applied sciences

MDPI

Article

A Scalable and Trust-Value-Based Consensus Algorithm for Internet of Vehicles

Zhiqiang Du [1], Jiaheng Zhang [1,*], Yanfang Fu [1,*], Muhong Huang [1], Liangxin Liu [1] and Yunliang Li [2]

[1] School of Computer Science and Engineering, Xi'an Technological University, Xi'an 710021, China; duzhiqiang@xatu.edu.cn (Z.D.); hmh19970615@gmail.com (M.H.); liuliangxin@st.xatu.edu.cn (L.L.)
[2] College of Computer and Data Science/College of Software, Fuzhou University, Fuzhou 350108, China; 231010014@fzu.edu.cn
* Correspondence: zhangjiaheng@st.xatu.edu.cn (J.Z.); fuyanfang@xatu.edu.cn (Y.F.)

Abstract: As blockchain technology plays an increasingly important role in the Internet of Vehicles, how to further enhance the data consensus between the areas of the Internet of Vehicles has become a key issue in blockchain design. The traditional blockchain-based vehicle networking consensus mechanism adopts the double-layer PBFT architecture, through the grouping of nodes for first intra-group consensus, and then global consensus. To further reduce delay, we propose a CRMWSL-PBFT algorithm (C-PBFT) for vehicle networking. Firstly, in order to ensure the security of RSU nodes in the network of vehicles and reduce the probability of malicious nodes participating in the consensus, we propose to calculate the reputation of RSU nodes based on multi-weighted subjective logic (CRMWSL) model. Secondly, in order to ensure the efficiency of blockchain data consensus, we improve the consensus protocol of traditional double-layer PBFT, change the election method of the committee and the PBFT consensus process, and improve throughput by reducing the number of consensus nodes. For the committee, we combine the credibility value and hash method to ensure the credibility of nodes, but also to ensure a certain degree of election randomness. For the PBFT consensus process, the regional committee consensus is carried out first, and then the regional master node carries out the global consensus. Through experimental comparison, we show that the C-PBFT significantly reduces consensus time, network overhead, and is scalable for Internet of Vehicles.

Keywords: Internet of Vehicles; consortium blockchain; hierarchical consensus; PBFT; reputation value

Citation: Du, Z.; Zhang, J.; Fu, Y.; Huang, M.; Liu, L.; Li, Y. A Scalable and Trust-Value-Based Consensus Algorithm for Internet of Vehicles. *Appl. Sci.* **2023**, *13*, 10663. https://doi.org/10.3390/app131910663

Academic Editor: Chilukuri K. Mohan

Received: 25 July 2023
Revised: 20 September 2023
Accepted: 20 September 2023
Published: 25 September 2023

1. Introduction

With the rapid development of the Internet of Things and the continuous progress of 5G technology, the Internet of Vehicles is gradually coming into people's view. The Internet of Vehicles plays an important fundamental role in the field of transportation. The collection and sharing of traffic data between vehicles can better optimize the service quality of intelligent transportation systems [1]. However, due to privacy and security concerns, vehicles may be reluctant to upload data to the Road Side Unit (RSU) for data sharing, thus hindering the development of future connected vehicles [2].

Due to the characteristics of blockchain technology such as distribution, anonymity, and non-comparability, many researchers have integrated blockchain technology with vehicle networking. Blockchain is used to establish a secure, trusted, and decentralized intelligent transportation ecosystem to solve part of the problem of vehicle data sharing [3]. However, after the introduction of blockchain, the system needs to consume a lot of computing resources and storage resources to meet the data-sharing service. At the same time, in a highly dynamic vehicular networking environment, it is difficult to maintain a long-term communication connection between vehicles and RSU nodes. When the data synchronization speed in the blockchain network does not match the moving speed of vehicles, the high latency may cause data inconsistency between nodes in different regions, resulting in meaningless old data for vehicles and other problems.

As an integral component of blockchain technology, consensus algorithms serve the pivotal role of ensuring data consistency among distributed nodes. Many of the current studies combining IoV and blockchain consensus algorithms are based on traditional methods, including proof-of-work (PoW), proof-of-stake (PoS), entrusted proof-of-stake (DPoS), and practical Byzantine fault Tolerance (PBFT). However, the limited computational resources of RSU nodes within vehicular networks render them inadequate for the execution of PoW-based algorithms. Furthermore, consensus mechanisms such as PoS and DPoS, which hinge on stake-based incentives, may potentially introduce disparities in outcomes. A comparative analysis conducted by Kim et al. [4] evaluated the efficacy of PoW, PoS, and PBFT, concluding that PBFT holds the highest promise as a consensus algorithm within the context of vehicular networks.

Although there are many researches on the PBFT consensus algorithm in IOV [5–7], most of them are based on traditional single-chain structure. As the number of nodes increases, the communication complexity of traditional PBFT consensus algorithm increases rapidly and the consensus performance decreases sharply. Therefore, it is a great challenge to directly apply the PBFT consensus algorithm in the Internet of Vehicles.

Therefore, this paper proposes a double-layer PBFT consensus algorithm by region. Meanwhile, the committee election algorithm elects appropriate RSU nodes to participate in the consensus according to the credibility value, which solves the problem of low scalability of the PBFT algorithm due to the superlinear complexity due to excessive RSU nodes.

The main contributions of this paper are summarized as follows:

(1) We propose a multi-weight subjective logic model to calculate the RSUs node's credit value more accurately.
(2) We propose a committee election algorithm to select appropriate nodes to participate in consensus based on node reputation, reduce communication complexity, and improve the scalability of blockchain.
(3) We propose a double-layer consensus structure algorithm, which firstly carries out regional consensus and then global consensus to reduce consensus latency and communication complexity.
(4) We experimentally tested the proposed reputation assessment model RCMWSL and the C-PBFT consensus algorithm.

The rest of the paper is organized as follows. Section 2 presents related research on the reputation mechanism of IoV and research related to the scalability of consensus protocols. Section 3 presents the system model. Section 4 presents the proposed C-PBFT consensus algorithm. Section 5 analyzes the security properties of the proposed consensus algorithm. Section 6 provides simulation experimental results. Section 7 concludes the paper and discusses future research directions.

2. Related Work

2.1. IoV Reputation

In recent years, researchers have designed reputation evaluation methods and models in the field of the Internet of Vehicles based on different theoretical methods. Li et al. [8] improved the subjective logical trust model and established a three-valued subjective logical trust model. The uncertainty of events is divided into a priori uncertainty and a posteriori uncertainty in the model, and the results of the events are simulated with Dirichlet-categorical distribution, and the propagation law of trust relationships among different entities is derived using Bayesian inference. Liu et al. [9] propose an improved reputation calculation method based on subjective logic. In this method, a concept of "familiarity" is introduced, that is, the weight of the evaluation opinion is high in the neighbor nodes that are familiar with the evaluated node. And this kind of the complexity of reputation calculation in this model is generally larger. Jaimes et al. [10] conducted reputation management based on entity. Due to the huge scale of the Internet of Vehicles network, it is easy to cause problems such as single-point bottlenecks and complicated calculation processes. Rivas et al. [11] considered all credit evaluation factors obtained from

neighboring vehicles, which may lead to inaccurate credit evaluation and even security problems such as collusion attacks. Lin et al. [12] put forward the reputation model based on subjective logic, which mainly uses the theory of subjective logic to quantify the reputation information of nodes. The subjective logic defines the representation and calculation methods of credibility quantitatively. Moreira et al. [13] evaluated the reputation of vehicle nodes in an in-vehicle self-assembling network by judging the reliability of message content through the reliability of the message source. Josang et al. [14] proposed a subjective logical trust model that predicts the probability that something turns out to be trustworthy using a beta distribution. Yang et al. [1] also proposed a decentralized trust management system to evaluate the trustworthiness of received vehicle data by using blockchain and PoW and PoS consensus schemes.

2.2. Consensus Protocol Scalability

Although the PBFT algorithm is a satisfactory consensus solution in distributed systems, its scalability is low and the number of nodes involved in consensus has a direct impact on the communication complexity of the PBFT consensus algorithm, so researchers have tried to streamline the number of nodes involved in consensus by forming a consensus committee from all the nodes of the system and then releasing the consensus results to other nodes, thus improving the scalability of the system.

