Blockchain-based security cooperation communication scheme for IoV

HUI ZHI+, YU HUANG AND YONG WANG
Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, Anhui University, Hefei 230601, China.
School of Electronic and Information Engineering, Anhui University, Hefei 230601, China.
E-mail: zhihui_0902@163.com;

Abstract

Due to the dynamic change of the network topology and no fixed structure of the Internet of Vehicles, it is difficult to maintain a stable end-to-end connection, so it needs the routing cooperation between vehicles. However, due to the packet loss of selfish nodes and the influence of malicious nodes tampering with information, existing Internet of Vehicles routing cooperation with blockchain lacks effective cooperative incentive mechanism and high data security guarantee. In order to solve this problem, this paper proposes a blockchain-based security cooperation communication scheme for Internet of Vehicles, and designs the detailed workflow of this scheme. In the workflow, a route cooperation scheme based on improved credit value and link lifetime algorithm, an electronic money incentive mechanism based on vehicle type and message type, and a practical byzantine fault tolerance consensus mechanism based on credit improvement (PBFT-CI) are designed for Internet of Vehicles. Analysis results show that the electronic money incentive mechanism can motivate vehicles to participate in cooperation and improve the security of information transmission. PBFT-CI can motivate road side units to participate in consensus and improve the security of the system. Simulation results show that when the number of vehicles is 100 and the number of selfish vehicles is 5, the proposed route cooperation scheme improves the delivery success rate by 0.27 when compared with greedy perimeter stateless routing (GPSR). In addition, the transaction throughput of PBFT-CI is about 1.72 times of that of practical byzantine fault tolerance (PBFT) consensus mechanism.

Keywords: Blockchain, Internet of Vehicles, Secure communication, Electronic money incentive mechanism, Consensus mechanism.

1 INTRODUCTION

Due to the dynamic change of the network topology and no fixed structure of the Internet of Vehicles (IoV), it is difficult to maintain a stable end-to-end connection. One of the solutions to the problem is using the routing cooperation between vehicles [1]. However, there are some urgent problems need to be solved in the routing cooperation between vehicles. For example, vehicles may not be willing to participate in routing cooperation due to rational considerations. Blockchain [2] can solve this problem. As a distributed ledger structure, blockchain has the characteristics of decentralization, programmability, traceability, and anti-tamper [3], so it can provide a trust foundation for untrusted distributed terminals [4-5].

There are some researches on the combination of blockchain and IoV. For example, [6] utilizes the channel characteristics of vehicle-to-vehicle (V2V) communication to generate link fingerprints, and uses a blockchain-based data sharing mechanism to achieve real-time data authentication between vehicles. The method in [6] only considers the communication between three vehicles, it is not applicable to the communication between more vehicles, but in our work, we consider the routing cooperation among more vehicles and improve the security of data communications. [7] proposes a secure communication strategy for the IoV based on blockchain, for the communication between vehicle and vehicle and between vehicle and road side unit (RSU), [7] designs processes such as identity registration based on elliptic curve algorithms, trust assessment, and secure communication to resist internal attacks and external attacks of the IoV and improve the security of data transmission. However, [7] only studies the communication between a source and a destination in IoV, and its Raft consensus mechanism cannot prevent attacks from external malicious nodes, and the entire network is relatively fragile when encountering external attack. [8] uses blockchain to achieve the trust management in high protocol layer for vehicle cooperative communication, selects the most credible vehicle to forward data. However, [8] does not design a corresponding incentive mechanism to reward the relay vehicle, and does not mention which consensus mechanism should be used to perform the block consensus, so it cannot guarantee the security of data communication in low protocol layer. [9] proposes a routing protocol based on

blockchain to improve the secure of IoV communication. Although the blockchain technology is combined with routing protocol, the routing protocol in [9] only focuses on the selection of vehicles to forward data packets for source and destination vehicles, and it does not consider the impact of packet loss of selfish vehicles and the link stability between vehicles, and does not consider the incentive strategy to motivate vehicles to participate in cooperation.

Summarizing literatures [6-9], it is found that although these existing researches combine blockchain with IoV routing cooperation communication, they do not consider the impact of packet loss of selfish vehicles, selfish vehicles may drop packets resulting in low delivery success rate. That's to say, these cooperative routing [6-9] cannot provide high delivery success rate for information transmission. Moreover, in researches [6-9], it is difficult to ensure that a vehicle will not tamper with the forwarding information, and there is no corresponding cooperative incentive mechanism to promote vehicles actively and honestly participate in communication. So, existing IoV routing cooperation with blockchain lacks effective cooperative incentive mechanism of vehicles and high security of data transmission. Therefore, this paper designs a blockchain-based security cooperation communication scheme for IoV, which improves the security of data transmission in routing cooperation, and adopts a cooperative incentive mechanism to motivate vehicles actively and honestly participate in cooperation.

Designing a blockchain-based security cooperation communication scheme for IoV needs to consider three aspects: the design of routing algorithm, the design of incentive mechanism to promote vehicles actively and honestly participate in cooperation, and the design of blockchain consensus mechanism that is suitable for IoV. The research backgrounds of these three aspects are described in details below.

In the design of routing algorithm in IoV, the traditional greedy perimeter stateless routing (GPSR) algorithm [10] only relies on the distance between neighbor vehicle and destination vehicle to select the next hop relay, due to the high-speed movement of the vehicles, when the distance between vehicles exceeds one hop communication distance, the transmission is failure. [11] proposes an improved GPSR routing algorithm adding link lifetime, which reduces the overall end-to-end delay and improves the delivery success rate. However, [10-11] do not consider the impact of packet loss of selfish vehicles and information tampering of malicious vehicles. [12] proposes an improved GPSR routing algorithm based on the Dempster-Shaffer (D-S) evidence theory, and its trust model effectively detects the malicious nodes in the network, and improves network safe. To sum up, researches in [10-12] do not consider blockchain, and do not establish the trust foundation between vehicles, so they cannot guarantee the security of the whole communication system. Considering the communication safety in IoV, this paper uses blockchain to establish the trust foundation between vehicles, and proposes an improved GPSR routing algorithm based on credit value and link lifetime (C-L) (which is referred to improved C-L algorithm), this algorithm uses data packets to record routing cooperation information. After the source vehicle collects the routing cooperation information, the credit values of vehicles are estimated. After the credit values are recorded in the blockchain in RSUs, effective management is implemented, and the credit values are considered in the routing selection, so as to improve the delivery success rate and the security of information transmission.

