Article

Blockchain-Assisted Reputation Management Scheme for Internet of Vehicles

Qian Liu [1,2,3], Junquan Gong [1,2,3], Qilie Liu [1,2,3,*]

[1] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2] Key Laboratory of the Ministry of Education on Mobile Communications Technology, Chongqing 400065, China
[3] Chongqing Key Laboratory of Mobile Communications Technology, Chongqing 400065, China
* Correspondence : liuql@cqupt.edu.cn

Abstract: With the rapid development of Internet of Vehicles (IoV), particularly the introduction of mobile edge computing (MEC), vehicles can efficiently share data with one another. However, edge computing nodes are vulnerable to various network attacks, posing security risks to data storage and sharing. Moreover, the presence of abnormal vehicles during the sharing process poses significant security threats to the entire network. To address these issues, this paper proposes a novel reputation management scheme, which proposes an improved multi-source multi-weight subjective logic algorithm. This algorithm fuses direct and indirect opinion feedback of nodes through the subjective logic trust model while considering factors such as event validity, familiarity, timeliness, and trajectory similarity. Vehicle reputation values are periodically updated, and abnormal vehicles are identified through reputation thresholds. Finally, blockchain technology is employed to ensure the security of data storage and sharing. By analyzing real vehicle trajectory datasets, the algorithm is proven to effectively improve the differentiation and detection rate of abnormal vehicles.

Keywords: IoV; MEC; Data Sharing; Reputation Management; Subjective Logic Trust Model; Blockchain

1. Introduction

In the era of intelligence, Internet of Vehicles (IoV) technology has gained significant attention as it seamlessly integrates with various industries such as automotive, electronics, information and communication, and road transportation [1]. A vast number of internet-connected vehicles can unlock numerous new application values; however, they may also contribute to increased traffic congestion and accidents simultaneously. To address these challenges, experts have proposed Intelligent Transportation Systems (ITS) [2]. As a vital branch of IoT technology applied in the transportation sector, IoV serves as a critical component of future ITS [3]. The IoV can unify intelligent vehicles with public infrastructure, sensors, computing nodes, pedestrians, and other system elements in the surrounding environment. This enhances the safety of all road users through a comprehensive information-exchange platform between vehicles and heterogeneous networks, ultimately fostering a higher quality public environment and space [4].

Numerous applications in the IoV, such as image-assisted navigation, intelligent driving, and gaming entertainment, require real-time computation and storage of large amounts of data [5]. However, owing to the limited computing resources of vehicles and the long latency of cloud computing, the IoV's application and development face significant challenges [6]. To address these issues and challenges, researchers have introduced Mobile Edge Computing (MEC) technology into IoV, forming a new network paradigm called Vehicular Edge Computing (VEC) [7]. MEC is a novel computing technology that shifts data processing and analysis tasks from central servers to edge devices on a network, thereby reducing the overall communication and computing latency [8]. By deploying servers near users, MEC provides abundant network resources for resource-constrained vehicles, minimizing the computational latency of vehicle applications and enhancing the computing and storage capabilities of the IoV [9,10]. However, vehicles must offload data and computing tasks to edge nodes before receiving processing results. This data often carries sensitive information, such as the vehicular driving status and location, which may be leaked or tampered with during the

 doi:10.20944/preprints202304.0449.v1

process, posing severe threats to vehicle safety [11]. Additionally, some abnormal vehicles in the VEC network may provide irrelevant or erroneous information to other vehicles due to defective components or malicious intent during information sharing [12], thereby posing significant security risks to the network. Therefore, efficient identification of unreliable vehicles in a network has become an essential research topic in VEC [13].

To address these challenges, the IoV requires a technical solution that ensures the authenticity and integrity of data storage while providing secure and trustworthy data sharing and transaction platforms. Additionally, an accurate calculation of vehicle reputation values is urgently required to differentiate between normal and unreliable vehicles during the sharing process.

2. Related Work

Numerous studies have focused on trust issues in data sharing and transactions in the IoV and have analyzed and modeled them. To detect abnormal vehicle nodes, various management schemes and trust models can be employed to assess the reputation of vehicle nodes in the network [14], determining the authenticity of the message content based on the message's reliability.

References [15,16] proposed to update and manage vehicle reputation levels through trusted authoritative nodes, which then determined whether a vehicle node could access the network. Vehicles must query central nodes for the reputation of other vehicles to evaluate the credibility of the messages. Reference [17] designed a reliable cooperative download reputation system to promote cooperation and penalize malicious vehicles. However, these centralized reputation management schemes face challenges such as single-point failures, high latency, and data leakage, making them unsuitable for the distributed network architecture of VEC.

