Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8870438, 10 pages
https://doi.org/10.1155/2020/8870438

Research Article

Blockchain-Based Internet of Vehicles Privacy Protection System

Tianhong Su,[1] **Sujie Shao**,[2] **Shaoyong Guo**,[2] **and Min Lei**[1]

[1]*Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China*

Correspondence should be addressed to Sujie Shao; buptssj@bupt.edu.cn

Received 16 July 2020; Revised 7 August 2020; Accepted 21 August 2020; Published 7 September 2020

Academic Editor: Chi-Hua Chen

With the development of wireless local area networks and intelligent transportation technologies, the Internet of Vehicles is considered to be an effective method to alleviate the severe situation of the current transportation system. The vehicles in the Internet of Vehicles system build the Vehicular Ad Hoc Networks through wireless communication technology and dynamically provide different services through the real-time driving information broadcast by the vehicles. Vehicle drivers can control the distance, planning the driving route, between vehicles according to the current traffic environment, which improves the overall safety and efficiency of the traffic system. Due to the particularity of the Internet of Vehicles system service, vehicles need to broadcast their location information frequently. Attackers can collect and analyze vehicle broadcast information to steal privacy and even directionally track the owner through the driving trajectory, bringing serious security risks. This paper proposes a blockchain-based privacy protection system for the Internet of Vehicles. The system combines the blockchain with the Internet of Vehicles system to design a safe and efficient two-way authentication and key agreement algorithm through encryption and signature algorithm, which also solves the central dependency problem of the traditional Internet of Vehicles system.

1. Introduction

With the improvement of living standards, traffic congestion becomes more and more serious with the increase of vehicles. With the emergence of 5th Generation, Bluetooth, sensor technology, cloud computing, big data, and other new technologies, the field of intelligent transportation has made great progress. In the Internet of Vehicles system, vehicles perceive the surrounding road condition environmental information through the on-board unit and communicate to roadside units and other vehicles in the network through the vehicle communication module so that the vehicle owner can obtain road condition information and navigation information, reducing traffic risks.

Because the Internet of Vehicles system is a complex system composed of vehicles, people, and other network facilities and it communicates through the wireless network, the system faces serious security problems. Therefore, how to protect user privacy while providing services is an urgent problem to be solved.

The concept of Vehicular Ad Hoc Networks (VANETS) originally originated from the Internet of Things and is the core technology of autonomous driving. The Internet of Vehicles system integrates advanced communication technology, and intervehicular communication, intravehicular communication, and vehicular mobile Internet are the three main communication components of the system [1].

Blockchain is essentially a decentralized and distributed database technology. It maintains a chain structure of data blocks among participating nodes, which is a continuously growing and immutable data record based on cryptography [2]. Each block can be logically divided into blockhead and block body; each block is concatenated with a hash value in the blockhead, and the transactions in each block are associated with the Merkle root. The blockchain will synchronize the transaction information to the entire network through the consensus mechanism, and each client stores the latest transaction information, forming a decentralized storage method. When some nodes fail, it will not affect the operation of the entire system [3].

In order to solve the problem of security and communication efficiency, this paper proposed the Blockchain-Based Internet of Vehicles Privacy Protection System. The system solves the problem of central failure caused by excessive access by managing the public key information of vehicles through a distributed mechanism. Due to the tamper-proof feature of blockchain, it can prevent the vehicle's public key information stored on the chain from being illegally tampered with. The system uses malicious behavior voting system to detect the message sent by the vehicle through the blockchain node, which prevents the vehicle from maliciously publishing illegal location information. The system uses blockchain and cryptographic algorithms to design efficient two-way authentication and key exchange strategies to reduce communication costs. At the same time, vehicles in the system can communicate anonymously with location service providers through blockchain, avoiding location service providers from stealing vehicle privacy. In summary, the Blockchain-Based Internet of Vehicles Privacy Protection System proposed in this paper is lower in cost, higher in security, and easier to maintain than the traditional Internet of Vehicles scheme.

The rest of the paper is organized as follows. Literature Review introduces existing techniques. Materials and Methods introduce the details of the system implementation. Security Analysis analyzes the security of the system. Results and Discussion present the performance results obtained for the system and provide a state-of-the-art comparison. Finally, Conclusions conclude the paper and outline some potential future work.