In real life, vehicles cannot selflessly forward information for other vehicles. Therefore, the blockchain-based security cooperation communication scheme for IoV needs to design a corresponding incentive mechanism to promote vehicles to participate in cooperation. [13] proposes an in-vehicle cloud incentive mechanism based on the stackelberg game. In the in-vehicle cloud incentive mechanism, the two-stage sub-games are introduced to maximize their own benefits, but the process of the two sub-games is relatively complicated, which cannot meet the low-latency requirements of IoV communication. In addition, [13] does not consider the distinguish of the types and priorities of messages. [14] proposes a peer-to-peer reciprocity strategy based on cooperation, which can improve the decision-making of bad behaviors in vehicular ad hoc networks, so as to strengthen the cooperation of the medium access control layer. However, the realization process of the incentive mechanism in [14] is complicated, and it cannot be applied to the asymmetric network environment. [15] proposes a hybrid incentive mechanism based on reputation mechanism. The incentive mechanism in [15] motivates vehicles to participate in cooperation through the behavior of source vehicles paying electronic money, and introduces fund management center to solve the problem of service pricing between vehicles and decrease the selfish behaviors of vehicles. Summary references [13-15], it can be found that the incentive mechanisms in [13-15] are bases on trusted third party to manage transactions. When the trusted third party is attacked by external threats, the entire system will face the risk of paralysis. Therefore, this paper proposes an incentive mechanism based on blockchain, which is the electronic money incentive mechanism based on

vehicle type and message type. It uses blockchain (trusted third party) to establish the trust foundation between vehicles, and considers the type of vehicle and the type of forward message. According to the vehicle type and message type, vehicles are rewarded with different electronic money, which improves the enthusiasm of the vehicle to participate in cooperation. In addition, the entire cooperative communication scheme records transaction information and vehicles' credit value based on the distributed storage structure of blockchain, and builds a secure and credible trading platform.

In the aspects of the consensus mechanism design in blockchain, [7] adopts the Raft consensus mechanism in the data consensus, uses RSU to store the historical information of the vehicle and execute the consensus. Although the Raft consensus mechanism has low consensus delay, it has poor security and cannot tolerate attacks from malicious nodes. [16] designs a blockchain-based fog computing resource management scheme, this resource management scheme encourages parked vehicles to contribute resources to RSU, so as to rapid achieve a large-scale proof of work (PoW) consensus. Although the PoW mechanism has the advantages of decentralization and high security, it requires all nodes to compete for "mining", which brings high computing resource consumption. Therefore, the consensus mechanisms of [7] and [16] are not suitable for IoV. [17] applies the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism to IoV to ensure the consistency of network ledger. Comparing with PoW, PBFT does not require nodes to rely on computing power to "mine", which reduces the resource consumption and reduces consensus delay. However, the selection of the leader node in PBFT is relatively random, and the optimality of the leader node cannot be guaranteed. When the selected leader node is a malicious node, the security of the system is greatly reduced. Moreover, the three-phase consensus of PBFT requires two times broadcast of all nodes, the communication overhead is high. In order to motivate RSUs to participate in consensus, improve the security of the system and reduce the communication overhead, this paper designs a PBFT consensus mechanism based on credit improvement (PBFT-CI) for IoV. On the basis of the PBFT, the leader node is selected according to credit value threshold (CVT), and in the commit stage, the communication overhead is reduced.

The main contributions of this paper are as follows:

(1) A blockchain-based security cooperative communication scheme for IoV is proposed, and the detailed workflow of this scheme is designed, includes system initialization, routing cooperation based on improved C-L algorithm, electronic money transaction and blockchain consensus based on PBFT-CI consensus mechanism.

(2) A routing cooperation scheme based on improved C-L algorithm is designed, it uses blockchain to record credit evaluation, and considers the credit value in the relay selection, so it can improve the delivery success rate of routing cooperation.

(3) An electronic money incentive mechanism based on vehicle type and message type is designed. According to the vehicle type and message type, vehicles are rewarded with different electronic money, which improves the enthusiasm of the vehicle to participate in cooperation.

(4) The PBFT-CI consensus mechanism is designed to improve the security of the system, motivate RSUs to participate in consensus and reduce communication overhead.

2 SYSTEM MODEL

As shown in Fig. 1, the system model for blockchain-based security cooperation communication scheme can be divided into three layers: data transmission layer, data consensus layer, the data storage layer. Vehicles and RSUs that participate in the network communication need to register their identity in the certificate authority (CA). A vehicle uses its own on-board unit (OBU) to communicate with other vehicles and RSUs, RSUs communicate with each other through wired optical fibers. In order to complete the multi-hop routing cooperation between vehicles, source vehicle and relay vehicles (collectively referred to as the sending vehicles) obtain the location and speed information of surrounding vehicles from RSUs. Then sending vehicles combine this information with pre-recorded vehicles' credit value (given by the credit value evaluation in section 4.1.1) and other information, carry out relay selection for cooperative communication (The routing cooperation scheme based on improved C-L algorithm is detailed in section 4.1). After the message transmission is completed, the related electronic money transaction is carried out, and the routing cooperation information of the vehicles will be uploaded to RSUs. In the data consensus layer, RSUs act as consensus nodes in the blockchain to perform data consensus. After all nodes reach a consensus for a new block, the leader node uploads the block to the data storage layer.

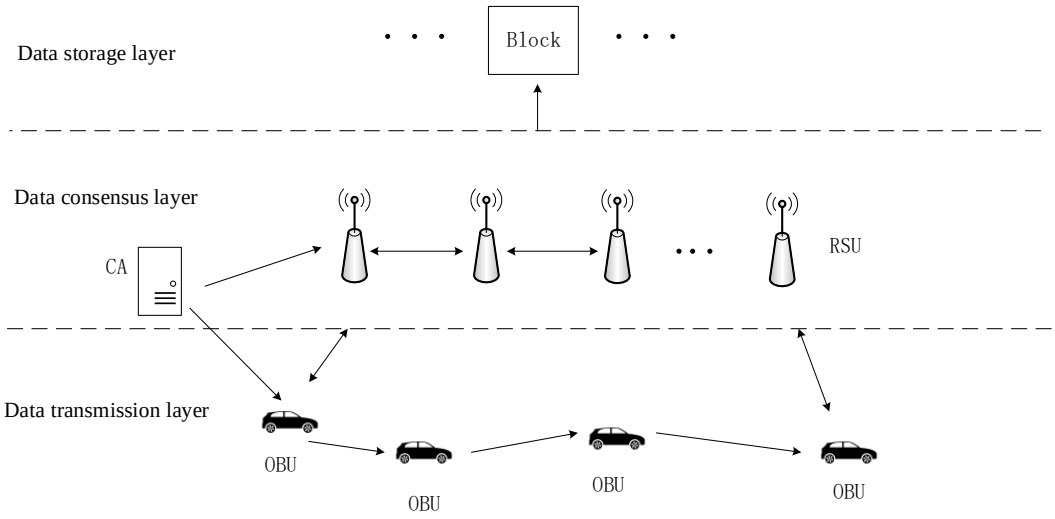

Fig. 1. System model for Blockchain-based security cooperation communication scheme

3 THE WORKFLOW OF BLOCKCHAIN-BASED SECURITY COOPERATIVE COMMUNICATION SCHEME

In order to realize the security cooperative communication for IoV, we design the workflow of blockchain-based security cooperation communication scheme for IoV. The detailed workflow is as follows.

