1 \times G_2 \longrightarrow G_T$. The bilinear map satisfies the following properties:

(1) *Bilinear*: $\forall a, b \in Z_q^*$, the mapping $e : G_1 \times G_2 \longrightarrow G_T$ is considered to be bilinear when it satisfies the following equation:

$$e\left(g_1^a, g_2^b\right) = e\left(g_1, g_2\right)^{ab}, \tag{1}$$

where g_1 and g_2 are generators of G_1 and G_2, respectively, and $a, b \in Z_q^*$. Among them, $Z_q^* = [1, 2, \ldots, q-1]$.

(2) *Nondegeneracy*: $e(g_1, g_2) \neq 1_{G_T}$.

(3) *Computable*: there is an efficient algorithm that easily computes the bilinear map $e : G_1 \times G_2 \longrightarrow G_T$.

4. Privacy Preserving Anonymous Authentication Scheme

This section describes the proposed pseudonym authentication framework. The framework consists of three parts: system initialization, registration, and mutual authentication of pseudonyms. The authentication framework is shown in Figure 3.

Pandi et al. [21] proposed an efficient anonymous identity authentication scheme to protect privacy. However, the random numbers in the parameters must be completely random, and it is unclear how collisions are prevented. On the basis of this, temporal parameters are added to avoid collisions when generating random numbers.

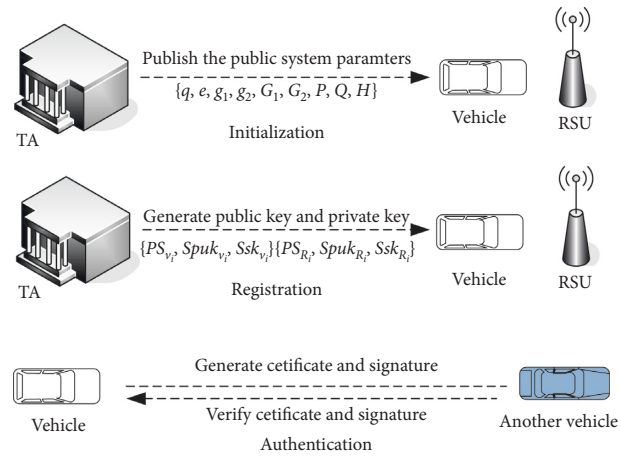

Figure 3: Block of authentication framework.

4.1. System Initialization. During system initialization, the TA is responsible for generating basic common parameters. First, the TA generates two random numbers, $m, k \in Z_q^*$, as private keys, where m is the primary key. That is, $\text{Mkey}_{\text{TA}} = m$. Because the values of g_1^m and g_1^k are repeatedly used in the following steps, the results are calculated in advance and saved in the form of parameters for subsequent use. Let $P = g_1^m$ and $Q = g_1^k$. The hash function $H : \{0,1\}^* \longrightarrow Z_q^*$ is then introduced. The common parameters of the system are expressed as $\text{pu\_sy} = \{q, e, g_1, g_2, G_1, G_2, G_T, P, Q, H\}$.

4.2. Registration Process. During the registration phase, the TA is responsible for generating public keys, private keys, and pseudonyms for the RSUs and vehicles. For a vehicle, for example, the public key, private key, and pseudonym are generated as follows:

Step 1. When a vehicle v_i moves into the TA's communication range, it transmits its name, address, license plate number, and other basic information to the TA—together with the sending time t_i of this message. Due to the TA's limited communication range and the high-speed movement of vehicles, few vehicles will be near the TA concurrently. Indeed, because the transmission time time_i of a vehicle is recorded in seconds, time_i is almost certainly unique. Therefore, this data can be used to identify the vehicle.

Step 2. The TA generates a random number $t \in Z_q^*$ by using time_i as the seed for the random number after receiving the basic information sent by vehicle v_i. The random number t is used as the system private key for vehicle v_i. That is, $\text{Ssk}_{v_i} = t$. Then, the TA calculates $\text{Spuk}_{v_i} = g_1^t$ as the system public key for vehicle v_i.

