Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 3013562, 11 pages
https://doi.org/10.1155/2019/3013562

Research Article

IOV Privacy Protection System Based on Double-Layered Chains

Yin Ru Chen, Jin Rui Sha, and Zhi Hong Zhou

Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China

Correspondence should be addressed to Zhi Hong Zhou; zhouzhihong@sjtu.edu.cn

Received 24 August 2018; Revised 26 November 2018; Accepted 23 January 2019; Published 7 March 2019

Academic Editor: Daojing He

Copyright © 2019 Yin Ru Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As the Internet of Vehicle (IOV) being widely applied throughout our daily life, how to secure data privacy of each vehicle is nowadays a hot topic. Taking an aim of solving this problem, a privacy protection system on double-layered chain basis is designed to eliminate the said security risk during vehicle data communication. At the same time, the nontampering nature of the block chain is used to realize reasonable arbitration in traffic accident disputes, vehicle insurance claims, and other states of affairs. Specifically, an IOV double-layered chain model is constructed to simulate a semicentralized system that is convenient for government to supervise; also, a RSA protocol based on zero-knowledge proof (ZKP) is designed to bring safety and zero-knowledge property to the system; finally, we give the application scenario of this IOV privacy protection system based on double-layered chain that it can be widely used in vehicle-sharing industry. The communication costs, respectively, under double-layered chain and single-layered chain frameworks, are compared to prove that the double-layered structure does save cost. Thus an IOV privacy scheme that is safer and more cost-efficient is given.

1. Introduction

With the rapid development of science and technology, vehicles have been used at a large scale in the modern society. But meanwhile, the development is accompanied with frequent occurrence of traffic accidents. In recent years, Internet of Vehicles (IOV) has been proposed to better avoid potential traffic problems, realizing the mutual communication between car-and-car and car-and-infrastructure units [1, 2].

Nowadays, the Internet of Vehicles uses wireless communication, which may cause problems like data surveillance, while data uploaded by vehicles includes the positions of users and driving routes among other information. In modern society, we do not wish to let vicious parties obtain our private data through plain texts, but the information shall be regulated by traffic command center. Therefore how to design conditional privacy protection for data is our top priority currently.

Traditional models for data protection and central supervision are mostly based on PKI system and cloud [3, 4]. However, the cloud assumed in the above model is credible, and this premise may not be true in real life. The cloud can conspire with a certain participant to tamper with the data, thus getting rid of accident liability or demanding more economic compensation in traffic accident disputes and other situations. In order to solve this problem, we consider making use of the nontampering nature of the block chain to ensure the authenticity of the data in traffic accident disputes, vehicle insurance claims, and other situations requiring arbitration.

On the basis of the above goal, our paper has proposed IOV privacy protection system based on double-layered chains. Encrypting real-time road privacy data ensures the privacy and completeness of data; making use of the double-layered chain structure of Internet of Vehicles that is semicentralized will facilitate the regulation of the government or authoritative organizations while reducing the expenditure of channel resources of the system. Meanwhile, we formulate the RSA digital signature agreement based on zero-knowledge proof. It prevents roadside unit from obtaining any information from signature and establishes the private data protection system for the automatic double-layered chain vehicle network. Moreover, it also increases the data credibility in traditional models, reduces the excessively channel resource consumption in vehicle network, and prohibits opponents from forging RSU to obtain information.

2. Related Works

As for the issue of data privacy protection in Internet of Vehicles, a lot of academic research and studies have been conducted in recent years. When it comes to privacy protection of vehicle identities, anonymous authentication is a feasible approach. Brickell proposed the zero-knowledge proof method for verifying identities [5]. Breg and his team proved that it is likely to reduce the number of unique vehicle certificates by sharing certificates among adjacent vehicles [6]. But the above scenarios only provide identity authentication. They fail to reveal the identity of the anonymous to meet real-life private conditions. For example, to find out who is responsible for traffic accidents, the traffic control center has the right to reveal the true identities.

Currently, in order to solve this issue, most solutions are conducted based on group signature and ring signature. Boneh conducted researches on effective group signature in the earlier years [7]. Lin proposed the vehicle communication protocol based on group signature [8]. Hu et al. introduces an efficient privacy-preserving protocol with confidentiality for vehicular ad hoc networks based on group signcryption [9]. Within the framework of group signature protocol, vehicles only need to retain secret keys and public group keys, thereby avoiding the leakage of identify information. However, when the number of nodes in the undo list increases linearly, the time also increases linearly with the number of nodes, which means the method of group signature consumes an excessive amount of time. For solving this problem, the academic community also came up with some solutions. However, the solutions were based upon the improvement of tamper-proofing hardware and devices, which means that if the enemies attacked the hardware [10, 11], system security would also be compromised. So the ring signature was proposed [12, 13]. Xiong and his team put forward the revocable ring signature technology and privacy protection protocol for Internet of Vehicles [14]. But this solution requires that the identification of traffic management agencies should be truthful. As for this problem, Zeng put forward the conditional anonymous ring authentication solution (CARS) for Internet of Vehicles, which reduced the reliance on traffic management agencies [15]. But the protocol is rather complicated to be widely applied. On the basis of bilinear mapping design, Liu came up with session keys for authentication in complex communication. This authentication protocol aims to optimize traffic load and reduce interactive sections. Wu designed a solution self-healing secret key allocation solution. It adds information verification codes to broadcast message and ensure the security and broadcasting authentication of group keys. Hence, the sliding window mechanism retrieves the lost session keys and reduces communication overhead for subgroups and communication among groups in Internet of Vehicles. In recent years, Hu et al. give an efficient and multilevel conditional privacy preservation authentication protocol in vehicular ad hoc networks (VANETs) based on ring signature [16]. And he introduces an efficient and trustworthy conditional privacy-preserving communication protocol for VANETs based on proxy resignature [17]. He also proposes a remote authentication protocol featured with nonrepudiation, client anonymity, key escrow resistance, and revocability for extra-body communication in the WBANs [18].