1. System initialization. Vehicles and RSUs participated in IoV communication register in CA. Vehicle j initializes its wallet address W_j, electronic money value BC_j, vehicle credit value (VCV) VCV_j, asymmetric keys and symmetric keys. RSU_n initializes its credit value RCV_n. The initial credit values of all vehicles and RSUs are equal to M. Each vehicle has a pair of asymmetric keys (including public and private keys) and a pair of symmetric keys (where the encryption and decryption keys are the same). The key pairs for each vehicle are different. The asymmetric keys are used to encrypt the symmetric key and to digitally sign, public key is public to all vehicles, and private key is only stored by the vehicle itself. The symmetric keys are used to encrypt the source message and can be updated at any time.
2. Routing cooperation based on improved C-L algorithm. The process of the routing cooperation scheme mainly includes: (1) Cooperation message initialization. Generating data packets for recording relay cooperation information and carrying encrypted source message. (2) Routing cooperation. The source vehicle transmits the data packet to the destination vehicle by adopting the relay decision based on improved C-L algorithm. (3) Credit evaluation. The source vehicle evaluates the credit values of relay vehicles according to the data packet information. The routing cooperation scheme based on improved C-L algorithm is detailed in section 4.1.
3. Electronic money transactions. According to the behavior of vehicles in routing cooperation stage, the electronic money incentive mechanism based on vehicle type and message type is used to reward relay vehicles with electronic money. The electronic money incentive mechanism based on vehicle type and message type is detailed in section 4.2.
4. Blockchain consensus based on PBFT-CI consensus mechanism. After the vehicle's routing cooperation and electronic money transaction, vehicles transmit electronic money transaction records and vehicles' credit values to RSUs, and RSUs conduct blockchain consensus based on PBFT-CI consensus mechanism to record transaction records and vehicles' credit values. The PBFT-CI consensus mechanism is detailed in section 4.3.

4. ROUTING COOPERATION SCHEME, ELECTRONIC CURRENCY INCENTIVE MECHANISM AND CONSENSUS MECHANISM

4.1 Routing cooperation scheme based on improved C-L algorithm

4.1.1 The process of route cooperative scheme based on improved C-L algorithm

The routing cooperation scheme based on improved C-L algorithm includes following steps:
1) Cooperation message initialization

In IoV communication, source vehicle needs to use a data packet to record relay cooperation information and carry source message to the destination vehicle. Fig. 2 shows the structure of the data packet. The data packet structure includes a header and a data part. The header contains the header length, service type, message ID, data type, message time to live (TTL), the routing protocol adopted (the routing cooperation scheme based on the improved C-L algorithm in this paper), the total length of the message, the sending time and the receiving time of the message, the ID information of source vehicle, destination vehicle and relay vehicles.

When the source vehicle needs to send a message, it first encrypts the source message by using its symmetric key, and then encrypts the symmetric key by using public key of the destination vehicle. After that, the source vehicle performs hash operation on the encrypted source message content to obtain the message digest, and digitally signs message digest by using its private key. So, the data part in the data packet (Fig.2) including the encrypted symmetric key, the digital signature of message digest and encrypted source message.

<table>
<tr><td rowspan="6">Hea-
der</td><td>Header length</td><td>Service type</td><td>message time
to live</td><td>Protocol</td></tr>
<tr><td>Message ID</td><td>Type of data</td><td colspan="2">Total length</td></tr>
<tr><td colspan="2">Send time</td><td colspan="2">Receive time</td></tr>
<tr><td colspan="4">Source ID</td></tr>
<tr><td colspan="4">Destination ID</td></tr>
<tr><td colspan="4">Relay ID (Variable length)</td></tr>
<tr><td colspan="5">Data part</td></tr>
</table>

Fig. 2. Structure of data packet

2) Routing cooperation

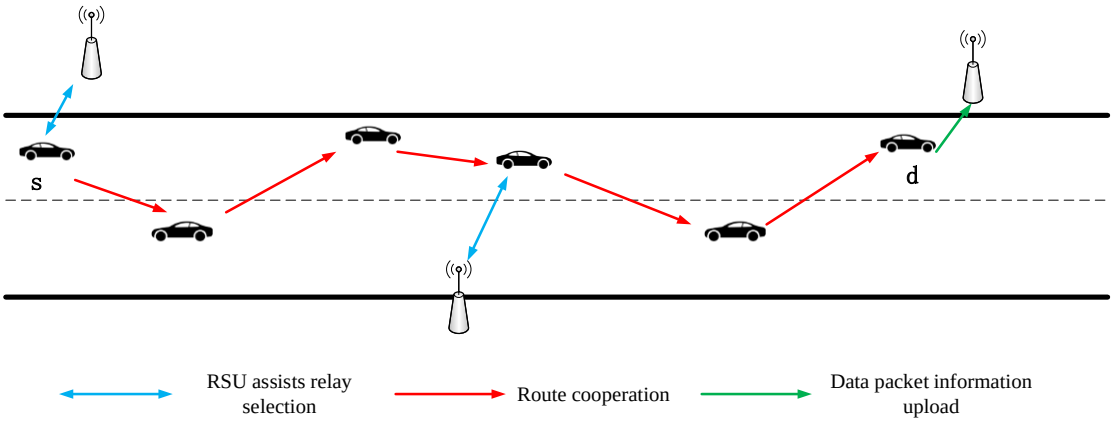

Fig. 3. Routing cooperation

As shown in Fig. 3, the source vehicle s needs to send data packet to the destination vehicle d, and RSUs assist s and relay vehicles to select the next hop vehicle. After obtaining the location and speed of the neighbor vehicle, the location of d, and the credit values (which are calculated by the credit evaluation in the next step) of vehicles, the improved C-L algorithm is used to make the next hop relay decision. Thus, data packet is transmitted to the destination vehicle via multiple hops.

In order to realize data confidentiality, the workflow of proposed cooperation communication scheme incorporates many encryption and decryption operations as confidentiality measures. During the

process of forwarding source message, each relay vehicle first decrypts the digital signature by using public key of previous relay vehicle (the first relay uses the public key of source vehicle) to confirm the validity of data packet while obtaining encrypted source message and message digest A. then, it calculates hash value of the encrypted source message to obtain the message digest B. Comparing A and B, if A and B are different, it can be determined that the previous relay tampered with the source message. If A and B are the same, it digitally signs message digest by using its private key, adds the digital signature into the data part (of data packet) and adds its relay ID into the header (of data packet), then sends the modified data packet to the next relay vehicle.

After the destination vehicle obtains the data packet, it also uses the operations as relay vehicle to verify whether the source message has been tampered. After the verification, destination vehicle uses its private key to decrypt the encrypted symmetric key (which is in the data part of data packet) and obtains the symmetric key of source vehicle, then it decrypts the source message by using this symmetric key. After all these operations, destination vehicle uploads the relay cooperation information to nearby RSU. And then, the relay cooperation information is transmitted to s through RSUs.

If data packet lost or tampered during the forwarding, that is, after RSU assists a relay vehicle to determine its next relay vehicle, but its next relay vehicle does not receive the forwarded information after a fixed time, or a relay verifies that its previous relay has tampered with the source message. The relay vehicle will upload the communication failure information (including the ID of malicious vehicles) to the nearby RSU, and transmit it to s through RSUs. Then, s will resend the source message.