Step 3. In order to avoid transmitting real information about the vehicle during the authentication process, a forged vehicle identification code, i.e., the pseudonym, is used as the identification during vehicle authentication. The pseudonym

is used to protect the privacy of vehicle v_i from other vehicles. The initial pseudonym $\mathrm{PS}_{v_i} = \mathrm{Spuk}_{v_i} \times P = g_1^{m+t}$ is calculated by the TA.

Step 4. The TA calculates $\mathrm{ID}_{v_i} = \mathrm{Spuk}_{v_i} \times P \times Q = g_1^{m+k+t}$ and considers it a fake ID for vehicle v_i.

Step 5. The TA stores the information $(\mathrm{PS}_{v_i}, \mathrm{ID}_{v_i})$ of vehicle v_i. At the same time, the TA sends the initial pseudonym, public key, and private key $(\mathrm{PS}_{v_i}, \mathrm{Spuk}_{v_i}, \mathrm{Ssk}_{v_i})$ to the vehicle.

The TA's registration process for the RSU also goes through the five steps described above. That is, the TA generates a random number $r \in Z_q^*$ as the system private key Ssk_{R_i} for the $i-$th RSU. It then calculates its system public key $\mathrm{Spuk}_{R_i} = g_1^r$, initial pseudonym $\mathrm{PS}_{R_i} = \mathrm{Spuk}_{R_i} \times P = g_1^{r+m}$, and fake ID $\mathrm{ID}_{R_i} = \mathrm{Spuk}_{R_i} \times P \times Q = g_1^{m+k+r}$. Finally, the TA stores $(\mathrm{PS}_{R_i}, \mathrm{ID}_{R_i})$ and sends $(\mathrm{PS}_{R_i}, \mathrm{Spuk}_{R_i}, \mathrm{Ssk}_{R_i})$ to RSU_i.

4.3. Anonymous Authentication Based on Privacy Preserving. The authentication process takes place in the intercommunicating vehicle network entities. Its purpose is to prove the legitimacy of the communication entities and the integrity of the data in the transmission process. If the information is sent directly, there will be a risk of privacy disclosure. Therefore, anonymity is used to verify the legitimacy of the communication entity. Because the link time of each entity in the communication process is very short, if we can ensure the dynamic changes of various data, we can enhance the privacy. Therefore, the execution process of the algorithm coupled with a timeliness judgment validates the data in the timeliness range. Otherwise, the invalid data need to be recalculated and verified.

4.3.1. Generating Anonymous Certificates and Anonymous Signatures. In this algorithm, the legitimacy and data integrity of communication entities are realized by verifying certificates and signatures. In order to prove the legitimacy of the communication entity, the certificate verifies whether the sending entity has the legal identity. If it does not, it will proceed by verifying the signature and disconnecting from the communication entity. Signature verification confirms that the data are complete and untampered during the transmission. Therefore, before verifying the validity and data integrity, it is necessary to generate vehicle certificates and signatures. The anonymous vehicle certificates are generated through the steps in Algorithm 1.

Assuming that the data to be transmitted for vehicle v_i is data and expressed as D, its anonymous signature Sig_{v_i} is generated as follows:

$$\mathrm{Sig}_{v_i} = g_2^{\left(H(D)+t_i+t\right)^{-1}}. \tag{2}$$

Finally, vehicle v_i proves its legitimacy by broadcasting messages msg, consisting of vehicle $v_i's$ anonymous certificate, the anonymous signature, and the system public key:

$$\mathrm{msg} = \left(\mathrm{Cer}_{v_i} \middle|\middle| \mathrm{Sig}_{v_i} \middle|\middle| \mathrm{Spuk}_{v_i}\right). \tag{3}$$