2. Literature Review

The traditional Internet of Vehicles system is based on PKI technology [4], which will generate a lot of communication costs. Due to the centralization of authentication nodes, the central node has heavy tasks, cannot be proxied, and is easy to be compromised, which brings the risk of leakage of user's sensitive information [5]. Salem et al. proposed a dynamic key distribution protocol based on PKI [6]. Vehicles do not need to store a large amount of key information but dynamically obtain keys from CA through RSU, which reduces the storage pressure on the vehicle side. When the vehicle certificate is revoked, the CA only needs to send a part of the revocation message without updating the entire Certificate Revocation List (CRL). Tan et al. proposed the SA-KMP algorithm and, based on the public key system, proposed a key agreement protocol based on the 3-dimension matrix to ensure secure communication between the vehicle and the RSU. In order to better protect the private data in the IoV system, Guo proposed a communication protocol based on pseudonyms [7]. The protocol combines homomorphic key agreement and digital signatures to manage and use pseudonyms to ensure the communication security and privacy protection of vehicles, but there is still the problem of central node dependence. Wang et al. proposed an anonymous certificate distribution mechanism for the Internet of Vehicles [8]. The vehicle obtains a temporary anonymous certificate from the passing RSU and uses it to broadcast messages. Therefore, there is no complicated certificate management problem, and the vehicle does not need to check the time-consuming CRL during the authentication process, which significantly improves authentication efficiency. Mei uses ring signatures and identity-based encryption technologies to authenticate communications between vehicles, but there is no experimental plan to analyze the complex network. Wei et al. proposed a fog-based privacy protection scheme that improves the security of a crowded vehicle network [9]. The schema can ensure that the fog user is anonymized during identity authentication between the fog user and the fog server. In order to reduce the central dependency problem, researchers combine blockchain technology with the Internet of Vehicles. The concept of blockchain was first proposed by Nakamoto in 2008 [10]. Lasla et al. proposed a blockchain-based lightweight authentication method to replace certificate authentication, using blockchain technology to track the certificate of each vehicle in a distributed immutable ledger, and proposed a completely distributed vehicle access mechanism [11]. Yang et al. proposed a blockchain-based vehicle reputation management system. In this system, the Bayesian inference model is used to evaluate adjacent vehicles and send rating information to the blockchain network which realized tamper-proof reputation information [12]. He proposed a key management mechanism of IoV based on blockchain technology [13], which improves the low efficiency of traditional key management schemes and enhances the security of keys.

In general, most of the relevant studies have flaws in communication efficiency, cost, or security. Combining the advantages and disadvantages of the abovementioned existing schema, this paper proposes a privacy protection system based on blockchain. Based on the open, self-organized, and fast-moving features of the Internet of Vehicles, the system uses the tamper-proof and distributed features of blockchain technology to design efficient two-way authentication and key agreement algorithm and an anonymous location service-providing algorithm which improves the security of the Internet of Vehicles system.

3. Materials and Methods

The architecture of the Internet of Vehicles system based on blockchain is shown in Figure 1. A large amount of real-time traffic information such as safety messages needs to be processed in the Internet of Vehicles. Due to the limited computing power of the vehicle, the system uses RSU as a blockchain network node. RSU has certain computing power and has routing and forwarding functions. It adopts a cloud computing strategy to forward the received data to the RSU server, which has powerful real-time computing power and enough storage space to provide necessary computing power for the blockchain system. The cloud server provides a high-speed data query interface for RSU. Cloud computing provides a guarantee for data storage and analysis in the Internet of Vehicles system [14]. The blockchain is used to manage the user's public key and other private information to prevent it from being illegally tampered with; the blockchain system can hold the relevant nodes accountable in the event of a

