Design of Internet of Vehicles Authentication Scheme Based on Blockchain

Chen Mao, Kaiyu Xie, Lei Gao, Mingjiang Wan, Shuxian Liu*
School of Information Science and Engineering, Xinjiang University, Urumqi 830046, China
liushuxian@xju.edu.cn

Abstract. While the Internet of Vehicles brings convenience to people, it also brings new challenges to vehicle safety. In view of the security problems of data destruction, replay, counterfeiting and monitoring in the information exchange of the Internet of Vehicles, the article aims to improve the security of identity authentication of the Internet of Vehicles, and relies on the framework of Hyperledger Fabric and divides it according to the characteristics of its modular components. Different participating nodes have designed a model of Internet of Vehicles application service platform based on Hyperledger Fabric based on this; using the decentralization of blockchain technology and the non-tamperable characteristics of the data to endorse the vehicle's identity authentication information as a substitute. The traditional CA certification center combines the blockchain technology with the traditional identity authentication technology based on cryptography, and proposes a solution for the Internet of Vehicles identity authentication based on the blockchain technology. Finally, the article makes a security analysis of the scheme, which shows the effectiveness of the method.

1. Introduction
Driven by the current computer technology and communication technology, the traditional automobile industry has established a smart networked car by installing sensor devices and communication devices on vehicles to enable communication between vehicles and between vehicles and infrastructure. This super-aware technology can bring a more comfortable, richer and more diversified driving experience to the vehicle. However, since the Vehicular ad-hoc network (VANET), which has the characteristics of large scale and open channels, sensitive information such as the vehicle's user identity and geographic location may be exposed to the network. If this information cannot be effectively protected, the communication in the Internet of Vehicles will bring users security issues such as privacy disclosure, identity fraud, and dissemination of false information. Typical attack methods include Sybil attack, worm hole attack, tunnel attack, etc. Therefore, in the Internet of Vehicles, a mechanism is needed to resist both internal and external network attacks, forming a trusted, controllable, and manageable network environment.

At present, the research on identity authentication in the Internet of Vehicles can be divided into two categories: one is the traditional identity authentication based on cryptography, such as: mutual trust authentication based on PKI certificate, group key, ring signature; the other The category is identity authentication using big data, artificial intelligence and other methods, such as: association analysis, behavior prediction and other authentication methods.

Although these authentication methods can effectively solve specific or most identity authentication problems, they have certain limitations in practical applications, such as in-vehicle
terminal computing power, universality of service platforms, and particularity of authentication centers. Therefore, this paper proposes a blockchain-based identity authentication scheme in order to improve the security of identity authentication while taking into account the needs of many aspects of reliability.

2. Authentication in IoV

IoV can realize the exchange of information between vehicles and vehicles, between vehicles and buildings, and between vehicles and infrastructure. It can even help realize the "dialogue" between cars and pedestrians, cars and non-motor vehicles. This kind of communication may involve sensitive information due to different needs, but the widely used VANET network in the Internet of Vehicles as an open network does not have good confidentiality itself. Therefore, it is particularly necessary to authenticate the legitimacy of the node's identity and the messages transmitted in the network.

2.1. Limitations of IoV

Unlike traditional networks, the Internet of Vehicles has the following limitations at this stage:

(1) Limited computing and storage resources: Take a certain Tesla car as an example, the vehicle is equipped with Intel Atom A3950 processor (quad-core 1.6GHz), 4GB RAM, 64GB eMMC storage, and most of the resources are based on It is used in the technology of automobile autopilot, leaving fewer resources for communication and computing.

(2) Specialization of service platform: The current application service platform of Internet of Vehicles presents the characteristics of service specialization, which will result in users needing to register authentication information on multiple platforms to obtain a diversified experience. The platform requires different authentication operations.

(3) Imperfect infrastructure: Road side unit (RSU) nodes that can provide IoV data access are not universal. Most of them are set up by service providers or directly connected to the Internet, which may cause waste of resources or network delays.

2.2. Solution

From the perspective of system security, to ensure the reliability of identity authentication security, first of all, the reliability of authentication information must be ensured. A certification center that cannot be tampered with can effectively guarantee this. Based on this, the scheme considers using blockchain technology. Considering the limitations of cross-platform services, the plan determines the technology alliance chain technology.