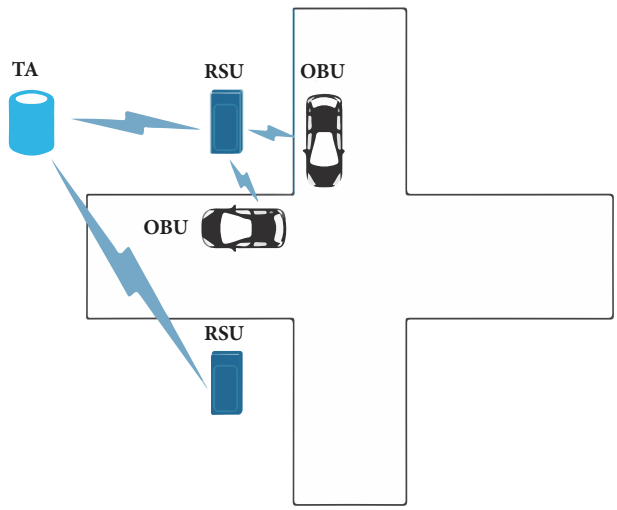


Figure 1: Network model of IOV.

However, most data of the above solutions are constructed based on cloud. Regardless of cloud servers for data storage by the authentication center (TA) or roadside unit (RSU), the cloud service providers are assumed to be reliable. But in real life, this assumption may not be valid because cloud servers and certain users may formulate conspiracy. For the above issues, Chen et al. introduce a light-weight and anonymous aggregation protocol based on fog computing-based V2I communication scenario [19]; this paper proposes the IOV privacy protection system based on blockchain design and solves the problem with its ability of anticollusion. With the help of double-layer technology in RScoin, we have designed a RSA digital signature scheme based on zero-knowledge proof. We simulate the double-layer certification systems for the authentication center (TA), roadside unit (RSU), and on-board unit (OBU). Besides, trace ability and nonrepudiation of blockchain also make it possible for conditional privacy

3. Model and Protocol Design

In this chapter, firstly, we introduce the components of traditional car networking model, propose the double-chain model, and consensus protocol. At the end of this chapter, we put forward the double-chain car networking model, and implement the RSA digital signature agreement based on zero-knowledge proof, thereby living up to the security and zero-knowledge of the system.

3.1. Internet of Vehicles Model. Internet of Vehicles is mainly made up of the three parts of Trusted Authority (TA), roadside unit (RSU), and on-board unit (OBU). The model of the Internet is shown in Figure 1 [20].

(i) Trusted Authority: TA is the center of trusted security of Internet of Vehicles. Also, it is the most

authoritative organization. In real life, it can be traffic command center among other organizations. TA has many authorities, including registering or revocating OBU and RUS in Internet of Vehicles, generation of public and private key pairs of OBU and RUS, keeping the identity of OBU and RSU, corresponding relationship with public keys, and so on.

(ii) Road side unit: RSU is an infrastructure deployed on the roadside, as the transfer of information dissemination, which is, however, easy to be attacked. Therefore, while transmitting information to RSU, we should try to reduce trust towards RSU as much as possible. In order to ensure safety, during each communication between RSU and TA, certificates should be issued and TA should conduct identity certification.

(iii) On-board unit: OBU is a piece of equipment installed on vehicles to prevent distortion and communicating with roadside and other vehicles in wireless form. OBU can store passwords and carry out encryption and decryption operations. In the driving process of vehicle, it can announce security information periodically, including position, time, speed, direction, traffic events, etc.

3.2. Double-Layered Chain Model. The double-layered chain model originates from the RScoin model, which was proposed by Bank of England in 2015 [21]. RScoin is the model of crypto currency. This coin is supplied and controlled by the central bank, in order to avoid the issue of "double payment".

In essence, the double-layered chain model of RScoin is similar to blockchain, but it is also different from the traditional model of blockchain in some respects. In traditional blockchain, every node is coped after broadcasting. Byzantine Agreement is used to maintain consistency. But RScoin is a centralized chain system, which uses one central node for maintain all the data. The mintette node only maintains part of the data. Compared with traditional blockchain model, the double-layered chain model has the following advantages:

(1) Favorable expand ability: with the number of agencies authorized by the central bank increasing, the whole system is able to handle more transactions.

(2) Controllability of currency issuance: the system separates money supply from account books. The central bank regulates the currency issuance. Account books are maintained by mintette and central bank. Mintette maintains some subaccount books, and the central bank maintains the general account books.

(3) Universality: different banks can utilize the RScoin platform to release digital coins.

3.2.1. Overall Framework of Double-Layered Chain. In this section, we still take RScoin as the example for the overall framework of double-layered chain. RScoin participants include three parties: central bank, mintette, and users. Mintette represents commercial institutions authorized by the central bank to collect and verify user transactions. It adopts two stages of agreement to verify transaction information. The first stage is voting: mintette verifies transaction and sends the information back to users. The second stage is submitting: user transactions are handled by mintette. Transaction information is stored in low-level block. The low-level block only includes the original information, which does not form the complete chain structures.

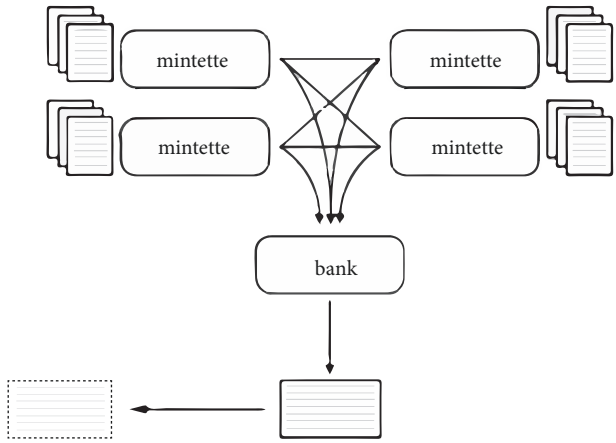


Figure 2: Two-layered chain architecture diagram.