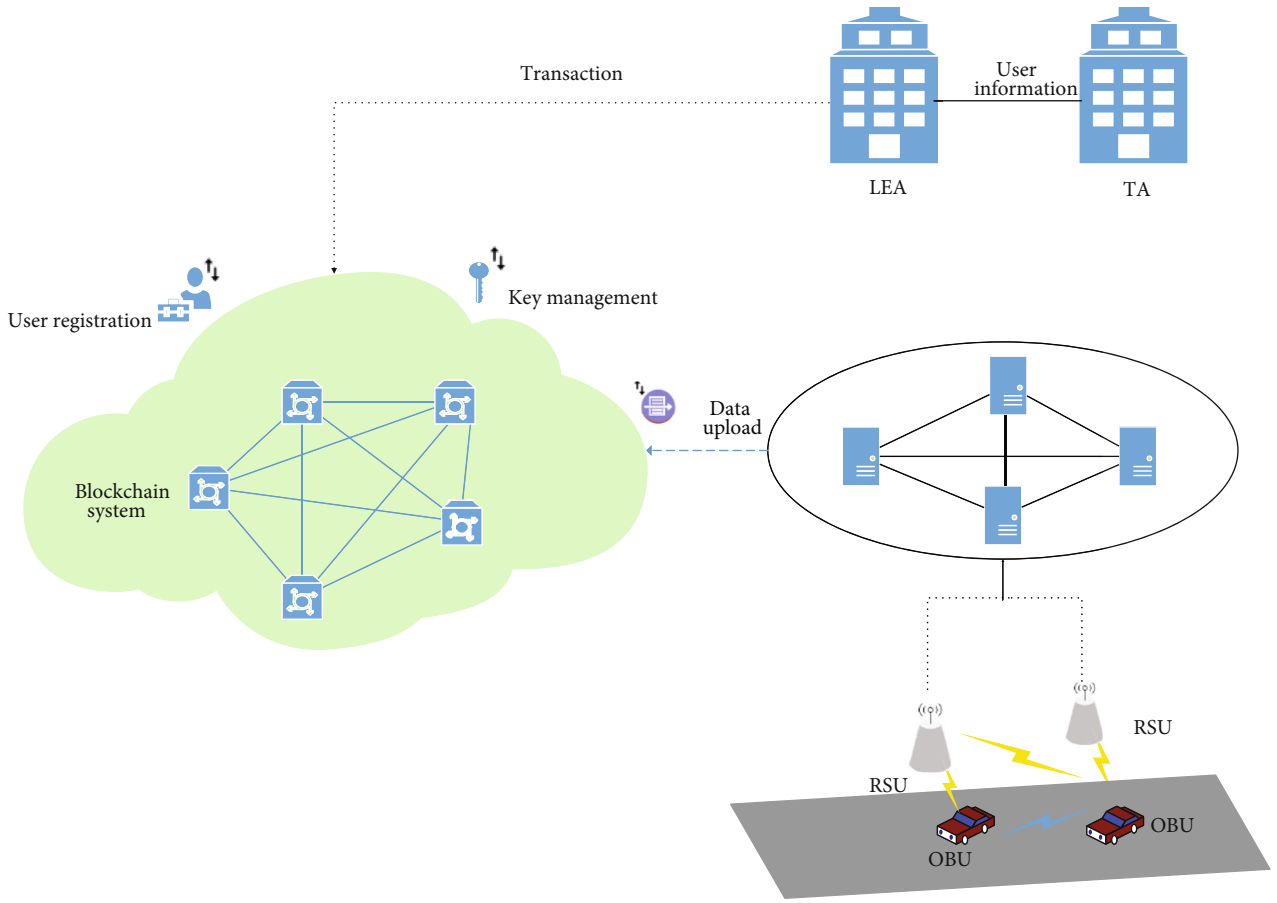

Figure 1: Blockchain-based IoV system.

dispute. Law Enforcement Agency (LEA) is also added to the system to review user information and TA-generated information, which is then signed and posted to the blockchain network (see Figure 1).

3.1. System Initialization. When the system is initialized, TA needs to create a blockchain account for each blockchain node, package the smart contract that implements the key management function into a transaction, and publish it to the blockchain network. TA records the contract address and interface information. When TA communicates with the blockchain node (RSU), it needs to provide the smart contract address to the node; only the correct contract address can trigger the contract to perform the predetermined function.

In order to realize the system's cryptosystem, TA needs to set the parameter $L = (p, a, b, G, n)$ for the system to determine the elliptic curve E in the finite field GF (p). TA needs to allocate public and private key pairs to the prearranged blockchain nodes (RSU) and upload the public key to the blockchain network.

3.2. Key Management. Key management is the core problem to be solved in the application system based on cryptography. In the traditional IoV system, the central authority has full authority to manage the binding of vehicle identity and public key, which requires huge communication and storage costs. As the number of vehicles increases in the system, it may cause the central server to crash. When the data in the central server is tampered and not discovered by the administrator in time, it will cause huge losses to the system.

The vehicles in the IoV system are traveling at high speed; vehicles need to make quick decisions. The central server cannot meet the communication delay problem due to the long communication distance [13]. The system proposed in this paper not only enhances the security of the key in the system but also reduces the communication delay.

3.2.1. User Registration. Before joining the Internet of Vehicles system, the vehicle needs to register with the local trusted agency. The detailed process is as follows:

(1) The owner sends the relevant personal information such as name, ID number, license plate number, vehicle type, and motor vehicle driving license to TA for review. The identity information needs to be strictly reviewed to ensure the legitimacy of the members in the system

(2) After TA reviews the user information, it generates a unique ID value for the user (UID), user public key (UPubK), user private key (UPriK), and validity

period VP (Valid Period) of the user public key information for the user

(3) TA submits the user information and the generated public key information to LEA for review. After checking the information, LEA encodes {UID, UPubK, VP} as hexadecimal data encapsulates it into a transaction and sends the transaction information to the blockchain network. Then, the blockchain node executes according to the logic defined by the registration function in the smart contract. After the contract is successfully executed, the transaction is successfully chained, and the blockchain system feeds back the successful execution result to TA

(4) After the TA obtains the execution result, it will package {UID, UPubK, UPriK, and VP} and send it to the vehicle user through the secure channel

3.2.2. Key Update. Regularly updating key information helps to enhance the security of the system. The key update is for keys whose validity period is about to expire. The user obtains a new set of public and private key pairs from the TA and continues to enjoy the services of the IoV system during the next validity period. The detailed process is as follows:

(1) The user packages the public key information and sends a key update request to the TA; the requested content includes the public key information before update like {UID, UPubK, and VP}

(2) TA reviews the user's request information and generates new public and private keys and validity period (newVP) information after verification, that is, {UID, newPubK, newPriK, and newVP}. TA encapsulates the information and sends an authentication request to LEA

(3) After receiving the verification request, LEA verifies the validity of the public key information, signs it after successful verification, packages it into a transaction, and sends it to the blockchain network

(4) After the blockchain receives the transaction information, the blockchain node executes the key update method in the smart contract. After the contract is successfully executed, the transaction is successfully chained and the blockchain system feeds back the successful execution result to TA

(5) After TA obtains the execution result, it packs the new user information and sends it to the vehicle user through the secure channel