3) Credit evaluation

After getting the relay cooperation information or communication failure information, s evaluates credit values of all participating relay vehicles. The credit value evaluation of vehicle *j* is

$$VCV_j = VCV_{j,i-1} + VCV_j^{prize} - VCV_j^{penalty} \tag{1}$$

where $VCV_{j,i-1}$ is the last evaluated credit value of vehicle j. $VCV_j^{prize} = P \times e$ is the reward credit value of the vehicle j. e is the number of times for honest forwarding information, P is the credit value reward by once honest forwarding, $VCV_j^{penalty} = Q \times g + N \times h$ is the penalty credit value, g,h represent the times of packet loss and malicious information tampering by vehicle j respectively. Q,N represent the credit value penalty weights for packet loss and information tampering occurs respectively.

4.1.2 Improved C-L routing algorithm

The improved C-L routing algorithm is an improvement on the traditional GPSR routing algorithm. In traditional GPSR routing algorithm, when the source vehicle wants to send message to the destination vehicle, the source vehicle knows the distances between neighbor vehicles (within the communication range of source vehicle) and destination vehicle, and selects the neighbor vehicle that is closest to the destination vehicle as the first relay vehicle. After the message is forwarded to the first relay vehicle, the first relay vehicle becomes the sending vehicle, and then the same method is used to select the second relay vehicle. This process is repeated until the destination vehicle receives the source message. That is to say, for traditional GPSR routing, the greedy algorithm is used to establish the routing. When the sending vehicle cannot find a neighbor vehicle that is closer to the destination vehicle than it is own (i.e., a routing hole occurs), the surrounding forwarding is used until the routing hole is avoided.

The link lifetime between the sending vehicle *i* and its neighbor vehicle *j* is

$$T_{i,j} = \frac{-(ab+cd) + \sqrt{(a^2+c^2)r^2 - (ad-bc)^2}}{a^2+c^2} \tag{2}$$

where $a = v_i \cos\theta_i - v_j \cos\theta_j$, $b = x_i - x_j$, $c = v_i \sin\theta_i - v_j \sin\theta_j$, $d = y_i - y_j$ .v_i,v_j represent the speed of the sending vehicle and the neighbor vehicle respectively, θ_i, θ_j represent the angle between v_i and the horizontal direction, and the angle between v_j and the horizontal direction respectively. x_i,y_i represent the horizontal and vertical coordinates of sending vehicle *i* respectively, x_j,y_j represent the horizontal and vertical coordinates of neighbor vehicle *j* respectively, r is the communication range of the sending vehicle.

The traditional GPSR routing only considers distance to determine the next hop relay. The improved C-L algorithm comprehensively considers distance, link lifetime and credit value, uses a utility function to determine the next hop relay. Then the utility function of the improved C-L algorithm is defined as

$$U_j = \xi_1 L + \xi_2 \frac{\lambda_1}{T_{i,j}} + \xi_3 \frac{\lambda_2}{VCV_j} \quad (3)$$

Where L is the distance between the neighbor vehicle and the destination vehicle, VCV_j is the credit value of the neighbor vehicle j, and ξ_1, ξ_2, ξ_3 are the weight factors ($\xi_1, \xi_2, \xi_3 \in (0,1)$), λ_1, $\lambda_2$are the harmonic factors. The improved C-L algorithm selects the neighbor vehicle with the smallest utility function value as the next hop relay vehicle. The longer the link lifetime $T_{i,j}$ and the higher the credit value VCV_j, the greater the probability of being selected as the next hop relay. The credit value needs to be obtained through honest forwarding message. According to expression (1), in order to be selected as a relay to obtain electronic money, vehicles are more willing to be honest nodes than malicious nodes. So, by linking credit value and link lifetime with next hop relay selection, the improved C-L algorithm can encourage vehicles to participate in cooperation, and improve the security of transmitted message.

4.2 Electronic money incentive mechanism based on vehicle type and message type

After the routing cooperation, electronic money rewards need to be given to the vehicles participating in cooperation. Based on the special application of IoV communication, this paper designs an electronic money incentive mechanism based on vehicle type and message type to promote vehicles to participate in cooperation. The specific steps of the electronic money incentive mechanism are as follows:

1) Determination the vehicle type for all participating vehicles. In the electronic money incentive mechanism, vehicle types are mainly classified as source vehicle, relay vehicle, and destination vehicle.
2) Determination the message type for all participating vehicles. In the IoV communication, messages are mainly divided into three categories: a) Warning messages: warning messages are sent by one vehicle to other vehicles, warning messages includes road hazards, vehicle collision warnings, etc. b) Notification messages: notification messages are sent by traffic system to vehicles. c) Service messages: service messages are multimedia resource information required by vehicles, such as audio and video information.
3) Determination the payer of electronic money reward. Warning messages are more urgent and have higher requirements of delivery delay than other messages, so the electronic money reward should be inversely proportional to the delivery delay. Notification messages are sent by traffic system, the corresponding source vehicle in table 1 represents the first relay vehicle to forward this message. Unlike warning messages that require low delivery delay, the longer vehicle forwarding time, the more electronic money rewards. Warning messages and notification messages are required by vehicles, so electronic money should be paid by system. For service messages, it is required by vehicles, so the electronic money should be paid by the destination vehicle and the electronic money reward is proportional to the delivery delay.

Table 1 shows the calculation method of electronic money reward (negative value means spending) for different vehicle types and different message types. m_1, m_2, and m_3 represent the base value of electronic money for warning, notification, and service message respectively. $Time^{delivery}$ indicates the time that the relay vehicle delivers (or forwards) the message. q_3 is the electronic money reward for a unit message block, $message_{size}$ is the size of the total forwarding service message, $message_{basis}$ is the size of a unit message block. δ is the electronic money deducted for discarding and tampering with message, if the vehicle honestly forwards message, $\delta = 0$. Therefore, vehicles can obtain different electronic money rewards by forwarding different messages, and these rules are fair and beneficial to all relay vehicles.

This electronic money reward mechanism may cause participating vehicles to consume electronic currency to a negative value. Once the electronic money of a participating vehicle becomes negative, it can apply for credit funds from the system. And, it can participate in routing cooperation to obtain electronic money, thereby making its electronic money return to positive. This measure can motivate more vehicles to actively and honestly participate in routing cooperation and ensure the continued viability of the system. Electronic money transactions are recorded in blockchain, so electronic money transaction based on blockchain can establish trust foundation among vehicles and promote vehicles to actively and honestly participate in information forwarding. That's to say, the electronic money incentive mechanism based on vehicle type and message type can form an effective incentive.

Table 1. The calculation method of electronic money reward

message type / electronic vehicle money type	warning message	notification message	service message
source vehicle	$m_1 \times \frac{1}{\text{Time}^{\text{delivery}}} - \delta$	$m_2 \times \frac{\text{Time}^{\text{delivery}}}{\text{TTL}} - \delta$	$q_3 \times \frac{\text{message}_{\text{size}}}{\text{message}_{\text{basis}}} - \delta$
relay vehicle	$m_1 \times \frac{1}{\text{Time}^{\text{delivery}}} - \delta$	$m_2 \times \frac{\text{Time}^{\text{delivery}}}{\text{TTL}} - \delta$	$m_3 \times \frac{\text{Time}^{\text{delivery}}}{\text{TTL}} - \delta$
destination vehicle			$-(m_3 \times \frac{\text{Time}^{\text{delivery}}}{\text{TTL}} + q_3 \times \frac{\text{message}_{\text{size}}}{\text{message}_{\text{basis}}})$

4.3 PBFT-CI consensus mechanism

4.3.1 The consensus process of PBFT-CI

The selection of the leader node in PBFT mechanism is random. If the malicious node is selected, system security cannot be guaranteed. And in PBFT, three-phase consensus needs nodes to broadcast block information to each other twice, the communication overhead is high. Therefore, in this paper, we improve the selection method of the leader node and simplify the consensus process of PBFT, propose PBFT-CI consensus mechanism.

