World Wide Web (2022) 25:2241–2263
https://doi.org/10.1007/s11280-022-01078-3

Design of vehicle certification schemes in IoV based on blockchain

Junhua Wu[1] · Zhenyu Jin[1] · Guangshun Li[1] · Zhuqing Xu[1] · Cang Fan[1] · Yuanwang Zheng[2]

Received: 28 October 2021 / Revised: 11 April 2022 / Accepted: 14 June 2022 /
Published online: 2 August 2022

Abstract
Because of a large number of vehicles in Internet of Vehicle(IoV), distributed nodes and complex driving environment, data security and certification speed are easily affected. Blockchain enables different devices that do not trust each other to work together, maintain the general state in the process of information dissemination and sharing, and protect the privacy of devices. However, at present, the speed of vehicle certification in IoV is slow, and the use of idle resources is not considered. To address this problem, this paper provides a blockchain-based vehicle identity verification scheme by using a hybrid identity code verification method to ensure the nodes in the network securely share information. Meanwhile, a task processing algorithm based on time window is proposed to optimize the utilization of idle resources. In addition, the method is evaluated by simulation experiment, and the designed scheme can reduce malicious behavior of a registered vehicle in the network, and can shorten the processing task delay.

Keywords Blockchian · Internet of Vehicle (IoV) · Certification mechanism · Task assignment

Zhenyu Jin and Guangshun Li are contributed equally to this work.

This article belongs to the Topical Collection: *Special Issue on Resource Management at the Edge for Future Web, Mobile and IoT Applications*
Guest Editors: Qiang He, Fang Dong, Chenshu Wu, and Yun Yang

✉ Guangshun Li
guangshunli@qfnu.edu.cn

Junhua Wu
shdwjh@163.com

Zhenyu Jin
1751760193@qq.com

[1] School of Computer Science, Qufu Normal University, 80 Yantai Road, RiZhao 276800, Shandong, China

[2] Shandong Huatong Used Car Information Technology Co., Ltd, JiNing, Shandong, China

1 Introduction

With the rapid development of the Internet of Things(IoT), the IoT has been widely used in intelligent furniture, urban management and other fields. Therefore, as an important part of the IoV, the complex self-organizing network has attracted wide attention [1]. For IoV due to open environment and constantly moving vehicles, data tampering and private data leakage may occur, which can lead to property loss and traffic accidents during data transmission [2]. For example, Sybil reports incorrect traffic conditions to the server by falsifying false identities and affecting normal order. In addition, when there are malicious vehicles on the network, the problem is more obvious. An attacker could deliberately spread fake news. For example, in the area where the actual traffic accident happened, the road broadcast by the malicious nodes was safe. These malicious behaviors can endanger traffic safety or affect the efficiency of the traffic system [3]. Using the Blockchain technology can solve this problem to some extent.

A single point of failure can lead to the collapse of the central structure. The central node may have a private mind, so there is an authoritative network that can not handle trust problems very well, and establishing a third party can increase the cost of data processing and transactions [4]. Transferring IoV devices from a centralized mode to a decentralized architecture will help IoV devices become more self-regulating and maintained [5]. The most important is that blockchain technology maintains global state through nodes that are not trusted with each other, to make it suitable for decentralized environments [6]. Moreover, its distributed nature avoids the disadvantages of a centralized structure, thus data is not easily tampered with. At the same time, different from other IoV devices, vehicles reduce the high power consumption in blockchain network [7].

Blockchain is applicable to fields involving assets and data information, such as digital rights, insurance, public services, etc. By analogy, blockchain has the following characteristics: Firstly it is a distributed database with no third-party governing body; Secondly its nodes can independently verify the authenticity of the information to ensure that it has not been tampered with. Thirdly decentralization is the most essential feature [8]. Due to the nature of decentralized storage and multiple database copies, nodes must agree on the correctness of the data to verify the transactions [9]. And only when 51% of the data nodes are mastered, the malicious nodes can manipulate the data modification, this reducing the influence of the data error or node deception on the database [10]. Blockchain technology uses SHA-256 encryption algorithm to provide privacy protection for nodes on the network. After verifying the block, avoid modifying the contents of the block. So that data in the blockchain is immutable. In addition, through anonymous information transmission, it is not necessary to disclose the identity of each block node.

Blockchain technology has become a very promising method to record transactions in the network and eliminate dependence on third parties [11]. Existing solutions fail to ensure the security certification of IoV devices, and neglect the utilization of idle vehicle resources. Therefore, this paper focuses on how to better achieve vehicle identification in IoV and solve the problem of malicious behavior of vehicles. In addition, this paper also considers how to solve the malicious behavior of nodes by implementing decentralized management of nodes. The main contributions of this paper are as follows.

- We propose an certification scheme based on blockchain, in which identity information and hash verification codes are used in the authentication process. Certification mechanism promotes active participation of the device.
- A multi-vehicle task allocation algorithm is proposed. In this model, the idle resources of vehicles waiting for processing tasks are considered, and a multi-vehicle coordination method based on waiting time window is proposed to ensure the real-time performance. At the same time, this scheme effectively allocates multi-vehicle resources and improves the utilization rate of idle resources.
- The experiment show that this scheme can effectively reduce the possibility of malicious behavior of vehicle in the IoV and reduce the amount of idle resource.

The rest of the paper is as follows: Section 2 describes the related work. Sections 3 and 4 describe two key steps in the system architecture and algorithm implementation, namely vehicle authentication and assignment of tasks to waiting vehicles. Section 5 is safety analysis and experimental verification. Finally, we came to conclusions and our thoughts in the future.

2 Related work

Blockchain technology has great research value and commercial benefits, so academia and industry pay more attention to its application. At the same time, exchanging data in IoV is beneficial for commercial entities to create new sources of revenue [12]. More and more vehicles are joining the business chain, and the data exchange process in IoV has the following characteristics [13]: 1) Multi-participation in the data exchange process (provider, sender and trusted third party), the transmission process is complex; 2) there is a conflict of interest between vehicle, and mutual trust can not be realized between vehicles; 3) Data sharing between vehicle depends on the guarantee and reputation of both parties, which increases the difficulty of accessing physical equipment. Blockchain technology is decentralized, tamper-proof, traceable, and promoting sustainable development of the data exchange ecosystem [14].

Song et al. [15] proposed that multiple vehicles with similar average speed and direction of travel should be grouped together, and communication could be made between groups and vehicles outside the group could not be received. It is vulnerable to malicious attacks due to the changing vehicle environment and the complicated verification process when the vehicle enter the area; Yein et al. [16] put forward an RSP-based message authentication scheme to solve the above problems by using the public key, so as to achieve privacy protection; In order to realize the secure communication between vehicles, Deng et al. [17] proposed a secure communication system of the IoV based on public key encryption technology. They realize the temporary certificates for vehicle-to-vehicle and vehicle-to-road communications by using a combination of permanently valid authentication integers and temporary pseudonym certificates. Kumar and Arora [18] enhance the confidentiality of data in the IoV through unicast communication in V2V (Vehicle to Vehicle) mode. Wu et al. [19] put forward a new and efficient identity-based message authentication scheme. They use the elliptic curve cryptography mechanism to build a lightweight secure authentication

protocol, which eliminates the use of bilinear pairing operations and reduces the complexity of the operation. Wang et al. [20] designed a scheme of selective data exchange between the data owner and the authorized user in the car network. Liu et al. [21] has designed a set of efficient debt credit mechanism in IoV, in which vehicle can borrow money on demand and pays interest. Xiao et al. [22] design game theory-based methods to solve data sharing problems. Li et al. [23] build a peer to peer (p2p) secure trading system through consortium blockchain, and proposed a credit-based payment scheme to take advantage of the Stackelberg game. Wang et al. [24] design blockchain-based incentive programs to optimize vehicle behavior. Because there is a complex certification process in the above-mentioned scenarios, it will lead to the consumption of computing power and resources. How to simplify the certification process and ensure the safety of equipment in the IoV is an urgent problem.