3.2.3. Key Revocation. Key revocation is the process in which the blockchain system analyzes the behavior of vehicles to judge malicious users and revoke their public keys. The system designs a malicious behavior voting mechanism through the blockchain to record the malicious behaviors by using the smart contract. The voting results will be encapsulated into transactions and stored in the blockchain. Key revocation is aimed at finding out malicious users in the system. The detailed process is as follows:

(1) After receiving the distorted broadcast message from the malicious user, the blockchain node (RSU) records the vehicle ID and malicious behavior, packages it into a transaction, uploads it to the blockchain, and calls the voting record function in the smart contract. The function first queries the voting record Vote_v according to this id and then saves the record after adding one. The blockchain system will judge whether the current Vote_v exceeds the threshold THR_v of malicious behavior set by the system. If $\text{Vote}_v > \text{THR}_v$, the system will determine the vehicle as a malicious vehicle and encapsulate the vehicle ID, public key, and other identifying information to send a public key revocation request to TA

(2) After receiving the public key revocation request, TA checks the voting process. If the voting process is correct, the malicious user's information {UID, UPubK, and newVP} will be sent to LEA

(3) LEA reviews the revocation request, encapsulates a key revocation transaction, and sends it to the blockchain network

(4) After receiving the key revocation transaction, the blockchain executes the revocation function in the smart contract, stores the public key revocation transaction on the chain, marks the malicious user's public key as revoked, and sends a successful receipt to TA

The RSU can verify its location through the positioning system. The detailed process of the malicious behavior voting system based on smart contracts is as follows.

After RSU receives the vehicle message, it extracts the location information provided by the vehicle and judges whether the message is severely distorted based on its own location information.

$$\text{bol} = C_L(L_{\text{RSU}}, L_V)\#. \tag{1}$$

If bol is false, it means that the message is severely distorted; the system will drop the data packet and query the current malicious behavior of the vehicle through the smart contract and save the query result after adding one.

If bol is true, it means that RSU determines that this communication is normal.

Key revocation is of great significance for maintaining system security. The system needs to set reasonable thresholds to reduce system risks and ensure the normal operation of the system.

3.3. Communication Technology

3.3.1. Authentication. In order to ensure the legality of vehicles entering the system, when the vehicle enters the network and requests to communicate with other vehicles, it needs to be authenticated by RSU.

(1) Blockchain network node (RSU) broadcasts its beacon message, including RSU ID information (RID), RSU public key information (RPubK), time information (TS_{RSU}), which is used to verify whether the message has expired, and RSU public key proof (Mer_v), which is part of the Merkle tree in the block header. It can be used to verify the existence of the RSU public key

(2) After receiving the RSU broadcast message, the vehicle uses the on-board unit to calculate Mer_v to verify the correctness of the RSU public key. After the successful verification, the vehicle ID (UID) and public key information (UPubK) are generated by the hash function to maintain the integrity of the information. To ensure efficient operation of the system, this calculation process can be done offline or when the processor is idle

$$H_v = \mathrm{SHA}(\mathrm{UID}, \mathrm{UPubK}). \tag{2}$$

In order to ensure the authenticity of the message source, the vehicle uses its private key to sign the generated summary information. To enable RSU to verify the legitimacy of messages and avoid replay attacks, the vehicle needs to send clock information TS_v to the RSU node.

$$\begin{aligned} \mathrm{Sig}_v &= \mathrm{Sig}_{\mathrm{UPriK}}(H_v) = \mathrm{Sig}_{\mathrm{UPriK}}(\mathrm{SHA}(\mathrm{UID}, \mathrm{UPubK}))\#, \\ \mathrm{Msg}_v &= (\mathrm{UID}, \mathrm{UPubK}, \mathrm{TS}_v, H_v, \mathrm{Sig}_v)\#. \end{aligned} \tag{3}$$

(3) After receiving the Msg_v from the vehicle, the RSU checks its own clock information T_{RSU}. Check whether $T_{RSU} - TS_v < THR_t$ is established; if the time is within the preset range, the communication is allowed to continue. Otherwise, the data packet will be dropped. After verification, the system uses the same algorithm to calculate H_v'. Compare H_v' and H_v. If it matches, it can prove that the public key information has not been modified. If the matching fails, the message will be discarded

$$H_{v'} = \mathrm{SHA}(\mathrm{UID}, \mathrm{UPubK})\#. \tag{4}$$

After verifying the integrity, the RSU extracts the public key information (UPubK) queries whether it exists in the blockchain. If the public key exists, it can be used to verify the signature information. Otherwise, the packet is discarded. It is assumed that the user's private key will not be disclosed to other nodes; so when the signature verification is successful, the RSU can confirm the current communication vehicle legal.

$$\mathrm{Ver}_v = \mathrm{Ver}_{\mathrm{UPubK}}(H_v, \mathrm{Sig}_{\mathrm{UPriK}}(H_v))\#. \tag{5}$$

(4) In order to prevent malicious nodes from impersonating RSU for communication, vehicles also need to verify the authenticity of RSU nodes. RSU will assign an authentication status code (ASC) and an authentication validity period (AVP) to vehicles that have successfully authenticated. RSU sends RID, ASC, AVP, and timestamp information (T_{Rsu}') to the vehicle node with the private key signed

$$\begin{aligned} S &= \{\mathrm{RID}, \mathrm{ASC}, \mathrm{AVP}\}\#, \\ \mathrm{Sig}_{\mathrm{Rsu}} &= \mathrm{Sig}_{\mathrm{RPriK}}(S)\#. \end{aligned} \tag{6}$$