Blockchain technology with its decentralized, tamper-proof, secure, and traceable features has been utilized to VEC scenarios [18]. With the immutability of distributed ledgers, blockchain allows for the establishment of trust relationships in a decentralized manner among untrusted entities. Therefore, using blockchain to assist VEC networks promotes information transparency among vehicles and ensures the secure storage and sharing of data [19,20]. Additionally, smart contract technology in the blockchain provides decentralized and reliable automated transactions among vehicles. References [21,22] proposed blockchain-based vehicle-reputation computation methods. Reference [21] used the consortium blockchain and considered direct and indirect opinion sources to calculate vehicle reputation values based on beta and exponential distributions. Reference [22] employed a Bayesian inference model based on a blockchain vehicle network to validate messages received from neighboring vehicles, generating binary positive and negative ratings for message sources, and calculating vehicle reputation based on weighted distances and events.

However, the aforementioned studies only considered simple binary logic and weighting to obtain the final reputation value, which cannot cope with the complexity of real-world events. Subjective Logic (SL) trust model [23,24] are widely applied mathematical tools for modeling vehicle reliability because it can quantify trust, doubt, and uncertainty [25] and consider the trustworthiness of opinion sources. By combining the probability theory and logical reasoning, SL models represent the objective truth of events more accurately than simple binary logic.

Blockchain-assisted reputation-management methods for VEC networks based on Subjective Logic (SL) trust model and their evolving models have garnered attention from researchers. Reference [26] introduced Subjective Logic (SL) trust model into mobile ad hoc networks and calculated fused direct and indirect reputation values by considering weights and weight-transfer formulas. Reference [27] introduced Subjective Logic (SL) trust model into fog computing for node-to-node trust computation and proposed a peer-to-peer bidirectional subjective logic trust management method that allows service requesters to verify the trustworthiness of service providers and vice versa. References [28,29] both proposed a Three-weight Subjective Logic (TWSL) algorithm based on VEC, considering factors such as vehicle familiarity, timeliness, and trajectory similarity for a more accurate vehicle reputation value computation. Reference [30] further presented a credit scheme based on a four-weight subjective logic trust model that considered factors such as node resource availability, event validity, familiarity, and timeliness. Reference [31] proposed an algorithm

based on a three-value subjective logic trust model to evaluate vehicle reputation values by considering factors such as vehicle historical cycle reputation values, feedback party reputation values, and familiarity with updating vehicle reputation values.

To summarize, the majority of existing studies on reputation management methods based on blockchain and Subjective Logic (SL) trust model do not address the simplicity and singularity of opinion sources, and do not consider the fusion of multiple opinion sources. While some schemes incorporate multi-hop indirect opinions, their validation is based on simulation software rather than real datasets to verify the algorithm's time complexity and scheme effectiveness. Additionally, majority of the studies only apply various weights to final opinions, without considering the feedback of the shared events themselves as dynamic weights.

This paper focuses on the background of reputation calculation in IoV with the assistance of blockchain technology, specifically exploring the issue of reputation value calculation in the process of vehicle information sharing. The main research objectives are as follows:

- Firstly, to ensure secure storage and sharing of data, the study leverages mobile edge computing and consortium blockchain technology to guarantee the security and authenticity of shared data in IoV. Additionally, by establishing a blockchain network among MEC servers, the computational and storage resources required for the blockchain are ensured simultaneously. Furthermore, MEC servers can achieve real-time data synchronization through wired connections, thereby resolving synchronization issues among different servers and vehicle concurrency problems in the network.
- Secondly, to enhance the accuracy and multi-sourcing of the vehicle reputation value calculation, the study proposes the Multi-Source Multi-Weight Subjective Logic (MSMWSL) algorithm. This innovative algorithm employs the Piel model of growth curve functions and utilizes historical interaction information stored in the blockchain to calculate the weights of positive and negative events. Additionally, it considers the weights of familiarity, timeliness, and trajectory similarity to comprehensively weigh and evaluate feedback, and subsequently obtain a direct combination of opinions based on these weights. Moreover, the algorithm ingeniously leverages the weight transfer formula and the subjective logical discount operator to derive indirect combined opinions. Ultimately, the algorithm employs the subjective logical fusion operator to acquire system opinions and final reputation values by integrating direct and indirect opinions.

The rest of the research article is organized as follows. Section 2 presents the literature review of the state-of-the-art works and the main contributions of this paper. Section 3 describes the system model and the specific process involved. Section 4 elaborates on the computational process of the proposed scheme. Simulation results and discussion are provided in Section 5. Lastly, Section 6 provides the conclusions.