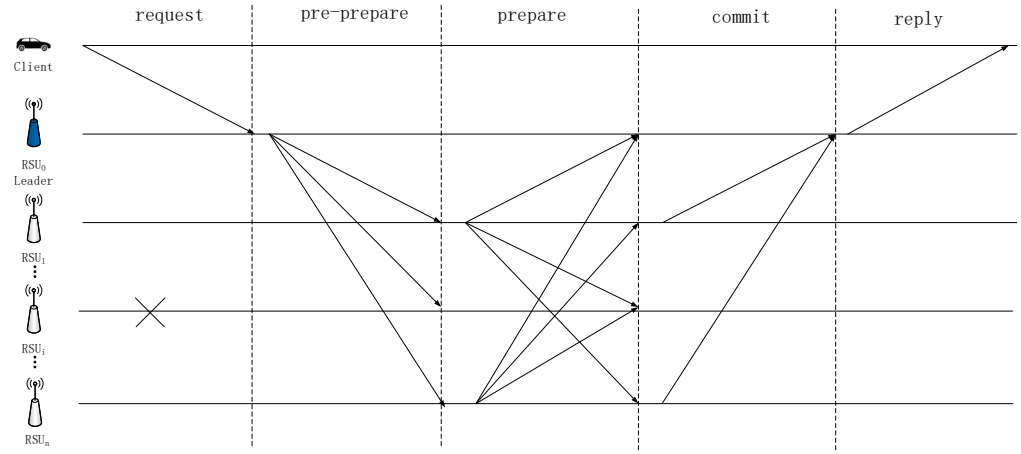

Fig. 4. The workflow of PBFT-CI consensus mechanism

As shown in Fig. 4, RSUs are consensus nodes, vehicles are client nodes that initiate consensus request. One replica node (i.e.RSU_0) acts as the leader node, $RSU_1 \ldots RSU_i \ldots RSU_n$ are backup nodes (consensus nodes except for leader node), RSU_i is malicious or faulty node, and the maximum number of malicious or faulty node is f=(n-1)/3. Unlike PBFT, in the commit stage in PBFT-CI, the leader node is responsible for collecting confirmation information. The detail process of the consensus mechanism is as follows:

(1) Request stage: When the block generation time comes, client nodes initiate a block request to the leader node (The leader node is selected through the leader node selection mechanism in section 4.3.2).

(2) Pre-prepare stage. The leader node packages all transactions (including electronic money transaction records and vehicles' credit values) to generate a new block and broadcasts the new block to all backup nodes.

(3) Prepare stage: Each backup node verifies the new block and send verification success or verification failing message to all other replica nodes. If the verification success message received by the replica node is greater than or equal to $2f+1$ [18], the prepare stage is completed.

(4) Commit stage: All backup nodes send confirmation messages to the leader node. If the leader node receives the verified confirmation messages sent by more than $2f+1$ nodes, it means that most nodes have reached a consensus on the new block. Otherwise, return to step (2), re-selecting a leader node, regenerating a new block and conducting the consensus of the new block until the consensus is success.

(5) Reply stage: The leader node replies to client nodes, and writes the new block into the blockchain.

4.3.2 Leader node selection mechanism

The leader node selection mechanism means a leader node is selected from RSUs whose credit value is greater than the credit value threshold (CVT). This selection mechanism can reduce the probability that a dishonest node is selected as leader node.

1) RSU credit value evaluation

Whether consensus nodes can successfully generate and verify blocks is important, so detecting node failures or malicious behaviors is an important factor that need to be considered in the credit value evaluation of RSUs. Therefore, the credit value of RSU n is defined as

$$RCV_{n,m} = RCV_{n,m-1} + \psi - \eta \quad (4)$$

Where $RCV_{n,m-1}$ is the last credit value of RSU_n. ψ is the credit value rewarded when RSU_n successfully generates block and verifies block. And η is the credit value punishment when RSU_n has failure or malicious behavior.

2) Selection of the leader node

The median value of all RSUs' credit values is set as CVT. The leader node is randomly selected from the nodes with credit value higher than CVT. In this way, high credit value of leader node can be guaranteed, and accounting rights will not be concentrated on malicious nodes (or dishonest node). So, this leader selection method can not only improve the security of system, but also ensure the fairness of consensus nodes. In addition, leader node can obtain accounting rewards given by the system, but only the RSU with high credit value can be selected as leader node, and the credit value can only be got from honest generating block and verifying block, so RSUs are more willing to participate in honest generating and verifying block to obtain accounting rights and rewards, this leader selection method (or PBFT-CI consensus mechanism) can motivate RSUs to participate in consensus and improve the security of system.

4.4 Advantages of blockchain-based security cooperation communication scheme

The proposed blockchain-based security cooperation communication scheme has the following advantages:

(1) The credit values of relay vehicles are recorded into blockchain, and the vehicle credit values are considered in routing selection, this can reduce the probability packet loss by selfish vehicles and information tampering by malicious vehicles, and improves the safe of information transmission.

(2) The electronic money incentive mechanism gives vehicles different electronic money rewards according to different vehicle types and message types, distinguishes the priority of messages, and improves the enthusiasm of vehicles to participate in cooperation.

(3) The PBFT-CI consensus mechanism selects the leader node with high credit value more than CVT, this can reduce the probability of dishonest node selected as leader node. In addition, PBFT-CI is simplified from PBFT, it can reduce communication overhead.

5. SIMULATION RESULTS AND DISCUSSION

5.1 Simulation results of routing cooperation scheme based on improved C-L algorithm

In order to illustrate the performance of the routing cooperation scheme proposed in this paper, simulations compare the performance of proposed routing cooperation scheme (improved C-L for short), the improved GPSR routing scheme with link lifetime considered in [9] (L-GPSR for short), and the traditional GPSR routing scheme in [8]. The experimental simulation parameters are given in table 2. Because the main performance index is the delivery success rate of routing cooperation, the influence of

selfish vehicles is mainly simulated, the analysis of malicious vehicles has been given in section 4.4.

Table 2. Simulation parameters

parameter	value
number of vehicles	1-200
number of selfish vehicles	1-20
area	1000m*1000m
vehicle communication radius	250m
number of RSUs	6
initial credit value M	100
P	10
Q	10
ψ	10
η	10
improved C-L algorithm weight factor ξ_1,ξ_2,ξ_3	0.8、0.1、0.1
L-GPSR algorithm weight factor ξ_1,ξ_2	0.9、0.1
λ_1,λ_2	1000、10000

Fig. 5 shows the variation of delivery success rate with the number of vehicles when the number of selfish vehicles is equal to 5. It can be clearly seen that the delivery success rate of the three schemes increases with the number of vehicles. When the number of vehicles exceeds 80, delivery success rates become almost no longer increased. And the delivery success rate of improved C-L and L-GPSR are significantly higher than that of GPSR. Mainly because improved C-L and L-GPSR take into account the impact of the link lifetime, which reduce the possibility of communication failure due to high-speed vehicle movement. When the number of vehicles is 100 and the number of selfish vehicles is 5, the improved C-L improves the delivery success rate by 0.27 compared with GPSR. It can also be seen that the delivery success rate of improved C-L is slightly higher than that of L-GPSR. The reason is that the vehicle credit is introduced in the selection of relay vehicles, and the packet loss from selfish vehicles is considered. In summary, when the number of vehicles beyond a certain number (about 40), the improved C-L can improve the delivery success rate.

