A Hierarchical Blockchain-Assisted Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks

Xingyu He 1,*, Xianhua Niu 1,2, Yangpeng Wang 1, Ling Xiong 1, Zhizhong Jiang 1 and Cheng Gong 1

1 College of Computer and Software Engineering, Xihua University, Chengdu 610039, China; ruurustef1212@gmail.com (X.N.); wangyangpeng089@gmail.com (Y.W.); lingxiong.swjtu@foxmail.com (L.X.); xhu_zzz@163.com (Z.J.); 15223789268@163.com (C.G.)
2 National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

* Correspondence: stephen0824jl@163.com

Abstract: Through information sharing, vehicles can know the surrounding road condition information timely in Vehicular Adhoc Networks. To ensure the validity of these messages and the security of vehicles, the message authentication, privacy-preserving, and delay problems are three important issues. Although many conditional privacy-preserving authentication schemes have been proposed to ensure secure communication, there still exist some imperfections such as frequent interactions or unlinkability. From this, our paper proposes a novel hierarchical blockchain-assisted authentication scheme to solve these existing issues comprehensively. First, unlinkability is achieved by a dynamic key derivation algorithm. Second, the proposed scheme can reduce correlation processing delay, queuing delay, and deployment costs by adopting hierarchical Vehicle Fog Computing. Third, cross-region authentication is achieved by taking advantage of the properties of blockchain. In addition, we demonstrate our scheme can fulfill the security criteria of the Vehicular Adhoc Network by security analysis. Furthermore, the simulations are carried out to show its availability by using JAVA and NS-3. The findings reveal that the suggested method outperforms earlier schemes in terms of computation cost and communication cost. All in all, making the authentication scheme more efficient and concise is the focus of our future research.

Keywords: privacy-preserving; hierarchical; authentication; blockchain

1. Introduction

Vehicular Adhoc Networks(VANETs) were proposed to ease traffic pressure and reduce traffic accidents [1,2]. VANETs take vehicles as the basic information units and realize the network connection between vehicles and X (e.g., vehicles, infrastructures) through the help of the new generation of information and communication technology. Figure 1 is a typical VANET. There are two basic modalities of communications, namely: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructures (V2I). By sharing information about the surrounding road conditions, other vehicles can replan their routes in time to avoid traffic jams and traffic accidents after receiving these messages. In addition, the Traffic Control Center (TCC) can make flexible adjustments to traffic timely to ease the traffic pressure. VANETs are seen as a potential technology in current intelligent transportation systems because of these benefits.

Since communications are exchanged wirelessly via open channels, it is simple for an attacker to intercept messages from communication channels and launch a series of harmful assaults (e.g., impersonate a legitimate vehicle to send a false message or tamper with messages) [3–6]. Once the recipient makes a wrong decision based on these malicious messages, it may lead to traffic jams or even car accidents. In addition, the identity information of vehicles, itinerary, and other factors may be used by the adversary to carry...
out an attack. Hence, security and privacy are two important factors that cannot be ignored in VANETs. In other words, the authenticity and the legitimacy of the messages should be guaranteed in VANETs.

Figure 1. A typical VANET structure.

To address the privacy and security issues that plague VANETs, a significant variety of privacy-preserving authentication schemes have been presented during the previous decade [7–10]. These solutions go a long way toward overcoming issues like conditional privacy and unlinkability. At the same time, it also provides the direction and theoretical basis for the subsequent researchers. Although these solutions can solve the problem of cross-region authentication, additional communication is required during cross-region authentication, which increases the related cost.

Blockchain technology provides a good idea for cross-region authentication. Lin et al. [11] adopted a dynamic key derivative algorithm to realize the unlinkability. Compared with the traditional scheme, this scheme can not only realize fast cross-region authentication but also avoid storing a large number of pseudonyms. However, in order to speed up the process, their scheme requires all RSUs to be trusted, which may increase the deployment costs of the infrastructure. In addition, this scheme has the defects of high queuing delay in theory due to all communications of vehicles being processed by a single trusted authority (TA).

With the increasing number of connected vehicles, Vehicle Fog Computing (VFC) was proposed to satisfy low latency and uninterrupted services for users. In this pattern, data, processing, and applications are centralized in devices at the edge of the network and can significantly reduce the delay of message processing. Furthermore, that is why VFC is considered as a promising technology to make the best utilization of these vehicular communication and computational resources [12,13]. Yao et al. [14] and Kaur et al. [15] adopted distributed VFC to reduce the delay by using multiple regional managers to handle vehicles’ communications instead of a single TA. Nonetheless, they did not take into account the unlinkability of messages. As a result, to assure the safety and privacy of vehicles and to reduce delay to realize real-time communications in VANETs, we designed a hierarchical effective blockchain-assisted conditional privacy-preserving scheme. The proposed scheme can reduce the time delay and deployment costs by using hierarchical distributed VFC. Furthermore, unlinkability is achieved through a dynamic key derived algorithm.

1.1. Contribution

In this study, we proposed a hierarchical blockchain-assisted conditional privacy-preserving authentication (CPPA) scheme for VANETs. The following are the paper’s significant contributions:
• First, to reduce the deployment costs and the associated processing time, the proposed scheme adopted distributed VFC, which uses multiple regional managers instead of a single TA.
• Second, to achieve unlinkability, the proposed scheme employs a dynamic key derivation algorithm to generate dynamic public-private key pairs for each communication of vehicles.
• Third, through Java and NS-3 simulation experiments, we show that our scheme is suitable for VANETs in terms of communication and computing overhead.

1.2. Organization

The following is a rough outline of the paper’s structure. Section 2 examines relevant CPPA schemes for VANETs. Section 3 presents the relevant preliminary knowledge for our scheme. Our system model and security and privacy requirements for VANETs and the details of our scheme are shown in Section 4. Security analysis is carried out in Section 5. In Section 6, we examine the corresponding computing and communication overhead and compare it to existing schemes. In the end, we provided a brief summary of this study in Section 7.

2. Related Work

To achieve effective communication in VANETs, many authentication schemes have been proposed. Picconi et al. [16] relied on PKI-based authentication, proposed a solution for validating aggregated data in V2V traffic information systems. Zhang et al. [17] adopted the $k$-anonymity to protect user identity privacy, while they are useful to some extent in addressing privacy issues VANET, the difficulties of certificate management make them impractical. To improve the efficiency of ID-based CPPA scheme, He et al. [8] proposed a novel CPPA scheme by utilizing the elliptic curve cryptography (ECC). Zhong et al. [18] employs pseudonym-based signatures for identity authentication for VANET. Furthermore, both of them also support batch validation, allowing the verifier to validate multiple messages simultaneously, which greatly improves the validation efficiency. However, then, these programs require a pre-established trust relationship between the regional management center and vehicles, which will not exist once a vehicle moves to another region. Wang et al. [19] adopted group-based message authentication algorithm to address the security issues in V2V communication. When a vehicle enters the coverage area of a new RSU, it must be re-authenticated to the new RSU, which undoubtedly increases the delay. Ali et al. [20] design an efficient conditional privacy-preserving hybrid signcryption scheme for heterogeneous vehicle communication based on bilinear pairing. The users’ privacy is protected to a certain extent, but the unlinkability cannot be guaranteed.