However, the problem of trust among the participants has not been solved well. In order to strengthen the trust between the participants, Wang et al. [25] designed an information resource sharing system based on blockchain. Xu et al. [26] designed a blockchain-based big data sharing framework to support cross-resource applications on various platforms. Shi et al. [27] put forward a group key generation protocol based on password and constrained authentication. This scheme is lightweight because it does not involve bilinear pairings and elliptic curves. Bayat et al. [28] proposed an anti-attack authentication mechanism for attacks, and the simulation experiment proved the effectiveness of this scheme. Azees et al. [29] put forward an anonymous authentication mechanism to limit privacy protection and reduce the storage cost of vehicle anonymous certificates. Ao et al. [30] proposed a framework for secure key management in heterogeneous networks, in which the security manager captures the departure information of vehicles, encapsulates blocks to transmit keys, and then updates the keys of vehicles within the same security domain. Park et al. [31] devoted themselves to the security of data transmission in the IoV, and proposed a centralized security mechanism based on the authentication of trust institutions and a decentralized security mechanism based on blockchain to realize the security of communication in the IoV. Lee et al. [32] proposed a batch authentication scheme based on bilinear pairing, which was used for message-by-message authentication, in order to reduce information delay and realize real-time message handling. Karati et al. [33] introduced an identity-based bilinear signature encryption scheme, which is used for low-bandwidth communication, but it is not suitable for RSU to verify many vehicles in a short time in traffic scenes because of the large amount of calculation.

In addition, Vijayakumar et al. [34] designed a two-factor authentication and key management mechanism for data transmission, which provided higher security for vehicles. Huang et al. [35] proposed an anonymous batch authentication and key agreement scheme which was used to authenticate multiple requests from different vehicles and establish different session keys for different vehicles. It meets the needs of identity authentication, and uses elliptic curve cryptography to reduce authentication delay and transmission overhead. Lai et al. [36] developed a reliable reputation system to ensure that vehicles send and receive data safely. When an honest vehicle finishes its task, it will perform a virtual inspection. It can encourage cooperation and punish malicious vehicles. Shao et al. [37] proposed a new authentication protocol in a decentralized group model by applying a new group signature scheme. The batch message processing technology can speed up the message verification of the front page of the vehicle and ensure the safety of the vehicle. Liu

et al. [38] proposed an efficient anonymous authentication protocol based on signature and message recovery, which solved the serialization problem of authentication. Batch operations is used to verify multiple signatures, which reduces transmission overhead and realizes the executability of the random prediction model. Compared to the above research, our method focuses on an effective vehicle authentication mechanisms based on blockchain and resource use. We are different in the following ways:

- We use a hybrid authentication mechanism, using identity information and hash authentication codes. Compared with previous scenario, this method shortens the authentication time of network devices;
- We consider the use of vehicle resources by allocating the resources of idle equipment to deal with emergencies in the region and improve the utilization rate of idle resources.

3 System architecture

3.1 Framework of blockchain-based security certification

The existing centralized framework cannot guarantee the security of the IoV. Therefore, this section designs a safe and reliable security certification framework to achieve vehicle security authentication. By storing vehicle privacy data on the blockchain, it is ensured that malicious nodes can not tamper with information by attacking a single IoV device unless the malicious node controls more than half of the computing power in the network. Deploying the blockchain into the IoV improves security, and the blockchain-based IoV security certification framework shown in Figure 1 consists of the following public entities.

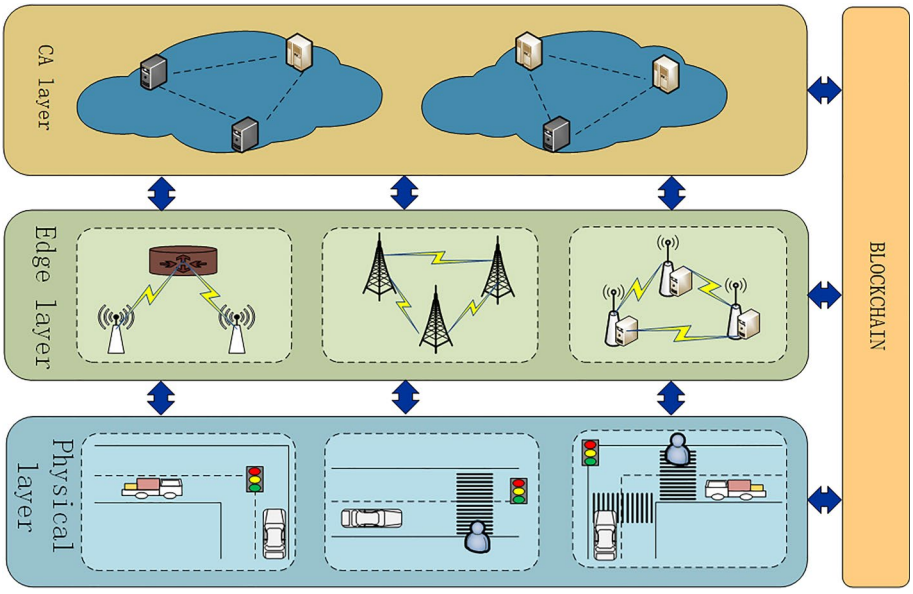

Figure 1 Overall view of IoV architecture

3.1.1 Physical layer

The physical layer in the certification framework consists of connected automobile entities, which add identity information to the network, including vehicles, sensors, pedestrians, and their intelligent equipment.

The main task of the physical layer is to receive information of the vehicles in the area, including data submitted during the registration stage and the verification codes provided during the authentication process. After the physical layer collects the data, it packages the data and provides it to the server at the edge layer, which is convenient for the subsequent services.

3.1.2 Edge layer

The server at the edge layer participates in the process of managing data transactions and submitting registration information and feedback requests. The edge layer forwards the information received from the physical layer to the next layer. At the same time, the edge layer will send information the information required by the compound to the requester based on the feedback of the upper layer. The verified device information will be stored on the blockchain deployed at the edge layer.

3.1.3 CA layer

At the CA layer, that is, the Certification Authority layer, parameters for registration are provided for entities in IoV. In the registration stage, the CA layer provides relevant parameters for the requested vehicles in the area to complete the legal registration of their identity in the network. When the CA receives a request from a legitimate vehicle, the layer will feed back data information that meets the requirements to the requested vehicle. The information of the vehicle will be stored in the blockchain after being verified by the edge layer.

3.1.4 Blockchain layer

The blockchain layer is the core unit of this architecture, which realizes decentralized security management. The blockchain layer is deployed on the IoV gateway server, which is used to store data and record information. Its stored data includes identity information and data exchange records, such as the id of devices in the IoV. By deploying blockchain in IoV, the safety and reliability certification of vehicles is realized.

3.2 The system composition of the certification mechanism

In this paper, we study an anonymous authentication scheme based on blockchain technology. The system model as shown in the Figure 2 mainly includes the following parts: Trust institutions (Ti), Road Side Unit (RSU), Trusted nodes and vehicles.