4.3.2. Identity Verification. Other vehicles or RSUs that receive msg will verify the identity of the sender. The verification process is as follows:

Step 1. Separately calculate the following:

$$\begin{aligned} X &= \mathrm{PS}_{v_i} \times L_4, \\ L_a &= \mathrm{Apuk}_{v_i} \times L_1' \times L_3', \\ L_b &= L_1' \times L_3', \\ L_c &= L_2' \times L_4. \end{aligned} \tag{4}$$

Step 2. Use parameters X, L_a, L_b, L_c to generate a new verification code Ac', as follows:

$$\mathrm{Ac}' = H\left(\mathrm{ApuK}_i \middle|\middle| L_a \middle|\middle| L_b \middle|\middle| L_c \middle|\middle| L_4 || X\right). \tag{5}$$

Step 3. Verify the validity of the identity of the vehicle sending the message by verifying whether $\mathrm{Ac} = \mathrm{Ac}'$ is valid. The composition of Ac and Ac' is compared, and it suffices to validate $L_1 = L_a, L_2 = L_b, L_3 = L_c, P = X$. The verification process is as follows:

$$\mathrm{Ac} = \mathrm{Ac}', \tag{6}$$

$$\begin{aligned} L_a &= \mathrm{Apuk}_{v_i} \times L_1' \times L_3' \\ &= g_1^{t_i} \times g_1^{a+b+c} \times g_1^{-c} \\ &= g_1^{t_i+a+b+c-c} \\ &= g_1^{t_i+a+b} \\ &= L_1, \end{aligned} \tag{7}$$

$$\begin{aligned} L_b &= L_1' \times L_3' \\ &= g_1^{a+b+c} \times g_1^{-c} \\ &= g_1^{a+b+c-c} \\ &= g_1^{a+b} \\ &= L_2, \end{aligned} \tag{8}$$

$$\begin{aligned} L_c &= L_2' \times L_4 \\ &= g_1^{b+c} \times g_1^{-t} \\ &= g_1^{b+c-t} \\ &= L_3, \end{aligned} \tag{9}$$

$$\begin{aligned} L_c &= L_2' \times L_4 \\ &= g_1^{b+c} \times g_1^{-t} \\ &= g_1^{b+c-t} \\ &= L_3, \end{aligned} \tag{10}$$

Step 1. Vehicle v_i uses the current time time$_i$ as the seed of random number to generate random number $t_i \in Z_q^*$ and calculates its authentication public key $\text{Apuk}_{v_i} = g_1^{t_i}$.
Step 2. Vehicle v_i generates 3 random numbers $a, b, c \in Z_q^*$ and computes authentication parameters $L_1 = g_1^{t_i+a+b}$, $L_2 = g_1^{a+b}$, $L_3 = g_1^{b+c-t}$, $L_4 = g_1^{-t}$, $L_1' = g_1^{a+b+c}$, $L_2' = g_1^{b+c}$, and $L_3' = g_1^{-c}$.
Step 3. Use authentication public key and authentication parameters $L_1 \sim L_4$ and system parameter P from function H to generate vehicle $v_i's$ authentication verification code $\text{Ac} = H(\text{ApuK}_i||L_1||L_2||L_3||L_4||P)$.
Step 4. Use $\text{Ac}, L_1' \sim L_3', L_4$, authentication public key, and pseudonym of vehicle v_i to combine an anonymous certification $\text{Cer}_{v_i} = \{\text{Ac}||L_1'||L_2'||L_3'||L_4||\text{Apuk}_{v_i}||\text{PS}_{v_i}\}$.

Algorithm 1: Generating anonymous certificate.

$$\begin{aligned} X &= \text{PS}_{v_i} \times L_4 \\ &= g_1^{m+t} \times g_1^{-t} \\ &= g_1^{m+t-t} \\ &= g_1^{m} \\ &= P. \end{aligned} \tag{11}$$

Therefore, $\text{Ac} = \text{Ac}'$ is established and the legal identity of the vehicle v_i is verified.