The Permacoin [15] algorithm then elects the leader based on the participant's free disk size. And the strategy for electing leaders can be used as a strategy for electing committees with slight modifications. The T-PBFT algorithm [16] combines the feature trust model with the consensus algorithm to evaluate the trust level of nodes, select some nodes with higher credit to participate in the consensus, and use the nodes with higher quality in the network to establish the consensus group instead of a single master node. PoPT [17] proposes an algorithm to measure the participation of nodes in a public chain system and elects a committee based on the participation ranking. The dBFT [18] algorithm elects the committee based on POS and associates nodes with the margin of node access to solve the disinterested problem of native POS. The Tendermint [19] algorithms elect committees based on PoS, which associate nodes with margins to solve non-benefit problems of native PoS. The Algorand algorithm [20] uses VRF to randomly select a subset of network nodes as a committee to ensure the unpredictability of committee members and improve the security and the scalability of the system. Due to the high communication complexity of the PBFT consensus algorithm in practical applications, many scholars have improved the PBFT algorithm from consensus structure. Li et al. [21] proposed a scalable multi-layer consensus mechanism based on PBFT. By layer-grouping nodes into different layers and limiting communication within groups, it was analyzed that the complexity of communication was minimal when the network was evenly distributed in subgroups in the second layer. Singh et al. [22] constructed a multi-level network model based on blockchain for security monitoring to ensure identity information security and enhance system reliability, but increased system management overhead. Fortino et al. [23] proposed a grouping algorithm based on reputation integral to improve the possibility of malicious nodes making errors, but did not consider the problem of reduced system communication performance when the number of nodes increased. Hou et al. [24] constructed a multi-layer blockchain to group users according to certain security levels and stored data of different levels into the chain of corresponding levels, to achieve secure data access control. Xu et al. [25] used a hashing algorithm to ensure that consistently nodes are grouped, which can avoid a large amount of communication between nodes, reduce the communication complexity of the network, and improve the scalability of the network, but cannot identify Byzantine nodes. Zhai et al. [26] proposed a bottom-up two-tier RSU chain consensus protocol (TLPBFT) based on blockchain and trust values, and the algorithm latency rises significantly when the number of regional nodes is high. Liu et al. [27] proposed a quality-of-service-based PBFT algorithm that reduces the inter-node consensus latency but does not consider the presence of malicious nodes in the group.

3. System Model

3.1. System Architecture

Figure 1 shows the blockchain IoV system model. The communication between vehicles or between vehicles and RSUs is wireless, while the communication between RSUs is wired communication. The model consists of the following main components:

(1) Vehicle: The vehicle is equipped with an intelligent On Board Unit (OBU), which enables it to have functions such as sensing, computing, and storage. The vehicle is responsible for uploading its interaction records, feedback ratings, and other information to the RSUs.

(2) RSU: Compared with the vehicles, the RSU has strong computing and storage resources as well as a sufficient energy supply, so the RSU is selected as the node of the blockchain network. In addition, the RSU needs to collect the communication data among vehicles within its communication range as well as the feedback rating data, update the reputation value of vehicles at the end of each cycle according to their behavior, and then package the results into blocks to be added into the blockchain network for global vehicles and other subjects to query.

(3) Reputation Center (RC): The reputation center stores the latest reputation of vehicles and RSUs in the network. When the reputation obtained by RSUs from the vehicle side is too different from that stored by RSUs, RSUs will request the latest reputation of the corresponding vehicles from the RC. At the same time, the RC issues certificates for legitimate vehicles and RSUs and distributes public and private keys of vehicles and RSUs through secure channels. The model assumes that the RC is completely credible.

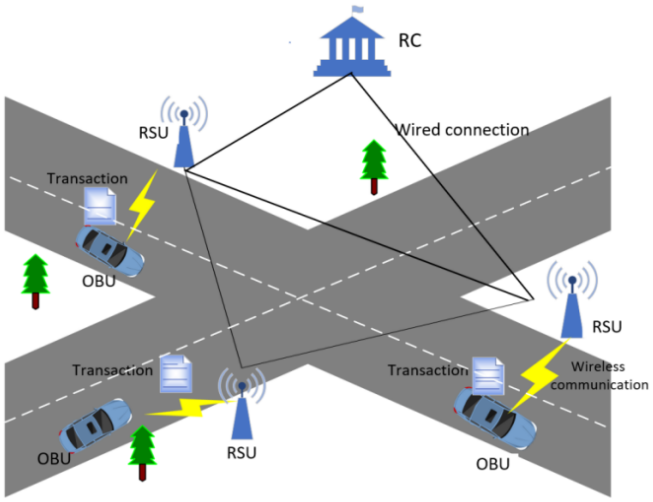

Figure 1. The blockchain-based system model for IoV.

3.2. Network Model

Our model uses a partial synchronization model with known latency bounds Δ and global stability time GST, where all transmissions between two replicas are reached in Δ time after GST.

3.3. Security Properties

The C-PBFT algorithm should have the following properties:

(1) Safety
At the same block height, any two honest nodes submit the same blocks.

(2) Liveness
If a transaction is received by an honest node, then that transaction will eventually be included in the honest node's ledger.

4. C-PBFT Consensus Algorithm

4.1. Algorithm Design Overview

In this section, we construct a double-layer consensus algorithm C-PBFT based on the PBFT consensus algorithm, one of the challenges of which is that the original PBFT algorithm selects master nodes arbitrarily, which may make malicious nodes become master nodes consecutively, thus wasting network resources, so we propose the multi-weight subjective logic model CRMWSL to calculate node reputation values, as seen in Section 4.2. Another challenge is that the scalability of the PBFT algorithm is poor. Therefore, the committee election algorithm is designed to select appropriate nodes to participate in the consensus based on node reputation value and reduce the number of nodes participating in the consensus, as shown in Section 4.3. At the same time, a double-layer consensus structure was designed, and nodes were divided into regions to carry out regional local consensus and interval global consensus, as shown in Section 4.4.

The key symbols used in this paper are listed in Table 1.

Table 1. The main symbols.

Notation	Definition
$\left\{b_{i\to j}, d_{i\to j}, u_{i\to j}\right\}$	A local opinion vector $\omega_{i\to j}$ from a vehicle V_i to RSU_j
$F_{i\to j}$	Vi's expected beliefs about RSU
α_i, β_i	The number of positive/negative interactions
χ, τ	The weight of positive/negative interactions
R_i	Reputation value of node i
n	Number of regions
u	Average number of nodes in each committee
m	Average number of nodes in each region
Y	The given decay parameter for event freshness
$\mathcal{E}$	The initial reputation value of the node predefined in the system

4.2. Reputation Calculation Using Multi-Weighted Subjective Logic Model

When a vehicle and an RSU interact positively, the vehicle generates a good rating for the RSU. Positive engagement indicates that the vehicle believes the RSU provides relevant and helpful services or that the data supplied by the RSU is accurate. On the contrary, some malicious vehicles may generate malicious evaluations for RSUs to provide false information, too many malicious evaluations will harm RSU node reputation, and false evaluations will result in some malicious nodes being elected to the committee, resulting in unreliable and insecure consensus networks.

Therefore, it is necessary to design a secure and efficient RSU node reputation value evaluation model and prevent collusion between RSUs and vehicles, and selecting suitable candidate nodes to build the consensus committee by reputation value can ensure a safe and reliable consensus process. In this section, a multi-weighted subjective logic model is proposed for the calculation of the reputation value of RSU nodes.

4.2.1. Local Opinions of Subjective Logic

The RSU_j corresponds to the vehicle V_i in the region, and based on its communication data interaction with the RSU_j and the predefined subjective logic model, the local opinion vector $\omega_{i\to j}^{t_x} := \{b_{i\to j}^{t_x}, d_{i\to j}^{t_x}, u_{i\to j}^{t_x}\}$ of the vehicle V_i in the time window evaluates the reputation value of the RSU_j:

$$\begin{cases} b_{i\to j}^{t_x} = \left(1 - u_{i\to j}^{t_x}\right) \frac{\alpha_{i\to j}^{t_x}}{\alpha_{i\to j}^{t_x} + \beta_{i\to j}^{t_x}} \\ d_{i\to j}^{t_x} = \left(1 - u_{i\to j}^{t_x}\right) \frac{\beta_{i\to j}^{t_x}}{\alpha_{i\to j}^{t_x} + \beta_{i\to j}^{t_x}} \\ u_{i\to j}^{t_x} = 1 - q_{i\to j}^{t_x} \end{cases} \tag{1}$$

In this case, vehicle V_i interacts with the RSU_j during traveling with data, such as crowd-sensing or vehicle data sharing. The local opinion of the subjective logic model V_i on the RSU_j can be formally described as a local opinion vector $\omega_{i\to j}^{t_x} := \{b_{i\to j}^{t_x}, d_{i\to j}^{t_x}, u_{i\to j}^{t_x}\}$, where $b_{i\to j}^{t_x}, d_{i\to j}^{t_x}, u_{i\to j}^{t_x}$ stand for trust, distrust, and uncertainty, respectively. $b_{i\to j}^{t_x}, d_{i\to j}^{t_x}, u_{i\to j}^{t_x} \in [0,1]$ and $b_{i\to j}^{t_x} + d_{i\to j}^{t_x} + u_{i\to j}^{t_x} = 1$, where $\{t_1, \cdots t_x, \cdots t_X\}$ represents part of the time period X as a time window. $\alpha_{i\to j}^{t_x}$ is the number of positive interactions between vehicle V_i and RSU_j, and $\beta_{i\to j}^{t_x}$ is the number of negative interactions between vehicle V_i and RSU_j, where positive interactions mean that vehicle V_i believes that the service provided by RSU_j is relevant and useful. A negative interaction means that vehicle V_i does not believe that the service provided by RSU_j is relevant and useful. $q_{i\to j}^{t_x}$ is the communication quality of the link between vehicle V_i and RSU_j, that is, the probability of successful packet transmission, which determines the uncertainty of $u_{i\to j}$ in the local opinion vector. Based on the local opinion vector $\omega_{i\to j}^{t_x} := \{b_{i\to j}^{t_x}, d_{i\to j}^{t_x}, u_{i\to j}^{t_x}\}$ in the time window of vehicle V_i, the expression of the initial credit value evaluated by vehicle V_i to RSU_j is determined as follows:

$$F_{i\to j} = b_{i\to j} + \gamma u_{i\to j} \tag{2}$$

where $0 \le \gamma \le 1$ is a given constant, representing the degree of influence of uncertainty on credit value.