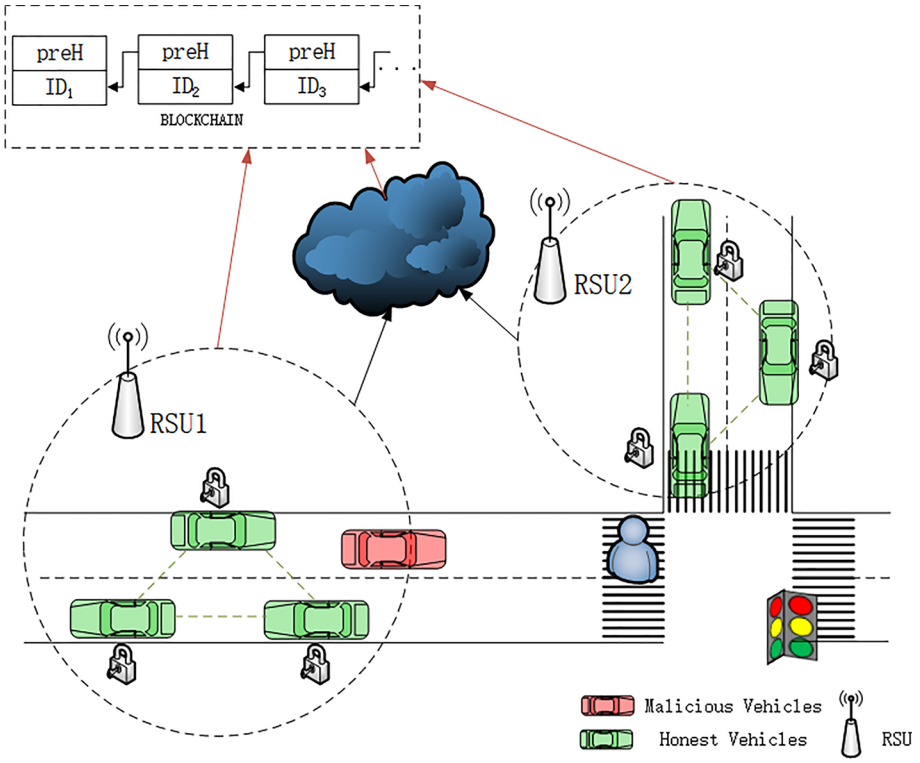

Figure 2 The equipment composition of the IoV

3.2.1 Trust institutions

Trusted institutions in IoV can store privacy information vehicles and generate the parameters needed for vehicle registration. At the same time, the trust institutions can identify illegal vehicles according to the verification results of the equipment information, and ensure the normal operation of the system.

3.2.2 Road side unit

The primary function of the road side unit in IoV is to collect vehicle information, such as identity of the vehicle, location information, destination and required information of the vehicle. Before receiving the services of roadside units, vehicles need to be inspected. Road side units refuse to provide services for vehicles that have not been verified.

3.2.3 Trusted nodes

Trusted nodes in IoV act as miners in the blockchain. In information transactions, the node that successfully answered the encryption challenge writes vehicle authentication results to the blockchain. All trusted nodes in the system have the same level.

3.2.4 Vehicles

Vehicles participating in the requested service in the network must be registered and certified by a road side unit. After confirming the identity of the vehicle as a guarantee, share the data with other services. After being verified, the vehicle can enjoy various services on the network. Service can only be requested after the vehicle is verified.

4 Algorithm design

4.1 Notation list

Table 1 shows the meanings of symbols and representations used by the algorithm.

Table 1 Notation List

Symbol	Quantity	Page Number
puk_{Ti}	trust institutions public key	8
prk_{Ti}	trust institutions private key	8
Id	the trust institutions of identity	8
Id_R	the road side units of identity	8
Id_v	the vehicle of identity	8
FID_v	false vehicle identity	8
puk_v	vehicle's public key	8
prk_v	vehicle's private key	8
T_i	target task	9
H_v	hash identification code	9
V_i	the attribute of the vehicle	10
C_v	candidate set	10
r_i^k	amount of resources for the attribute	10

4.2 Blockchain-based vehicle certification process

The vehicle anonymous authentication process proposed in this paper includes four stages: information initialization, registration of IoV equipment, vehicle identification, and regional consensus.

4.2.1 Information initialization phase

By using the key information of the trust institution, the prerequisites for key generation of other devices is provided. Trust institutions generate public and private keys puk_{Ti}, prk_{Ti} and identity certificate Pro, and broadcasting the public key to the network at the same time. After receiving the broadcast from the trust institution, the rest of the vehicles in the IoV need to borrow the public key information to generate their own public and private keys during the registration stage. This reduces the possibility of malicious nodes directly joining the network. Trust institutions generates an identity certificate based on the following equation.

$$Pro = gen\left(Id, prk_{Ti}, timestamp\right) \tag{1}$$

4.2.2 IoV equipment registration phase

Roadside units and vehicles complete the registration process at this phase. When the vehicles in the area receive the information broadcast by the trust institutions to the network, they will generate their own public and private keys through the key generation algorithm and the public key pair of the trust institutions. Roadside units and vehicles become legitimate nodes through the registration process. After the key pair is generated, the private information is stored on the blockchain through the roadside unit. At this stage, the registration task is completed. The public key and private keys of trust institution are used to ensure the trustworthiness of roadside units, which are generated according to the following equations.

$$prk_R = keygen\left(Id_R, puk_{Ti}\right) \tag{2}$$

$$puk_R = keygen\left(prk_R, puk_{Ti}\right) \tag{3}$$

The hybrid identity verification code used in this scheme mainly uses the vehicle identity information to generate a hash verification code, so as to hide the real identity of the vehicle. The registration process of a vehicle includes two steps: generating a false identity and generating a public key and private key based on the identity; Using the Id_v of the vehicle to perform hash operation to obtain a false vehicle identity $FID_v = Hash(Id_v)$; Then, trust institutions generates the vehicle's public key and private key puk_v and prk_v of the vehicle according to the generated fake vehicle

identity FID_v and saves them. In the whole process of authentication, the trust institution is completely trustworthy.

$$prk_v = keygen\left(FID_v, puk_{Ti}\right) \tag{4}$$

$$puk_v = keygen\left(prk_v, puk_{Ti}\right) \tag{5}$$

4.2.3 Vehicle identification phase

The roadside unit verifies the vehicles in the range and broadcasts the verification results. By verifying the identity of vehicles within the scope and broadcasting the verification results, malicious vehicles in the area can be screened out. If the identity is true and reliable, the trusted node will use the consensus protocol to write the verification result into the blockchain. In this way, the vehicle can be verified again after replacement, and the vehicle information is compared with the data stored in the blockchain, so as to realize quick authentication. When the vehicle enters the area managed by the roadside unit, the vehicle uses the previously generated FID_v, Id_v, as well as the public key, to calculate the hash identification code

$$H_v = HMAC\left(Pro_{Ti}, FID_v, puk_v\right) \tag{6}$$

Roadside units use the public keys, FID_v and Id_v and the private keys of registered vehicle

$$H'_v = HMAC\left(Pro_{Ti}, FID_v, puk_v\right) \tag{7}$$

to calculate hash identification numbers and verify that the $H_v = H'_v$ is true. The roadside unit searches the local database to verify the existence of the information, and if the verification results exists, updates the verification results. If the verification is passed, it means that the vehicle is honest and registered in the previous step. If the verification fails, it means that the vehicle is verified with false information, and the vehicle will be marked as malicious after the roadside unit transmits this information to a trusted institution. At the same time, roadside units broadcasts the certification results, providing data sharing and path planning services for the vehicles that have passed the certification.

4.2.4 The consensus phase within the region

When the vehicle is successfully registered, the roadside unit makes a broadcast. After the trusted node receives the authentication results, the validation results are written to the blockchain using a Practical Byzantine Fault Tolerance algorithm. Suppose there are k trusted nodes. Every time the result is written in the blockchain, a trusted node is needed as the master node, which is selected by $Primary = h \bmod k$, where h is the current block height. In this way, disadvantages of using third-party organizations are avoided, and the possibility of concentration of computing power is reduced.