4.3.3. Verifying Data Integrity. The integrity of the transmitted data is ensured by verifying the signature. As such, the data are untampered. The receiver uses equation (11) to verify the integrity of the data. If equation (11) holds, the data are untampered, and the receiver receives the message. Otherwise, the message is rejected:

$$e\left(g_1^{H(D)} \cdot \text{Apuk}_{v_i} \cdot \text{Spuk}_{v_i}, \text{Sig}_i\right) = e(g_1, g_2). \tag{12}$$

The process of checking this is as follows:

$$\begin{aligned} e\left(g_1^{H(D)} \cdot \text{Apuk}_{v_i} \cdot \text{Spuk}_{v_i}, \text{Sig}_i\right) &= e\left(g_1^{H(D)} \cdot g_1^{t_i} \cdot g_1^{t}, g_2^{\left(H(D)+t_i+t\right)^{-1}}\right) \\ &= e\left(g_1^{H(D)+t_i+t}, g_2^{\left(H(D)+t_i+t\right)^{-1}}\right) \\ &= e(g_1, g_2)^{\left(H(D)+t_i+t\right)\times\left(H(D)+t_i+t\right)^{-1}} \\ &= e(g_1, g_2). \end{aligned} \tag{13}$$

Therefore, the integrity of the data is verified, indicating that it has not been tampered with during the transmission process.

5. Pseudonym Changing Mechanism

In this section, we describe the proposed pseudonym changing mechanism in detail. We assume that each vehicle has a set of pseudonyms pregenerated by the TA. In addition, each pseudonym has a short duration, called the stable time. In other words, each vehicle has to change its pseudonym frequently. The model for the pseudonym changing mechanism is shown in Figure 4.

5.1. Resolved Problem. Even when vehicles change their pseudonyms, attackers can discover the relationship between the pseudonyms by various means. Consequently, the position of vehicles can be tracked. This attack is called a pseudonym linking attack, as shown Figure 5. To illustrate this, we consider a case with three vehicles (A, B, and C). If only vehicle B changes its pseudonym from $B1$ to $B2$ during Δt, an attacker can discover that $B1$ and $B2$ are associated with B.

The proposed pseudonym changing mechanism prevents this type of attack by making it more difficult for the attacker to link pseudonyms. The main purpose of the proposed pseudonym changing mechanism is to determine where and when a vehicle should change its pseudonym [10].

5.2. Mix-Context-Based Cooperative Pseudonym Mechanism. In the proposed MPCPA, each vehicle decides independently where and when to change its pseudonym; in this way, each pseudonym has a stable time. Once this stable time expires, the vehicle is ready to change its pseudonym and is able to check whether the mix-context condition is satisfied. If this is the case, the vehicle changes its pseudonym immediately. Otherwise, the vehicle waits until the maximum wait time expires, at which time it must change its pseudonym. The mechanism is shown in Figure 6.

As shown in Figure 6, the mix-context condition is a substantial element in the proposed mechanism. Thus, we analyzed this condition in detail.

In VANETs, vehicles need to broadcast their beacons at the same time, and synchrony is achieved with GPS clocks. Therefore, we make use of these beacons by inserting two flags into each beacon, as shown in Figure 7.

Here, the wait-flag indicates whether a vehicle is waiting to change its pseudonym. If the wait-flag is 1, the vehicle is waiting to change its pseudonym. Otherwise, it is not. The ready-flag indicates whether the vehicle is ready to change its pseudonym during the next time slot. If the ready-flag is 1, the vehicle is ready to change its pseudonym. Both the wait-flag and ready-flag are initially set to 0.

In addition, the proposed MPCPA is a cooperative model. Each vehicle needs to construct a list of neighbors. Let L_v denote the set of vehicles neighboring vehicle v. The list of neighbors is generated by data received by the beacons.