(5) After receiving the RSU information, the vehicle node first checks its own clock information T_v. Calculate $T_v - T_{Rsu}' < THR_t$ to verify whether the timestamp information is within the allowed range. After verification, use the RSU public key received previously to verify the RSU signature message. If the verification is successful, the vehicle saves ASC and AVP. Two-way authentication is completed

$$\mathrm{Ver}_v = \mathrm{Ver}_{\mathrm{UPubK}_v}(S, \mathrm{Sig}_{\mathrm{UPriK}}(S))\#. \tag{7}$$

After two-way authentication, the blockchain will record the authentication status and the validity period. If the vehicle enters the scope of other RSU management within the validity period, cross-domain certification can be quickly completed.

After the certified vehicle enters the communication range of other RSU and receives the RSU broadcast message, the vehicle needs to verify the authenticity of the RSU public key through public key proof in the broadcast message first. After successful verification, the vehicle sends ID information, ASC, and signature information to RSU; RSU determines whether the authentication status code and validity period are legal by querying the blockchain for the authentication information corresponding to the vehicle's public key. If so, RSU uses the private key to sign its own public key information to verify the validity of the RSU to the vehicle to complete the two-way authentication. If not, the RSU sends a reauthentication request to the vehicle.

If the vehicle is not within the communication range of the RSU, the vehicle needs to send a broadcast message requesting communication with the RSU to other vehicles within the communication range of the current vehicle. After receiving the message, vehicles within the RSU communication range forward the request message to the RSU. If the RSU verifies the public key information of the requested vehicle, the RSU broadcasts a beacon message, and the vehicles within the RSU communication range will try to forward the message to the requesting vehicle. The system provides

rewards for successfully forwarded vehicles. The rest of the steps are the same. If the vehicle does not have an RSU within its own communication range and there are no other vehicles, it cannot communicate.

3.3.2. Key Agreement. Since the symmetric cryptosystem has a faster encryption and decryption speed than the asymmetric cryptosystem, the system adopts symmetric cryptography in communication, and it is necessary for both parties to complete the key agreement before transmitting the information.

(1) The vehicle generates a random number A and Initial Key. The seed of the random number is dynamically generated from the identity information and the timestamp information to ensure the randomness of the number. Packages the message M_0 and uses the hash algorithm to generate a message digest

$$\begin{aligned} M_0 &= \{\text{RID, UID, } A\text{, Initial Key}\}\#, \\ H_1 &= \text{SHA}(M_0)\#. \end{aligned} \tag{8}$$

Pack the message M_0, summary result and timestamp information, encrypt it with the verified RSU public key, and send the ciphertext to RSU.

$$C_1 = E_{\text{RPubK}}(\text{RID, UID, } A\text{, Initial Key}, H_1, \text{TS}_v)\#. \tag{9}$$

(2) After receiving the message, RSU uses its private key to decrypt the message to obtain the plaintext content and then uses its own clock information T_{RSU} to check $T_{\text{RSU}} - \text{TS}_v < \text{THR}_t$,

$$M_1 = D_{\text{RPriK}}(C_1) = (\text{RID, UID, } A\text{, Initial Key}, H_1, \text{TS}_v)\#. \tag{10}$$

Verify message integrity. Use the received {RID, UID, A, and Initial Key} to calculate the message digest value $H_1{}'$; checks whether H_1 and $H_1{}'$ are equal; if so, it can be proved that the message has not been tampered with.

$$H_{1'} = \text{SHA}(\text{RID, UID, } A\text{, Initial Key})\#. \tag{11}$$

After verifying the integrity, the RSU extracts the random number A and generates a random number B. Using the random number A, B and Inital Key jointly generate Basic Key and its validity period. Store generated results. Finally, use Basic Key, random number A, random number B, RSU identification (RID), and vehicle identification (UID) to generate the final session key.

$$\begin{aligned} \text{Basic Key} &= \text{Generate}(\text{Initial Key}, A, B)\#, \\ \text{SK} &= \text{Generate}(\text{RID, UID, Basic Key}, A, B)\#. \end{aligned} \tag{12}$$

After generating the session key, the RSU uses the session key to generate the HMAC verification code.

$$\text{HMAC}_1 = \text{HMAC}_{\text{SK}}(\text{RID, Basic Key}, A, B)\#. \tag{13}$$

The RSU encapsulates the RID, A, B, Basic Key, summary information, and timestamp information, encrypts it with the vehicle public key, and sends it to the vehicle.

$$C_2 = E_{\text{UPubK}}\left(\text{RID}, A, B, \text{Basic Key}, B_{\text{key}}\text{VP}, \text{HMAC}_1, \text{TS}_{\text{RSU}}\right)\#. \tag{14}$$