Mintette conducts digital signature in every low-level block. After a period of time, contents of low-level blocks are sent to the central bank. After the central bank verifies the validity of low-level blocks, they are united to higher-level blocks. Moreover, higher-level blocks are integrated to the main chain, becoming a section in the block chain of central bank. The specific structures are shown in Figure 2

According to the above sections, in the overall structures of double-layered chain, higher-level blocks and low-level blocks have their own functions. Higher-level blocks are in control of block issuance, node authorization, examination, and stimulation, as well as maintenance of account books. Low-level blocks are maintained by nodes, in order to handle user transactions, verify validity, record transactions, and update scripts. In particular, in comparison with other digital currencies, the biggest difference is that different nodes do not require transaction synchronization. In other words, each node has its own chains. The chains also include information of other nodes for cross validation, thus reducing the communication load.

3.2.2. The Consensus Algorithm of Double-Layered Chain. Two-step consensus protocol is adopted for the consensus algorithm of double-layered chain. We divide the consensus into two steps. Before that, we provide the symbol and definition of RScoin first, as shown in Table 1.

The first step in consensus protocol is between users and nodes, users initiate a transaction and find out all the owner of the output address corresponding to UTXO in this transaction through allocation index (centralized service), different addresses correspond to different owners, allocation index is a centralized service, it helps users find out the owners corresponding to different addresses quickly, and owners examine the transactions delivered by users,

Table 1: RScoin symbols and definitions.

addr	the address and the corresponding account number
addrid	an output associated with an address, which consists of the hash(tx) of the transaction, the index(I) of the output address, and the value(v) of the transaction
UTXO_list	all of the unspent output
txset_list	record transactions on the account books
pset_list	UTXO that has been linked to transactions for some time but has not been credited

including the legality of transactions, whether addresses are managed by them and whether the UTXO corresponding to the address have double connection.

In the second step of consensus protocol, whether the address is managed by owners of collection address should be confirmed, and then whether all the output has been confirmed by the majority of owners and whether the signature is correct should be examined. If the examination is passed, the owners add them to their UUXO list (becoming new UTXO) and add the transaction to TXSET list. Owners then notify users to add transactions to advanced blocks (if they are not added, users will call owners to account, taking this as the evidence). After a while, all the owners send TXSET list to central bank for merging.

3.3. Double-Layered Chain Model for Internet of Vehicles. Based on traditional model for Internet of Vehicles, we conduct design improvement on the basis of double-layered chain structure in RScoin and propose the double-layered chain model for Internet of Vehicles. Meanwhile, symmetrical encryption is adopted for data, and asymmetric encryption is utilized for secret keys, thereby reducing the excessive communication loads of traditional Internet of Vehicles.

3.3.1. Overall Frame of Internet of Vehicles of Double-Layered Chains. In the model of Internet of Vehicles of double-layered chains, the chain is still made up of three parts, including owner, mintette node, and central node, owner represents OBU in Internet of Vehicles, after vehicles have been issued root certificates by the central node of Trusted Authority, and real-time data on the road (position, time, speed, road information, etc.) will be symmetrically encrypted; while encrypting, OBU will make use of keys generated by random number generator and encrypt the symmetric key to public key publicized by Trusted Authority. Meanwhile, RSA digital signature plans on the basis of zero-knowledge proof will be made use of in encrypting, there will be signatures on encrypted data, and in the end, the encrypted data and signature will be sent to corresponding mintette nodes, or the RSU that is closest to the vehicle on the road.

RSU certifies the signature sent by OBU. As the signed protocol is zero-knowledge proof, RSU can only be informed whether the signature is sent by OBU, but it cannot obtain any information, further ensuring that minimal trust can be obtained by RSU. If the certification is passed, then the encrypted data will be signed with private keys in the same way. Then we will pack the encrypted real-time data of OBU and signature of OBU and RSU every once in a while and send them to TA. On the contrary, if the certification is not passed, the data will be thrown away.

TA certifies the signature of OBU and RSU. If all of the certification is passed, hash the data, and merge them on advanced blocks. If not, drop the data. The specific network model is shown in Figure 3.

3.3.2. The Consensus Algorithm for Double-Layer Chain Networking. In our model, our team ameliorated the two-step consensus algorithm based on the double-layered chain; thus we obtained the two-step consensus algorithm for the Internet of on-boards. For the traffic command center, we can consider it credible. All other nodes are authorized and known in the traffic command center. Under this assumption, the security requirements for the overall security of the system can be relatively reduced, and the design is more biased towards performance considerations. The concrete consensus algorithm is implemented in two steps.

The first step is between the on-board unit (OBU) and the roadside unit (RSU). At the time of registration, the on-board unit (OBU) finds the corresponding TA node in the traffic command center through the address index, and the different addresses correspond to different TA nodes. Address index is a central service, which is convenient for on-board nodes to quickly find the corresponding central nodes. The center node will check the application submitted by the on-board node, including the legality of the application and whether the address is managed by the application.

In the second step, the central node verifies that the on-board unit belongs to its management and then checks whether the authentication is correct by most nodes. If the check can be passed, the on-board unit is added to the corresponding list of the traffic command center, and the center node returns the certificate and private key of the on-board unit to its authenticated certificate. After that, the on-board unit can encrypt its message symmetrically and send it to the roadside node together with the symmetric encryption key and the signature and authentication certificate encrypted by TA public key. After a period of time, the roadside unit sends all the encrypted information to the traffic command center, which is processed by hash and merged into the advanced block.

3.4. RSA Digital Signature Scheme Based on Zero-Knowledge Proof (ZKP). As the prover, on-board unit (OBU) owns parameter n and public key e and private key d generated by test authority (TA), Remote Subscriber Unit (RSU), the verifier, owns parameter n, and public key e.