3. The Framework of Blockchain-Assisted Reputation Management Scheme for IoV

3.1 System Model

In a consortium blockchain, a distributed ledger is created, audited, and shared by multiple authorized nodes, offering cost effectiveness and better suitability for VEC network scenarios [32]. Therefore, the system model in this study is based on a consortium blockchain and VEC consisting of the edge, consensus, and cloud layers. The system model is shown in Figure 1:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

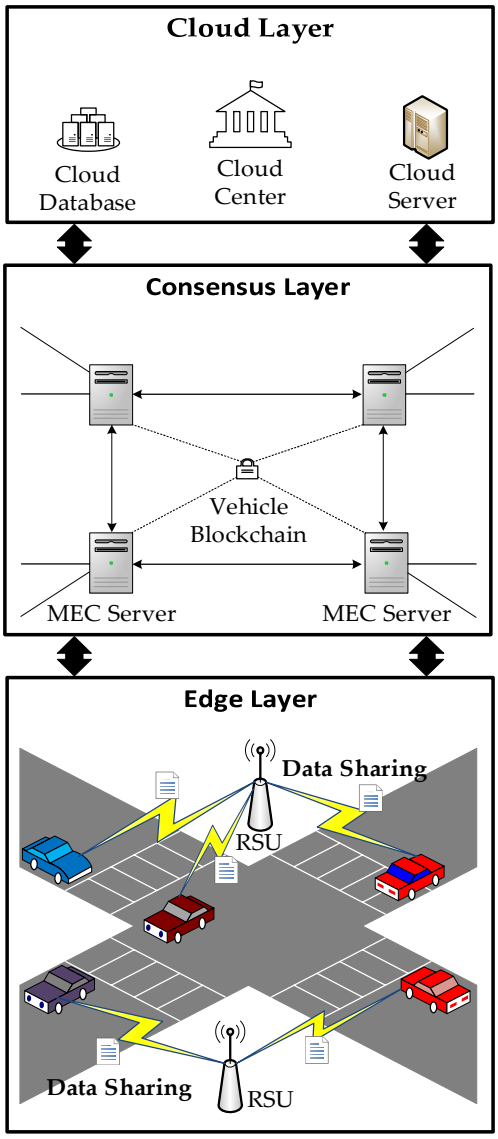

Figure 1. System model.

The cloud layer centrally manages cloud servers, data centers, etc., and is primarily responsible for complex data processing, analysis, optimization, storage, and other functions. It is also responsible for identity verification and authorization of the consortium blockchain. A central cloud can permanently store large amounts of data and perform complex delay-tolerant computing tasks for vehicles. Frequently used data and time-sensitive tasks in vehicles can be completed using a consensus layer.

In the consensus layer, a vehicle edge cluster is formed by connecting Roadside Units (RSUs) deployed along the road to the MEC servers and interconnecting them. This formation enables real-time data synchronization among the MEC servers within the cluster, thus addressing synchronization issues and vehicle concurrency problems in the network. Each vehicle communicates with the nearest RSU to access the local vehicle-edge cluster. The layer's primary focus is on aggregating and managing data and reputation values, selecting and allocating resources, and transmitting data to the central cloud via wired connections when necessary.

In the edge layer, vehicles equipped with onboard units can access services by communicating with the RSUs. Onboard units perform simple computations, collect local traffic condition data from sensor devices, and upload the data to the consensus layer through the RSUs. This layer is primarily responsible for data generation, transmission, and sharing.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

3.2 Sharing Process

To reduce the costs associated with establishing and operating a blockchain, this study employs consortium blockchain technology to construct a vehicle blockchain and utilizes smart contract technology to facilitate distributed data storage and secure data sharing. The process schematic of this approach is illustrated in Figure 2.

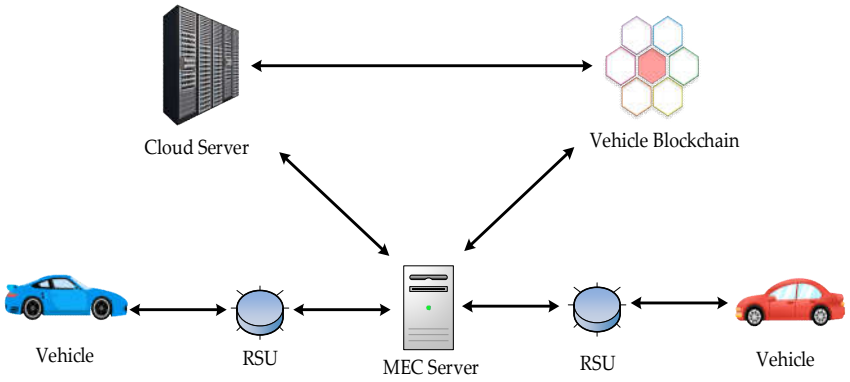

Figure 2. Flow diagram.