4.2.2. Multi-Weight Local Opinions of Subjective Logic

Local opinions using the subjective logic model are affected by different factors. When considering weighted operation, traditional subjective logic evolves to multi-weighted subjective logic. We consider the following weights to form a partial opinion:

- Interaction Frequency: The higher the interaction frequency means that vehicle V_i has more prior knowledge of RSU_j, so the calculation of V_i's credit value to RSU_j is more accurate and reliable. The interaction frequency of V_i with RSU_j is the number of times V_i interacts with RSU_j, the ratio of V_i to the number of times V interacts with RSU_j and other interactions in a time window. For distinction, the frequency of interaction between vehicle V_i and RSU_j in this step is expressed as $IF_{i\to j}^0$:

$$IF_{i\to j}^0 = \frac{N_{i\to j}}{\sum_{z=1}^{N} N_{i\to z}} \tag{3}$$

  $N_{i\to j} = (\alpha_{i\to j}^{t_x} + \beta_{i\to j}^{t_x})$, where z is the set of all RSUs interacting with vehicle V_i in the time window, with N elements. The higher the interaction frequency, the higher the reputation expectation of vehicle V_i on RSU_j.
- Timeliness of Interaction: Recent behavioral events with a higher degree of freshness are weighted more heavily than past events. In order to reflect the effect of reaction time on reputation, a freshness decay function is defined to represent the freshness of a behavioral event: $\psi(t_x) = \psi_x = \mathrm{Y}^{X-x}$, where $\mathrm{Y} \in (0,1)$ is a given decay parameter about the freshness of an event. In a time period X, the local opinion vector of vehicle V_i on the evaluation of RSU_j is expressed as

$$\begin{cases} b_{i\to j} = \frac{\sum_{x=1}^{X}\left(\psi_x b_{i\to j}^{t_x}\right)}{\sum_{x=1}^{X}\psi_x} \\ d_{i\to j} = \frac{\sum_{x=1}^{X}\left(\psi_x d_{i\to j}^{t_x}\right)}{\sum_{x=1}^{X}\psi_x} \\ u_{i\to j} = \frac{\sum_{x=1}^{X}\left(\psi_x u_{i\to j}^{t_x}\right)}{\sum_{x=1}^{X}\psi_x} \end{cases} \tag{4}$$

where ψ_x represents the freshness attenuation function, $b_{i\to j}^{t_x}$, $d_{i\to j}^{t_x}$ and $u_{i\to j}^{t_x}$ are shown in Formula (1).

- Interaction Effects: Positive interactions increase the reputation value of RSU nodes, while negative interactions decrease the reputation of RSU nodes. In general, the effects of negative events are much more serious in public opinion than positive effects, so the interaction effects of messages have higher weights on local opinions. The weight of positive interaction is χ, and the weight of negative interaction is τ, where $\chi + \tau = 1$, $\chi < \tau$. Combining the interaction timeliness and the weight of the interaction effect, the positive and negative interaction effects of V_i and RSU_j are expressed as follows:

$$V_{i\to j}^{\alpha} = \frac{\sum_{x=1}^{X}(\psi_x \chi \alpha_{i\to j}^{t_x})}{\sum_{x=1}^{X}\psi_x} \tag{5}$$

$$V_{i\to j}^{\beta} = \frac{\sum_{x=1}^{X}(\psi_x \tau \beta_{i\to j}^{t_x})}{\sum_{x=1}^{X}\psi_x} \tag{6}$$

Among them, $V_{i\to j}^{\alpha}$ represents the positive interaction between V_i and RSU_j, while $V_{i\to j}^{\beta}$ represents the negative interaction effect between V_i and RSU_j.
Therefore, according to Formulas (3), (5), and (6), the interaction frequency of V_i and RSU_j is updated as follows:

$$IF_{i\to j} = \frac{V_{i\to j}^{\alpha} + V_{i\to j}^{\beta}}{\sum_{x=1}^{N} N_{i\to x}} \tag{7}$$

where $IF_{i\to j}$ is the result of updating the $IF_{i\to j}^{0}$ of formula (3).

- Distance Factor: Considering the influence of the geographical location where the vehicle Vi sends the message, that is, the farther the geographical location where the message is generated is from the geographical location where the event occurs, the lower the event weight. Assuming that the distance between the location where the event is generated and the location where the message is sent is 0-L, we believe that the information is credible in terms of distance factors.
The factors influencing distance are shown as follows:

$$\begin{cases} DF_{i\to j} = 1, \Delta L \le L \\ DF_{i\to j} = \frac{L}{2\sqrt{|X_i - X|^2 + |Y_i - Y|^2}}, \Delta L > L \end{cases} \tag{8}$$

where $\Delta L = \sqrt{|X_i - X|^2 + |Y_i - Y|^2}$, (X_i, Y_i) and (X, Y) are the location coordinates of the message generated by vehicle Vi and the geographic location coordinates of the message generation, respectively.
Therefore, the overall credibility value weight of the local opinion is $\delta_{i\to j} = \rho_1 * IF_{i\to j} + \rho_2 * DF_{i\to j}$, where $\rho_1 + \rho_2 = 1, 0 < \rho_1 \le 1, 0 < \rho_2 \le 1$.

4.2.3. Recommended Opinions of Subjective Logic

For each vehicle, the vehicle collects the local opinion vector of other vehicles that have communication data interaction with the RSU_j to evaluate the RSU_j's credit value within a time period and the corresponding credit value weight δ, and uses the collected local opinion vector corresponding to the credit value weight δ to merge all the collected local opinion vectors into one recommended opinion. The formula expression is as follows:

$$\begin{cases} b_{s\to j}^{rec} = \frac{1}{\sum_{s\in S}\delta_{s\to j}} \sum_{s\in S} \delta_{s\to j} b_{s\to j} \\ d_{s\to j}^{rec} = \frac{1}{\sum_{s\in S}\delta_{s\to j}} \sum_{s\in S} \delta_{s\to j} d_{s\to j} \\ u_{s\to j}^{rec} = \frac{1}{\sum_{s\in S}\delta_{s\to j}} \sum_{s\in S} \delta_{s\to j} u_{s\to j} \end{cases} \tag{9}$$

Vehicle V_i merges to get a recommendation as $\omega_{s\to j}^{\text{rec}} := \{b_{s\to j}^{\text{rec}}, d_{s\to j}^{\text{rec}}, u_{s\to j}^{\text{rec}}\}$, where $S \in \mathcal{S}$ indicates that vehicle S belongs to the recommended vehicle set $\mathcal{S}$.

4.2.4. Combining Local Opinions with Recommended Opinions

After obtaining a local opinion vector for the RSU from other vehicles, a particular vehicle has a subjective opinion for each RSU based on its interaction history. This partial opinion should still be taken into account when forming the final initial credit rating of a single vehicle to avoid deception.

After V_i combines the local opinion vector of its own credit evaluation of RSU_j in a time period with the merged recommendation opinion, the resulting credit opinion can be expressed as $\omega_{s\to j}^{\text{final}} := \{b_{s\to j}^{\text{final}}, d_{s\to j}^{\text{final}}, u_{s\to j}^{\text{final}}\}$.

$$\begin{cases} b_{i\to j}^{\text{final}} = \frac{b_{i\to j} u_{s\to j}^{rec} + b_{s\to j}^{rec} u_{i\to j}}{u_{i\to j} + u_{s\to j}^{rec} - u_{s\to j}^{rec} u_{i\to j}} \\ d_{i\to j}^{\text{final}} = \frac{d_{i\to j} u_{s\to j}^{rec} + d_{s\to j}^{rec} u_{i\to j}}{u_{i\to j} + u_{s\to j}^{rec} - u_{s\to j}^{rec} u_{i\to j}} \\ u_{i\to j}^{\text{final}} = \frac{u_{s\to j}^{rec} u_{i\to j}}{u_{i\to j} + u_{s\to j}^{rec} - u_{s\to j}^{rec} u_{i\to j}} \end{cases} \tag{10}$$

Similar to Equation (2), Vi's final reputation opinion on RSU is

$$F_{i\to j}^{\text{final}} = \varepsilon + \tanh\left(b_{i\to j}^{\text{final}} + \gamma u_{i\to j}^{\text{final}}\right) \tag{11}$$

where ε is the initial creditworthiness of any predefined node in the system and is a negligible non-zero positive number.