When the stable time expires, the wait-flag is set to 1. The ready-flag is then set to 1 when the vehicle finds at least k neighboring vehicles with a wait-flag equal to 1 and $k \leq L$, where L denotes the number of neighboring vehicles.

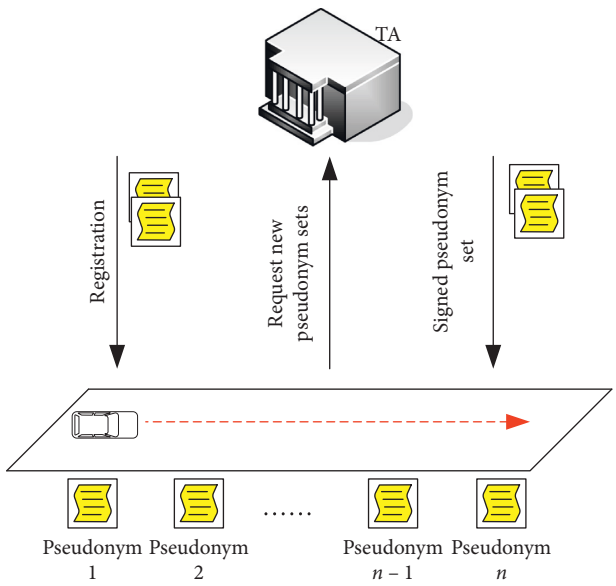

Figure 4: Model for the pseudonym changing mechanism.

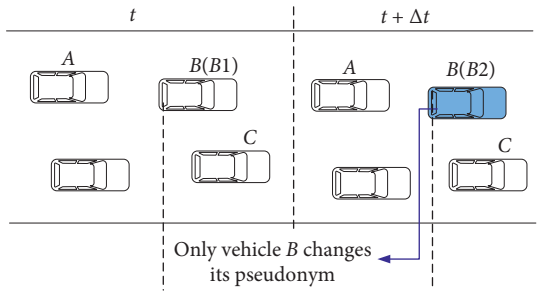

Figure 5: Pseudonym linking attack.

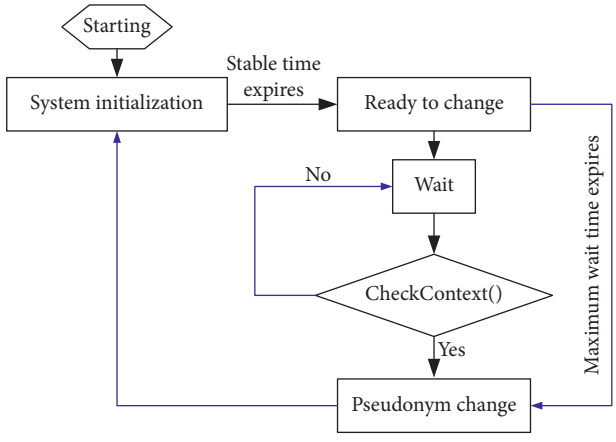

Figure 6: Diagram of the proposed pseudonym mechanism.

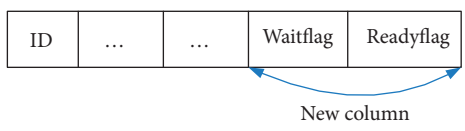

Figure 7: Beacon format.

The conditions for changing a pseudonym are shown in Algorithm 2. The vehicle will change its pseudonym when at least k neighboring vehicles are ready to change their pseudonyms, or when one of neighboring vehicles has k or more neighbors ready to change their pseudonyms.

Specifically, num_nb is used to count the number of neighboring vehicles with a ready-flag equal to 1. When $\text{num\_nb}(v) = 3$, for instance, there are three neighboring vehicles with a ready-flag equal to 1.

6. Performance Analysis

In this section, we analyze the performance of the proposed MPCPA.