OBU firstly gives digital signature on message m using the RSA signature algorithm, obtaining signature s; and then a zero-knowledge proof (ZKP) is given for the signature s, so that the RSU believes that the prover P has the signature s for the information m, but it cannot get any useful information about s from the protocol. Therefore, the protocol is with zero-knowledge. According to the following

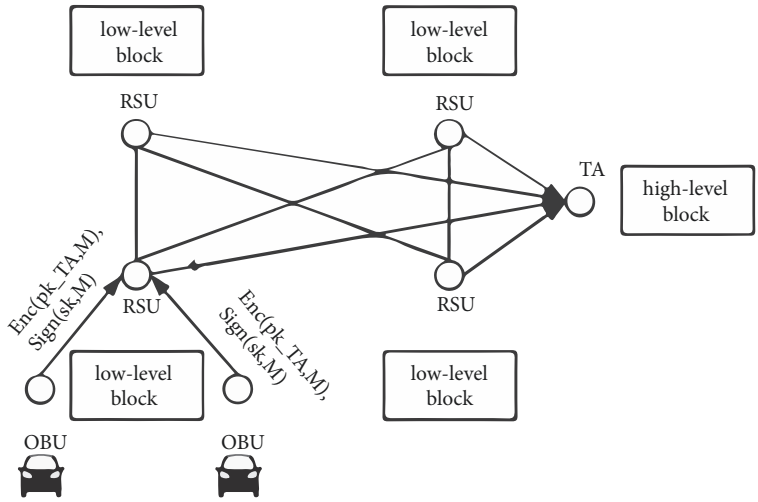


Figure 3: Network model of double-layered chain IOV.

INPUT: $m, r_1, r_2, ..., r_l, n, e, d$
OUTPUT: *result*
1: **function**
2: $s = [H(m)]^d \bmod n$
3: **if** c[i]=0 **then**
4: $s_i = r_i \bmod n$, $p_i = s_i^e \bmod n$
5: **else**
6: $s_i = \frac{r_i}{s} \bmod n$, $p_i = H(m) s_i^e \bmod n$
7: **end if**
8: $c, P_{id}, timestamp, N\ once, s_1, \cdots, s_l \longleftarrow OBU$
9: **if** $c = H(m|n|e|P_{id}|timestamp|N\ once|p_1|p_2|...|p_n)$ **then**
10: **return** *true*
11: **else**
12: **return** *false*
13: **end if**
14: **end function**

Algorithm 1: RSA digital signature scheme based on ZKP.

steps, we made Algorithms 1. Firstly, we define the following parameters:

$$s_i = \begin{cases} r_i \bmod n & c[i] = 0 \\ \frac{r_i}{s} \bmod n & c[i] \neq 0 \end{cases}$$
$$p_i = \begin{cases} s_i^e \bmod n & c[i] = 0 \\ H(m)\, s_i^e \bmod n & c[i] \neq 0 \end{cases} \quad (1)$$

Step 1. Generate the signature $s = [H(m)]^d \bmod n$ of message m by using the RSA algorithm, where $H(m)$ is the binary string at the length of l, obtained after hashing the message.

Step 2. OBU choose a random number r_1,r_2,...,r_l and secretly calculate the $c = H(m|n|e|P_{id}|timestamp\ |N\ once\ |p_1\ |p_2\ |\cdots|p_n)$, where $P_{id}$is the identity mark of OBU, and timestamp is the time stamp of conducting ZKP, and Nonce is the random number chosen for withstanding message replaying.

Step 3. OBU sends ZKP message group c, P_{id}, *timestamp*, *N once*, s_1,..., s_l to RSU.

Step 4. RSU verifies if the equation $c = H(\ m|\ n\ |e\ |P_{id}\ |timestamp\ |N\ once\ |p_1\ |p_2|\ \cdots|p_n)$ can be established.

Step 5. If the equation was established, RSU accepts the proof of OBU; if not, RSU rejects.

4. System Design

In this chapter, we will provide the specific realization of privacy protection of real-time data of vehicles in the system and analyze the corresponding security. The plan will be

INPUT: ID_A
OUTPUT: $cert_A, sk_A$
1: **function**
2: $ID_A \longleftarrow$
3: **if** $ID_A istrue$ **then**
4: $cert_A, sk_A \longleftarrow A$
5: $(A, pk_A) \longleftarrow database$
6: **else**
7: **return** *error*
8: **end if**
9: **end function**

Algorithm 2: OBU identity registration.

INPUT: ID_B
OUTPUT: $cert_B, sk_B$
1: **function**
2: $ID_B \longleftarrow$
3: **if** ID_B is valid **then**
4: $cert_B, sk_B \longleftarrow B$
5: $(B, pk_B) \longleftarrow database$
6: **else**
7: **return** *error*
8: **end if**
9: **end function**

Algorithm 3: RSU identity registration.

divided into four stages: system setting, identity registration, identity revocation, and information transmission.

4.1. System Setting. TA publishes its own public key: pk_{TA} on chains: the corresponding private key sk_{TA} will be stored in the system. The function of the private key is to decode the encrypted data with private key when certification center wants to obtain the data of vehicles on a certain section. For example, in traffic accidents, there can be reasonable arbitration through transferring the data of the vehicle at the time when accidents happen. Meanwhile, TA will also store the ID and corresponding public key of each OBU that has been successfully registered and each RSU.

4.2. Identity Registration. Before OBU and RSU join Internet of Vehicles, they need to register through TA; here, TAs function is similar to CA, and it is capable of issuing certificates to OBU and RSU. Therefore, the identity registration here includes the identity registration of OBU and RSU.

About OBU registration, TA examines the identity information of users, when the information is examined and verified, certificates will be issued, and registration will be permitted. TA binds vehicles and public keys through one-to-one mapping, upload information to database; meanwhile, write the certificates that have been issued the information of public keys in vehicles system of preventing distortion. According to the following principle, we made Algorithms 2.

(i) Vehicle A submits identity authentication ID_A to the Vehicle Network Certification Center or the test authority (TA).

(ii) TA verifies the ID_A submitted by vehicle A. If the verification failed, no more registration would be allowed or accepted.

(iii) Public and private keys that are corresponding to the OBU are generated by RSA algorithm, and the public key is written on the certificate. After that, the certificate and the private key are saved to the Defacement System of OBU.

(iv) The pairing map of the vehicle A and its public key, namely, (A, pk_A), is saved in the database of TA.