With the popularity of blockchain technology, many scholars employ blockchain to realize cross-region authentication. Yao et al. [14] proposed a BLA for distributed VFS to achieve a flexible cross-region authentication. The public key and identity information of vehicles are placed on a consortium blockchain so that different regional managers can verify the messages sent by legal vehicles and then provide VFS for them. Kaur et al. [15] present an effective cross-region authentication and key-exchange scheme based on Yao [14], which realize mutual authentication between vehicles and service managers. However, unlinkability cannot be satisfied. Wang et al. [21] present trustworthiness evaluation to achieve a time-efficient V2I-handover authentication. It seems only considered V2I communication scenarios. Lu et al. [22] adopted the Merkle Patricia tree (MPT) to extend the conventional blockchain and record the activities of the semiTAs in blockchain to achieve the certificate and revocation transparency. However, it requires vehicles to interact frequently with the certificate center to generate anonymous certificates, resulting in low efficiency. Inspired by the HD Wallet, Lin et al. [11] proposed a novel BCPPA by using key derivation algorithms and smart contracts. The public key certificate of each communication of vehicles is pre-placed in the blockchain for vehicles to retrieve, saving the overhead of storing a large number of certificates in OBUs. However, it seems to be burdensome for
Certificate Authorities (CA) to generate a public key certificate for every communication of all vehicles. For clarification, a brief summary is given in Table 1.

Table 1. Summary of related work.

| Scheme         | Key Technology                   | Pros                                              | Cons                                           |
|----------------|----------------------------------|---------------------------------------------------|------------------------------------------------|
| Picconi [16]   | Challenge the aggregator to provide a proof | ● Easy to verify                                   | Certificate management is difficult            |
| Zhang [17]     | $k$-anonymity                    | ● Guarantee security and privacy preservation     | Certificate management is difficult            |
|                |                                  | ● Strong scalability                              |                                                 |
| He [8]         | Elliptic Curve Cryptography      | ● Support batch verification                       | The implementation of cross-region authentication is complex |
|                |                                  | ● Fast validation                                 |                                                 |
| Zhong [18]     | Pseudonym-based signatures       | ● Support batch verification                       | The implementation of cross-region authentication is complex |
|                |                                  | ● Fast validation                                 |                                                 |
| Wang [19]      | Pseudonyms-based and group-based signatures | ● Easy to verify                                   | Require frequent authentication                |
|                |                                  | ● Guarantee security and privacy preservation     |                                                 |
| Ali [20]       | Hybrid signature                 | ● Easy to verify                                   | No consideration for unlinkability             |
|                |                                  | ● Support batch verification                       |                                                 |
| Yao [14]       | Multiple VFC, Blockchain-based   | ● Flexible cross-region authentication             | No consideration for unlinkability             |
|                |                                  | ● Convenient subsequent certification             |                                                 |
| Kaur [15]      | Key-exchange, Distributed VFC, Blockchain-based | ● Flexible cross-region authentication             | No consideration for unlinkability             |
|                |                                  | ● Convenient subsequent certification             |                                                 |
|                |                                  | ● Support mutual authentication                   |                                                 |
| Wang [21]      | Trustworthiness evaluation mechanism, Blockchain-based | ● Flexible cross-region authentication             | Require frequent interaction                   |
|                |                                  | ● Guarantee security and privacy preservation     |                                                 |
| Lu [22]        | MPT, Blockchain-based            | ● Realize transparency of certificate and revocation | Require frequent interaction                   |
|                |                                  | ● Flexible cross-region authentication             |                                                 |
| Lin [11]       | Dynamic key derivative algorithm, Smart contract, Blockchain-based | ● Flexible cross-region authentication             | High message processing and queuing latency    |
|                |                                  | ● Guarantee unlinkability of message              |                                                 |

3. Preliminaries

The relevant preliminary knowledge was briefly presented in this part.

3.1. Broadcast Encryption

Broadcast encryption may be thought of as a type of key encapsulation scheme. In our proposed scheme, we adopt a broadcast encryption case from [23] to complete the identification of vehicles by legitimate SMs. The whole process can be divided into the following three parts.

1. Setup: In our proposal, the maximum number of SMs is set to be $n$. Let $L$ stand for a set where $L \subseteq \{1, \ldots, n\}$. This step is mainly TA distributes a key $d_j$ for each $SM_j$, for $j \in L$. Then TA publish a public parameter $PK$.

2. Enc($PK, L$): A vehicle want to join the internet of vehicles, it uses $PK$ to calculate the encryption key $K$ and the header $Hdr$. The vehicle then encrypts a message $M$ using $K$ as a symmetric encryption key. Let $E_K(M)$ be the encryption of $M$. Finally, it broadcast $<E_K(M), Hdr>$.

3. Dec($PK, L, k, d_k, Hdr$): Let $SM_k$ be an example to decrypt $E_K(M)$. If $k \in L$, by inputting $PK$, the set $L$, the key $d_k$ and $Hdr$, $SM_k$ can easily compute a message encryption key $K'_k$. It’s remarkable that $K'_k = K$, this indicates that $SM_k$ can decrypt $E_K(M)$ and retrieve $M$ by using $K'_k$.

3.2. Mathematical Complexity Assumptions

The security of broadcast encryption relies on the bilinear Diffie-Hellman Exponent Assumption (BDHE). Generally, we define $\zeta$-BDHE in group $G_1$ as follows: input a vector
with $2^\zeta + 1$ elements where $(h, g, g^a, g^{a^2}, \ldots, g^{a^{\zeta+1}}) \in G_1^{2^\zeta+1}$. Then, output $e(g, h)^{(a^\zeta+1)} \in G_T$. Since $g^{a^{\zeta+1}}$ is not included in the vector, we cannot able to compute the required $e(g, h)^{(a^\zeta+1)}$ by the bilinear map.

For convenience, we let $g_i = g^{(a^i)} \in G_1$ while $g$ and $a$ are given. An algorithm $A$ has $\epsilon$ advantage to tackle $\zeta$-BDHE in $G_1$ if $Pr[A(h, g, g^{\zeta}, \ldots, g^{\zeta+2}, \ldots, g^{2\zeta}) = e(g^{\zeta+1}, h)] \geq \epsilon$. Note that $g$ and $h$ are random picks in $G_1$, $\alpha$ is random pick in $Z_q$, and $A$ picks the bits randomly.

Homoplastically, the definition of Decisional $\zeta$-BDHE (D-$\zeta$-BDHE) in $G_1$ is as follows. Let $y_{g, a, \zeta} = (g_1, \ldots, g^{\zeta+2}, \ldots, g^{2\zeta})$. An algorithm $B$ has advantage $\epsilon$ to output a bit $\psi \in \{0, 1\}$ to tackle D-$\zeta$-BDHE in $G_1$ if $|Pr[B(g, h, y_{g, a, \zeta}, e(g^{\zeta+1}, h)) = 0] - Pr[B(g, h, y_{g, a, \zeta}, T) = 0]| \geq \epsilon$. Similarly, $g$ and $h$ are random picks in $G_1$, $\alpha$ is a random pick in $Z_q$, $T$ is a random pick in $G_T$ and $B$ picks the bits randomly. Here, we let $\mathcal{P}_{BDHE}$ to present the left and $\mathcal{R}_{BDHE}$ to present the right.