After successfully writing the verification result to the blockchain, the primary node broadcasts the result to the rest of the trusted nodes, and sends suggestions to all

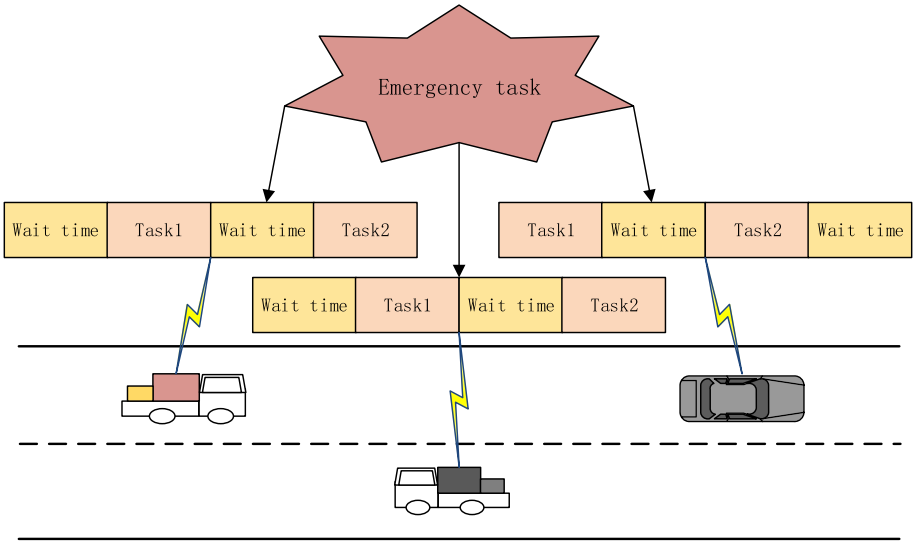

Figure 3 Multi-vehicle collaboration process

trusted nodes. After the trusted node receives the broadcast information, it will feedback the improvement information to confirm that the information has been received, and each trusted node receives at least $k - f$ messages. Where $k > 3f + 1$, f represents the maximum number of malicious nodes allowed in the system, so as to ensure the normal operation of the network even if there are malicious nodes in it.

4.3 Multi-vehicle cooperation algorithm based on waiting time

The urgent task arriving later will be processed at the end of the processing list. When it is the task's turn to be processed, the time of the task has already exceeded. In actual scenarios, it may be necessary to give priority to the more urgent tasks.

When there is an urgent task request in the IoV, the traditional solution is still to deal with general tasks, ignoring the timeliness of urgent tasks, which eventually leads to the failure to handle the task in time and causes losses. Aiming at the phenomenon that the remaining resources in the roadside unit area can not be fully utilized, and the problem that urgent tasks can not be handled in time, a multi-vehicle collaborative algorithm is designed in this section to utilize the idle resources of vehicles during waiting time. This process is shown in Figure 3.

Assuming that there are N vehicles in the area managed by the roadside unit that need to be handled by M, the tasks are denoted as $T = \{T_1, T_2, \cdots, T_M\}$, in which each task contains two attributes: resource requirement and time requirement. The type and quantity of resources needed to process task T_i is expressed as $R_i = \{R_i^1, R_i^2, \cdots, R_i^m\}$, where R_i^m represents the resource required to handle urgent task T_i. Vehicles with the same attributes in the same area can cooperate to complete the processing of urgent tasks.

Algorithm 1 Time-window-based algorithm.

Input: Vehicle set
Output: Task processing set I_T

Initial vehicle set $C_v = \Phi$
if $R_i < I_j \forall A_j \in I_v$ **then**
    select A_j to form the preparation set C_v
end if
calculate V_n, the number of vehicles in I_v
for $i = 1$ to V_n **do**
    if $\sum_{i=1}^{n} V_i^k r_i^k \geq R_i^k, k \in \{1, 2, \cdots, m\}$ **then**
        the collaboration fails
    end if
    if C_v only contains A_j or $\sum_{i=1}^{n} V_i^k r_i^k \leq R_i^k$ **then**
        break
    end if
end for
initialize the task collaboration set $I_T = \Phi$
if $\sum_{i=1}^{n} V_i^k r_i^k \geq R_i^k, k \in \{1, 2, \cdots, m\}$ **then**
    add A_j to task set I_T
else
    go to 23
end if
while $\sum_{i=1}^{n} V_i^k r_i^k \leq R_i^k, k \in \{1, 2, \cdots, m\}$ **do**
    add A_j to task set C_v
end while
return I_T

For emergency tasks to require timely response and processing, the number of idle vehicle resources *Idle* must meet the needs of the target task T_i, that is

$$\sum_{Idle} V_i^k r_i^k \geq R_i^k, \ k \in \{1, 2, \cdots, m\} \tag{8}$$

$V_i^k = 1$ indicates that the attribute of the vehicle V_i meets the requirements of the target task T_i; r_i^k represents the amount of resources for the k th attribute of vehicle V_i.

When an emergency task occurs in this area, vehicles with available surplus resources cooperate on the emergency task. During the current time period, the vehicle has proper idle time to meet the task requirements. To solve the problem of multi-vehicle task assignment based on waiting time, we propose a multi-vehicle task assignment algorithm based on time cooperation. First, when there is an urgent task in the area, the roadside unit immediately broadcasts the task set. Vehicles with enough spare resources will be added to the candidate set C_v. After that, we send information about the task T_i to the collaboration vehicle, which inserts the task into their task list and processes it accordingly. The time window-based algorithm is as Algorithm 1.

5 Security analysis and experimental verification

5.1 Security analysis

The design scheme of this paper needs to meet the following security requirements: confidentiality, anonymity and traceability. At the same time, it needs to be able to resist replay attacks and denial of service attacks.

5.1.1 Confidentiality

This section combines the vehicle identity information and hash verification code, and realizes the anonymous way of vehicle identity authentication in scene of IoV. In the phase of public key distribution, a public-private key pair is generated by using the false identity of the vehicle and the public key of the trusted institution, which ensures the reliability of each device key. In the certification phase, the verification information includes a hash authentication code, and only legally registered vehicles can pass the verification. In addition, the signature and pseudonym of the transmitting vehicle are attached to the security message at the same time, which ensures confidentiality and message integrity of the vehicle during the communication authentication process. Furthermore, only nodes that have been legally authorized can access the blockchain. In the service delivery phase, even if the sent message is obtained by the enemy, it can only obtain a pseudonym can be acquired from it, that is, the hash verification code can not acquire the real identity of the vehicle. Therefore, the proposed scheme ensures the confidentiality of key information throughout the whole process.

5.1.2 Anonymity

In order to achieve the anonymity of the scheme, no enemy can extract true identity. During the authentication phase, the vehicle sends a message to a nearby roadside unit. The message contains a pseudonym based on real identity, rather than the real identity of the vehicle. In this way, even if it is stolen, it is false identity information and will not reveal the true privacy. And if a car changes its pseudonym, it just needs to be re-authenticated, and the roadside unit broadcasts to the trusted authority, updating the records stored in the blockchain. In addition, the authentication results are recorded in the blockchain, and only legally authorized entities can access the blockchain. Malicious vehicles will not get the real identity of the vehicle, thus ensuring the anonymity of the mechanism.

5.1.3 Traceability

The purpose of the trust is to ensure the realization of traceability. When a vehicle in the network is found to be in violation of regulations, the trusted organization marks the illegal anonymous vehicle and revokes its key pair, thus ensuring the traceability of the illegal vehicle. At the same time, the identity of the illegal vehicle will be broadcast to the network, making it impossible for it to conduct normal transactions, thus realizing traceability and non-repudiation in the certification process.