6.1. Security Analysis. The proposed scheme satisfies anonymous vehicle authentication and privacy protection.

6.1.1. Anonymous Vehicle Authentication. As explained in Section 4.3 and detailed in Algorithm 1, a vehicle v generates an anonymous certificate and an anonymous signature for message M. Message M contains a signature and a certificate. Vehicle v is successfully authenticated only when equation (6) is satisfied.

6.1.2. Privacy Protection. The privacy of the vehicles is protected using a digital signature and the mix-context cooperative pseudonym changing mechanism, as detailed in Algorithm 2. Each vehicle has a set of pseudonyms, and a vehicle changes its pseudonym only when the mix-context conditions are satisfied. This mechanism protects vehicle privacy and prevents vehicles from being tracked.

6.2. Computation Cost and Verification Time of Anonymous Authentication. We selected two main evaluation metrics to evaluate the performance of the proposed authentication mechanism: the computation cost and the verification time. Both metrics reflect the complexity of the algorithm. The computation cost refers to the total amount of time required for the authentication process. In addition, we compared the performance of MPCPA to that of four well-known authentication mechanisms, viz., IBBV [11], GSCP [17], key-insulated pseudonym self-delegation (KPSD) [23], and secure authentication scheme for VANETs with batch verification (SABV) [24].

Let t_p, t_h, and t_m denote the execution time for the pairing operation, hash operation, and multiplication operation, respectively. Accordingly, t_e and t_s are the execution time required for the exponentiation operations in G_1 and G_2, respectively.

The total amount of consumed time for the various schemes is shown in Table 1. We can observe that our MPCPA algorithm outperforms existing schemes in terms of the computational cost. As such, the proposed scheme has a relatively fast execution time. In particular, for one certification and signature, MPCPA required only $2t_p$, $2t_e$, and $2t_h$ for the verification process.

Input: $L_v = \{0, \ldots, N\}, k$
Output: pseudonym changing
  If num_nb$(v) \geq k$ **then**
  Vehicle v changes the pseudonym
  Else
    for $i = 1$ to N
      If num_nb$(i) \geq k$ **then**
      Vehicle v changes the pseudonym
    End if
  End for
End if

Algorithm 2: Mix-context cooperative pseudonym changing mechanism.

Table 1: Total amount of consumed time.

Scheme	Execution time for operation			
	Pairing	Hash	Multiplication	Exponentiation
MPCPA	$(1+n)t_p$	nt_h	—	$(1+n)t_e$
GSCP	$(2+3n)t_p$	$2nt_h$	$(n+5)t_m$	—
KPSD	$(3+n)t_p$	nt_h	—	$(4+n)t_e + 5nt_s$
IBBV	$3nt_p$	$3nt_h$	$(2n+5)t_m$	—
SABV	$(2+3n)t_p$	nt_h	—	nt_e

Next, the verification time of MPCPA was compared to that of IBBV, GSCP, KPSD, and SABV. Figure 8 shows the results of this experiment. Indeed, with an increase in the number of received messages, the verification time will increase. Compared to IBBV, GSCP, KPSD, and SABV, the proposed MPCPA performed better in terms of the verification time. For example, with 120 received messages, our MPCPA algorithm required merely 600 ms to complete the verification process, whereas the other algorithms needed more than 900 ms.

6.3. Avoiding Pseudonym Linking Attacks. According to the above analysis, the purpose of the proposed pseudonym mechanism is to defend against attackers seeking to track vehicles and stealing private information with a pseudonym linking attack. In order to analyze the effectiveness of the proposed mechanism, the tracking model in [25] was introduced to determine the tracking probability.

We denote the number of vehicles ready to change their pseudonyms at Δt by $N(\Delta t)$. According to a Poisson process, $N(\Delta t)$ is distributed as follows:

$$\Pr\{N(\Delta t) = i\} = \frac{(\lambda \Delta t)^i e^{-\lambda \Delta t}}{i!}, \tag{14}$$

where the vehicles are uniformly distributed with rate λ.