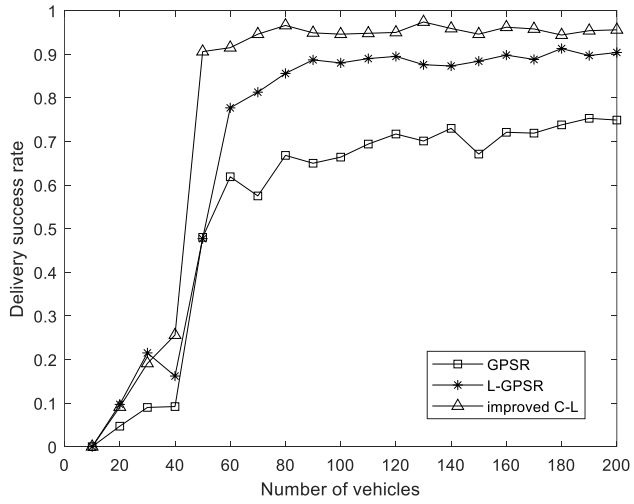

Fig. 5 The delivery success rate varies with the number of vehicles

Fig. 6 shows the delivery success rate varies with the number of selfish vehicles. It can be seen that, as the number of selfish vehicles increases, the delivery success rate of L-GPSR and traditional GPSR decreases significantly, while the delivery success rate of improved C-L decreases slightly. The main reason is that the increase of selfish vehicles leads to serious packet loss in L-GPSR and GPSR. However, the improved C-L chooses relay vehicles with high credit values, so it can avoid selfish vehicles as much as possible. This means that the improved C-L can reduce the impact of selfish vehicles on packet loss and improve the delivery success rate.

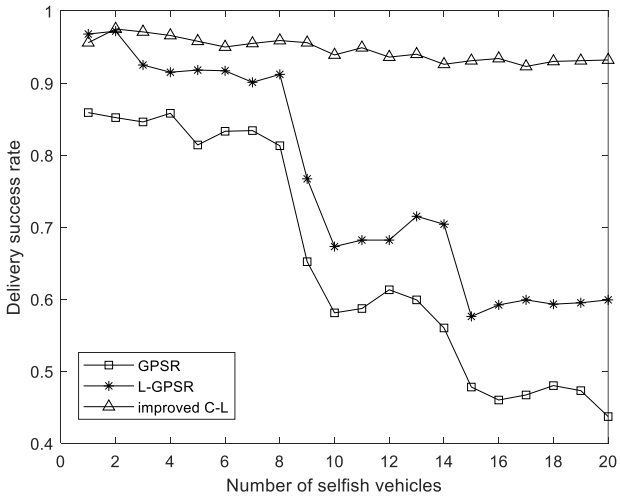

Fig. 6 The delivery success rate varies with the number of selfish vehicles

Fig. 7 reflects the change of the delivery success rate with the maximum speed of vehicles when the number of selfish vehicles is equal to 5. From Fig. 7, it can be clearly seen that with the increase of maximum vehicle speed, delivery success rate of GPSR decreases rapidly, while the delivery success rate of improved C-L and L-GPSR has no obvious decrease. This is because the higher the maximum vehicle speed, the more unstable the link between vehicles. However, improved C-L and L-GPSR consider the link lifetime, so their delivery success rate tends to be stable. The delivery success rate of improved C-L is higher than that of L-GPSR, that is because improved C-L considers vehicle credit value and selects vehicles that honestly participate in cooperation (without tampering with information). That's to say, improved C-L can reduce the impact of packet loss of selfish vehicles and information tampering of malicious vehicles, and improves the security of information transmission.

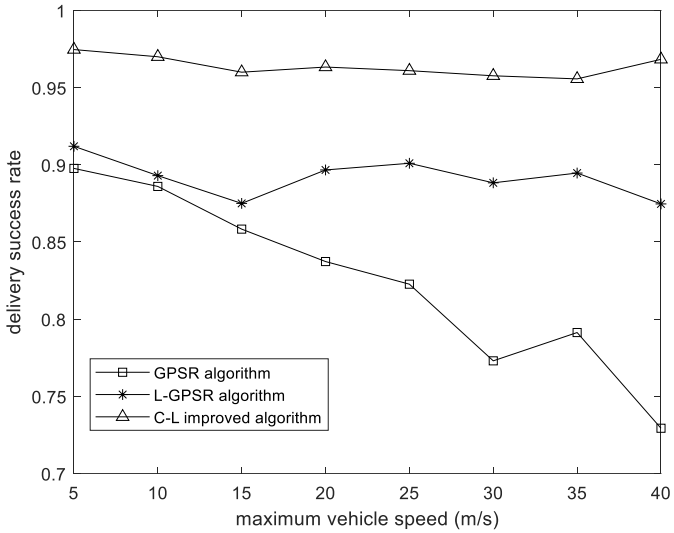

Fig. 7 The delivery success rate varies with the maximum speed of vehicles

Therefore, from Figs. 5,6,7, it can be concluded that the proposed routing cooperation scheme (i.e., improved C-L) has the advantage of improving delivery success rate.

Fig. 8 shows the change of delivery latency with the number of vehicles. It can be seen from the figure 8 that when the number of vehicles is small, as the number of vehicles increases, the number of selectable relays increases, resulting in the decrease in delivery latency for GPSR, L-GPSR, and improved C-L. When the number of vehicles is large, the number of selectable relays saturates, and the delivery latency changes of GPSR, L-GPSR, and improved C-L are no longer obvious. What's more, the improved C-L routing algorithms can obtain the smallest delivery latency when comparing GPSR and L-GPSR. This is due to that the long delivery latency is caused by message delivery failure and the improved C-L has the highest delivery success rate.