INPUT: $(M, IDSign(M, ID, sk))$
OUTPUT: true or false
1: **function**
2: $(M, IDSign(M, ID, sk)) \longleftarrow$
3: **if** $Sign(M, ID, sk)$ is valid **then**
4: $pk \longleftarrow RL$
5: **return** *true*
6: **else**
7: **return** *false*
8: **end if**
9: **end function**

Algorithm 4: Identity revocation.

RSU registration is similar to OBU registration. According to the following principles, we made Algorithms 3:

(i) RSU B submits identification ID_B to TA.

(ii) TA verifies the ID_B submitted by RSU B. If the verification failed, no more registration would be allowed or accepted.

(iii) Public and private keys that are corresponding to the RSU are generated by RSA algorithm, and the public key is written on the certificate. After that, the certificate and the private key are saved to the Defacement System of RSU.

(iv) The pairing map of the RSU B and its public key, namely, (B, pk_B), is saved in the database of TA.

4.3. Identity Revocation. Users can apply to TA for the reimbursement and breakdown of vehicles and log off the OBU that has been registered; after TAs examination and verification, corresponding public keys can be put in RL. We made Algorithms 4 with the principles below.

(i) TA receives information$(M, IDSign(M, ID, sk))$ and verifies whether the signature is valid

(ii) After the signature takes effect, find out the pk_i of private key according to ID.

(iii) Add pk_i to Revocation List (RL).

INPUT: M_A
OUTPUT: *result*
1: **function**
2: $X_A = F(k, M_A)$
3: $K_A = Enc(pk_{TA}, k)$
4: $Sign_A = H(M_A|n|pk_A|ID_A|t|N\ once|p_1|p_2|\cdots|p_n)$
5: $Sign_A, ID_A, t, Nonce, s_1, \cdots, s_l, n, K_A, X_A, cert_A \longleftarrow RSU$
6: **if** $Sign_A$ is valid **then**
7: $D_{RSU} = H(X_A \mid ID_{RSU})$
8: $Sign_{RSU} = Enc(sk_{RSU}, D_{RSU})$
9: $X_A, Sign_{RSU}, C_{RSU} \longleftarrow TA$
10: **else**
11: **return** *error*
12: **end if**
13: **if** $Sign_{RSU}$ is valid **then**
14: $M'_A = H(M \mid t)$
15: **else**
16: **return** *error*
17: **end if**
18: **end function**

Algorithm 5: Information dissemination.

Similarly, RSU can also apply for revocation, Traffic Command Center will regularly send people to test, if there is damage in RSU, the corresponding identity identification will be recorded, and the corresponding public keys will be looked for and added to revocation list.

4.4. Information Dissemination. In order to ensure the privacy of the information of each vehicle, the real-time data sent by OBU to RSU will be transmitted through encrypting. First and foremost OBU makes use of random number generator to generate symmetric encrypted keys. In this system, we encrypt with AES algorithm. Afterwards, TAs public keys will be used for encryption.

Afterwards, the RSA digital signature plan is based on zero-knowledge proof to sign in encrypted information; finally, vehicles send their real-time road information, encrypted code, signature; and TAs certificate to the nearest RSU for examination.

After RSU obtains the encrypted real-time road information, encrypted code, signature, and TAs certificate, it makes use of the public key in the certificate to examine the signature; if the examination is passed, RSU will carry out summary calculation on the real-time road information that has been encrypted and its own ID, make use of private key in signature, and send everything obtained from OBU and its own signature and certificates to TA. (In particular, RSU does not need zero-knowledge proof for TA; since TA is the highest authority, it can obtain all information; therefore, RSUs signature can be signed directly.)

TA examines RSUs signature. If the certification is passed, TA will carry out hash processing on encrypted real-time information and store the information in the advanced blocks corresponding to TA. We completed Algorithms 5 with the principles below.

(i) Vehicle A generates real-time road data M_A, and the system generates a symmetric encryption key k. Then, the M_A is symmetrically encrypted with the key k, generating $X_A = F(k, M_A)$.

(ii) The key k is symmetrically encrypted using public key of TA, generating $K_A = Enc(pk_{TA}, k)$.

(iii) Vehicle A uses the RSA digital signature protocol based on ZK to sign the encrypted data, resulting in $Sign_A = H(M_A|n|pk_A|ID_A|t|N\ once|p_1|p_2|\cdots|p_n)$, and then the message group $Sign_A$,ID_A,t,$N\ once$,s_1,...,s_l,n,K_A, the encrypted message X_A, and the certificate issued by TA to the OBU $cert_A$ are sent to the nearest RSU.

(iv) RSU verifies if the signature of A $Sign_A$ is valid.

(v) If it is valid, then RSU conducts summary calculation $D_{RSU} = H(X_A \mid ID_{RSU})$ on encrypted message M_A and generates signature $Sign_{RSU} = Enc(sk_{RSU}, D_{RSU})$ applying the private key.

(vi) The RSU sends the certificate $X_A Sign_{RSU}$ and C_{RSU} to TA after a while.

(vii) Then, TA uses the certificate C_{RSU} to verify whether the signature of RSU $Sign_{RSU}$ is valid.

(viii) If the signature was valid, TA adds time stamp on the encrypted message M_A and hashes it, generating $M'_A = H(M \mid t)$, and then merges it onto the high block.

4.5. Arbitration Mechanism. We completed the framework design of IOV privacy protection system based on double-layered chains before this section, but the system defaults vehicles are believable. Once the intentional transmission of invalid information by malicious vehicles has occurred, it will cause the storage resources on the chain to be consumed. To solve this problem, we add the vehicle detection function on the basis of this system. According to the following principles, we made Algorithms 6.