When the stable time of the pseudonym expires, the vehicle is ready to change its pseudonym. Thus, we assume that at least one vehicle has changed its pseudonym. The probability P_t that a new pseudonym will be linked to the same vehicle is derived as follows [26]:

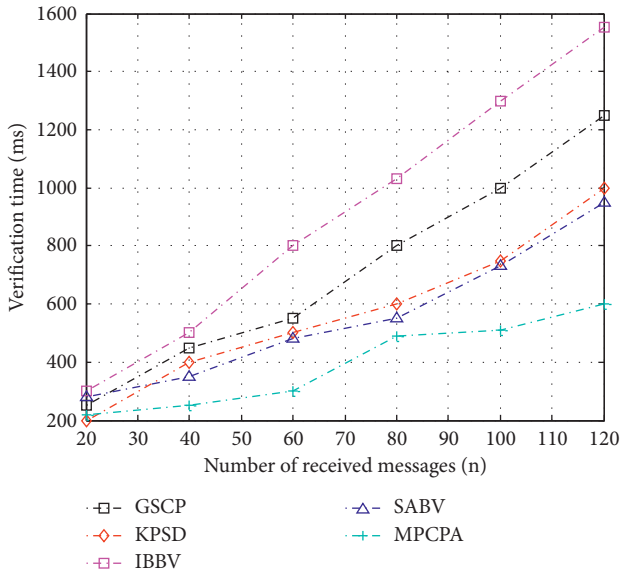

Figure 8: Verification time of various schemes.

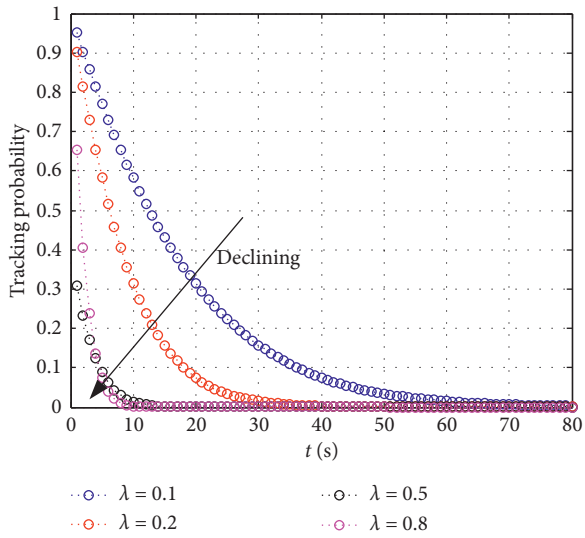

Figure 9: Tracking probability over 80 s.

$$P_t = \Pr\{N(\Delta t) = 1 \mid N(\Delta t) \geq 1\} = \frac{\Pr\{N(\Delta t) = 1\}}{1 - \Pr\{N(\Delta t) = 0\}} = \frac{(\lambda t) e^{-\lambda t}}{1 - e^{-\lambda t}}. \tag{15}$$

Note that in Algorithm 2, parameter k plays an important role in defending against a pseudonym linking attack. Therefore, the impact of parameter k on the probability P_t is relevant. Given that $\lambda = k/L_v$, Figure 9 shows tracking probabilities under different λ values. As shown in the figure, the probability drastically decreases as k increases. This is expected. The more vehicles simultaneously changing their pseudonyms, the less likely they are to be tracked.

7. Conclusion and Future Work

In this paper, we proposed a privacy-preserving authentication scheme for secure communication in VANETs. The proposed MPCPA introduces an anonymous authentication mechanism to preserve the privacy of the vehicles. Furthermore, a mix-context-based cooperative pseudonym changing mechanism protects the location of vehicle users. The proposed authentication scheme is efficient in terms of its computational complexity. Our evaluation demonstrated that MPCPA greatly reduces computational overhead and provides an efficient means for preserving the privacy of vehicles.