Table 2 Security Comparison

	Authen-ticabil-ity	Anonymity	Traceability	DDoS	Anti-replay attack
Scheme [19]	√	√	√	–	√
Scheme [28]	√	√	√	×	√
Scheme [32]	√	√	×	×	√
Scheme [17]	√	√	×	×	–
Scheme [31]	√	√	–	√	–
Scheme [30]	√	√	√	√	√
Scheme [35]	√	√	–	–	√
Scheme [37]	√	√	–	–	–
Scheme [38]	√	√	–	–	–
Our scheme	√	√	√	√	√

Table 3 Simulation Parameters

Parameter	Numeric value
Number of vehicles	10-50
Vehicle speed	20-60km/h
intersection	12
Simulation steps	0.5s
Simulation time	14 400s

Check the timeliness by adding timestamp when the message is sent. If the timestamp is valid, the service request of the vehicle can be answered by the roadside unit, otherwise, the service will be denied. By verifying whether the timestamp is valid, replay attacks can be prevented, and the same service request will not be answered to multiple times. The scheme designed in this paper is based on blockchain technology and has the characteristics of decentralization and de-redundancy. In the blockchain network, even if one node is destroyed, other nodes will not be affected, so it can resist DDoS attacks.

Combined with the authentication requirements in the car networking scenario, the main characteristics of this chapter scheme are compared with other authentication schemes, and the results are shown in Table 2.

5.2 Experimental verification

In this section, we will assess the performance of the proposed method. Through the performance evaluation, it is proved that this scheme reduces malicious behavior in the IoV. The main simulation parameters are shown in Table 3.

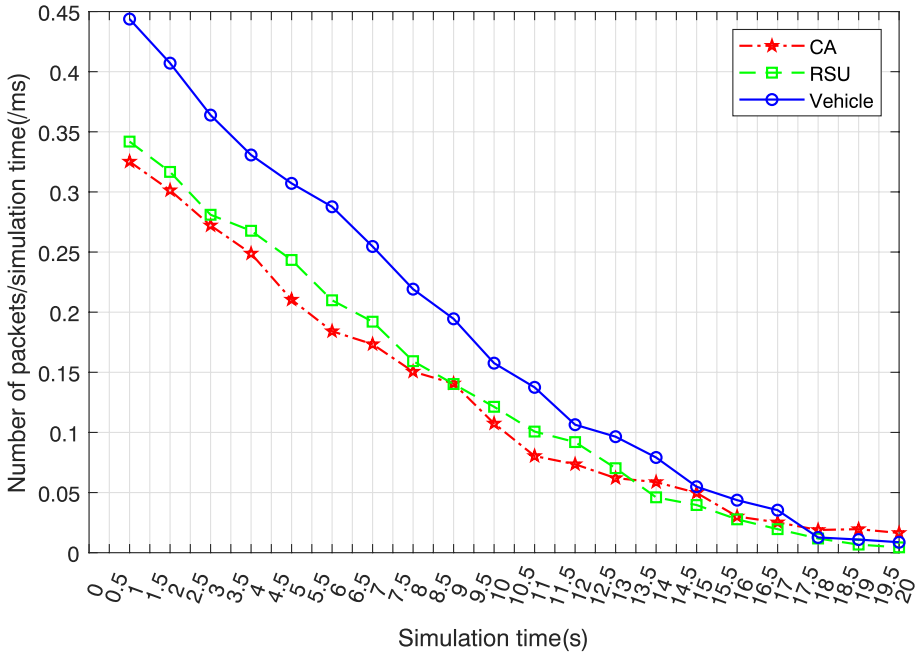

Figure 4 Transceiver data packet diagram

5.2.1 Time required to send and receive data

By simulating the time required to send and receive data between the devices of the vehicles on IoV, the time period for data sharing between vehicles can be represented. The horizontal axis represents the experiment time, and the vertical axis represents the approximate value of the total number of packets divided by the time, so as to make the trend more clearer.

In Figure 4, the difference and delay time between sending and receiving data packets of three types of nodes are compared.

It can be seen from the experiment that in the early stage of the experiment, there are fewer vehicles registered in IoV. Moreover, the registration process also takes a certain amount of time, and the experimental results are unsatisfactory. In the middle stage of the experiment, that is, the image in the middle part, because some vehicles have already completed the process of identities registration, the steps for identity authentication are reduced, and the time required is beginning to shorten. In the end of the experiment, more and more vehicles registered in the IoV, and the amount of vehicle information stored in the system begins to increase. When the vehicle changes its position, the steps required for data sharing become simpler, and required time begins to decrease. In the last stage of the experiment, the trend of the line graph tends to be stable. The experimental results show that with the increase of the number of registered devices in the IoV, the time to send and receiving data is gradually shortened.

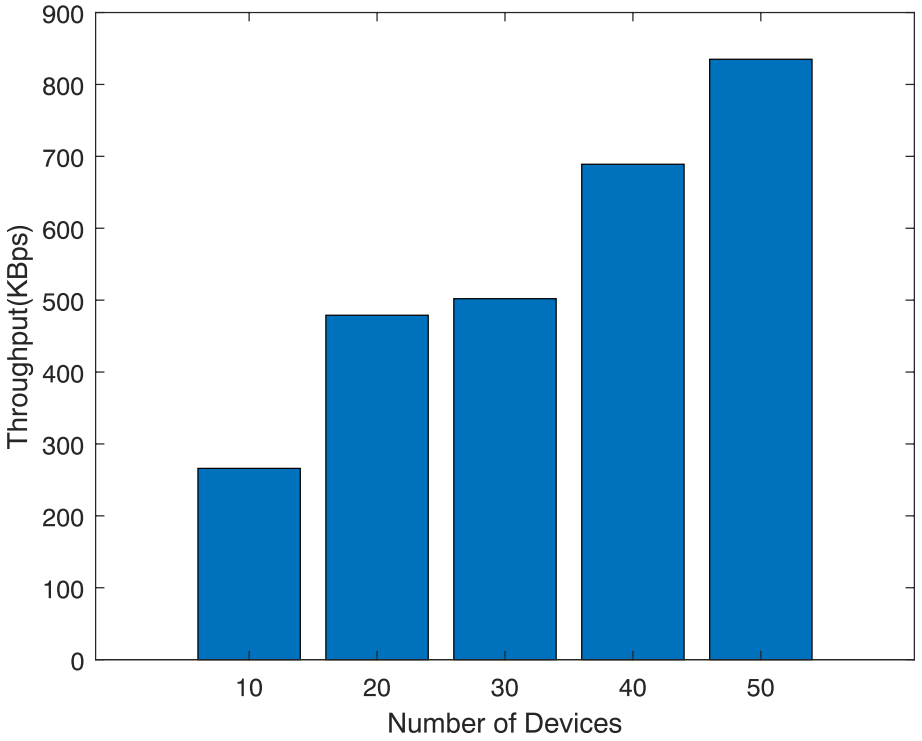

Figure 5 The relationship between throughput and the number of vehicles

5.2.2 The amount of data transferred per unit time

We increased the number of vehicles simulated in the experiment from 10 to 50 in order to analyze the overall data transmission volume in the unit time area, that is, the change rule of throughput with the number of vehicles. Figure 5 shows the relationship between the number of devices and throughput in the frame.

The number of tasks in the set area is a definite value. As shown in the figure, the throughput increases with the increase of the number of vehicles. When the number of vehicles in a region increases, the idle resources of the number of vehicles in the region will also increase. By integrating the resources of idle vehicles to handle task, the overall throughput of the region is improved. The experimental results show that when more vehicles are registered successfully, more vehicles will join the candidate set at the same time, and when there is an urgent tasks in the area, the tasks can be dealt with in time.