INPUT: N_A
OUTPUT: *result*
1: **function**
2: $X_A = F(k, N_A)$
3: $K_A = Enc(pk_{TA}, k)$
4: $Sign_A = H(N_A|n|pk_A|ID_A|t|N\ once|p_1|p_2|\cdots|p_n)$
5: $Sign_A, ID_A, t, N\ once, s_1, \cdots, s_l, n, K_A, X_A, cert_A \longleftarrow RSU$
6: **if** $Sign_A$ is valid **then**
7: $D_{RSU} = H(X_A \mid ID_{RSU})$
8: $Sign_{RSU} = Enc(sk_{RSU}, D_{RSU})$
9: $X_A, Sign_{RSU}, C_{RSU} \longleftarrow TA$
10: **else**
11: **return** *error*
12: **end if**
13: **if** $Sign_{RSU}$ is valid **then**
14: **if** N_A is valid **then**
15: A gets reward for TA
16: **else**
17: A gives loss to TA
18: **end if**
19: **else**
20: **return** *error*
21: **end if**
22: **end function**

Algorithm 6: Information dissemination.

(i) Vehicle A sends notification message N_A about vehicle B and the system generates a symmetric encryption key k. Then, the N_A is symmetrically encrypted with the key k, generating $X_A = F(k, N_A)$.

(ii) The key k is symmetrically encrypted using public key of TA, generating $K_A = Enc(pk_{TA}, k)$.

(iii) Vehicle A uses the RSA digital signature protocol based on ZK to sign the encrypted data, resulting in $Sign_A = H(N_A|n|pk_A|ID_A|timestamp|N\ once|p_1|p_2|\cdots|p_n)$,
and then the message group $Sign_A$,ID_A, *timestamp*, $N\ once$,s_1,$\cdots$,s_l,n,K_A, the encrypted message X_A, and the certificate issued by TA to the OBU are sent to the nearest RSU.

(iv) RSU verifies if the signature of A $Sign_A$ is valid.

(v) If it is valid, then RSU conducts summary calculation $D_{RSU} = H(X_A \mid ID_{RSU})$ on encrypted message N_A and generates signature $Sign_{RSU} = Enc(sk_{RSU}, D_{RSU})$ applying the private key.

(vi) The RSU sends the certificate $X_A Sign_{RSU}$ and C_{RSU} to TA after a while.

(vii) Then, TA uses the certificate C_{RSU} to verify whether the signature of RSU $Sign_{RSU}$ is valid.

(viii) If the signature is valid, TA will obtain the notification message N_A. By analyzing the data of vehicle B, the notification message N_A can be arbitrated.

(ix) If the arbitration result is true, vehicle A is rewarded and the identity of vehicle B is revoked. If the arbitration result is false, vehicle A will give TA some economic compensation.

4.6. Safety Proof. In this section, we will analyze the security and zero knowledge of the system.

We will state the following four aspects for security:

(1) Nonforgery: in this system, each vehicle is certified by the certification center TA, so the enemy cannot forge a new on-board node (OBU) into the system.

(2) Data integrity: in this system, each roadside node (RSU) uses the hash function to package and upload the data to the authentication center (TA), so as to ensure the integrity of the data, in case the authentication center can collect evidence or find the data.

(3) Data privacy: in this system, each on-board node (OBU) uses symmetric encryption to ensure the limited use of the resource with the data uploaded by vehicles, such as route sand locations. Then, it encrypts the symmetric key by using the public key of (TA) to transmit the ciphertext, which guaranteed the conditional privacy of data.

(4) Nontampering: this system makes use of the nontampering property of block chain. Once the arbitration event occurs, the data can guarantee the truth.

The system also satisfies three basic properties of zero-knowledge proof: completeness, validity, and zero-knowledge.

(i) Completeness: c is obtained from the hash function, which is unpredictable. Therefore, when the signature

declared by OBU to RSU is true, V accepts the proof of P with a probability of close to 1.

(ii) Validity: if OBU cheats RSU without a signature, the probability of success is $1/2^l$. When l is large enough, this is a small probability event, which can be ignored, so V rejects the proof of P with a probability of $1-1/2^l$.

(iii) Zero knowledge: with the RSA algorithm, the protocol does not leak any information about s, so the protocol is zero knowledge.

To sum up, the advantage of using block chain technology lies in its ability of anticollusionin order to solve the problem that cloud may not be trusted in real life. At the same time, the trace ability and nonrepudiation of block chain are also conducive to the realization of application scenarios of conditional privacy. In this chapter, we have given the security description and zero-knowledge description of the authentication protocol for privacy protection of the system, so as to show that the privacy protection system of the Internet of Vehicles based on the double-layered chain is safe and will not disclose users' privacy.

5. Performance Analysis

In this section, we will analyze the system performance. In the previous article, we mentioned the advantages of using block chain technology, so in this section, we compare the single-layered chain system with the double-layered chain system.

In recent years, with the rapid development of the vehicle-sharing industry, many vehicles can be shared for people's convenience to go out. The privacy protection system of Internet of Vehicles (IOV) based on double-layered chain designed in this paper can well realize the scenes of sharing cars. Users will first register their identity. After being approved by the certification authority (TA), they can rent the vehicles from vehicle-sharing company. When a user rents a vehicle and drives, the vehicle's privacy information will be sent to the roadside unit (RSU) by on-board unit (the OBU) in the encrypted form. Then the roadside unit (RSU) sent the overall information to the authentication center (TA) for storage after data compression. At the end of the trip, the user can submit an application to the authentication center (TA) and directly pay his/her fee on the chain. When the user wants to quit the car-sharing service, he/she can also submit an application to the authentication center (TA), which will confirm the identity and then revoke his/her identity.

Here we take Shanghai's scenes of sharing cars as an example. By the end of 2016, there are more than 3 million vehicles in Shanghai, with 16 districts. In this system, we take vehicle-mounted nodes as vehicles and trust center nodes as districts.

5.1. Communication Complexity. In a single-layered chain system, there are about 3 million in-vehicle nodes that function as computing nodes. Therefore, for each block-making vote it requires 3 million information exchanges; in the double-layered chain structure of this IOV system designed herein, only TA will generate new blocks. So, it only takes 16 exchanges to complete each block-making. In other words, the double-layered chain structure reduces the number of computing nodes, and thereby greatly decreases communication complexity.