In a certain period, RSU_j receives all vehicles in the corresponding area to evaluate its credit value and gets the initial credit value, and then adds it to get its own node credit value R_j.

4.3. Committee Election Algorithm

This section defines the election function $f_{Sele_H}(\cdot)$ for the consensus committee. In order to ensure the randomness of the election, it is necessary to ensure the fluidity of the node election committee that meets the credibility threshold. Elections provide two important attributes, namely public key pk and node reputation R, node p_i first performs $h_j \leftarrow H(pk_j, R_j)$ operations on its own public key pk and reputation value R_i to obtain the hash value h_i, which is basically evenly distributed between 0 and $2^{\text{hashlen}(h_j)} - 1$. Therefore, whether to be selected to the committee is randomly selected according to the credibility of the nodes. When $R_j - \frac{h_j}{2^{\text{hashlen}(h_j)}} > 0$, where the hashlen(.) function is used to calculate the bit length of a given hash, node p_i meets the inclusion condition, and node p_i is added to the committee CO.

The algorithm pseudo-code is described in Algorithm 1.

Algorithm 1 Reputation election $f_{Sele_H}(\cdot)$

Input: pk_j, R_j
Output: CO
Initializaion: $CO \leftarrow \varnothing$
1. $h_j \leftarrow H\left(pk_j, R_j\right)$
2. $f(x) \leftarrow R_j - \frac{h_j}{2^{\text{hashlen}\left(h_j\right)}}$
3. if $f(x) > 0$ then
4. $CO \leftarrow CO \cup p_i$
5. *else*
6. $CO \leftarrow CO$
7. *endif*

4.4. Double-Layer Consensus Structure

In the Internet of Vehicles environment, due to the wide range of vehicle activities, a large number of RSU nodes, and high communication complexity, it is necessary to design a network structure with scalability and flexibility to cope with the rapid change in network topology when vehicles are running.

In this paper, we propose a double-layer PBFT consensus structure, as shown in Figure 2, with n nodes in the first layer and m nodes in each region in the second layer, i.e., a total of $n + m$ nodes. Where the replica of the committee in the first layer is noted as r_i^1 (superscript 1 indicates the number of layers, and subscript i indicates the region), r_i^1 serves as the leader of the corresponding replica of each regional committee in the second layer r_i^2. An upper layer r_i^1 together with the r_i^2 in its region forms a regional consensus committee.

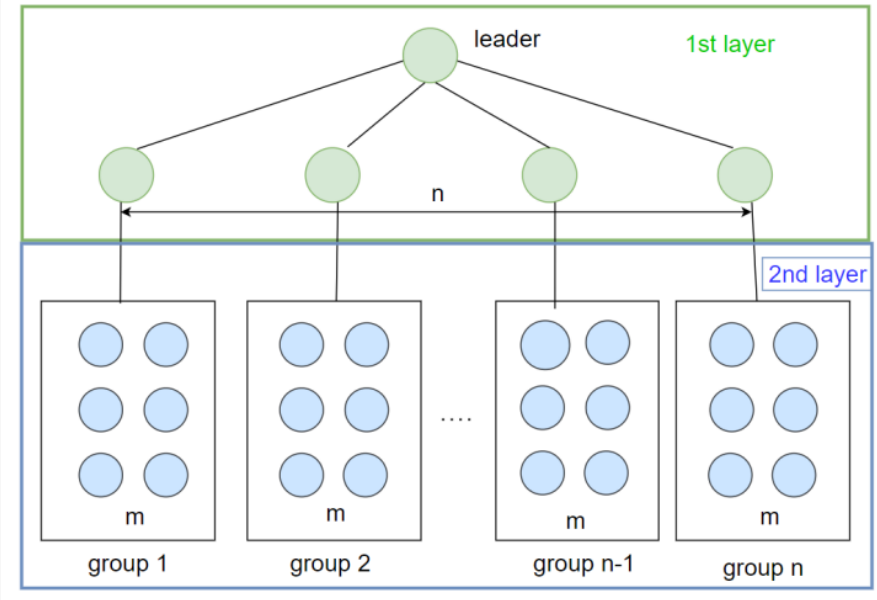

Figure 2. Topology of C−PBFT system.

As shown in Figure 3, the C−PBFT consensus process is divided into two parts: first, regional local consensus is carried out, and then global consensus is carried out.

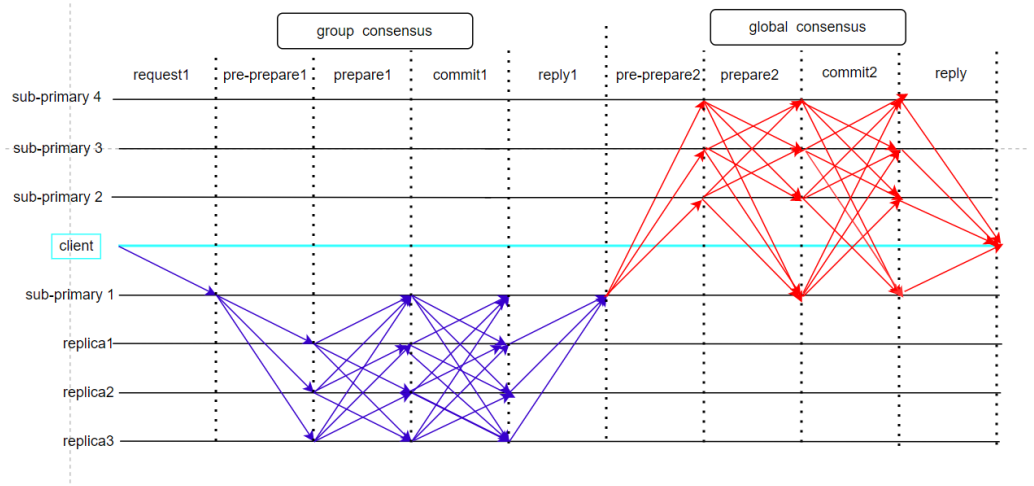

Figure 3. The whole process of C-PBFT's consensus.

4.4.1. Regional Local Consensus

Node RSU_k receives the request message m sent by the requesting vehicle in the target area in the format of $< REQUEST^2, o, t, c > \sigma_c$, and node RSU_k puts the request message e into the transaction pool in the target area, where O indicates that node RSU_k receives the request message e sent by the requesting vehicle in the target area in the format of $< REQUEST^2, o, t, c > \sigma_c$, and node RSU_k puts the request message e into the transaction pool in the target area, where O indicates the specific operation to be performed, t indicates the timestamp, which is the time when the requesting vehicle sends the request message to the RSU_k, c indicates the requested vehicle number, and σ_c indicates the request for vehicle signature, $REQUEST^2$'s superscript 2 indicates the request at the second layer.

(1) Pre-prepare Phase

The regional master node p of the target regional committee assigns the serial number to the request message in the transaction pool and broadcasts the preparatory message $\langle \langle PRE - PREPARE^2, v, h, d \rangle_{\sigma_p}, e \ > $ to all nodes of the regional committee. $\langle PRE - PREPARE^2, v, h, d \rangle_{\sigma_p}$ is the signature of the master node p of the target regional committee using its own private key, v indicates the view number, h indicates the sequence number assigned to the request message e, and d represents a summary of the request message e.

(2) Prepare Phase

After receiving the $PRE - PREPARE^2$ message from the primary node p, node RSU_k uses the corresponding public key for verification. After the verification is successful, node RSU_k sends a $< PREPARE^2, v, h, d, k >_{\sigma_k}$ message, indicating the signature message of node RSU_k, to other nodes in the owning area committee, including the primary node.

(3) Commit Phase

If RSU_k receives $2f + 1$ $PREPARE^2$ messages that pass the authentication, RSU_k enters the confirmation phase. The $\langle COMMIT^2, v, h, d, k \rangle_{\sigma_k}$ multicast message is sent to the node that receives $2f + 1$ $PREPARE^2$ messages that pass the authentication.

(4) Reply Phase

If node RSU_k receives $2f + 1 COMMIT^2$ messages that pass the authentication, it indicates that most nodes in the current regional committee have reached a consensus. Node RSU_k sends a reply message $< REPLY^2, v, t, c, k, r >_{\sigma_k}$ to the area master node p of

the region, where r represents the execution result of the requested operation. Master node p of the area confirms that the area has reached a consensus by checking that more than $f+1$ members in the current area, including itself, reply to the $REPLY^2$ message with the same serial number. The regional master node sends a request to the first-layer master node p to send the consensus data m to the first-layer master node, opening a new round of consensus requests.