However, throughput will change with the number of vehicles. The reason is that throughput increases with the number of vehicles: when there are more vehicles, more vehicles are added to the candidate set, so when an emergency comes, more vehicles will wait.

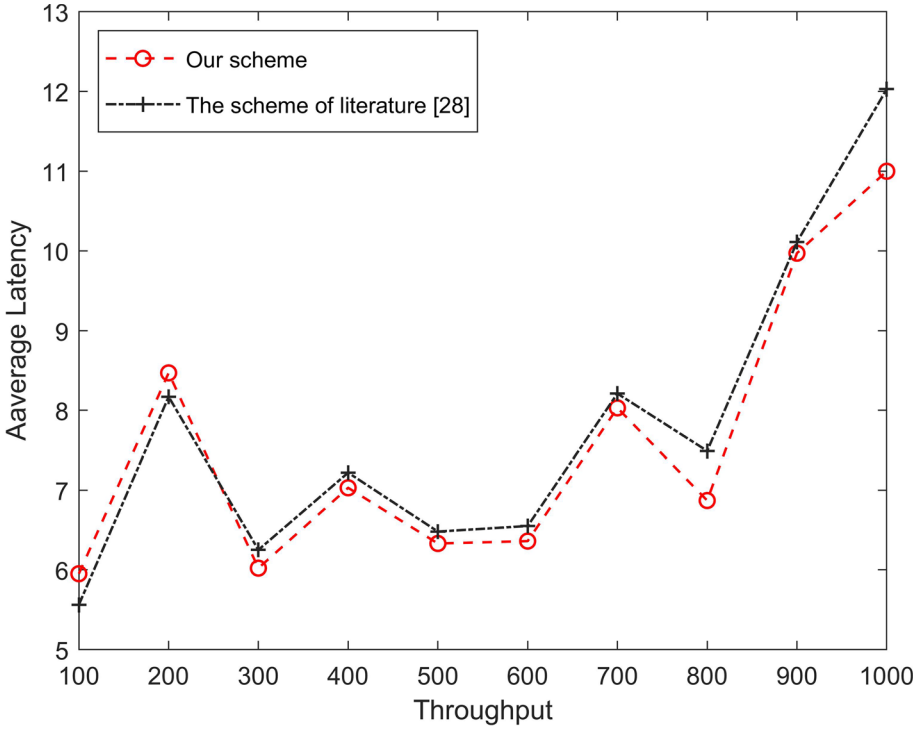

Figure 6 Average latency of the proposed framework

5.2.3 The time required to wait for the vehicle to respond

Latency refers to the time required for one device to respond to a command or request from another device. In terms of time, it is the maximum value(transaction completion time) - the minimum value(transaction deployment time), and the latency is measured in milliseconds. Figure 6 shows the difference between this article and the previously designed solution in terms of average latency and throughput.

There are very few vehicles registered at the beginning, and the previous scheme [28] and our scheme all require identity registration, which takes a long time. In the beginning, there were few registered vehicles, and both the previous scheme and our scheme needed identity registration, which caused a higher latency. The start of the hybrid authentication mechanism starts from the verification based on two pieces of information, so the latency is increased. As the increase of registered vehicles increases, the advantages of our design scheme are beginning to appear. Due to the optimization of the vehicle certification scheme and the implementation of the multi-vehicle cooperation scheme, the certification time will be reduced, and the latency will be correspondingly reduced. It can be seen from the figure that the experimental results are gradually superior to the existing design.

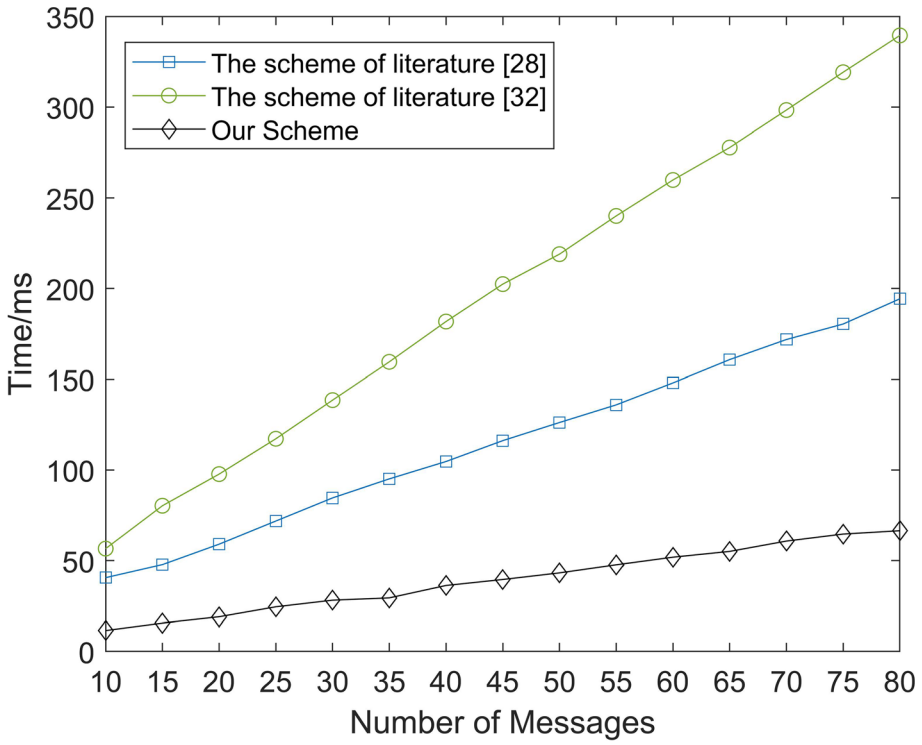

Figure 7 The relationship between authentication time and the number of messages

However, with the increase of the number of vehicles, the overall throughput of this region increases, which also increases the pressure on the system and increases latency.

5.2.4 Communication cost analysis

We have compared the performance of our scheme with previous schemes. Figure 7 shows the linear relationship between the computational cost of batch authentication and the number of messages in three authentication schemes. In the batch authentication stage, the computational cost of each authentication scheme increases linearly with the increase of in the number of messages. Therefore, the calculation cost analysis shows that the scheme in this paper has great advantages in calculation cost, and better meets requirements of IoV for efficient verification algorithms.

Figure 8 is the relationship between packet loss rate and the traffic density of the three schemes in the simulation experiment. The greater the business density, the greater the traffic volume of the whole system. As can be seen from Figure 4, with the increase of traffic density, the packet loss rates of the three schemes are all increasing. The message loss rate of the schemes in literature [28] and literature cite32 both