(3) After receiving the message, the vehicle uses its private key to decrypt the message to obtain the plain text content. Check the vehicle clock information T_V, and check $T_V - \text{TS}_{\text{RSU}} < \text{THR}_t$ to ensure that the message was received within the threshold

$$M_2 = D_{\text{UPriK}}(C_2) = (\text{RID}, A, B, \text{Basic Key}, \text{HMAC}_1, \text{TS}_{\text{RSU}})\#. \tag{15}$$

The vehicle node extracts the Basic Key and uses the same algorithm to generate the final session key (SK$'$). Use SK$'$ to generate the verification code.

$$\text{HMAC}_{1'} = \text{HMAC}_{\text{SK}'}(\text{RID, Basic Key}, A, B)\#. \tag{16}$$

Compare $\text{HMAC}_{1'}$ with HMAC_1; if they are equal, it means that the key agreement is completed, store the Basic Key, and its validity period feedback the message that the key agreement is completed to the RSU. Subsequent communications can be encrypted using the session key SK.

(4) RSU packages the key agreement process into transactions and stores them in the blockchain for verification

In order to facilitate the communication parties to update the session key, when the communication parties update the key within the validity period of the Basic Key, they only need to exchange random numbers with each other and use the Basic Key and the new random number to directly generate a new session key. The nodes in the system will periodically check the saved Basic Key data and clear the invalid data.

3.4. Location-Based Service. The Internet of Vehicles system will provide many services based on location information. The traditional IoV system requires users to send personal information and real-time location information to the service provider during driving. It brings a lot of security risks.

In this system, assuming that the service provider believes in the blockchain, users only need to send their public key information and service request information to the service provider when registering for the service. To improve the efficiency of verification and ensure the real-time performance

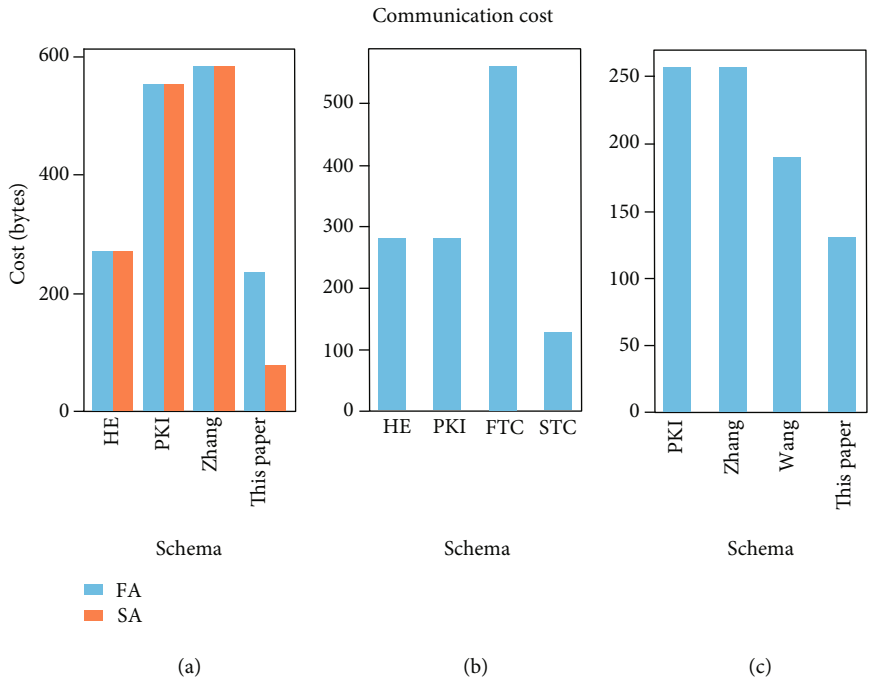

Figure 2: Communication cost. (a) Authentication cost in a different number of vehicles. (b) Key agreement communication cost in a different number of vehicles. (c) Message authentication communication cost in a different number of vehicles.

of zero-delay tolerant services, each service provider has a local cache of public key information in the blockchain. After receiving the message, the service provider will verify the authenticity of the public key from the blockchain cache; if the public key is true, record the user's public key information and feedback the user service application success information. The cache will be updated regularly. The public key can be used as the "pseudonym" of the user's identity information. Assuming that the TA will not disclose user registration information to other organizations, service providers cannot match the collected user location information with user identity information when providing services. When users apply for LBS while driving, they need to send the location information and service application information to the blockchain; the blockchain node verifies whether the location information is true. If it is true, the request information is signed and forwarded to the service provider. If not, the voting mechanism is used to record the malicious behavior of the user and the communication service is terminated.

4. Security Analysis

4.1. TA Security. TA has strong identity authentication. TA processes private information through salt value and hash function and stores private information such as keys in ciphertext. In the worst case, even if the private information is leaked, the attacker cannot know the plaintext information corresponding to the private information.

4.2. Public Key Security. The consensus algorithm adopted by the system is proof of work (Pow). When a malicious user wants to tamper with the user's public key information, it is necessary to control more than 51% of the computing power of the whole network. With the current computing power and the attacker's attack ability, such a large number of nodes cannot be controlled. And with the current computing power, the currently used 256-bit elliptic curve password cannot be cracked. In summary, the price that illegal users want to decipher the system exceeds its deciphering ability, so the public key in the system is safe.