In future research, we will study cooperative message verification and batch signature verification to reduce computational overhead further, and we will subject our scheme to extensive experimentation to verify its authentication scheme. It is noteworthy that the proposed MPCPA is not independent from the RSU. Consequently, we will consider ways of carrying out privacy preserving authentication without the need for the RSU.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partly supported by Zhejiang Province Natural Science Foundation of China (LY18G020008, LQ18F020002), Zhejiang Province Soft Science Foundation of China (2019C35006), National Natural Science Foundation of China (61202290), Huzhou University's Scientific Research Foundation in 2018 (2018XJKJ63), and Huzhou City Zhejiang Province Key Industry Project of China (2018GG29).

References

[1] X. Huang, M. Zeng, J. Fan, X. Fan, and X. Tang, "A full duplex D2D clustering resource allocation scheme based on a K-means algorithm," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 1843083, 8 pages, 2018.

[2] H. Wang, H. Luo, and X. Liu, "Evidential reasoning method based on isometric mapping in internet of vehicular Ad-hoc NETworks," *System Engineering Theory and Practice*, vol. 35, no. 6, pp. 1582–1595, 2015.

[3] P. Vijayakumar, M. Azees, and L. Jegatha Deborah, "CPAV: computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks," in *Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, pp. 62–67, New York, NY, USA, November 2015.

[4] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, no. 9, pp. 19–30, 2017.

[5] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Location verification systems for VANETs in rician fading channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5652–5664, 2016.

[6] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 25, no. 5, pp. 24011–24022, 2017.

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

[8] R. Lu, X. Lin, and T. Luan, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012.

[9] P. Papadimitratos, L. Buttyan, and T. Holczer, "Secure vehicular communication systems: design and architecture," *IEEE Communications*, vol. 46, no. 11, pp. 100–109, 2018.

[10] A. Boualouache, S. M. Senouci, and M. Samira, "A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks," *IEEE Communications Surveys and Tutorials*, vol. 3, no. 7, pp. 1–21, 2017.

[11] C. Zhang, R. Lu, and X. Lin, "An efficient identity-based batch verification scheme for vehicular sensor networks," *Proceedings of IEEE infocom*, pp. 816–824, 2008.

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

[13] T. Thenmozhi and R. M. Somasundaram, "Pseudonyms based blind signature approach for an improved secured communication at social spots in VANETs," *Wireless Personal Communications*, vol. 82, no. 1, pp. 643–658, 2015.

[14] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, pp. 943–955, 2018.

[15] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[16] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[17] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "Non-cooperative location privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 2, pp. 84–98, 2013.

[18] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5631–5641, 2015.

[19] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random pseudonym change scheme in VANETs," *Cluster Computing*, vol. 17, no. 2, pp. 413–421, 2014.

[20] D. Eckhoff, C. Sommer, and T. Gansen, "Strong and affordable location privacy in VANETs: identity diffusion using time-slots and swapping," in *IEEE Vehicular Networking Conference*, pp. 174–181, Jersey City, NJ, USA, December 2016.

[21] V. Pandi, A. Maria, and V. Chang, "Computationally efficient privacy preserving authentication and key distribution

techniques for vehicular ad hoc networks," *Cluster Computing*, vol. 20, no. 3, pp. 2439–2450, 2017.

[22] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[23] R. Lu, X. Lin, and T. H. Luan, "Pseudonym changing at social spots: an effective strategy for location privacy in VANET," *IEEE Transaction on Vehicle Technology*, vol. 61, no. 1, pp. 86–96, 2012.

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

[25] K. Sampigethaya, M. Li, and L. Huang, "AMOEBA: robust location privacy scheme for vanet," *IEEE Journal of Selected Area in Communications*, vol. 25, no. 8, pp. 1569–1589, 2016.

[26] H. Xu, "Proxy re-encryption-based secure location service in VANETs," *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, vol. 30, no. 6, pp. 835–841, 2018.