5.2. Communication Throughput Capacity. Based on the above analysis on communication complexity, we may assume the information exchange between single-layered chain and double-layered chain, so as to calculate the communication throughput capacity. Private data contain content data and image data. Content data include speed and path ways, and image data include road conditions, or photo records of accident scenes, etc. To save more space, our image data can be compressed to bit strings through hash processing. So the private data are uploaded in bit strings with different lengths. We may also assume that private data of each vehicle is 3KB. In single-layered chain, vehicles upload private data and signature to the chains. Suppose building one block costs 1s, then throughput capacity of the single chain is $(3 * 10^3)/(1/3 * 10^6) = 9 * 10^9 bit/s$. In double-layered chains, a block is formed every 10 min. Meanwhile, if one vehicle passes by every second, then $10 * 60 = 600$ vehicles pass through the roadside unit within 10 min. The uploaded private data is $600 * 3KB = 1800KB$. Hence, the throughput capacity of double-layered chain is $(1800 * 10^3)/(600/16) = 4.8 * 10^4 bit/s$. It can be seen that communication throughput capacity of double-layered chain is far less than the communication throughput capacity of single-layered chain. We made Figure 4 with the data above to represent the communication through capacity of single-layer chain and double-layer chain.

5.3. Number of Signatures. In a single-layered chain system, the number of information is equal to the number of in-vehicle nodes, namely, 3 million. And the corresponding number of signatures is 6 million. In the double-layered chain structure designed herein, each roadside node will sign k vehicles at the closest distance, where k is the expected number of privacy information accepted by each roadside node. Therefore, the number of signatures to be verified on the main chain is 600k, which means it reduces the number of signatures and further shortens the time spent on identity authentication during block-making. We made Figure 5 about number of signatures of single-layer chain and double-layer chain with data above.

5.4. Transaction per Second (TPS). The memory of a traditional block is sized at 3M. For a single-layered chain system, we can set each block to correspond to 1,000 transactions, and each transaction is about 3K in size; while in the double-layered chain system, the advanced block stores hash value, a 256-bit value, of each piece of information; that is to say, the size of each transaction is 32 bits. Therefore, TPS of double-layered chain system is about 100 times that of the single-layered chain system.

5.5. Data Storage Capacity. In a single-layered chain system, it stores about 103 transactions; in a double-layered chain system the transaction storage capacity is about 3M 32bit

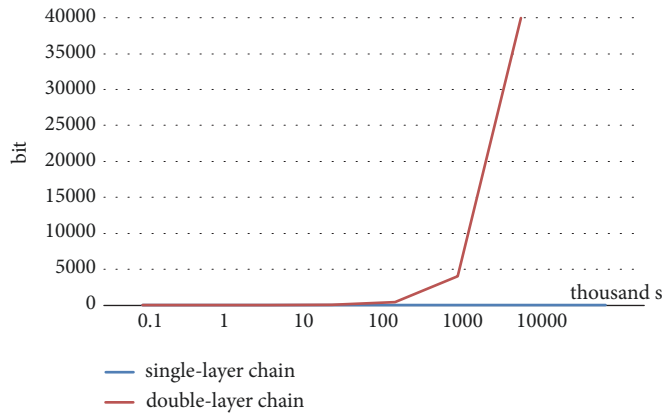


Figure 4: Communication throughput capacity.

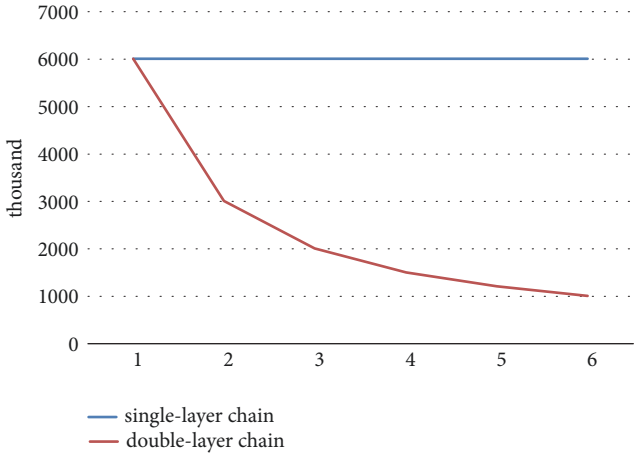


Figure 5: Number of signatures.

Table 2: Efficiency comparison of single-layer chain and double-layer chain.

	single-layer chain	double-layer chain
Communication complexity (secondary exchange of information)	$3 * 10^6$	16
Communication throughput (bit/s)	$9 * 10^9$	$4.8 * 10^4$
Number of signatures (thousand)	6000	6000/k
Trading volume per second	1000	10^5
Data storage	1000	10^5

= 105. It is thus clear that in the double-layered chain IOV system each block can store 100 times more of transaction information.

We made Table 2 with all the data in Section 5 to compare efficiency of single-layer chain and double-layer chain. In conclusion, compared with the traditional single-layered chain model, the double-layered chain model adopted by the IOV system herein can reduce the communication complexity, communication throughput capacity, and the time consumed by identity authentication, while improving the system's TPS and transaction storage capacity, thus greatly improving the system performance.

6. Conclusion

In this paper, we have designed a double-layered chain IOV model by investigating the current privacy protection model of vehicle network, which aimed at the assumption that the cloud is not necessarily credible in real life.

On one hand, the data is guaranteed to be true by using the unauthorized modification of block chain; on the other hand, the double-layered chain architecture reduces the communication complexity and throughput of the system, which not only improves the TPS of the system, but also makes it easier for the government to supervise by using the unique semicentralized structure of the double-layered chain.

At the end of this paper, we design a RSA digital signature scheme that based on zero-knowledge proof, which can realize the zero-knowledge between the vehicle-and-roadside unit and the vehicle-and-vehicle unit. We have completed the fully automatic double-layered chain privacy protection scheme for vehicle network, which is better applied in accident disputes, vehicle insurance claims, and other state of affairs.

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 research is supported by the National Key Research and Development Program of China (no. 2017YFB0802500).