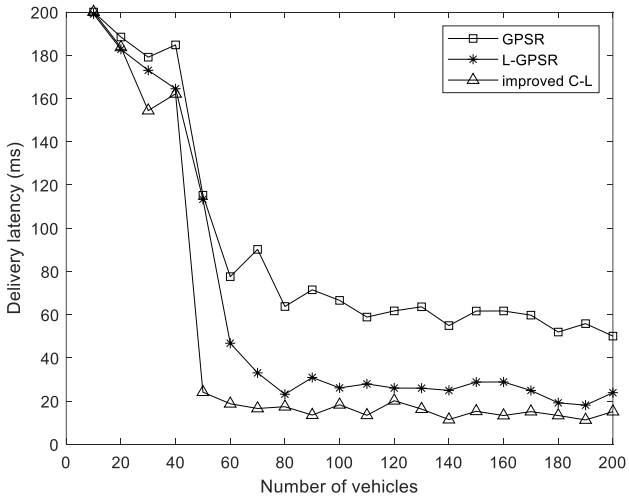

Fig. 8 The delivery latency varies with the number of vehicles

Fig. 9 shows the performance of different settings of ξ_1, ξ_2, ξ_3 for improved C-L algorithm, where (a), (b) and (c) show the performance of the number of message delivery, the lifetime of the link, and the credit value of vehicles, respectively. When $\xi_1 = 0.8, \xi_2 = 0.1, \xi_3 = 0.1$, improved C-L algorithm focuses more on selecting the relay vehicle that is closer to the destination vehicle, so in Fig. 8(a), the number of message delivery for $\xi_1 = 0.8, \xi_2 = 0.1, \xi_3 = 0.1$ is the smallest. When $\xi_1 = 0.1, \xi_2 = 0.8, \xi_3 = 0.1$, improved C-L algorithm focuses more on selecting the relay vehicle with longer link lifetime, so in Fig. 8(b), the link lifetime for $\xi_1 = 0.1, \xi_2 = 0.8, \xi_3 = 0.1$ is the largest. When $\xi_1 = 0.1, \xi_2 = 0.1, \xi_3 = 0.8$, improved C-L algorithm focuses more on selecting the relay vehicle with larger credit value, so in Fig. 8(c), the credit value of vehicles for $\xi_1 = 0.1, \xi_2 = 0.1, \xi_3 = 0.8$ is the largest. In practical systems, suitable ξ_1, ξ_2, ξ_3 can be selected based on different performance requirements of the system.

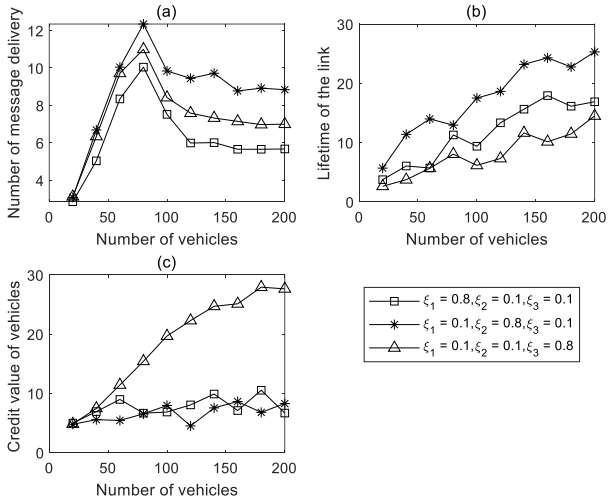

Fig. 9 The performance of different settings of ξ_1, ξ_2, ξ_3

5.2 Simulation results of the effects of encryption and decryption operations on system performance

In order to realize data confidentiality, the workflow of proposed cooperation communication scheme incorporates many encryption and decryption operations as confidentiality measures, such as encryption and decryption of source message, digital signature and verification signature, hash operation. To show the effects of implementing confidentiality measures on the overall efficiency of message transmission and the consumption of computational resources, we give the simulation results of message transmission delay in Fig. 10, and the relay processing time in Fig. 11.

Fig. 10 shows the delay of message transmission for encryption (which means sending message with the encryption and decryption operations in this paper) and without encryption (which means sending message without encryption and decryption). Because the size of the message content encrypted by AES encryption algorithm is about twice that of the without encryption, the transmission delay of each relay vehicle will be twice the original message. When the number of vehicles is small, the success rate of message delivery is low, so the delay is large and the delay gap is small. When the number of vehicles increases, the success rate of message delivery is high, and the delay of encryption and decryption is about twice that of the without encryption and decryption.

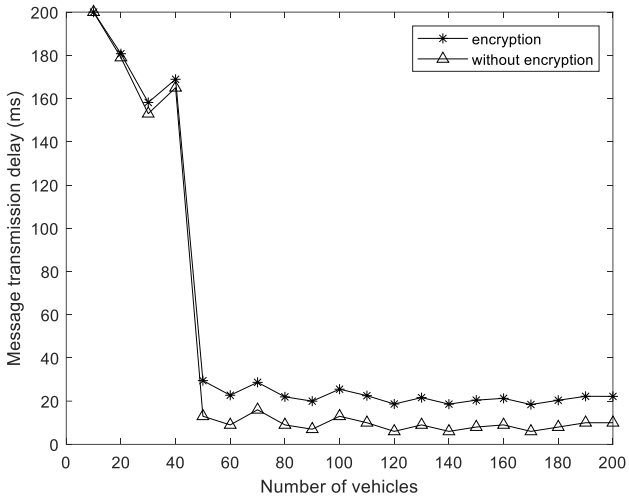

Fig. 10 The message transmission delay for encryption and without encryption

Fig. 11 shows the relay processing time for encryption and without encryption. We use AES symmetric encryption algorithm and RSA asymmetric encryption algorithm in simulations. The AES symmetric encryption algorithm is used to encrypt the source message, and the RSA asymmetric encryption algorithm is used to encrypt the AES key. The destination node uses RSA algorithm to decrypt the AES key, and uses the AES key to decrypt the source message. In Fig. 8, we can see that, the encryption and decryption operations increase processing time by approximately 5ms, due to the proportional relationship between processing time and computing resource consumption, encryption and decryption operations have a little impact on computing resource consumption.

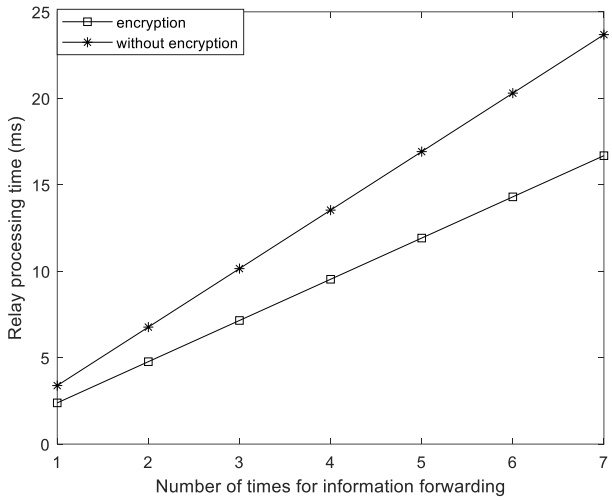

Fig. 11 The relay processing time for encryption and without encryption

5.3 Simulation results of PBFT-CI consensus mechanism

The consensus mechanism is simulated through java language programming. We use message priority queue to simulate the consensus interaction process between multiple consensus nodes, the

number of consensus nodes is set to 6, the initial mining difficulty value is set to 7, and 10000 transactions are generated per second. The capacity of a block is set to 512Mbit, and 1Mbit capacity can record about 6 transactions. In simulations, the PoW in [19], the Casper friendly finality gadget (Casper FFG) in [20] and the PBFT are compared with PBFT-CI consensus mechanism. Fig. 12 shows the changes of throughput with the times of consensus for these four consensus mechanisms. Among them, the PoW has the lowest throughput, mainly because the PoW relies on node computing power for "mining", which greatly increases the block generation time. The reason for the fluctuation of PoW throughput is that the mining difficulty will be adjusted for each consensus. The Casper FFG adds Proof of Stake verification to PoW. The reason why its throughput is higher than that of PoW is that Casper FFG is based on the ethereum platform, the block generation time is about 15s, so its throughput is maintained at 20 tps, “tps” means transactions per second. The throughput of PBFT and PBFT-CI is much higher than that of Casper FFG and PoW. The main reason is that PBFT and PBFT-CI do not rely on the computing power of nodes, and their consensus is three-phase protocol. The transaction throughput of PBFT-CI is about 1.72 times of that of PBFT. This is because that PBFT-CI is improved from PBFT, the leader node is selected through the credit value and CVT, and this method can reduce the probability that a malicious node is selected as leader. In the commit stage in PBFT-CI, the number of messages sent and received between nodes are reduced, so the throughput can be improved, and the consensus efficiency can be improved.