3.3. Key Derivation

We anticipate that a vehicle will be able to employ distinct public and private key pairs to achieve unlinkability and not need to exchange keys or preload abundant key pairs. Therefore, we adopt a key derivation algorithm which proposed by [11]. This algorithm is separated into two parts: public key generation algorithm and private key generation algorithm. We have developed a flow chart in Figure 2 and included a quick explanation below to make it simpler to understand.

**Figure 2.** Key generation algorithm.

- **Private key generation algorithm:** The goal of this algorithm is for vehicles to generate a private key for subsequent communication. A vehicle randomly selects a seed to create the root private key ($sk_{root}$) and root chain code ($chain_{root}$). Then calculates the appropriate root public key ($pk_{root} = sk_{root} \cdot P$) and sends <$pk_{root}, chain_{root}$> to public key generator (i.e., SM). Based on $sk_{root}$, $chain_{root}$ and serial number of the current communication ($i$), the vehicle can derive a different private key.

- **Public key generation algorithm:** The purpose of this algorithm is for SMs to generate corresponding public keys for subsequent communication of vehicles. According to Figure 2, for the same serial number $i$, $pk_i = sk_i \cdot P$. It ensures that the public key retrieved by the verifier corresponds to the private key of the vehicle.
4. Scheme Description

In this section, we first introduced the system model and related security requirements, and then described our solution in detail. On the whole, The proposed scheme can mainly be divided into five phases, namely Initialization Phase, Registration Phase, Identity Authentication Phase, Consensus Phase and Message Authentication Phase. Note that we assume that there are \( n \) SMs in the system. Table 2 shows the definitions of the notations used in this article.

| Notations | Definition |
|-----------|------------|
| \( L \subseteq \{1, \ldots, n\} \) | \( q, \overline{q} \) two large prime integers |
| \( G \) | an additive cyclic group of prime order \( q \) |
| \( p \) | a generator of \( G \) |
| \( n \) | the number of SMs |
| \( G_1, G_T \) | two multiplicative cyclic groups of prime order \( \overline{q} \) |
| \( g \) | a generator of \( G_1 \) |
| \( e \) | a bilinear map where \( G_1 \times G_1 \rightarrow G_T \) |
| \( t_{st} \) | current timestamp |
| \( ID \) | real identity |
| \( PID \) | pseudonym |
| \( E_K(\cdot) \) | symmetric encryption utilizing \( K \) |
| \( D_K(\cdot) \) | symmetric decryption utilizing \( K \) |
| \( H \) | hash function |
| \( \oplus \) | exclusive-OR operation |
| \( \| \) | concatenation operation |

4.1. System Model

Figure 3 depicts our system model. In conclusion, we separated the entire system into a number of regions, and each region is managed by a single SM. The functions of each entity in our system are described as follows.

1. Trusted Authority (TA): TA is a completely trusted department that generally has strong computing and communication capabilities. In our system, TA is required to complete registration SMs and vehicles. If necessary, TA can find out the real identity of a malicious vehicle through a relevant message.

2. Service Manager (SM): an SM is mainly responsible for the identification of new vehicles joining VANETs in its region. Furthermore, SM is also responsible for the calculation of public keys and pseudonyms for subsequent communication of its certified vehicles.

3. Road Side Unit (RSU): RSU is a semi-trusted roadside infrastructure that can communicate wirelessly with vehicles according to the Dedicated Short Range Communication (DSRC) protocol [24]. Furthermore, RSUs are also responsible for forwarding messages between vehicles and SMs and providing VFS to vehicles.

4. Vehicle: as moving nodes, vehicles are outfitted with On-Board Units (OBUs), which are wireless communication devices. OBU is a tamper-proof device that also has certain computation and communication capabilities. By using OBUs, vehicles may exchange their current road traffic circumstances and driving status with the adjacent vehicles and RSUs in real-time via DSRC protocol. What’s more, OBU’s information will never be revealed.
4.2. Security and Privacy Requirements

1. Identity authentication: SM can effectively verify the legitimacy of new vehicles joining VANETs.
2. Message authentication: for any received message, the verifier can verify that the message is valid.
3. Identity privacy preservation: except for TA, no one can deduce the true identity of vehicles from the intercepted messages.
4. Unlinkability: it will be impossible for an adversary to link two messages transmitted by the same vehicle.
5. Traceability: if required, TA can determine the message sender’s true identity. This guarantees that messages are held accountable.
6. Resist various attacks: our scheme also assures that other assaults in VANETs, such as the replay attack, the impersonation attack and the modification attack, can be easily identified.

4.3. Initialization Phase

This phase is mainly performed by TA to create a series of system parameters. The following are the specifics.

- Picks two random large prime integers \( p, q \) and choose an additive group \( G \) generated by a point \( P \) with order \( q \) on a non-singular elliptic curve \( E : y^2 = x^3 + vx + w \mod p \) where \( v, w \in F_p \).
- Picks two large prime numbers \( p, q \) at random and chooses two multiplicative groups \( G_1, G_T \) generated by a point \( g \) with order \( q \).
- Selects a number \( sk_{TA} \in Z_q^* \) at random as its private key, then computes \( pk_{TA} = sk_{TA} \cdot P \) as its public key.
- Chooses a random number \( a \in Z_q^* \), calculates \( g_\gamma = g^a \in G_1 \) for \( \gamma = \{1, 2, \ldots, n, n + 2, \ldots, 2n\} \).
- Picks a random number \( \beta \in Z_q^* \), and then computes \( v = g^\beta \in G_1 \). Next, TA set \( PK = (g, g_1, g_2, \ldots, g_n, g_{n+2}, \ldots, g_{2n}, v) \in G_1^{(2n+1)} \).
- Choose a secure hash function \( H \), where \( H : G \to Z_q \).
Finally, the TA sends the public parameters \( \{G, G_1, G_T, q, P, g, pk_{TA}, PK, H\} \) to all SMs and vehicles.

### 4.4. Registration Phase

This phase is mainly divided into SMs and vehicles registration. Figure 4 briefly depicts this process. It’s worth noting that this process only needs to be done once. An SM’s registration details are as follows.

1. Computes public key information
   - Assume that \( j \)th SM’s real identity is \( ID_{SM_j} \). It chooses a random integer \( sk_{SM_j} \) as its private key and calculates \( pk_{SM_j} = sk_{SM_j} \cdot P \) as public key. Then sends \( \langle ID_{SM_j}, pk_{SM_j} \rangle \) to TA through a secure channel.

2. \( \langle pk_{root}, chain_{root}, ID_{V_i} \rangle \)
   - TA first checks the availability of \( ID_{SM_j} \) in its database after getting this registration request. If a match is found, TA will reject this registration request. Otherwise, TA computes \( d_j = v^{\alpha_j} \) for \( SM_j \) to decrypt broadcast messages. Then TA stores \( ID_{SM_j} \) and \( pk_{SM_j} \) into its database and returns \( d_j \) to \( SM_j \) through a secure channel.

3. \( \langle S, PWD \rangle \)
   - \( SM_j \) stores \( d_j \) into its database.

4. \( \langle ID_{SM_j}, pk_{SM_j} \rangle \)

5. \( \langle sk_{SM_j}, d_j \rangle \)

The specific operations of a vehicle’s registration are as follows.