Finally, comprehensively consider the application scenarios, hardware resources, and security requirements, and consider the following ways to meet the corresponding needs:

(1) Using the Hyperledger Fabric platform, open source projects both reduce development costs and are universal. Modular pluggable components can be deeply customized according to requirements.

(2) The use of alliance chain technology can not only allow different service providers to join the network in the form of an organization, but also allow service providers to share data.

(3) Separate the vehicle from the blockchain network through the division of authority, which not only ensures timeliness but also reduces computing power and storage overhead, and at the same time reduces the scope of possible malicious nodes.

(4) Through the active detection mechanism, malicious nodes are prevented from publishing false information and forging identity information to achieve the purpose of attack.

3. Scheme design and definition

The design of the scheme consists of two parts, one is a service platform model based on Hyperledger Fabric, and the other is an authentication messaging framework based on blockchain technology.
3.1. Service platform model based on Hyperledger Fabric

The Hyperledger Project was founded by the Linux Foundation and is dedicated to providing a distributed ledger with blockchain as the underlying layer that can be developed collaboratively. The Fabric platform uses a licensing system. Unlike public networks that do not require permission, participants are not anonymous and completely trustless.

The biggest advantage of the Fabric platform is that the nodes can be defined in the form of components, so that different stages of tasks can be completed by different nodes, and no nodes of the entire network are required to participate, which greatly improves the concurrency of the solution and can According to the task characteristics of the node, a security maintenance strategy is formulated to greatly improve the security.

At the same time, the Fabric platform allows different organizations to dynamically join the Channel, which greatly improves the scalability of the platform and makes cross-service platform cooperation possible. At the same time, data can be shared among different service platforms by establishing Channel separately. The RSU with the Client component provides a unified interface for customers to perform identity authentication or obtain authentication information, while the vehicle-mounted terminal only needs to complete the initial registration on the service platform to achieve cross-platform service.

Therefore, this paper designed a service platform model based on Hyperledger Fabric (as shown in Figure 1), the platform consists of the following parts:

1. On-Board Unit (OBU): OBU obtains authentication information or submits authentication request through the unified interface provided by RSU, and can also obtain other services through RSU.

2. Road-Side Unit (RSU): RSU as the client of the blockchain is responsible for responding to OBU service requests.

3. Channel: It can isolate transactions, so that members outside the channel cannot access and modify the data inside the channel, and realize the permission management of blockchain data. All nodes inside the channel maintain the same ledger.

4. Peer: Peer node serves as the anchor node of the service provider to access the blockchain network. At the same time, RSU can also serve as a client of the blockchain network to submit requests to Peer nodes.

5. Organization: Different service providers join the blockchain network in the form of organizations, and service providers are responsible for maintaining Peer nodes; at the same time, different service providers can share authentication information in the form of separate channels.

6. Ordering Service: responsible for sorting the legal transactions collected in a certain period of time, and then forming block data broadcast to the blockchain network.
3.2. Authentication Information Delivery Framework
This article divides the design of the authentication information delivery framework of the whole scheme into four layers (as shown in Figure 2). Through the nesting of layers and the division of permissions to meet the needs of all aspects of the system as much as possible. There is a nested and progressive relationship between layers, and service request messages are authenticated through the transfer between layers and finally get a response. The division of access rights at different levels can be configured through the Membership Service Provider (MSP) of Hyperledger Fabric.
The outermost layer of the framework is composed of on-board terminals (OBU). Communication between vehicles is realized by the VANET network. At the same time, a request for identity authentication is submitted to the RSU through the VANET network.

The second layer is a request response layer composed of RSU, which responds to the identity authentication request and identity cancellation request submitted by the vehicle. The vehicle queries the identity authentication information of all vehicles in the current system by accessing a specific port of the RSU node. At the same time, RSU will monitor the messages published by OBU in the VANET network. If a vehicle releases false information or forges its identity, it will cancel the vehicle's identity authentication information.