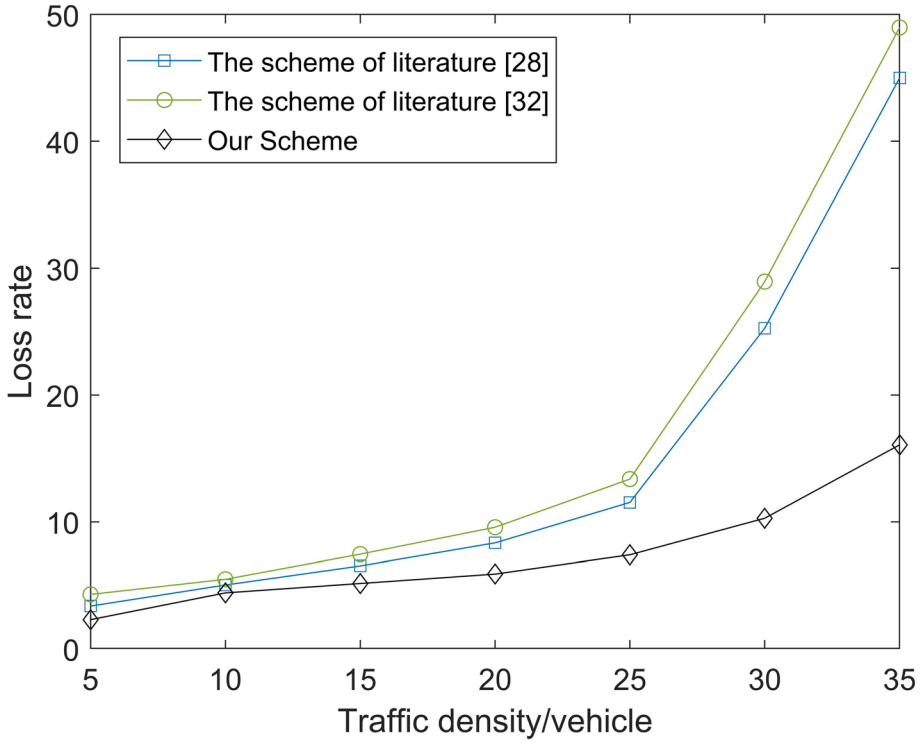

Figure 8 The relationship between message loss rate and traffic density

increase rapidly, while the loss rate of this scheme increases slowly and has the lowest value. This is mainly because the scheme proposed in this paper reduces the time of message authentication and improves the speed of message reception and processing.

Figure 9 shows the relationship between message delay and traffic density in the simulation experiments of the three schemes. As the increase of traffic density, the message delay of this scheme increases, but the growth rate is smaller than that of the schemes in [28] and [32]. The simulation results further verify that the proposed scheme can reduce message delay and improve the system performance.

5.2.5 The percentage of time increase in the number of devices and the number of tasks

We conducted a simulation experiment on the relationship between the number of devices and the number of tasks, as shown in Figure 10 and Table 4. Regardless of the number of tasks, when the number of tasks is fixed, the percentage begins to decrease with the increase of the number of devices .

When the number of fixed tasks increases with the increase of the number of vehicles in the area, it means that there are a lot of idle resources and fewer tasks need

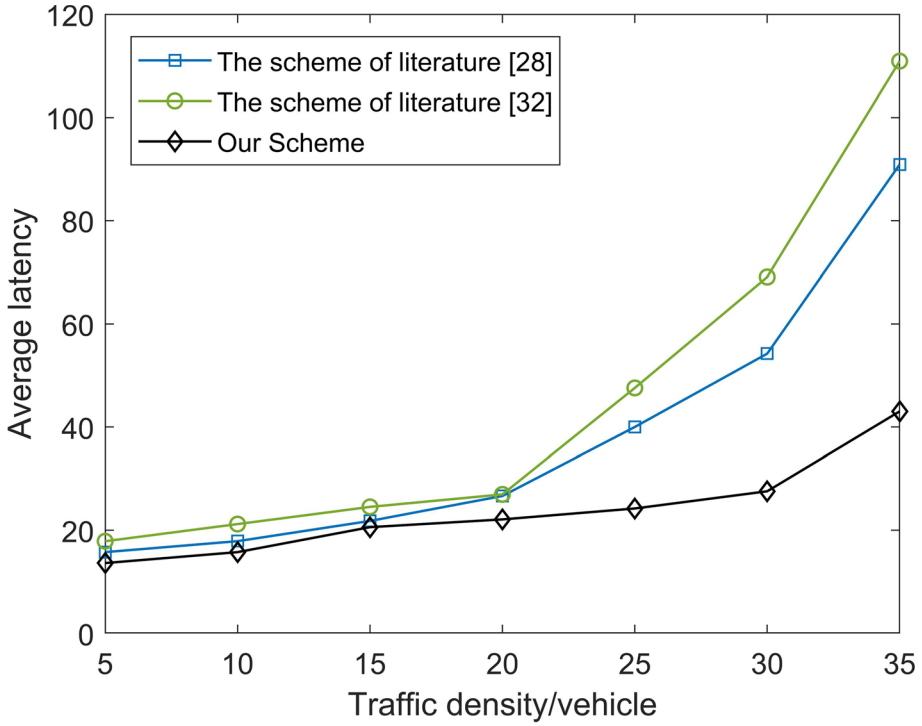

Figure 9 The relationship between message delay and traffic density

Table 4 Number of Tasks and Vehicles

	Task num1	Task num2	Task num3
Vehicles num 10	87.2310	80.5530	40.1160
Vehicles num 20	78.4530	58.3180	21.8420
Vehicles num 30	70.3340	44.5790	18.0920
Vehicles num 40	58.6160	35.4940	15.3630
Vehicles num 50	49.3520	30.4150	14.7080
Vehicles num 60	46.0190	27.8840	13.5510
Vehicles num 70	44.7730	25.0460	12.2370
Vehicles num 80	43.8010	23.5860	11.2330
Vehicles num 90	41.6950	24.3120	12.5900
Vehicles num 100	40.3250	24.5720	11.0210

to be handled. When there are fewer vehicles, each vehicle has more assigned tasks, higher utilization rate of idle resources and higher percentage of advance; On the contrary, when there are few vehicles, each vehicle is assigned many tasks. Because the

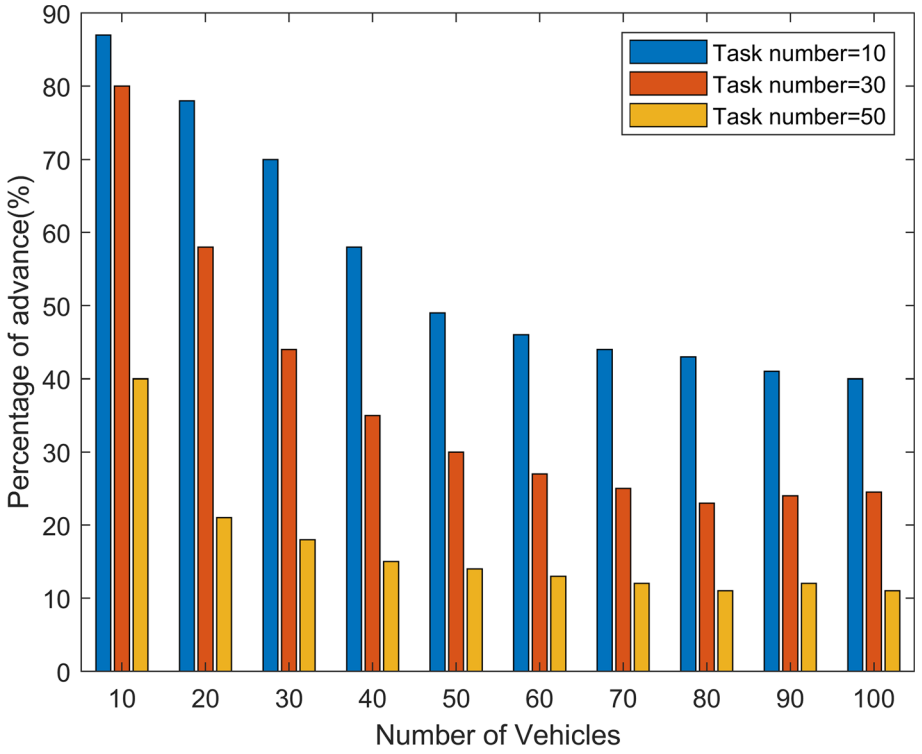

Figure 10 Percentage of time advance related to the number of vehicles and the number of tasks

number of tasks at this time has exceeded the limit that the vehicle equipment can handle.

Therefore, when the number of vehicles is fixed, this means that the mechanism becomes more efficient because it becomes more task-driven.