The algorithm pseudocode is described in Algorithm 2.

Algorithm 2 Regional Local Consensus Pseudocode

Input: $< REQUEST^2, o, t, c >_{\sigma c}$
Output: $< REPLY^2, v, t, c, k, r >_{\sigma k}$
1. **while** valid $< REQUEST^2, o, t, c >_{\sigma c}$ received = True **do**
2. broadcast $<< PRE-PREPARE^2, v, h, d >_{\sigma p}, e_2 >$ to r^2 in same consensus group.
3. **end while**
4. **while** valid $<< PRE-PREPARE^2, v, h, d >_{\sigma p}, e_2 >$ received = True **do**
5. broadcast $< PREPARE^2, v, h, d, k >_{\sigma k}$ to r^2 in same consensus group.
6. **end while**
7. **while** valid $< PREPARE^2, v, h, d, k >_{\sigma k}$ received = True **do**
8. **if** number of valid $< PREPARE^2, v, n, d, k >_{\sigma k} > 2f+1$ **then**
9. broadcast $< COMMIT^2, v, h, d, k >_{\sigma k}$ to r^2 in same consensus group.
10. **end if**
11. **end while**
12. **while** valid $< COMMIT^2, v, h, d, k >_{\sigma k}$ received = True **do**
13. **if** number of valid $< COMMIT^2, v, h, d, k >_{\sigma k} > 2f+1$ **then**
14. broadcast $< REPLY^2, v, t, c, k, r >_{\sigma k}$ to r^2 group leader.
15. **end if**
16. **end while**

4.4.2. Global Consensus

The primary node of Layer 1 makes global consensus according to the time order of messages in the transaction pool. The primary node of Layer 1 sends $<< PRE-PREPARE^1, v, h, d >, e >_{\sigma i}$ messages to all regional primary nodes, where σ_i represents the signature of the primary node of Layer 1, i. The preparation phase, preparation phase, and confirmation phase in the global consensus are similar to those in the local consensus and will not be repeated here.

All regional master nodes will reply to the message $\langle REPLY^1, v, t, c, i, r \rangle_{\sigma i}$ directly to the requesting vehicle. If the requesting vehicle receives $f+1$ $REPLY^1$ messages, the consensus is successful. i indicates the number of the primary node in the area, $REPLY^1$ is the flag description, v indicates the number of the current view, t stands for the timestamp, c indicates the requested vehicle number, and r indicates the result of the requested operation. After the above process is completed, the master nodes in all areas send the reply message $REPLY^1$ directly to the client, that is, to request the vehicle. After the client receives $f+1$ $REPLY^1$, the consensus is successful. After the two−tier consensus of the target regional committee is completed, the remaining nodes of the blockchain network copy the data locally.

The algorithm pseudocode is described in Algorithm 3.

Algorithm 3 Global Consensus Pseudocode

Input: $< REPLY^2, v, t, c, i, r >_{\sigma i}$
Output: $< REPLY^l, v, t, c, i, r >_{\sigma i}$
1. **while** valid $\langle REPLY^2, v, t, c, i, r \rangle_{\sigma i}$ received = True **do**
2. **if** number of valid $< REPLY^2, v, t, c, i, r >_{\sigma i} > f + 1$ **then**
3. broadcast $< REQUEST^l, o, t, c >_{\sigma c}$ to superior r^l leader.
4. **end if**
5. **end while**
6. **while** valid $\left\langle REQUEST^l, o, t, c \right\rangle_{\sigma c}$ received = True **do**
7. broadcast $<< PRE - PREPARE^l, v, n, d >_{\sigma p}, e_1 >$ to r^l all nodes.
8. **end while**
9. **while** valid $<< PRE - PREPARE^l, v, n, d >_{\sigma p}, e_1 >$ received = **True do**
10. broadcast $< PREPARE^l, v, n, d, i >_{\sigma i}$ to r^l all nodes.
11. **end while**
12. **while** valid $< PREPARE^1, v, n, d, i >_{\sigma i}$ received = True **do**
13. **if** number of valid $< PREPARE^1, v, n, d, i >_{\sigma i} > 2f + 1$ **then**
14. **broadcast** $< COMMIT^l, v, n, d, i >_{\sigma i}$ to ${r_i}^l$ all nodes.
15. **end if**
16. **end while**
17. **while** valid $< COMMIT^1, v, n, d, i >_{\sigma i}$ received = True **do**
18. **if** number of valid $< COMMIT^1, v, n, d, i >_{\sigma i} > 2f + 1$ **then**
19. **reply** $< REPLY^1, v, t, c, i, r >_{\sigma i}$ to client.
20. **end if**
21. **end while**

5. Theoretical Analysis

5.1. Safety Analysis

First, the committee election algorithm elects suitable nodes in each region to participate in consensus, the selected committee meets the honest majority, and the regional committee performs the PBFT algorithm for consensus, because the PBFT algorithm, for all locally confirmed client requests, all normal replica nodes in the system must agree on the message serial numbers of these requests, so it ensures the consistency within the region, and regional consensus is completed. After the regional master node sends a message to the leadership master node, the leadership master node broadcasts for inter-regional consensus, and after the inter-regional PBFT consensus is completed, the data is synchronized among the regions, which ensures the data consistency across regions. Therefore, our algorithm satisfies the security.

5.2. Liveness Analysis

If the master node is evil, our proposed reputation value evaluation algorithm quickly reduces the master node reputation value so that it does not satisfy the master node condition, while the PBFT view replacement protocol replaces the master node, specifically, our algorithm can handle the situation where consensus cannot be reached and prevent malicious master nodes from not forwarding messages to honest nodes. Thus, the activity of the system is ensured.

5.3. Honest Majority of the Committee

Lemma 1. *Among the elected members, more than half of the nodes are honest, except for the negligible probability* $\delta(m)$.

Proof. In the worst case, all nodes have a reputation value of 1. The committee election can be viewed as an independent random sampling problem, and the probability that node p_i is elected to the committee is

$$\Pr[p_i \text{ is elected }] = \frac{m\mu_j}{\sum_{i=1}^{n} \mu_i} = \frac{m}{n} \tag{12}$$

where m is the committee size, k is the node number, and μ_j is the reputation value of each node p_i.

Suppose that the probability that the node representing the election is an honest node and the probability that the node representing the election is a Byzantine node, the random variable A represents the number of honest nodes in the committee, and the random variable B represents the number of Byzantine nodes in the committee. The random variables A and B satisfy the following binomial distribution:

$$\Pr[A = k] = \binom{n}{k} \left(\alpha \frac{m}{n}\right)^k \left(1 - \alpha \frac{m}{n}\right)^{n-k} \tag{13}$$

$$\Pr[B = k] = \binom{n}{k} \left(\beta \frac{m}{n}\right)^k \left(1 - \beta \frac{m}{n}\right)^{n-k} \tag{14}$$

Let X and Y be denoted as

$$X = \left\{ A : 0 \leq A \leq \left\lfloor \frac{m}{3} \right\rfloor \right\} \tag{15}$$

$$Y = \left\{ B : \left\lceil \frac{m}{3} \right\rceil \leq B \leq n \right\} \tag{16}$$

When neither X nor Y holds, the nature of the honest majority of the committee holds. $\Pr[X \cup Y]$ represents the probability that at least one of X and Y holds:

$$\begin{aligned} \Pr[X \cup Y] &= \Pr[X] + \Pr[Y] - \Pr[X \cap Y] \\ &\leq \Pr[X] + \Pr[Y] \\ &= \Pr\left[A \leq \left\lfloor \frac{m}{3} \right\rfloor\right] + \Pr\left[B \geq \left\lceil \frac{m}{3} \right\rceil\right] \\ &= F\left(\left\lfloor \frac{m}{3} \right\rfloor, n, \alpha \frac{m}{n}\right) + F\left(n - \left\lceil \frac{m}{3} \right\rceil, n, 1 - \beta \frac{m}{n}\right) \end{aligned} \tag{17}$$

where $F(k, n, p) = \Pr[X \leq k]$ is the cumulative distribution function (CDF) of the random variable $X \sim B(n, p)$. Note: $\Pr[X \geq k] = F(n - k, n, 1 - p)$. By the Binomial Tail Inequality [28], it follows that:

$$\begin{aligned} & F(\lfloor \tfrac{m}{3} \rfloor, n, \alpha \tfrac{m}{n}) + F(n - \lceil \tfrac{m}{3} \rceil, n, 1 - \beta \tfrac{m}{n}) \\ & \leq \exp\left(-2n\left(\alpha \tfrac{m}{n} - \tfrac{\lfloor \frac{m}{3} \rfloor}{n}\right)^2\right) + \exp\left(-2n\left((1 - \beta \tfrac{m}{n}) - \tfrac{n - \lceil \frac{m}{3} \rceil}{n}\right)^2\right) \\ & = 2\exp(-2n\left(\tfrac{\lfloor \frac{m}{3} \rfloor - \beta m}{n}\right)^2) = \delta(m) \end{aligned} \tag{18}$$

where n and β are constants. Thus, in the worst case, except for the negligible probability, the committee honest nodes will be in the majority.