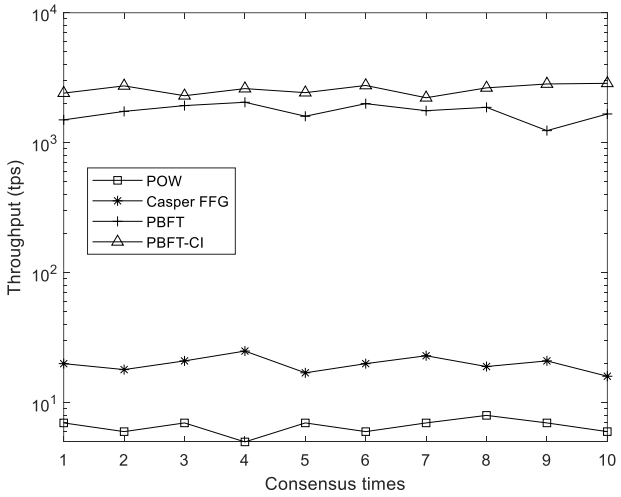

Fig. 12 The throughput varies with the number of consensus nodes

6. CONCLUSIONS

This paper proposes a blockchain-based security cooperation communication scheme for IoV. The detailed workflow of this scheme is designed. In the workflow, a routing cooperation scheme based on improved C-L algorithm, an electronic money incentive mechanism based on vehicle type and message type, and a PBFT-CI consensus mechanism are designed. Theoretical analysis shows that the electronic money incentive mechanism distinguishes the type of vehicle and the priority of messages, uses electronic money to motivate vehicles to actively and honestly participate in cooperation, and it can improve the enthusiasm of vehicles to participate in cooperation. Simulation results show that the routing cooperation scheme based on improved C-L algorithm considers vehicle credit value in routing cooperation, improves the delivery success rate with low delivery latency, and improves the security of information transmission. Comparison with PBFT, proposed PBFT-CI consensus mechanism improves transaction throughput and consensus efficiency.

REFERENCES

1. A. khan, M. Ishtiaq, S. Anwar and M. A. Shah, "A Survey on secure routing strategies in VANETs," *2019 25th IEEE International Conference on Automation and Computing (ICAC)*, 2019, pp. 1-6.
2. Y. K. Tomov, "Bitcoin: Evolution of Blockchain Technology," *in 2019 IEEE International Scientific Conference Electronics (ET)*, 2019, pp. 1-4.
3. C. Dai, H. Luan, X. Yang, X. Guo, Z. Lu, B. Niu, "Overview of Blockchain Technology," *Computer Science*, Vol. 48, 2021, pp. 500-508.
4. H. Zhi, Y. Wang, H. Ge, "A cooperative communication scheme based on blockchain," *AEU - International Journal of Electronics and Communications*, Vol.142, 2021.
5. Z. Liao, X. Pang, J. Zhang, B. Xiong , J. Wang, "Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, 2022, pp. 1159-1175.
6. M. Kamal, G. Srivastava, M. Tariq, "Blockchain-Based Lightweight and Secured V2V Communication in the Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, no. 7, 2021, pp. 3997-4004
7. Z. Li, G. Zhang, W. Chen, "Blockchain-based Secure Communication Strategy for Internet of Vehicles," *Computer Engineering*, Vol. 47(10), 2021, pp. 43-51.
8. E. M. Ghourab, M. Azab, N. Ezzeldin, "Blockchain-Guided Dynamic Best-Relay Selection for Trustworthy Vehicular Communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, 2022, pp. 13678-13693.
9. K. Mershad, B. Said, "A Blockchain Model for Secure Communications in Internet of Vehicles," *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, 2020, pp. 1-6.
10. Brad Karp, H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp.243–254.
11. K. Liu, "Research and implementation of VANET routing," Beijing University of Posts and Telecommunications, 2018. MA thesis.
12. J. Yang, Y. Zhang, B. Liu, P. Xu, Y. Chi., "Improved GPSR algorithm based on D-S theory in VANET," *Computer Engineering and Design*, Vol. 40, 2019, pp.2411-2415.
13. H. Liu, "Research on vehicle cooperation incentive mechanism toward vehicle cloud," Beijing Jiaotong University, 2018. MA thesis.
14. D. Al-Terri, H. Otrok, H. Barada, M. Al-Qutayri, Y. Al Hammadi, "Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs," *Computer Communications*, Vol. 104, 2017, pp. 108-118.
15. H. WANG, Z. Chen, J. WU and L. WANG, "Node Incentive Mechanism in Selfish Opportunistic Network," *KSII Transactions on Internet and Information Systems*, Vol. 13, 2019, pp.1481-1501.
16. M. Kong, J. Zhao, X. Sun and Y. Nie, "Secure and efficient computing resource management in blockchain-based vehicular fog computing," *China Communications*, Vol.18, no.4, 2021, pp.115-125.
17. Z. Ma, L. Wang and W. Zhao, "Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network," *IEEE Sensors Journal*, Vol. 21, no. 22, 2021, pp.25472-25479.
18. S. Gao, T. Yu, J. Zhu, W. Cai, "T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm," *China Communications*, Vol. 16 no. 12, 2019, pp.111-123.
19. Nakamoto S. "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf. Accessed 2008.
20. Buterin V, Griffith V. "Casper the Friendly Finality Gadget," *ArXiv* ,2017.

HuiZhi received the M.S. degree and PhD degree in communication and information engineering from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2009 and in 2013, respectively. Since 2013, she has been a teacher at Anhui University, Hefei, China. She is currently a researcher in the Key Laboratory of Computational Intelligence and Signal Processing, Ministry of Education of China. Her current research interests include blockchain, cooperative communications, network coding and wireless sensor networks.

YuHuang received the B.S. degree in communication engineering from Nanchang University in 2020 and is currently studying for a master's degree in electronics and communication engineering at Anhui University, China. Since 2021, he has been engaged in wireless communication research at the Key Laboratory of Computational Intelligence and Signal Processing, Ministry of Education of China. His research interests include blockchain, device-to-device communication, mobile edge computing and IoT communication.

YongWang received his bachelor's degree in communication engineering from Tongling University in 2019 and his master's degree in electronics and communication engineering from Anhui University in 2022. During 2019-2022, he stay in wireless communication research at the Key Laboratory of Computational Intelligence and Signal Processing, Ministry of Education of China. His research interests include blockchain in cooperative communication, cellular mobile communication and mobile edge computing.