References

[1] J. F. Paniati, "Vehicle infrastructure integration," in *VII Public Meeting*, 2005.

[2] R. Bishop, "A survey of intelligent vehicle applications worldwide," in *IEEE Intelligent Vehicles Symposium*, 2002.

[3] I. Furgel and K. Lemke, "A review of the digital tachograph system," *Embedded Security in Cars: Securing Current and Future Automotive IT Applications*, pp. 69–94, 2006.

[4] D. Llusia, R. Mrquez, J. F. Beltrn, C. Moreira, and J. P. D. Amaral, "Ieee 802.11p: towards an international standard for wireless access in vehicular environments," in *Proceedings of the Vehicular Technology Conference*, pp. 2036–2040, May 2008.

[5] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proceedings of 11th ACM conference on Computer and communications security*, pp. 132–145, ACM, USA, October 2004.

[6] E. Van Den Berg, T. Zhang, and S. Pietrowicz, "Blend-in: a privacy-enhancing certificate-selection method for vehicular communication," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 9, pp. 5190–5199, 2009.

[7] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 3152, pp. 41–55, 2004.

[8] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[9] H. Xiong, G. Zhu, Z. Chen, and F. Li, "Efficient communication scheme with confidentiality and privacy for vehicular networks," *Computers and Electrical Engineering*, vol. 39, no. 6, pp. 1717–1725, 2013.

[10] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.

[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[12] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proceedings of the International Conference on the Theory Application of Cryptology Information Security*, vol. 2248 of *Lecture Notes in Comput. Sci.*, pp. 552–565, Springer, 2001.

[13] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret: theory and applications of ring signatures," in *Theoretical Computer Science*, vol. 3895 of *Lecture Notes in Comput. Sci.*, pp. 164–186, Springer, Berlin, 2006.

[14] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *Proceedings of the 2010 IEEE International Conference on Communications, (ICC '10)*, pp. 1–6, May 2010.

[15] S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, 2015.

[16] H. Xiong, Z. Chen, and F. Li, "Efficient and multi-level privacy-preserving communication protocol for VANET," *Computers & Electrical Engineering*, vol. 38, no. 3, pp. 573–581, 2012.

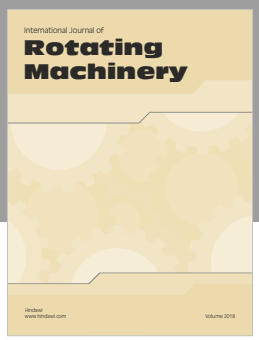
[17] H. Xiong, Z. Chen, and F. Li, "Efficient privacy-preserving authentication protocol for vehicular communications with trustworthy," *Security and Communication Networks*, vol. 5, no. 12, pp. 1441–1451, 2012.

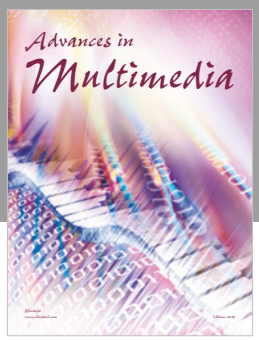
[18] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1442–1455, 2015.

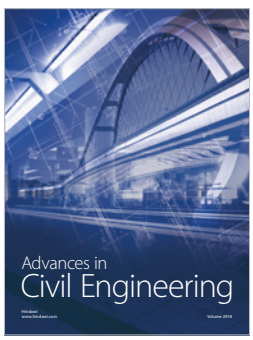
[19] Y. Chen, Z. Lu, H. Xiong, and W. Xu, "Privacy-preserving data aggregation protocol for fog computing-assisted vehicle-to-infrastructure scenario," *Security and Communication Networks*, vol. 2018, Article ID 1378583, 14 pages, 2018.

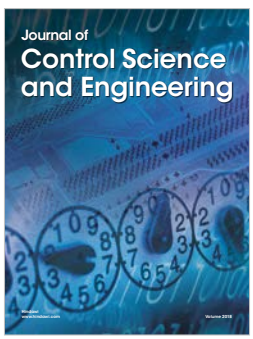
[20] L. Delgrossi and Z. Tao, *Vehicle Safety Communications: Protocols, Security, and Privacy*, vol. 103 of *Information and Communication Technology Series*, John Wiley & Sons, 2012.

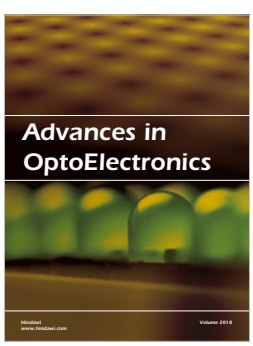
[21] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," *Cryptography and Security*, 2015.

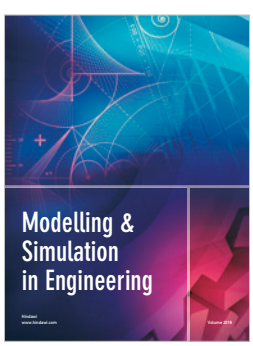


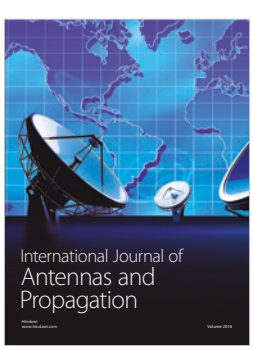


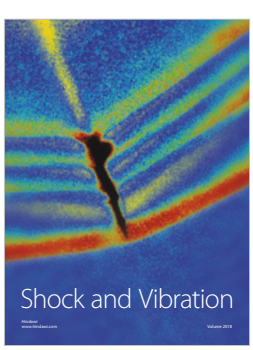


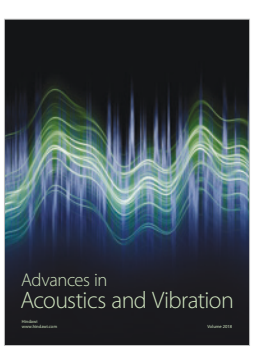












Hindawi

Submit your manuscripts at
www.hindawi.com