The third layer and the fourth layer are the Channel layer composed of Peer nodes of the alliance chain and the ordering service layer composed of Orderer nodes. The Channel layer is composed of multiple Peer nodes. Peer nodes are responsible for receiving accounting requests submitted by RSU clients. At the same time, after authentication, the received requests are broadcast to other Peer nodes in the Channel layer. Peer anchor nodes and Orderer of the ordering service layer The nodes communicate. The sorting service layer is composed of one or more Orderer sorting nodes, which sorts the legal transactions collected in a certain period of time, and then reaches consensus through a consensus algorithm, and selects an Orderer node to form block data to join the area Blockchain and broadcast to the blockchain network.

The participants mentioned in the framework design complete the following tasks:

(1) OBU: On-board unit, also called on-board equipment, is composed of various sensors and electronic devices installed on the vehicle. Through these sensors and electronics, vehicles can collect, process, and exchange data in various forms for security purposes.
(2) RSU: As a service provider, RSU provides functions such as responding to vehicle requests, forwarding messages, and interception detection. It also serves as a client of the alliance chain to implement functions such as initiating transactions, monitoring messages, and updating configurations in the alliance chain network.

(3) Peer: includes Endorser endorsement node and Committer confirmation node. The Endorser endorsement node checks the received request according to the policy formulated in advance, calculates the transaction execution result, and signs and returns if it meets the requirements. Committer confirms that the node is responsible for writing transactions to the block and updating the local copy of the ledger.

(4) Ordering service node (Orderer): Sort the legal transactions collected in a certain period of time in a certain order, and then form the block data broadcast to the blockchain network. The consensus mechanism used by the ranking service is pluggable, and the degree of decentralization can be chosen by oneself.

3.3. V2X communication encryption algorithm and pseudonym

When OBU publishes or receives messages via VANET network, it will use asymmetric encryption algorithm to complete key generation and digital signature tasks. Due to the limited computing and storage capacity of the vehicle itself, the application of algorithms such as SHA and AES in the field of Internet of Vehicles identity authentication becomes unsuitable. Compared with this, the ECC-based public key encryption system has a short key length, small storage space requirements, low transmission bandwidth, and a small number of required logic gates. Under the same security level, SM2 has higher efficiency and smaller The computing power overhead can be well adapted to the needs of vehicles with low computing power.

Therefore, this solution uses the ECC-based SM2 encryption algorithm as the encryption algorithm for V2X communication in the VANET network. The public key and private key are generated by the vehicle itself before entering the identity authentication information, and the public key generated by the vehicle is submitted when entering the identity authentication information.

Pseudonymity is a technique used for a user to access a resource or service without disclosing its user identity. While ensuring the user's anonymity, accessing the resource or service can still be responsible for the behavior. This means that the subject can perform an action without revealing its user identity to a third party, which can protect the user's private information to a certain extent.

4. Blockchain-based Internet of Vehicles identity authentication mechanism

4.1. Registered identity authentication information

The mechanism sets the vehicle's identity authentication information as public key information. The specific steps for vehicle A to register its identity with the system are as follows (where RSU is the client of the blockchain network, E is the encryption function, and BlockWeb is the blockchain network):

1. Vehicle A uses RSU's public key PRSU to encrypt the service request code S1, information M1 (including the unique identification code ID), time stamp, and random number R1 submitted at the time of registration, and sends the encryption result to RSU through VANET;

2. After RSU obtains the information, it decrypts it with its own private key KRSU, obtains S1, R1, time and M1, judges whether the timestamp time is valid, and reviews the content to determine whether the true identity of the vehicle is legal, and generates a random number if it is true R2, encrypted with random number R1 and sent to vehicle A through;

3. Vehicle A decrypts the random number R2 after receiving the message, decrypts its public key group GPA=\{PA1, PA2, PA3...\} and timestamp time with the random number R2 and sends it to RSU through the VANET network;
(4) RSU A: EPA1 (G[pseudonym, PA]), After verifying that the content of the message is legal, the RSU assigns a pseudonym pseudonym to each PA of the public key group GPA of vehicle A to form a set of "pseudo-public key" key-value pairs G[pseudonym, PA] = {[pseudonym1, PA1], [Pseudonym2, PA2], [pseudonym3, PA3], ...}, and encrypt it with PA1 to send to vehicle A through VANET network. At the same time, RSU records in the server database [Vehicle Unique ID, G[pseudonym, PA]];

(5) RSU BlockWeb, RSU, as the client of the blockchain network, calls the initDate function designed by the chaincode through the SDK to submit an accounting request to the peer node of the blockchain network, and the "pseudonym -Public Key" key-value pair in G[pseudonym, PA] One by one to the Peer node of the blockchain network. After verifying the correctness of the RSU identity, the Peer node endorses the transaction and sends it to the ordering node Orderer. The Orderer node packages the transaction into blocks and writes the block after reaching consensus according to the consensus algorithm.