- Assume that \( i \)th vehicle’s real identity is \( ID_{V_i} \). \( V_i \) first randomly chooses a private seed to generate the private information (\( sk_{root} \) and \( chain_{root} \)). Then \( V_i \) computes \( pk_{root} = sk_{root} \cdot P \). Finally, \( V_i \) sends \( \langle ID_{V_i}, pk_{root}, chain_{root} \rangle \) to TA via a secure channel.

- When the TA receives this registration request, it first checks whether \( ID_{V_i} \) is valid. If not, the TA will reject this request. Otherwise, the TA issue a password \( PWD \) and a certificate \( S \) for \( pk_{root} \) and \( chain_{root} \), where \( S = \text{Sign}_{sk_{TA}}(pk_{root}||chain_{root}) \). Finally, the TA stores \( \langle ID_{V_i}, pk_{root}, chain_{root} \rangle \) into its repository and returns \( \langle S, PWD \rangle \) to \( V_i \) via a secure channel.

- \( V_i \) save \( \langle S, chain_{root}, sk_{root} \rangle \) into its repository.

### 4.5. Identity Authentication Phase

The main purpose of this phase is to authenticate the identity of vehicles through the corresponding SMs. After verification, SMs will generates corresponding pseudonym and public key pairs for future communications of vehicles. The detailed process is shown in Figure 5. When a registered vehicle \( V_a \) first access VFS, it will executes the following operations to complete the authentication.

Figure 4. Registration phase.

Figure 5. Identity authentication phase.
Sensors 2022, 22, 2299

Figure 5. Identity authentication phase.

- Picks a random integer \( r \in \mathbb{Z}_q^* \) and then computes symmetric encryption (e.g., AES) key \( K = e(g_r, g_1)^r \). Then \( V_a \) sets the header \( Hdr = (C_0, C_1) \in \mathcal{C} \), where \( C_0 = g^r \) and \( C_1 = (v \cdot \prod_{\omega \in \Lambda} g_{n+1-m})^r \).
- Calculate the signature \( \theta = \text{Sign}_{sk_a} (ID_{V_a} || |tst|||pk_{root}||\text{chain}_{root}) \). where \( tst \) is current timestamp and \( ID_{V_a} \) is real identity of \( V_a \).
- Compute the ciphertext \( CT = E_k (\theta || ID_{V_a} || |tst||S||pk_{root}||\text{chain}_{root}) \). Then \( V_a \) sends \( <CT, Hdr, tst> \) to the nearest RSU, let us assume it is RSU\(_m\) and its region manager is SM\(_k\).
- RSU\(_m\) will transmit \( <CT, Hdr, tst> \) to SM\(_k\).
- SM\(_k\) will execute the following operations after receiving \( <CT, Hdr, tst> \) transmitted by RSU\(_m\).
  - Check whether \( tst \) is fresh. SM\(_k\) will reject this message if \( tst \) is not fresh.
  - Compute \( K'_k = e(g_{\omega}, g_{\omega+1-\omega}^{r_0}) \). Then SM\(_k\) executes \( D_{K'_k} (CT) \) to extract \( \theta, S, ID_{V_a}, pk_{root} \), and \( \text{chain}_{root} \).
  - Verify \( \theta \) by using \( pk_{root} \) and verify \( S \) by using TA’s public key. SM\(_k\) will reject this message as long as there is a validation failure. Then SM\(_k\) calculates corresponding pseudonyms and public keys pairs \( <PID_{V_a}, pk_{V_a}> \) for \( V_a \) future communications by excuting public key generation algorithm described in IV-D. Here \( <PID_{V_a}, pk_{V_a}> = \{ (PID_{V_a, 1}, pk_{V_a, 1}), (PID_{V_a, z}, pk_{V_a, z}) \} \), \( z \) is the number of elements in each set. For any \( u \in \{ 1, \ldots, z \} \), \( PID_{V_a, u} = (PID_{V_a, u, 1}, PID_{V_a, u, 2}) \) where \( PID_{V_a, u, 1} = \text{chain}_{V_a} \cdot P \) and \( PID_{V_a, u, 2} = ID_{V_a} \oplus H(\text{chain}_{V_a} \cdot pk_{TA}) \).
  - Send \( <PID_{V_a}, pk_{V_a}> \) to blockchain.

4.6. Consensus Phase

We assume that there are \( n \) SMs in our system, and all of them are trusted. Under the circumstances, SMs acts as commit nodes according to the serial number. As we discussed earlier, SMs will send these related messages to the blockchain each time it completes the derivation of the pseudonyms and public key pairs of the vehicle it certifies. Assume that the time to produce a block is \( \tau \). During this time, SMs briefly store these pseudonyms and public key pairs it receives in their own memory. After \( \tau \) time, the current commit node will publish the relevant information it has stored in memory as a new full block. Any SM, upon receiving a block, deletes the information in its own memory that is duplicated with the block and then performs the next consensus.

4.7. Message Authentication Phase

At this phase, as long as \( V_a \) communication number does not exceed \( Z \), re-authentication is not required regardless of whether \( V_a \) has left SM\(_k\)’s jurisdiction. Figure 6 gives a brief description of this process, and the details are described below.

- Assume the current serial number of \( V_a \) is \( b \), \( V_a \) first initiates a request to the OBU by entering \( PWD \) and \( ID_{V_a} \). OBU will reject the request if it does not match its own stored information, otherwise it goes to the next step.
• OBU calculates the current private key private key \( sk_{Va,b} \) and chain \( VA \) based on private key generation algorithm. Then, calculates the current pseudonym \( PID_{Va,b} = (PID_{Va,1}, PID_{Va,2}) \) where \( PID_{Va,1} = chain_{Va} \cdot P \) and \( PID_{Va,2} = ID_{Va} \oplus H(chain_{Va} \cdot PK_{TA}) \).

• Finally, returns < \( sk_{Va,b}, PID_{Va,b} \) > to \( V_a \).

• Upon receiving the above information, \( V_b \) calculates signature \( \delta = \{\text{Sign}_{sk_{Va,b}}(M || tst || PID_{Va,b}) \} \) and then broadcasts the message \( \{\delta, M, tst, PID_{Va,b} \} \).

• When a receiver wants to verify the message, it first checks whether the timestamp is valid. If valid, search for the corresponding public key \( pk_{Va,b} \) on blockchain according to the pseudonym. The receiver will reject the message if the query fails. Finally, the receiver validates the signature by using \( pk_{Va,b} \). If the authentication succeeds, the message is trusted.

![Figure 6. Message authentication phase.](image)

5. Security Analysis

We examine the security of our proposed VANET system in light of the design goals set out in Section 3. The details are given as follows.

5.1. Correctness

For the proof of the correctness of our proposed scheme, we need to verify \( K'_k = k \) to ensure SM can decrypt the message send by \( V_a \). The details are as follows.

\[
K'_k = \frac{e^{(g, c_1)}}{e^k \cdot \prod_{\omega \in L, \omega \neq k} g^{n+1-\omega+k} c_0} = \frac{e^k \cdot (g, g)}{e^k \cdot (g, g)} = K
\]

5.2. Security Model

We define chosen ciphertext security (CCS) of a broadcast encryption system against a static adversary. Security is defined by following game between an algorithm \( A \) and a challenger. In addition, \( n \) (i.e., the total number of users.) is the input for algorithm \( A \) and the challenger \( C \).