4.3. Session Key Security. Since the session key is generated by the Initial Key and the random number negotiated by both parties through a key generation algorithm and the two parties need to exchange new random numbers when the key is updated, even if the randomness of the Initial Key cannot be guaranteed, the attacker cannot predict the random number generated in each round during the key agreement process, so the session key is safe.

4.4. Antieavesdropping Attack. Eavesdropping attack means that an attacker listens to the communication channel between the two parties to obtain sensitive data that is not encrypted by both parties. In the system proposed in this paper, the vehicle needs to complete the two-way authentication to confirm the user's legitimacy after entering the RSU communication range, and at the same time, the key agreement needs to be conducted after the authentication. All subsequent communications are encrypted and transmitted by using the session key to ensure that the information is not eavesdropped by unauthorized users.

4.5. Antireplay Attacks. Replay attacks refer to malicious nodes republishing legitimate data packets in the previous system to deceive the trust of legitimate vehicles. After receiving the message, the node first verifies whether the difference

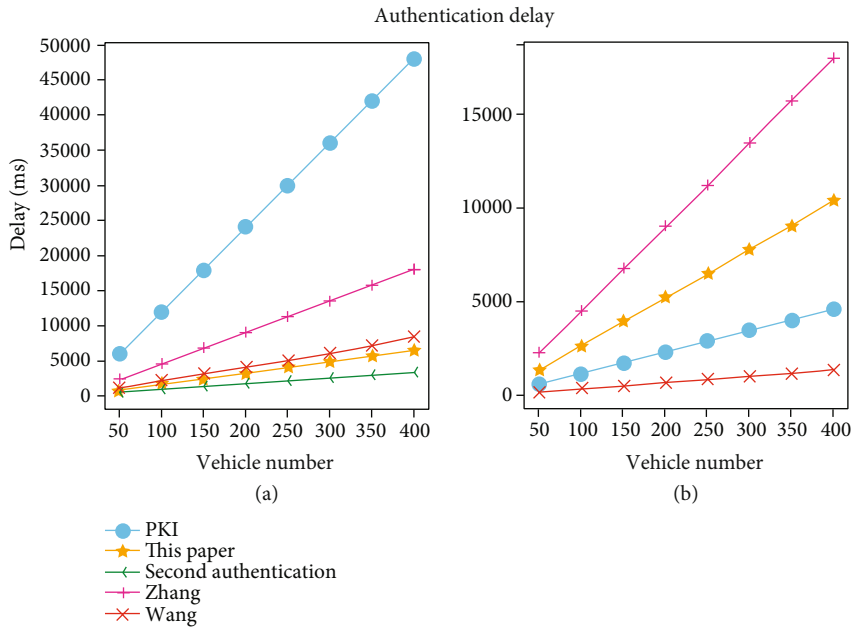

Figure 3: System delay. (a) Two-way authentication delay in a different number of vehicles. (b) Key agreement delay in a different number of vehicles.

Table 1: Storage cost.

Schema	Storage cost (byte)
PKI	126∗(number of certificates)
SA-KMP	37∗XR (the number of RSUs certified)
He	96 + 64 ∗ XV
Wang	128 + 125 ∗ XR
This paper	96 + 11 ∗ XR + 38 ∗ XV (number of key agreement nodes)

between the synchronous clock information and the timestamp is less than the threshold THR. Only when the time difference is within the allowable range is the message considered valid.

4.6. Prevent Sybil Attack. Sybil attack refers to a malicious vehicle disguised as the identity of a legal vehicle and released distorted information. The system needs to complete the two-way authentication before communication, and both of them need to sign with their own private keys; the attacker cannot obtain the private key information, so it cannot impersonate the legitimate vehicle. At the same time, the malicious behavior of vehicles will be recorded by the voting mechanism of the blockchain system.

4.7. Location Information Protection. LBS service providers manage users by using public keys as pseudonyms and verify the public key information through blockchain. The pseudonym information in this authentication mechanism is difficult to forge.

5. Results and Discussion

The experimental equipment is a computer equipped with Intel Core i5-9400f cpu@2.90 Ghz and 16 GB RAM win10 system processor.

5.1. Communication Cost

5.1.1. Two-Way Authentication. According to the experimental situation, the entire key agreement process requires an interaction between the two parties (excluding broadcast messages), and the total required communication load is 237 bytes. If there is reauthentication within the validity period of the authentication code, the communication cost is 79 bytes. According to the IEEE1609.2 trial standard [4], two interactions are required to achieve two-way authentication in the traditional PKI system, totaling 554 bytes. Zhang et al. proposed an authentication system that requires CA participation [15]. The communication process required a round of interaction between the RSU and the vehicle and a round of interaction between the RSU and the CA, and the cost was 584 bytes. The scheme proposed by He requires

RSU to interact with the vehicle once to complete two-way authentication [13], and the cost is 272 bytes.

5.1.2. Key Agreement. Define the ciphertext length standard as 213 bytes, the signature length is 64 bytes, and the message payload as 67 bytes. Traditional PKI technology requires encrypted communication at the key agreement stage, and the cost is 280 bytes. He uses random polynomials to maintain key security [13], and the communication cost is 280 bytes. The system proposed in this paper conducts asymmetric encryption twice, and the cost is 560 bytes, and only 128 bytes are needed for the second agreement process within the Basic Key validity period.