4.2. Query authentication information
The specific steps for vehicle A to obtain all vehicle certification information in the system are as follows:

(1) A→[RSU: port], Vehicle A connects to the designated port of RSU to query all the “pseudo-public key” key-value pairs of the ledger database;

(2) RSU→A, After receiving the query request, RSU, as the client of the blockchain network, calls the getAllDate function designed by the chaincode through the SDK to submit the query request to the Peer node. After the Peer node passes the query, it directly queries the local ledger database and returns the result to the RSU. RSU is receiving After reaching the result, output it on the designated port;

Vehicle A constantly updates the local ledger by regularly connecting to the designated port of the RSU.

4.3. Cancel identity verification information
The specific steps for vehicle A to actively cancel its identity to the system are as follows:

(1) A→RSU: EPRSU (S2||R1||M1||time), Vehicle A uses RSU's public key PRSU to encrypt the service request code S2, information M1 (including the unique identification code ID'), timestamp
time, and random number R1 submitted at the time of cancellation, and sends the encrypted result to RSU through VANET;

(2) RSU ® A: ER1(R2), After RSU obtains the information, it decrypts it with its own private key KRSU, obtains S2, R1, time and M1, judges whether the timestamp time is correct, and reviews the content. If the content is true, it generates a random number R2 and uses the random number R1 is encrypted and sent to vehicle A through VANET;

(3) A ® RSU: ER2 (G’[pseudonym, PA]||time), After receiving the message, vehicle A decrypts it to obtain random number R2, encrypts its "pseudonym-Public Key" key value group G’ [pseudonym, PA] and timestamp time with the random number R2, and sends it to RSU through the VANET network;

(4) RSU ® BlockWeb, After receiving the message, the RSU decrypts it with R2 to obtain G’[pseudonym, PA] and time, and judges whether the time stamp is correct. If it is correct, it queries the server database through the unique identification code ID’ in the M1 received previously [ID, G[pseudonym, PA]], compare G[pseudonym, PA] with G’[pseudonym, PA], and if the comparison is successful, RSU, as the client of the blockchain network, calls the chaincode through the SDK The designed deleDate function submits the accounting request to the Peer node of the blockchain network, and sends the pseudonym in G[pseudonym] one by one to the Peer node of the blockchain network. After the Peer node verifies the correctness of the RSU identity, it will endorse the transaction And sent to the ordering node Orderer, the Orderer node packages the transaction into blocks and writes it into the blockchain after reaching consensus according to the consensus algorithm, and deletes the corresponding data in its own ledger database;

Fig. 5 Proactive deregistration

The specific steps of vehicle B being cancelled by the system are as follows:

(1) RSU monitors all the messages published by OBU through the VANET network, obtains the pseudonym information from the collected information, and compares it with the server database. Vehicle B uses multiple pseudonyms to publish messages at the same time;

(2) RSU ® BlockWeb, Obtain the G[pseudonym] of vehicle B by querying the server database, and then as the client of the blockchain network User calls the deleDate function designed by the chaincode through the SDK to submit an accounting request to the Peer node of the blockchain network, and transfer G[pseudonym] The pseudonym in the one by one is sent to the Peer node of the blockchain network. After the Peer node verifies the correctness of the RSU identity, the transaction is endorsed and sent to the ordering node Orderer. The Orderer node packages the transaction into blocks after reaching consensus according to the consensus algorithm. Into the blockchain, and delete the corresponding data in its own ledger database;
4.4. Publish messages in VANET
The specific steps for vehicle A to publish messages on the VANET network are as follows:

A→VANET (pseudonym||M2 ||time||DS), Vehicle A sends a digitally signed DS packet containing pseudonym pseudonym, information M2 (including position, speed, acceleration, etc.), time stamp time and the above content in clear text at any time in the VANET network.