6 Conclusion

Blockchain technology can solve authentication and false identity problems in IoV. Blockchain can also be used to encrypt the identity of the vehicle and prevent user's privacy from leaking. In this paper, blockchain technology is further applied to IoV. We adopted an anonymous vehicle authentication scheme based on blockchain technology, and design a new vehicle access network mechanism, which adopted a hybrid authentication mechanism based on identity information and hash ID code; A multi-vehicle task assignment model and a multi-vehicle coordination method based on waiting time are put forward, which improves the utilization rate of vehicle resources. Experiments shows that the authentication scheme designed in this paper improves the utilization rate of vehicle resources and reduces malicious behavior in IoV.

7 Future ideas

Because the consistency algorithm needs to be replaced frequently, this leads to a waste of resources. We sort the nodes according to their honesty, and choose a more reliable master node by using the method of master node rotation. At the same time, the consistency protocol in the consistency algorithm is optimized to reduce resource consumption.

Declarations

Conflict of Interests The authors states that they have no conflict of interest.

References

1. Gupta, A.K., Johari, R.: IOT based electrical device surveillance and control system. In: International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp 1–5 (2019)
2. Wasef, A., Lu, R., Lin, X., Shen, X.: Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]. IEEE Wirel. Commun. **17**(5), 22–28 (2010)
3. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C.M.: Blockchain-Based Decentralized trust management in vehicular networks. IEEE Internet of Things Journal **6**(2), 1495–1505 (2019)
4. Liang, W., Tang, M., Long, J., Peng, X., Xu, J., Li, K.: A secure fabric blockchain-based data transmission technique for industrial internet-of-things. IEEE Transactions on Industrial Informatics **15**(6), 3582–3592 (2019)
5. Alaslani, M., Nawab, F., Shihada, B.: Blockchain in IoT systems: end-to-end delay evaluation. IEEE Internet of Things Journal **6**(5), 8332–8344 (2019)
6. Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2018)
7. Wang, X., Zeng, P., Patterson, N., Jiang, F., Doss, R.: An improved authentication scheme for internet of vehicles based on blockchain technology. IEEE Access **7**, 45061–45072 (2019)
8. Xiao, T., Choi, T., Cheng, T.C.E.: Pricing and benefit of decentralization for competing supply chains with fixed costs. IEEE Trans. Eng. Manag. **65** (1), 99–112 (2018)
9. Chen, C., Wu, J., Lin, H., Chen, W., Zheng, Z.: A secure and efficient Blockchain-Based data trading approach for internet of vehicles. IEEE Trans. Veh. Technol. **68**(9), 9110–9121 (2019)
10. Shrestha, R., Nam, S.Y.: Regional blockchain for vehicular networks to prevent 51% attacks. IEEE Access **7**, 95033–95045 (2019)
11. Zhang, C., Ota, K., Jia, J., Dong, M.: Breaking the blockage for big data transmission: Gigabit road communication in autonomous vehicles. IEEE Commun. Mag. **56**(6), 152–157 (2018)
12. Hu, Y., Chen, C., He, J., Yang, B., Guan, X.: Iot-based proactive energy supply control for connected electric vehicles. IEEE Internet of Things Journal **6**(5), 7395–7405 (2019)
13. Hong, Z., Huang, H., Guo, S., Chen, W., Zheng, Z.: Qos-aware cooperative computation offloading for robot swarms in cloud robotics. IEEE Trans. Veh. Technol. **68**(4), 4027–4041 (2019)
14. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet of Things Journal **5**(2), 1184–1195 (2018)
15. Song, J., Wong, V.W.S., Leung, V.C.M.: Wireless location privacy protection in vehicular Ad-Hoc networks. IEEE International Conference on Communications, 1–6 (2009)

16. Yein, A.D., Huang, Y.H., Lin, C.H., Hsieh, W.S., Lee, C.N., Luo, Z.T.: Using a random secret predistribution scheme to implement message authentication in VANETs. Appl. Sci. **5**(4), 973–988 (2015)
17. Deng, Q., Huang, S., Tian, S., Liu, H., Cao, J., Jia, S.: A security trust mechanism for data collection with mobile vehicles in smart city. In: 2020 IEEE/CIC International Conference on Communications in China (ICCC), pp 512–517 (2020)
18. Kumar, K., Arora, S.K.: Review of vehicular ad hoc network security. Int. J. Grid Distrib. Comput. **9**, 17–34 (2016)
19. Xie, Y., Wu, L., Zhang, Y., Shen, J.: Efficient and secure authentication scheme with conditional privacy-preserving for VANETs. Chinese Journal of Electronics **25**(5), 950–956 (2016)
20. Feng, X., Wang, L.: S2PD: A selective sharing scheme for privacy data in vehicular social networks. IEEE Access **6**, 55139–55148 (2018)
21. Liu, K., Chen, W., Zheng, Z., Li, Z., Liang, W.: A novel Debt-Credit mechanism for Blockchain-Based Data-Trading in internet of vehicles. IEEE Internet of Things Journal **6**(5), 9098–9111 (2019)
22. Xiao, L., Chen, T., Xie, C., Dai, H., Poor, H.V.: Mobile crowdsensing games in vehicular networks. IEEE Trans. Veh. Technol. **67**(2), 1535–1545 (2018)
23. Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y.: Consortium blockchain for secure energy trading in industrial internet of things. IEEE Transactions on Industrial Informatics **14**(8), 3690–3700 (2018)
24. Wang, Y., Su, Z., Zhang, N.: BSIS: Blockchain-Based secure incentive scheme for energy delivery in vehicular energy network. IEEE Transactions on Industrial Informatics **15**(6), 3620–3631 (2019)
25. Wang, L., Liu, W., Han, X.: Blockchain-Based Government information resource sharing. In: IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), pp 804–809 (2017)
26. Xu, C., et al.: Making big data open in edges: a Resource-Efficient Blockchain-Based approach. IEEE Transactions on Parallel and Distributed Systems **30**(4), 870–882 (2019)
27. Shi, A., et al.: A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Futur. Gener. Comput. Syst. **35**(84), 216–227 (2018)
28. Bayat, M., et al.: A secure authentication scheme for VANETs with batch verification. Wireless Networks **21.5**, 1733–1743 (2015)
29. Azees, M., Vijayakumar, P., Deboarh, L.J.: EAAP: Efficient Anonymous authentication with conditional Privacy-Preserving scheme for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **18**(9), 2467–2476 (2017)
30. Ao, L., et al.: Blockchain-Based Dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal **99**, 1–1 (2017)
31. Park, M., Gwon, G., Seo, S., Jeong, H.: RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications. IEEE Journal on Selected Areas in Communications **29**(3), 644–658 (2011)
32. Lee, C.C., Lai, Y.M.: Toward a secure batch verification with group testing for VANET. Wireless Networks **19.6**, 1441–1449 (2013)
33. Karati, A., Islam, S.H., Biswas, G.P., Bhuiyan, M.Z.A., Vijayakumar, P., Karuppiah, M.: Provably secure Identity-Based signcryption scheme for crowdsourced industrial internet of things environments. IEEE Internet of Things Journal **5**(4), 2904–2914 (2018)
34. Vijayakumar, P., Azees, M., Kannan, A., Jegatha Deborah, L.: Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **17**(4), 1015–1028 (2016)
35. Huang, J., Yeh, L., Chien, H.: ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology **60**(1), 248–262 (2011)
36. Lai, C., Zhang, K., Cheng, N., Li, H., Shen, X.: SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs. IEEE Trans. Intell. Transp. Syst. **18**(6), 1559–1574 (2017)
37. Shao, J., et al: A Threshold Anonymous Authentication Protocol for VANETs. IEEE Transactions on Vehicular Technology **65.3**, 1711–1720 (2016)
38. Liu, Y., et al: An efficient anonymous authentication protocol using batch operations for VANETs. Multimedia Tools and Applications **75.24**, 17689–17709 (2016)