Init. \( A \) generates a set \( L^* \subseteq \{1, \ldots, n \} \) of users that it wishes to assault.

Setup. \( C \) executes \( Setup(n) \) to gain \( PK \) and \( d_1, \ldots, d_n \). Then, sends \( PK \) and all \( d_f \) to \( A \), where \( f \notin L^* \).
Theorem 1. $A$ sends out adaptive decryption queries $q_1, \ldots, q_m$. Here, $(u, L, Hdr)$ is included in all decryption queries where $L \subseteq L^*$ and $u \in U$. Then, $C$ returns $\text{Dec}(PK, L, u, h, Hdr)$ as response.

Challenge. $C$ executes $\text{Enc}(PK, L)$ to generate $(Hdr', K)$ where $Hdr'$ is another header, $K$ is a finite key set and $K \in K$. Then, selects a bit $\psi \in \{0, 1\}$ randomly. Next, sets $K_\psi = K$ and selects a random $K_{1-\psi} \in K$. Finally, returns $(Hdr', K_0, K_1)$ to $A$.

Query phase 2. Adaptively, $A$ send out more decryption queries $q_{m+1}, \ldots, q_{q_D}$, where $q_i = (u, L, Hdr)$ for $L \subseteq L^*$ and $u \in U$. Notice that $Hdr \neq Hdr'$. Then, the $C$ returns same response as phase 1.

Guess. $A$ outputs its $\psi' \in \{0, 1\}$ guess regarding $\psi$. If $\psi = \psi'$ is held, $A$ will win this game.

Here, let $\text{AdvBr}_{A,n}$ represent the probability of $A$ wins the game.

Definition 1. The broadcast encryption is $(t, e, n, q_D)$ chosen ciphertext attack (CCA) secure if for all $t$-time algorithm $A$ make $q_D$ times decryption queries, we have that $|\text{AdvBr}_{A,n} - \frac{1}{2}| < \epsilon$.

Similarly, we define semantic security of the broadcast encryption by preventing the attacker from issuing decryption queries.

Definition 2. The broadcast encryption system is $(t, e, n)$ semantically secure assuming it is $(t, e, n, 0)$ CCA secure.

Definition 3. The $D-(t, e, \zeta)$-BDHE assumption is hold in $G_1$ assuming no $t$-time algorithm has at least $\epsilon$ advantage to tackle the $D-(t, e, \zeta)$-BDHE problem in $G_1$.

5.3. Formal Analysis

Theorem 1. For any positive integers $I$, $n$ ($n > 1$), our $I$-broadcast encryption system is $(t, e, n)$ semantically secure if the $D-(t, e, I)$-BDHE assumption is hold in $G_1$.

Proof of Theorem 1. Assuming $\mathcal{A}$ is a $t$-time adversary, for a given $I$, $\text{AdvBr}_{A,n} > \epsilon$ is hold. Build a new algorithm $B$ that has $\epsilon$ advantage to tackle the $D-I$-BDHE problem in $G_1$. $B$ picks a random $D-I$-BDHE challenge $(g, h, y_{g, a, l}, Z)$ as input, where $y_{g, a, l} = \prod g_{1+i}$ and $Z$ is either $e(g_{1+i}, h)$ or a random member of $G_T$. The following is how $B$ continues.

Init. $B$ executes $\mathcal{A}$ and get $L$ of users that $\mathcal{A}$ wants to assault.

Setup. $B$ is responsible for generating $PK$ and all $d_i$ for $i \notin L$. Let $j = \lceil \frac{q_D}{q} \rceil$. Note that the choice of $v_1, \ldots, v_j$ is the key of the proof.

$B$ picks random $u_i \in Z_2$ for $1 \leq i \leq j$. Here, we define two subsets $\tilde{L}_i$ and $L_i$ as $\tilde{L}_i = L \cap \{(i-1)I + 1, \ldots, iI\}$ and $L_i = \{x - iI + 1 | x \in \tilde{L}_i\} \subseteq \{1, \ldots, I\}$, respectively. For $1 \leq i \leq j$, $B$ makes $v_i = g^{u_i} \left( \prod_{f \in L_i} g_{1+I-f} \right)^{-1}$. Then, $B$ returns the public key $PK$ to $\mathcal{A}$, where $PK = (g, g_{1}, \ldots, g_{I+2}, \ldots, g_{2I})$ and $Z$ is either $e(g_{1+i}, h)$ or a random member of $G_T$. In this case of $B$ continues.

Get $d_i = (g^{u_i} \prod_{f \in L_i} g_{1+I-f}^{-1})^{v_i} = v_i^{(a)}$ as required. Furthermore, we know that $b \notin L_d$ because of $i \notin L$, so $d_i$ does not include the term $g_{1+i}$.

Challenge. $B$ sets $Hdr$ as $(h, h^{u_1}, \ldots, h^{u_j})$. Then, chooes a random bit $\psi \in \{0, 1\}$ and makes $K_\psi = Z$ and randomly selects a $K_{1-\psi} \in G_T$. Finally, returns $(Hdr, K_0, K_1)$ as the challenge to $\mathcal{A}$. We claim $(Hdr, K_0, K_1)$ is a reasonable challenge to $\mathcal{A}$ while $Z = e(g_{1+i}, h)$ (i.e., the input to $B$ is a $B$-BDHE tuple from $P_{BDHE}$ sampling). Moreover, for some (unknown) $t \in Z_q$, we write $h = g^t$. Then, for all $i = 1, \ldots, j$, we have $h^{u_i} = (g^{u_i})^t = (g^t)^{\prod_{f \in L_i} g_{1+I-f}^{-1}} = (\prod_{f \in L_i} g_{1+I-f})^t = (v_i \prod_{f \in L_i} g_{1+I-f})^t$. Here, for key $e(g_{1+i}, g^t)$, $(h, h^{u_1}, \ldots, h^{u_j})$ is a valid encryption. Furthermore, since $e(g_{1+i}, g^t) = e(g_{1+i}, h) = Z = K_{\psi}$, $e(g_{1+i}, g^t)$...
(\(H_{dr, K_0, K_1}\)) is a reasonable challenge to \(A\). In addition, \(K_0, K_1\) are both picked randomly from \(G_T\) while \(Z\) is chosen randomly from \(G_1\) (i.e., the input to \(B\) is a \(\mathcal{B}\)-BDHE tuple from \(\mathcal{P}_{BDHE}\) sampling).

**Guess.** \(A\) outputs \(\psi'\) guess regarding \(\psi\). \(B\) outputs 0 if \(\psi' = \psi\) (i.e., \(Z = e(g^{s_{g_{1+1}}, h})\)). Otherwise, outputs 1 (i.e., \(Z\) is a random element in \(G_T\)). We can find that \(\Pr[\mathcal{B}(g, h, y_{g^{a_{2}}, t}, Z) = 0] = \frac{1}{2}\) if \((g, h, y_{g^{a_{2}, t}}, Z)\) is sampled from \(\mathcal{R}_{BDHE}\). Similarly, \(\Pr[\mathcal{B}(g, h, y_{g^{a_{2}, t}}, Z) = 0] = \frac{1}{2}\) if \((g, h, y_{g^{a_{2}, t}}, Z)\) comes from \(\mathcal{P}_{BDHE}\). Therefore, \(B\) has advantage at least \(\epsilon\) to tackle D-I-BDHE in \(G_1\). So we have proved the Theorem 1.  