Under normal conditions, the reputation values of all honest nodes and a few Byzantine nodes are close to 1, while the reputation values of the remaining Byzantine nodes are smaller than the reputation values of honest nodes. This indicates that the reputation value of a node basically correctly reflects the probability of a node being an honest node. According to the probability of each node being elected to the committee as $\frac{m\mu_j}{\sum_{i=1}^{n} \mu_i}$, it is clear that nodes with higher credibility are more honest and more likely to become committee members. Therefore, there are

$$\Pr[\text{ Dishonestmajority }]_{\text{Normal-case}} < \Pr[\text{ Dishonestmajority }]_{\text{Worst-case}} = \delta(m) \tag{19}$$

It shows that, in the process of election committee, the probability of honest majority is higher in normal circumstances than in the worst case. □

5.4. Attacks Discussion

Next, we discuss the possible attacks on the consensus algorithm proposed in this paper, which include both internal and external attacks, and show how they are mitigated and defended against by our algorithm.

Internal Attacks. An attacker may collude with nodes in the blockchain network or inject malicious nodes into the blockchain network in order to perform malicious acts and attack the consensus process from within the network.

Internal attacks can be classified into two cases depending on the type and behavior of the node.

(1) The master node may be a malicious node.
Malicious primary nodes intentionally generate divergent pre-prepared messages and transmit them to other nodes. In the PBFT's prepare and commit phases, nodes engage in voting amongst themselves. If the pre-prepared messages from the primary node are inconsistent, replica nodes can readily detect this discrepancy. Consequently, replica nodes will abandon the consensus proposed by the primary node and await the re-presentation of transactions by other nodes. Simultaneously, the credibility assessment mechanism and the view change protocol ensure that the malicious behavior of the primary node is curtailed within reasonable bounds.

(2) The malicious nodes predict the master node in advance to carry out the attack.
Our proposed consensus algorithm utilizes a committee election mechanism to randomly designate primary nodes. This approach ensures a certain degree of randomness while still maintaining the requirement that nodes meet the credibility threshold. This prevents the scenario wherein the node with the highest reputation consistently acts as the primary node, thereby thwarting malicious nodes from preemptively predicting the primary node.
External attack. An attacker may maliciously attack the nodes in the blockchain network to make them behave maliciously and thus attack the consensus algorithm from the external network.

This paper mainly includes the following cases:

(1) The data is tampered and forged.
The RSU nodes within the system employ techniques such as pseudonymous identification, hash algorithms, and digital signatures. To safeguard against data tampering, the blockchain system utilizes asymmetric encryption technology. As a result, nodes lacking the requisite private keys are incapable of forging the identities of other nodes or the signatures of their messages. The integration of blockchain technology and digital signatures substantially elevates the cost of successful impersonation by potential attackers, thereby reinforcing the overall system's reliability.

(2) On-off attack by malicious nodes.
The so-called On-off attack is when the attacker performs well for a period of time to enhance its reputation value, and when it accumulates to a high reputation value, it suddenly launches an attack until the reputation value is about to drop to a certain value, and then stops doing evil and becomes a normal node.

Our CRMWSL reputation value calculation model can achieve high-precision reputation calculation. Due to the recommendation of other vehicles and the multi-weight calculation of nodes, the reputation value of evil nodes will drop sharply, and below the threshold value will be withdrawn from the committee to participate in consensus. Also according to different environments, the trust threshold can be increased appropriately, which will distinguish more abnormal nodes.

6. Performance Evaluation

This experiment is divided into two parts of testing, which are divided into testing the CRMWSL reputation value calculation model and testing the performance of the C-PBFT consensus algorithm. The consensus algorithm test part uses go language to simulate the

C-PBFT algorithm, and the throughput and latency are evaluated for 30, 60, 90, 120, 150, 180, and 210 nodes, respectively. The experimental test was performed 100 times, each time the client sent 200 request messages, and the average of 100 times was taken as the test result. Major parameters used in the simulation are listed in Table 2.

The CRMWSL model test uses the San Francisco taxi data set, which records the moving tracks of 536 taxis in a month. Figure 4 shows the track distribution points of 200 taxis in a month,whose latitude and longitude are 37.73~37.80 and −122.50~−122.38, respectively. 400 RSUs are deployed in this area for testing, and the update period of RSU reputation is 1 min.

Table 2. Parameter setting in the simulation.

Parameter	Setting
Frequency of interaction between vehicle and RSU	[50,200] times / week
Coverage range of RSUs	[300,500] m
Speed of vehicles	[50,150] km/h
Weighting parameters	$\chi = 0.4$, $\tau = 0.6$, $\rho_1 = 0.5$, $\rho_2 = 0.5$
Rate of compromised vehicles	[10%, 90%]
Successful transmission probability of data packets	[0.5,1]
Vehicle to RSU bandwidth	20 MHz

Figure 4. Vehicle track distribution map.

6.1. Reputation Value Change Rate

In the proposed CRMWSL scheme, vehicles calculate the reputation values of candidate nodes based on local opinions and recommendations from other vehicles. The CRMWSL scheme is compared with the traditional subjective logic (TSL) scheme [29] and the MWSL scheme [30], which is a typical model that uses linear functions to calculate reputation.That is, $T^{l}_{i\to j} = (1-k)T_{\text{ave}} + kT_{\text{las}}$, where $T_{\text{ave}} = b^{\text{ave}}_{x\to j} + 0.5u^{\text{ave}}_{x\to j}$ and $T_{\text{las}} = b^{\text{las}}_{i\to j} + 0.5u^{\text{las}}_{i\to j}$, where k is the weight, set to 0.5. $b^{\text{ave}}_{i\to j}$ and $u^{\text{ave}}_{i\to j}$ are the average values of $b_{i\to j}$ and $u_{i\to j}$ of other vehicles, respectively. $b^{\text{las}}_{i\to j}$ and $u^{\text{las}}_{i\to j}$ of the RSU are the latest $b_{i\to j}$ and $u_{i\to j}$ in the local opinion of vehicle V_i.

Assuming that the probability of abnormal behavior of the abnormal vehicle is 70%, and the abnormal vehicle interacts with other normal vehicles through RSUs, the reputation value of the target RSU decreases over time. Figure 5 shows the change in the reputation of the malicious miner candidates for three schemes: (i) MWSL scheme, (ii) TSL scheme, and (iii) CRMWSL scheme. It can be seen that the CRMWSL scheme updates the reputation value more accurately, resulting in a lower reputation value for anomalous RSUs. After 7 min, the reputation value drops to 0.5, which is lower than that of the TSL and MWSL schemes, implying that the probability of anomalous RSUs being detected is higher in the CRMWSL scheme when the trust threshold is 0.5. Due to the weight of interaction frequency, timeliness, and interaction effects on the recommended and local opinions, the reputation value of RSU nodes in the CRMWSL scheme falls below the trust threshold faster than in the TSL scheme and MWSL scheme. Therefore, the proposed scheme achieves more accurate reputation calculation and is more secure and fair during committee elections.

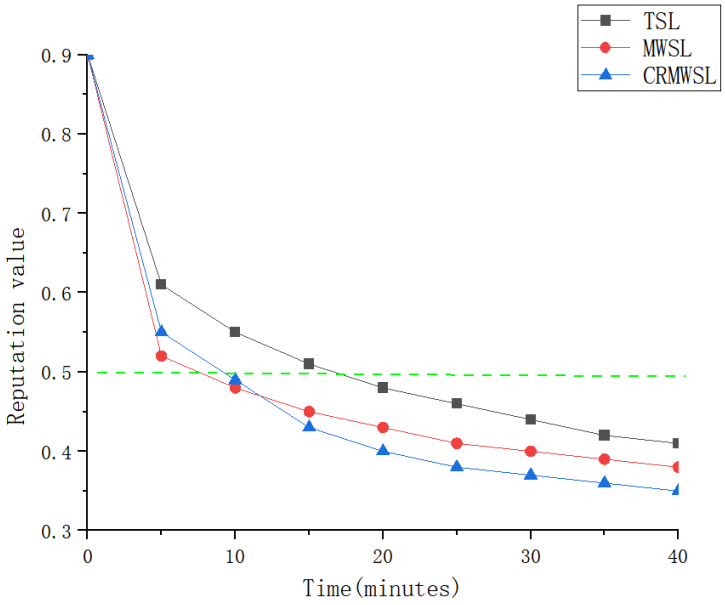

Figure 5. The change rate of reputation value of malicious RSUs.