4.5. Receive messages in VANET
VANET→A: (pseudonym'||M2' ||time' ||DS'), Vehicle A receives the data packet from the VANET network to obtain pseudonym's pseudonym', information M2', timestamp time', and digital signature DS'. After judging that the timestamp is correct, seek the pseudonym pseudonym', information M2', and timestamp time'. Hopefully hash1, find the corresponding public key in the local database through pseudonym's pseudo-code, use the SM2 algorithm to decrypt DS' with the public key, get the hash value hash2, compare hash1 and hash2, confirm the message M2' is reliable, Otherwise, discard the data packet.

5. Security analysis

5.1. Authentication security analysis
In terms of identity authentication, first endorse the vehicle's authentication information by storing the vehicle's identity authentication information in the blockchain. The blockchain technology guarantees the authenticity of the authentication information with its recognized decentralization and immutability. It is better than reliability; secondly, the use of asymmetric encryption digital signature technology in vehicle communication not only ensures the reliability of message authentication but also ensures that the obtained message has not been tampered with, and adds a timestamp to the message, which can be effective Defends against replay attacks. Since the key pair used by the vehicle is generated by the vehicle itself, this will avoid the leakage of the private key caused by the traditional CA node being controlled. This scheme has designed an active detection mechanism to prevent malicious nodes from simultaneously using multiple legal identities to create "ghost cars" and other attacks.

5.2. System security analysis
The scheme divides the various types of nodes in the system into four layers. Security defenders can prevent and control malicious behaviors according to the characteristics of the tasks completed at different levels, which will greatly reduce the safety maintenance costs of the IoV system and reduce the influence of malicious nodes improves the disaster tolerance of the system.
6. Conclusion

6.1. Summary
The security of the Internet of Vehicles involves many aspects. In the face of increasing security threats, this paper focuses on the direction of identity authentication of the Internet of Vehicles. Based on previous research, this paper proposes a service platform model based on Hyperledger Fabric and an Internet of Vehicles identity authentication solution based on blockchain technology. The combination of blockchain technology and SM2 algorithm improves the efficiency of encryption and decryption, greatly reduces the safety maintenance cost and disaster tolerance of the Internet of Vehicles system, and satisfies all aspects of identity authentication.

6.2. Outlook
The identity authentication of the Internet of Vehicles has expanded the scope of identity authentication due to its particularity. The identity authentication of the Internet of Vehicles is no longer limited to the traditional static defense mechanism of identity and message authentication, but also includes multiple identity authentication methods such as vehicle behavior and dynamic detection and comparison of vehicle trajectories; the location privacy aspects of the Internet of Vehicles It is divided into three categories: trajectory blurring, pseudonym replacement and trajectory encryption. In addition, the detection of malicious behaviors in the Internet of Vehicles is the top priority of the security of the Internet of Vehicles, which will further improve and optimize the scheme design framework of this article.

Acknowledgments
This work was financially supported by the National Natural Science Foundation of China (61762085).

References
[1] Douceur J R. The Sybil Attack[C]. international workshop on peer to peer systems, 2002: 251-260.
[2] Thing V L, Wu J. Autonomous Vehicle Security: A Taxonomy of Attacks and Defences[C]. green computing and communications, 2016: 164-170.
[3] Asuquo P, Cruickshank H, Morley J, et al. Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures[J]. IEEE Internet of Things Journal, 2018, 5(6): 4778-4802.
[4] Vinel A, Ma X, Huang D, et al. Guest Editors’ Introduction: Special Issue on Reliable and Secure VANETs[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(1): 2-4.
[5] Hu Y, Perrig A, Johnson D B, et al. Wormhole attacks in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 370-380.
[6] Golle P, Greene D H, Staddon J. Detecting and correcting malicious data in VANETs[C]// Proceedings of the First International Workshop on Vehicular Ad Hoc Networks, 2004, Philadelphia, PA, USA, October 1, 2004. ACM, 2004.
[7] Studer A, Shi E, Bai F, et al. TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs[C]// Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON ’09. 6th Annual IEEE Communications Society Conference on. IEEE, 2009.
[8] Albert Wasef, Xuemin (Sherman) Shen. REP: Location Privacy for VANETs Using Random Encryption Periods[J]. Mobile Networks and Applications.2009,15(1):172-185.