### 5.4. Nonformal Analysis

- **Identity authentication:** Because of the security of ECDSA, without TA’s private key, no one can impersonate TA and fabricate a certificate. Therefore, SMs can determine whether the vehicle is a legitimate vehicle as long as it verify the certificate sent by the vehicle with TA’s public key.

- **Message authentication:** According to the security of ECDSA, without signature key, no one can fake a legitimate message. It simply implies that a verifier only needs to compare the received signature message to the appropriate key to verify whether the message is legitimate.

- **Identity privacy preservation:** In **Identity Authentication phase**, Only legal SMs are able to decode the communication and determine a vehicle’s true identification. In **Message Authentication phase**, this real identity will be hidden under a pseudonym, which means no one (besides TA, who has its private key \(sk_{TA}\)) could deduce a vehicle’s true identification from the delivered communications. Therefore, our scheme can satisfy the identity privacy preservation.

- **Unlinkability:** The vehicle produces a new private key and pseudonym each time it transmits a message \(M\), then signs \(M\). Because the pseudonym is linked to the chain code of vehicles, to link two message delivered by the same vehicle, adversary should own the chain code \(chain_{root}\) and \(pk_{root}\) of this vehicle. However, this two information only known by TA and the regional managers. Hence, our proposal can meet the security property requirement of Unlinkability.

- **Traceability:** Note that only TA owns its private key \(sk_{TA}\). Since \(sk_{TA} \cdot ID_{V_{h_1}} = sk_{TA} \cdot chain_{V_{h_2}} \cdot P = chain_{V_{h_2}} \cdot pk_{TA}\), when necessary (e.g., a vehicle sends a message that causes a traffic accident), TA can retrieve the vehicle’s genuine identifying information through \(ID_{V_h} = PID_{V_{h_2}} \oplus H(sk_{TA} \cdot PID_{V_{h_1}})\).

- **Resist various attacks:** Other assaults that our plan can withstand are outlined below.
  - **Replay attack:** Either in the identity authentication phase or in the message authentication phase, the timestamp \(tst\) is included in the messages sent by the vehicle. The repeat of the message could be discovered by SMs and other verifiers by checking the freshness of \(tst\). Therefore, our proposal can resist replay attack effectively.
  - **Impersonation attack:** An attacker must create a valid signature for a message in order to spoof a legitimate vehicle. Based on the above discussion, this is impossible for an attacker and the verifier can easily detect such a malicious attack by validating this signature.
  - **Modification attack:** To alter a message \(M\) to \(M'\), an attacker need to generate a valid signature for message \(M'\). It impossible for the attacker without sender’s private key, and this modified message will be discard by verifiers. As a result, our approach is resistant to modification.
  - **Stolen Verifier Table Attack:** The proposed sc-heme does not require the verifier to maintain a verification table to complete the authentication. It means that the attacker will not be able to steal any verifier tables for nefarious purposes.
5.5. Security Comparisons

We evaluate the security of our proposed approach to three proposed ID-based CPPA schemes [11,14,20] that have been presented.

None of the three previous schemes, according to Table 3, can fulfill all of these security requirements. For Yao [14] and Ali [20], since pseudonym of a vehicle is a constant, they cannot able to realize Unlinkability. In addition, although Lin [11] is able to provide Traceability, TA need to store the relevant public key information for every communication of all vehicles, which is a huge burden for TA. In VANETs, on the other hand, our suggested approach can meet all of these security criteria. On the other hand, TA does not need to maintain any information in order to trace out a vehicle’s genuine identity, which greatly reduces the workload of TA.

Table 3. Security comparisons.

|                      | Yao [14] | Lin [11] | Ali [20] | Ours |
|----------------------|----------|----------|----------|------|
| Identity authentication | ✓        | ✓        | ✓        | ✓    |
| Message authentication | ✓        | ✓        | ✓        | ✓    |
| Identity privacy preservation | ✓     | ✓        | ✓        | ✓    |
| Unlinkability         | ✗        | ✓        | ✗        | ✓    |
| Traceability          | ✓        | ✓        | ✓        | ✓    |
| Resist various attacks | ✓        | ✓        | ✓        | ✓    |

✓: The requirement is satisfy. ✗: The requirement is not satisfy.

6. Performance Analysis

In this section, we looked at the performance of the suggested strategy. Firstly, we analyzed the overhead incurred by the proposed scheme, including computing overhead and communication overhead. Then, compared the performance of the proposed scheme with [11,14,20]. Finally, we simulated the scheme based on NS-3 and proved that our scheme is suitable for VANET environment.

6.1. Computing Overhead

Due to the pre-set of Initialization Phase and Registration Phase and consensus phase is a completely independent process, we only evaluates the overheads of Identity Authentication and Message Authentication phases. The following are various notations for execution time.

- \( T_{bp} \): the time required for a bilinear pairing.
- \( T_{sig-ecc} \): the time required for a signature based on ECC.
- \( T_{ver-ecc} \): the time required for a validation based on ECC.
- \( T_{sm-ecc} \): the time required for a scale multiplication operation based on ECC.
- \( T_{enc-aes} \): the time required for an encryption related to AES.
- \( T_{dec-aes} \): the time required for a decryption related to AES.
- \( T_{pm} \): the time required for a point multiplication operation (i.e., \( g_1 \cdot g_2^{-1} \)), where \( g_1 \) and \( g_2 \in G \) and the inverse of \( g_2 \) is \( g_2^{-1} \).
- \( T_{ex} \): the time required for an exponentiation operation \( g_1^\theta \) where \( g_1 \in G_1 \) and \( \theta \in Z_q \).
- \( T_h \): the time required for a general hash function operation. in \( G \).

To compare the computing overhead with [11,14,20] we measured the execution time of the relevant operations through the Java environment with an Intel (R) Core (TM) i7-8750H CPU 2.20 GHZ and 8 GB RAM. The pairing-based library was used in our simulation and Type A pairings were constructed on the curve \( y^2 = x^3 + x \) over the field \( F_q \) for some primes \( q = 3mod4 \). We performed 1000 times on each operation and ignore the much cheaper operations such as point addition. The average times obtained are shown in Table 4.

To have a better comparison, we separate the communication into two parts to calculate the computing cost, respectively: Vehicle-SM(V2S) communication and Vehicle-
Vehicle(V2V) communication. Since TA completes the calculation of public key for all vehicle communication, V2S communication is no longer required for Lin [11]. Instead, we let SMs to do this job to relieve pressure and burden of TA. Similarly, Ali’s [20] scheme does not require this stage because it uses a fixed public-private key pair.