6.2. Malicious RSUs Detection Success Rate

As depicted in Figure 6, our observations reveal distinct trends in the detection rates of 10 malicious RSU nodes over a 60-min interval. Notably, as the trust threshold increases, the scheme's capability to distinguish abnormal nodes also grows. In this context, our CRMWSL scheme outperforms both the MWSL and TSL schemes in successfully detecting malicious RSUs.

More specifically, when the detection success threshold is set to 0.45, the CRMWSL scheme achieves a 100% detection rate, which significantly surpasses the performance of the MWSL and TSL schemes. These results underscore the CRMWSL scheme's ability to reliably identify potential security threats, thereby enhancing the overall security level of the system.

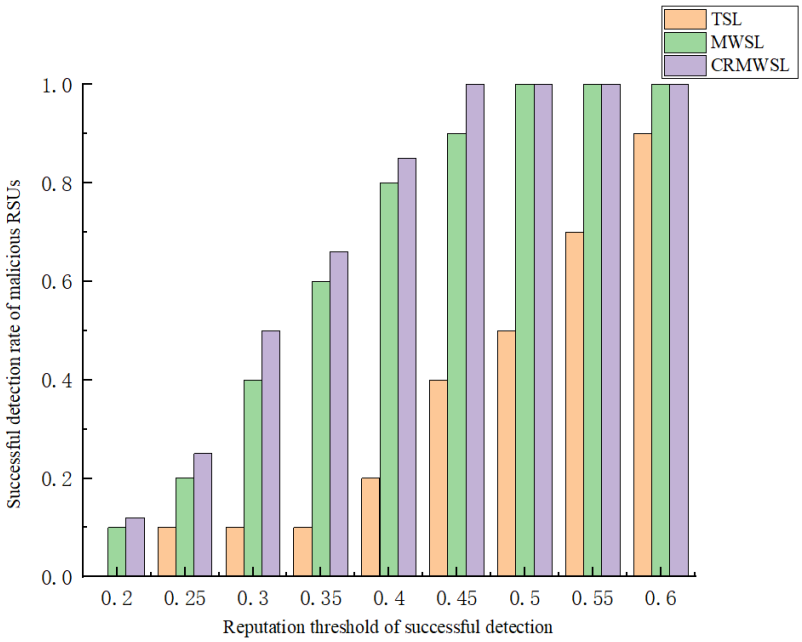

Figure 6. Detection rate under different trust thresholds.

6.3. Communication Overhead

The communication complexity analysis of the C-PBFT consensus algorithm: Local consensus is performed first in the region.

(1) In the pre-prepare phase, each group master node broadcasts the message to each node of the committee, and the communication overhead is u −1 at this time.
(2) In the prepare phase, when each RSU node that receives the message sends a verification message to all nodes in the group except its own node, and the overhead is (u − 1)(u − 1) at this time.
(3) In the commit phase, in which all nodes receive verification messages from other nodes in the previous phase, the nodes confirm and count the number of messages received, and the overhead is u(u − 1) at this time.
(4) In the reply phase, each node sends a reply message to the master node, and the communication volume is u − 1.

The first layer of node consensus is performed, and since there are n groups involved in consensus, a total of n nodes are involved in the first layer.

(1) In the pre-prepare phase, when the master node in each region receives enough feedback messages, this message is put into the first layer transaction pool, and the first layer master node reads the transaction and broadcasts it to all nodes in the first layer, at this time the communication overhead is n − 1.
(2) The communication overhead of the prepare and commit phases is similar to that of the first round of consensus in the bottom layer; then, its communication overhead is n(n − 1) + (n − 1)(n − 1).
(3) In the reply phase, each regional master node sends a reply message to the master node, and the communication is n − 1.

Therefore, the number of communications for the improved C-PBFT consensus algorithm to complete a consensus process is the total communication complexity, as shown in Equation (20).

$$C_1 = 2u^2 + 2n^2 - 2u - n + 1 \tag{20}$$

The number of communications in a consensus process of the original PBFT consensus algorithm is $C_2 = 2m^2n^2 - 2mn$.

Figure 7 shows a comparative analysis of the communication overhead between PBFT and C-PBFT consensus algorithms. It is clear that the communication overhead generated by C-PBFT is significantly lower throughout the blockchain network, and this overhead gradually increases as the number of consensus nodes increases. The reduction of communication overhead is mainly attributed to the reduction of the scale of consensus nodes by the C-PBFT algorithm. A node only needs to send messages to regional committee nodes instead of to all nodes. When the number of network nodes is 180, the communication overhead of PBFT is 43,832, and that of C-PBFT is 20,608 (three groups). This represents a significant 68% reduction in communication overhead.

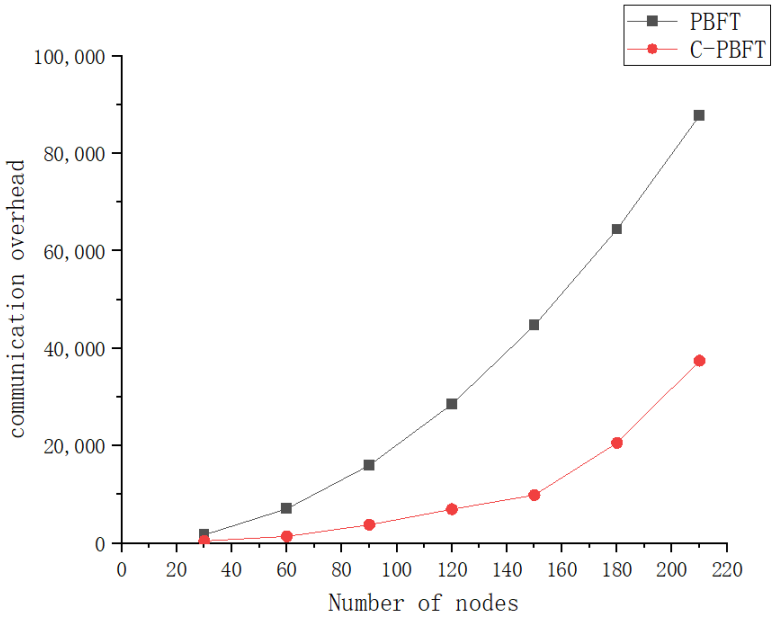

Figure 7. Comparison of communication overhead between C-PBFT and PBFT.

6.4. Consensus Latency

As can be seen from Figure 8, the consensus delay of the three algorithms increases gradually as the number of nodes increases. The consensus delay of PBFT is the highest when the number of nodes is different, and the C-PBFT algorithm is lower than PBFT and TLPBFT on the whole, because the reputation calculation model of the C-PBFT algorithm is more flexible than TLPBFT, and the reputation value of nodes is obtained through the integration of local opinions and recommendation opinions. The identity of the primary node selected by the C-PBFT algorithm is not easy to be attacked by malicious prediction, and the consensus node cluster is more credible, does not lead to frequent view conversion, has lower consensus delay and higher consensus efficiency, and further reduces the number of consensus nodes by using committee strategy.

6.5. Throughput

As shown in Figure 9, with the continuous increase of the number of nodes, the throughput of the three algorithms shows a trend of decline. The throughput of the C-PBFT algorithm is higher than that of PBFT and TLPBFT, because C-PBFT elects committees in each region to participate in the consensus, reducing the number of consensus nodes, thus reducing the communication overhead, and the advantage becomes more obvious as the number of nodes increases. Therefore, in the networking of vehicles, the C-PBFT algorithm can maintain high efficiency and stability.

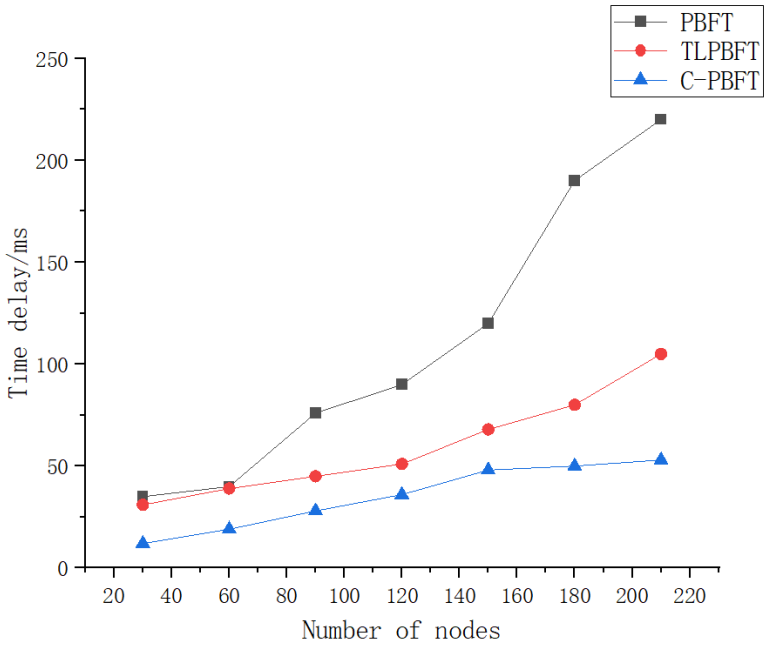

Figure 8. The consensus latency of the three consensus algorithms.