5.1.3. Message Authentication. During the message authentication process, the traditional PKI system needs to transmit certificates and signature information. The total message size is 257 bytes. The message size in the system proposed by Zhang is 257 bytes. The message cost in the scheme proposed by Wang is 190 bytes. This system manages key information based on blockchain, and the message size is 131 bytes (see Figure 2).

5.2. Delay

5.2.1. Authentication Delay. The traditional PKI technology needs to check the certificate revocation table in real time when completing the authentication. In this system, the key information is managed through the blockchain, which reduces the query time of the certificate. The schema proposed by Wang et al. [8] completes two-way authentication through certificates. The schema proposed by Zhang et al. [6] requires the participation of the CA. Before authentication, the vehicle needs to be authenticated with CA. In this paper, the security is enhanced within the allowable range of time delay and has better delay efficiency when the same vehicle is certified for the second time.

5.2.2. Key Agreement Delay. This system uses a random number-based key agreement strategy. There are two asymmetric encryption operations and three key generation operations during the first key agreement process, but only two symmetric encryptions are required during the second process. The scheme proposed by Wang encrypts the message through an authentication certificate, and there is no key agreement process (see Figure 3).

5.3. Storage Cost. The storage cost mainly calculates the cost of OBU. The storage cost of each schema is shown in Table 1.

6. Conclusions

The Internet of Vehicles is an important application in the field of intelligent transportation and has received widespread attention in the academic community. The issue of privacy protection is the top priority of the Internet of Vehicles system. This paper proposes a privacy protection system for the Internet of Vehicles based on blockchain. It introduces secure user registration, efficient key management schema, two-way authentication based on blockchain, a key agreement algorithm based on random numbers, and anonymous communication technology between vehicle and service provider to ensure the confidentiality of security information. The system uses the decentralization feature of the blockchain to prevent the central failure problem. After comparing with the existing scheme, the system proposed in this paper has better performance in communication efficiency and communication security. However, the consensus algorithm based on proof of work currently used by the system will consume computing resources, and the system's key exchange strategy will bring certain storage pressure.

In the future, we plan to design a more efficient consensus algorithm to replace the proof of work algorithm and design a more reasonable communication data structure to reduce system costs and improve system efficiency and user experience. We will continue to study how to reduce the delay required to query public keys to better support real-time communication.

Data Availability

The data used to support the findings of this study are included in this article.

Conflicts of Interest

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

Acknowledgments

This work is supported by the National Key R&D Program of China (2018YFB1402704).

References

[1] M. Priyan and G. U. Devi, "A survey on Internet of vehicles: applications, technologies, challenges and opportunities," *International Journal of Advanced Intelligence Paradigms*, vol. 12, no. 1/2, pp. 98–119, 2019.

[2] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[3] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: platforms, applications, and design patterns," in *Financial Cryptography and Data Security*, M. Brenner, Ed., vol. 10323 of Lecture Notes in Computer Science, Springer, Cham, Switzerland, 2017.

[4] Intelligent Transportation Systems Committee, *IEEE trial-use standard for wireless access in vehicular environments(-WAVE)-security services for applications and management messages*, IEEE Std, 2006.

[5] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "PTAS: privacy-preserving thin-client authentication scheme in blockchain-based PKI," *Future Generation Computer Systems*, vol. 96, pp. 185–195, 2019.

[6] A. H. Salem, A. Abdel-Hamid, and M. A. el-Nasr, "The case for dynamic key distribution for PKI-based VANETs," *International Journal of Computer Networks & Communications*, vol. 6, no. 1, pp. 61–78, 2014.

[7] X. Y. Guo, *Research on the Privacy Preservation in Security Communication for VANET*, Shenyang Aerospace University, 2017.

[8] W. Qinglong, Q. Rui, F. Na, and D. Zongtao, "An efficient conditional anonymity authentication scheme for VANETs," *Journal of Beijing Jiaotong University*, vol. 43, no. 5, pp. 80–86, 2019.

[9] J. Wei, X. Wang, N. Li, G. Yang, and Y. Mu, "A privacy-preserving fog computing framework for vehicular crowdsensing networks," *IEEE Access*, vol. 6, pp. 43776–43784, 2018.

[10] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008.

[11] N. Lasla, M. Younis, W. Znaidi, and D. B. Arbia, "Efficient distributed admission and revocation using blockchain for cooperative ITS," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, February 2018.

[12] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[13] W. He, *Research on Key Management Mechanism of Internet of Vehicles Based on Blockchain Technology*, Xidian University, 2019.

[14] H. J. D. Lopez, M. Siller, and I. Huerta, "Internet of vehicles: cloud and fog computing approaches," in *2017 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI*, Bari, Italy, 2017.

[15] J. Zhang, F. Li, R. Li, Y. Li, J. Song, and Q. Zhou, "Research on identity authentication based on elliptic curve encryption algorithm in V2X communication," *Automotive Engineering*, vol. 42, no. 1, pp. 27–32, 2020.