Table 4. The average time for each algorithm.

| Algorithm | Average Time (ms) |
|-----------|------------------|
| $T_{bp}$  | 4.6003           |
| $T_{sig-ecc}$ | 1.5271           |
| $T_{ver-ecc}$ | 6.5458           |
| $T_{sm-ecc}$ | 0.7088           |
| $T_{enc-aes}$ | 0.0434           |
| $T_{dec-aes}$ | 0.0198           |
| $T_{pm}$  | 0.0118           |
| $T_{ex}$  | 0.6871           |
| $T_{h}$   | 0.0047           |

In V2S communication phase, the vehicle can calculate the relevant information in advance based on the public parameters, such as symmetric key, the header and so on. As a result, at this phase, the vehicle just needs to deliver ciphertext to the nearest RSU. Upon receiving the message, RSU is responsible for forwarding it to its region manager SM. When SM receives the message, it will authenticate the message. Similarly, $PK$ is public information, SM only needs to perform two bilinear pairings and one point multiplication operation to calculate the corresponding symmetric key. Then, perform a symmetric decryption operation to get the certificate. Finally, verify the signature by $pK_{root}$ and verify the certificate by using public key of TA. In a word, the execution time of this step is $2T_{bp} + T_{dec-aes} + T_{pm} + 2T_{ver-ecc} \approx 22.3196$ ms. For the phase of Yao [14], SM need to execute $k + 4$ point multiplication operations which is tied to the $k$ SMs, and perform three hash operations. Therefore, the execution time is $(k + 4)T_{sm-ecc} + 3T_{h} \approx (0.7088k + 0.0141)$ ms.

For the V2V communication phase of our proposed scheme, vehicle can calculate the subsequent keys and pseudonyms according to key derivation algorithm in advance. Vehicle sign a message by a new private key and send to nearby RSUs or vehicles. Then RSU will forward this message to SM if this message is a request to access the VFC. Otherwise, adjacent vehicles will verify the message. The verifier(an SM or vehicle) retrieve the corresponding public key by pseudonym and then verify the message. Therefore, the execution time of this step is $T_{sig-ecc} + T_{ver-ecc} \approx 11.1461$ ms. On the other side, the execution flow of Yao [14] and Lin [11] are the same as us, so the execution time are also 11.1461 ms. However, for Ali [20], it need to perform two bilinear pairings, three scale multiplication operations, four hash function operations and one exponentiation during this whole process. So the execution time is $2T_{bp} + 3T_{sm-ecc} + T_{ex} + 4T_{h} = 12.0269$ ms.

To compare the computational overhead of the three schemes more clearly, the execution time of four schemes in V2S communication phase and V2V communication phases are shown in Table 5. In V2S communication phase, the execution time of our scheme is a constant value. However, in Yao [14], this time will increase with the increasing of $k$ (i.e., the number of SMs). Once $k$ exceed 32, Yao [14] execution time will beyond ours. In practice, the number of SMs is much bigger than 32. In addition, the execution time during the V2V communication phase is the same for Lin [11], Yao [14] and our scenarios. However, for Ali [20], because of the complicated bilinear pairing process involved in verification phase, the whole communication cost is also the largest among the four schemes. The proposed scheme was reduced about 7% compared with Ali [20]. From the above comparison, our scheme has good efficiency in both stages.
Table 5. Comparison of computing cost.

| V2S Communication | V2V Communication |
|--------------------|--------------------|
| Yao’s scheme [14]  | $T_{\text{sig-ecc}} + T_{\text{ver-ecc}} \approx 11.1461 \text{ ms}$ |
| Lin’s scheme [11]  | $T_{\text{sig-ecc}} + T_{\text{ver-ecc}} \approx 11.1461 \text{ ms}$ |
| Ali’s scheme [20]  | $2T_{\text{bp}} + 3T_{\text{sm-ecc}} + 1T_{\text{ex}} + 4T_{\text{h}} = 12.0269 \text{ ms}$ |
| Our scheme         | $T_{\text{sig-ecc}} + T_{\text{ver-ecc}} \approx 11.1461 \text{ ms}$ |

6.2. Communication Overhead

We primarily study and compare the communication overhead of our method with three other techniques (i.e., [11,14,20]) in this paragraph. Since Identity Authentication phase only needs to be performed once in our scheme, we only consider the communication overhead associated with Message Authentication phase. Furthermore, because $p$ and $p$ have sizes of 64 bytes (512 bits) and 20 bytes (160 bits), the elements in $G_1$ and $G$ have sizes of $64 \times 2 = 128$ bytes and $20 \times 2 = 40$ bytes, respectively.

In each V2V or V2S communication, take the $b$th communication of $V_b$ for example, it will broadcast $\delta = \{\text{Sign}_{sk_{V_b}}(M|\text{tst}|\text{PID}_{V_{sb}}), M, \text{tst}, \text{PID}_{V_{sb}}\}$ is an ECDSA signature (i.e., 64 bytes), $M$ is a message (where we set as 32 bytes), $\text{tst}$ is current timestamp (where we set as 4 bytes) and $\text{PID}_{V_{sb}} = (\text{PID}_{V_{sb,1}}, \text{PID}_{V_{sb,2}})$. As a consequence, the presented solution is $= 64 + 32 + 4 + 2 \times 40 = 180$ bytes.

For the same step in Yao [14], $\{\text{Sign}_{sk_{V_b}}(\text{PID}_{V_b}, M, \text{tst}), \text{PID}_{V_b}, M, \text{tst}\}$ will be transmitted by $V_b$, where $\text{PID}_{V_b}$ is a random pick in $Z_q$ (i.e., 20 bytes) that represents its pseudonym. Therefore, the communication overhead is 120 bytes.

In Lin [11], the sender needs to get the transaction identity ($\text{TxID}$, i.e., 32 bytes) from the smart contract by the corresponding $pk_{V_b}$ first. Then, $\{\text{Sign}_{sk_{V_b}}(M, \text{tst}, \text{TxID}), M, \text{tst}, \text{TxID}\}$ will be transmitted. Here, $|pk|$ is a element of $G$ (i.e., 40 bytes). Therefore, the communication cost of Lin [11] is 304 bytes.

Similarly, in the Ali’s scheme [20], the vehicle broadcasts $(\text{PID}_a, \text{pdb}, S_a, \text{tst})$ where $\text{PID}_a = (\text{PID}_{a,1}, \text{PID}_{a,2}), \text{pdb} = M \oplus h(\theta_s \text{pk}_a)$ and $S_a = \theta_s \text{pk}_a$. Since $\text{PID}_{a,1}, \text{PID}_{a,2}, S_a \in G$, the length of $S_a$ is 64 bytes (i.e., suppose the SHA-512 is used), the total communication cost is 188 bytes.

The comparison results are shown in Table 6. It is not difficult to see that the communication overhead of our scheme is lower than that of Lin [11] and Ali [20]. The communication cost reduces 41% compared with Lin [11] and reduces 4% compared with Ali [20]. Furthermore, even though communication overhead of our scheme is higher than Yao [14], this expense is acceptable because our strategy includes a bonus function (Unlinkability). Therefore, we believe that our solution is more suitable for VANETs in this respect.

Table 6. Comparison of communication cost.

| Communication Cost (bytes) |
|---------------------------|
| Yao’s scheme [14]         | 120            |
| Lin’s scheme [11]         | 304            |
| Ali’s scheme [20]         | 188            |
| Our scheme                | 180            |

6.3. Message Authentication Delay and Packet Loss Rate

We also perform a simulation by using NS-3 in a personal computer (Lenovo with Intel Core i7-10875H 2.30 GHz, 16 GB RAM and Ubuntu 20.04 OS) to measure the average message authentication delay and average packet message loss rate. Figure 7 shows a map with 0.5 x 0.5 km² which we adopt in our simulation scenario. The block is maintained by an SM and the interval of broadcast messages is 100 ms. In addition, the packet size in our
simulation is 288 bytes. Other parameters like Channel, Propagation, Phy and Mac are set as WirelessChannel, TwoRayGround, WirelessPhy and 802.11, respectively. The simulation time in each simulation are set as 100 s.