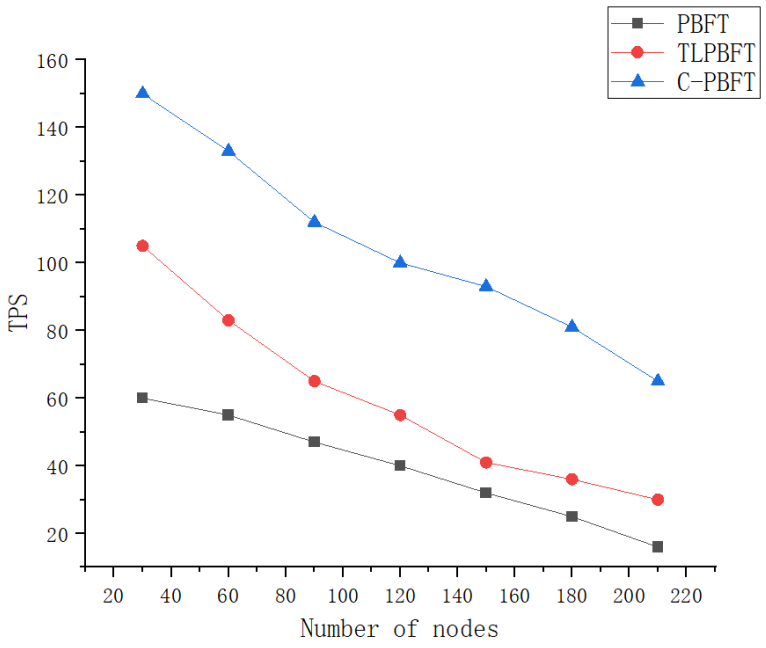

Figure 9. The throughput of the three consensus algorithms.

7. Conclusions

To meet the requirements of vehicle speed, latency, and communication overhead in the actual environment of vehicle networking, this paper modified the original PBFT consensus structure and designed an extensible double-layer PBFT consensus algorithm. In addition, a multi-weight subjective logic model CRMWSL for calculating reputation value is proposed, in which factors such as interaction frequency, event timeliness, and distance are taken into account to achieve accurate calculation of RSU node reputation value. Meanwhile, suitable nodes are elected into the committee to participate in consensus according to their reputation values, which further reduces communication overhead and improves blockchain scalability.

The experimental results show that the proposed CRMWSL model has great advantages over TSL and MWSL in improving the detection rate of malicious nodes, and the proposed C-PBFT consensus algorithm is superior to PBFT and TLPBFT in terms of transaction latency, throughput, and communication overhead.

In our future work, we will think about adding more weights to further increase the node reputation value's correctness and extending the double-layer consensus method to multi-layer research to further reduce consensus time and increase consensus performance. In order to provide more safe and effective services for the Internet of Vehicles, we will also aim to employ blockchain technology to solve network security issues in the Internet of Vehicles.

Author Contributions: Methodology, J.Z.; Formal analysis, J.Z.; Investigation, Z.D. and Y.L.; Resources, Y.F.; Data organization, M.H. and L.L.; Writing—original draft, J.Z.; Writing—review and editing,J.Z., Y.F. and Z.D.; Visualization, Y.F.; Supervision, Z.D.; Funding acquisition, Z.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by the National Foreign Expert Program of the Ministry of Science and Technology (Grant No.G2023041040L).

Informed Consent Statement: Not applicable.

Data Availability Statement: All the data are included in the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yang, Z.; Yang, K.; Lei, L.; Zheng, K. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
2. Yue, L.; Junqin, H.; Shengzhi, Q. Big data model of security sharing based on blockchain. In Proceedings of the 3rd International Conference on Big Data Computing and Communications (BIGCOM), Orlando, FL, USA, 15–18 December 2017.
3. Yuan, Y.; Wang, F.Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Changsha, China, 17–18 December 2016.
4. Kim, K.S. The trailer of blockchain governance game. *arXiv* **2018**. [CrossRef]
5. Liu, X.; Huang, H.; Xiao, F.; Ma, Z. A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs. *IEEE Internet Things J.* **2020**, *7*, 4101–4112. [CrossRef]
6. Zhang, X.; Chen, X. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network. *IEEE Access* **2019**, *7*, 58241–58254. [CrossRef]
7. Gao, J.; Agyekum, O.; Sifah, E.B.; Acheampong, K.N. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. *IEEE Internet Things J.* **2020**, *7*, 4278–4291. [CrossRef]
8. Li, U.G.; Yang, Q.; Wang, H. Trust Assessment in Online Social Networks. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 994–1007. [CrossRef]
9. Liu, Y.; Li, K.; Jin, Y. A novel reputation computation model based on subjective logic for mobile ad hoc networks. *Future Gener. Comput. Syst.* **2011**, *27*, 547–554. [CrossRef]
10. Jaimes, L.M.S.; Ullah, K. ARS: Anonymous reputation system for vehicular ad hoc networks. In Proceedings of the 2016 8th IEEE Latin-American Conference on Communications (LATINCOM), Medellin, Colombia, 15–17 November 2016.
11. Rivas, D.A.; Guerrero-Zapata, M. Chains of trust in vehicular networks: A secure points of interest dissemination strategy. *Ad Hoc Netw.* **2012**, *10*, 1115–1133. [CrossRef]
12. Lin, H.; Ma, J.; Hu, J. SLCRM—Subjective logic based cross layer reputation mechanism for wireless mesh networks. *China Commun.* **2012**, *5*, 10572.
13. Moreira, E. An Evaluation of Reputation with Regard to the Opportunistic Forwarding of Messages in VANETs. *EURASIP J. Wirel. Commun. Netw.* **2019**, *10*, 993–1004.
14. Josang, A.; Hayward, R.; Pope, S. Trust Network Analysis with Subjective Logic. In Proceedings of the Twenty-Ninth Australasian Computer Science Conference, Cap Esterel, France, 25–31 August 2006.
15. Miller, A.; Juels, A. Permacoin: Repurposing bitcoin work for data preservation. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014.
16. Gao, S.; Yu, T.; Zhu, J. T-PBFT: An eigentrust-based practical byzantine fault tolerance consensus algorithm. *China Commun.* **2019**, *5*, 9761. [CrossRef]
17. Xiang, F.; Huaimin, W. Proof of previous transactions (PoPT): An efficient approach to consensus for JCLedger. *IEEE Trans. Syst.* **2019**, *19*, 332. [CrossRef]

18. Wang, Q.; Yu, J.; Peng, Z. Security analysis on dBFT protocal of NEO. In Proceedings of the International Conference on Financial Cryptography and Data Security, Montreal, QC, Canada, 22–25 October 2020.
19. Kwon, J. Tendermint: Consensus without Mining. 2022. Available online: https://tendermint.com/static/docs/tendermint (accessed on 10 March 2023).
20. Gilad, Y. Algorand: Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, Gino-wan, Japan, 25–28 March 2017.
21. Li, W.Y.; Feng, C.L.; Zhang, L. A scalable multi-layer PBFT consensus for blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2020**, *32*, 1146–1160. [CrossRef]
22. Singh, A.K. A multi-layered network model for blockchain based security surveillance system. In Proceedings of the 2020 IEEE International Conference for Innovation in Technology, Bangluru, India, 6–8 November 2020.
23. Fortino, G.; Messina, F.; Rosaci, D. Using blockchain in a reputation-based model for grouping agents in the internet of things. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1231–1243. [CrossRef]
24. Hou, Y.C.; Liu, W.X.; Lin, H. Multi-layer access control mechanism based on blockchain for mobile edge computing. In Proceedings of the 2020 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, Exeter, UK, 17–19 December 2020.
25. Xu, G.X.; Wang, Y.S. Improved PBFT Algorithm Based on Vague Sets. *Secur. Commun. Netw.* **2022**, *6*, 144664 . [CrossRef]
26. Zhai, B.Q.; Wang, J.; Han, L. Hierarchical proxy consensus optimization for IoV based on blockchain and trust value. *Chin. J. Netw. Inf. Secur.* **2022**, *212*, 109048.
27. Liu, W.; Zhang, X.H.; Feng, W.L. Optimization of PBFT algorithm based on QoS-aware trust service evaluation. *Sensors* **2022**, *22*, 4590. [CrossRef] [PubMed]
28. Wikipedia. Binomial Distribution. Available online: https://en.wikipedia.org/wiki/Binomial_distribution (accessed on 15 April 2023).
29. Huang, X.; Yu, R.; Kang, J.; Xia, Z. Software defined networking for energy harvesting internet of things. *IEEE Internet Things J.* **2018**, *5*, 1389–1399. [CrossRef]
30. Kang, J.W. Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]