![Map with dimensions](image)

Figure 7. The map with $0.5 \times 0.5$ km$^2$.

Here, we increased the number of vehicles from 5 to 30 and increased the speed of the cars from 7.5 to 40 m/s. The final results are shown in Figure 8. From Figure 8, we can observe that the average packet loss rate is essentially unchanged and until the number of vehicles increases to 30, it increases a little. On the other hand, the average delay increases as the number of vehicles increases. This could be owing to an increase in the number of vehicles on the road, which would result in an increase in the number of broadcast messages, eventually making an increase in average delay. However, this value is still within our acceptable range.

![Graph](image)

Figure 8. The impact of density in delay and packet loss ratio.
7. Conclusions

With the serious traffic congestion and frequent accidents in real life, VANETs is expected to relieve traffic pressure, for example, changing driving route or reasonable change of traffic lights by the control center through traffic information sent by nearby vehicles. Hence, in this paper, we proposed a hierarchical blockchain-assisted CPPA scheme for VANETs with following advantages: (i) Adopted distributed VFC to reduce the delay effectively in theory. (ii) Attacker unable to link two messages transmitted by same vehicle because the vehicle uses different public key and pseudonym everytime it broadcasts a message. (iii) The proposed scheme has better performance in computing and communication than the previous scheme, which is shown by simulation experiments. The findings reveal that the proposed scheme is available. In the future, how to adopt a more efficient algorithm to design the authentication scheme, whether there is a better way to replace the offline registration of vehicles, will be our focus to improve the efficiency of authentication.

Author Contributions: Formal analysis, X.H., X.N., Y.W., L.X. and Z.J.; methodology, X.H.; project administration, X.H.; writing-review & editing, X.H.; funding acquisition, X.N.; software, Y.W.; validation, L.X.; data curation, C.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The work of this paper was supported by the National Science Foundation of China (No. 62171387), the China Postdoctoral Science Foundation (No. 2019M663475), the Spring Plan of the Ministry of Education of China in 2018 (No. 191629), Science and Technology Fund of Sichuan Province (No. 2020JDBC029), Xihua Cup Innovation and Entrepreneurship Foundation (Grant No. 2021054), and the Key Projects of Xihua University (No. Z202001)

Conflicts of Interest: We wish to confirm that there are no conflict of interest associated with the submission of this manuscript and we confirm that this manuscript has been read and approved by all named authors. We further confirm that we have given due consideration to the protection of intellectual property associated with this work and that there are no impediments to publication, including the timing of publication, with respect to intellectual property. In so doing we confirm that we have followed the regulations of our institutions concerning intellectual property.

References

1. Zeadally, S.; Hunt, R.; Chen,Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (vanets): Status, results, and challenges. *Telecommun. Syst.* 2012, 50, 217–241.
2. Toor, Y.; Muhlethaler, P.; Laouiti, A.; La, A. Vehicle ad hoc networks: Applications and related technical issues. *IEEE Commun. Surv. Tutor.* 2008, 10, 74–88. [CrossRef]
3. Mejri, M.N.; Ben-Othma, J.; Hamdi, M. Survey on vanet security challenges and possible cryptographic solutions. *Veh. Commun.* 2014, 1, 53–66.
4. Raya, M.; Papadimitratos, P.; Hubaux, J.P. Securing vehicular communications. *IEEE Wirel. Commun.* 2006, 13, 8–15. [CrossRef]
5. Isaac, J.T.; Zeadally, S.; Camara, J.S. Security attacks and solutions for vehicular ad hoc networks. *IET Commun.* 2010, 4, 894–903. [CrossRef]
6. Hubaux, J.P.; Capkun, S.; Luo, J. The security and privacy of smart vehicles. *IEEE Secur. Priv.* 2004, 2, 49–55. [CrossRef]
7. Lu, Z.; Qu, G.; Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. 2018, 20, 760–776. [CrossRef]
8. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* 2015, 10, 2681–2691. [CrossRef]
9. Zhang, C.; Lin, X.; Lu, R.; Ho, P.H. RAISE: An efficient rsu-aided message authentication scheme in vehicular communication networks. In Proceedings of the IEEE International Conference on Communications, Beijing, China, 19–23 May 2008.
10. Zhang, J.; Xu, M.; Liu, L. On the security of a secure batch verification with group testing for vanet. *Int. J. Netw. Secur.* 2014, 16, 355–362.
11. Lin, C.; He, D.; Huang, X.; Kumar, N.; Choo, K.-K.R. BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. *IEEE Trans. Intell. Transp.* 2020, 22, 7408–7420. [CrossRef]
12. Shojafar, M.; Cordeschi, N.; Baccarelli, E. Energy-efficient adaptive resource management for real-time vehicular cloud services. *IEEE Trans. Cloud Comput.* 2019, 7, 196–209. [CrossRef]
13. Hou, X.; Li, Y.; Chen, C.; Wu, D.; Jin, D.; Chen, S. Vehicular fog computing: A viewpoint of vehicles as the infrastructures. *IEEE Trans. Veh. Technol.* **2016**, *65*, 3860–3873. [CrossRef]

14. Yao, Y.; Chang, X.; Misc, J.; Misc, V.B.; Li, L. BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. *IEEE Internet Things J.* **2019**, *6*, 3775–3784. [CrossRef]

15. Kaur, K.; Garg, S.; Kaddoum, G.; Gagnon, F.; Ahmed, S.H. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 22–24 May 2019.

16. Picconi, F.; Ravi, N.; Gruteser, M.; Iftode, L. Probabilistic validation of aggregated data in vehicular ad hoc networks. In Proceedings of the Third International Workshop on Vehicular Ad Hoc Networks, VANET 2006, Los Angeles, CA, USA, 29 September 2007.

17. Zhang, Y.; Wen, J. The iot electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 983–994. [CrossRef]

18. Zhong, H.; Wen, J.; Cui, J.; Zhang, S. Efficient Conditional Privacy-Preserving and Authentication Scheme for Secure Service Provision in Vanet. *Tsinghua Sci. Technol.* **2016**, *21*, 620–629. [CrossRef]

19. Wang, P.; Liu, Y. SEMA: Secure and Efficient Message Authentication Protocol for VANETs. *IEEE Syst. J.* **2021**, *15*, 846–855. [CrossRef]

20. Ali, I.; Lawrence, T.; Omala, A.A.; Li, F. An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in vanets. *IEEE Trans. Veh. Technol.* **2020**, *11266–11280*. [CrossRef]

21. Wang, C.; Shen, J.; Lai, J.; Liu, J. B-TSCA: Blockchain Assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1386–1396. [CrossRef]

22. Lu, Z.; Wang, Q.; Qu, G.; Zhang, H.; Liu, Z. A blockchain-based privacy-preserving authentication scheme for vanets. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2019**, *27*, 2792–2801. [CrossRef]

23. Boneh, D.; Gentry, C.; Waters, B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Proceedings of the Advances in Cryptology—CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2005.

24. Boukerche, A.; Oliveira, H.A.B.F.; Nakamura, E.F.; Loureiro, A.A.F. Vehicular ad hoc networks: A new challenge for localization-based systems. *Comput. Commun.* **2008**, *31*, 2838–2849. [CrossRef]