3.2.1. Network Initialization

Initially, the RSUs at the edge layer accept the vehicle registration information and send the data to the MEC servers, which collect and organize the data before forwarding them to the central cloud for review.

Subsequently, the central cloud obtains the vehicle's electronic identity and legal documents from the vehicle management department, based on which it conducts audits and registrations.

Finally, the approved vehicle information is added to the certificate list. The central cloud issues identity certificates and public-private key pairs for the blockchain to the corresponding vehicles and distributes the latest permit list to all MEC servers and RSUs.

3.2.2. Information Upload

Mobile vehicles are equipped with computing and storage resources, as well as various sensors, including LiDAR, millimeter-wave radar, GPS terminals, and high-definition cameras. These vehicles continuously transmit trajectory data and environmental information, such as latitude and longitude information, road conditions, weather conditions, and parking space utilization rates, to RSUs, which package this data into "blocks." These "blocks" are eventually sorted and stored in the consortium blockchain by MEC servers, and can be provided to other users in the system for browsing and downloading. To protect user security and privacy, data should be anonymized, encrypted, and accompanied by the digital signature of the data provider.

3.2.3. Information Sharing

Initially, data requesters download shared data blocks within a specific range from the vehicle blockchain via the RSUs and search for the data they are interested in using an information index. Based on their actual needs and the data provider's reputation, data requesters select the best provider and generate a smart contract that reflects their needs and the data provider’s reputation.

Upon receiving the request, the RSUs first verify the identity of the data requester and send information such as the requester's public key to a nearby MEC server. The MEC server then verifies the data requester's certificate and locates the requested shared information within the vehicle blockchain. The information is encrypted using the data requester's public key and then sent directly to the requester.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

After obtaining the shared data, the data requester automatically pays the provider according to the contract and generates a record of the data-sharing event. This record, in the form of a data block, is added to the blockchain.

Finally, at the end of the transaction, the data requester provides feedback to the system based on the actual data situation, indicating whether the event was positive or negative. Based on this feedback, the system periodically updates the reputation values. The MEC server packages all transactions and updates reputation values into a block, which is then broadcasted to the network to reach a consensus. After the PBFT consensus process, the block is recorded in the blockchain.

Based on the PBFT consensus mechanism, all participating nodes have equal status, with one node selected as the primary node and the remaining nodes serving as backup nodes. The PBFT algorithm comprises three stages: pre-preparation, preparation, and commit. In each stage, when a node receives replies from more than 2/3 of the other nodes, it proceeds to the next stage.

4. The MSMWSL Algorithm for Reputation Management

4.1 Direct Opinion Combination

Based on the Subjective Logic (SL) model, by considering the direct opinion weights between shared vehicle nodes such as familiarity, timeliness, and trajectory similarity, a more accurate quantification of the differences in subjective opinions between vehicle nodes can be achieved, resulting in a direct opinion combination.

4.1.1 Direct Opinion Three Weights

1. Familiarity

Familiarity measures the degree of familiarity between vehicles; a higher familiarity implies a higher interaction frequency and more prior information, resulting in more reliable feedback. In this study, the familiarity between vehicle nodes is the ratio of the total interaction count between vehicle nodes within a certain period to the average interaction count of other vehicle nodes, denoted as $F_{i\to j}$:

$$\begin{cases} F_{i\to j} = N_{i\to j} / \overline{N_j} \\ \overline{N_j} = \dfrac{1}{N}\sum_{m\in M} N_{\mathrm{m}\to j} \end{cases}, \tag{1}$$

where i and j represent data users and data providers, $N_{i\to j}$ denotes the total number of information interactions between vehicle i and j within a specific time window, $\overline{N_j}$ represents the average interaction count of vehicle j with other vehicle nodes, N denotes the total number of vehicles j interacting with, and M represents the set of vehicles that have interacted with the vehicle node.

2. Timeliness

Newly uploaded data are emphasized for information sharing. This study defines the timeliness of direct opinions from vehicle nodes to vehicle nodes as an $TIM_{i\to j}$:

$$TIM_{i\to j} = \eta(t_i - t_j)^{-\varepsilon}, \tag{2}$$

where η and ε are predefined parameters for adjusting the timeliness, t_i represents the time point when the data user i completes the transaction, and t_j represents the time point when the data provider j uploads shared information.

3. Trajectory Similarity

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

Trajectory similarity measures the similarity between the driving states of the data user and the data provider. In this study, similarity is calculated based on the velocity and direction of the trajectory data in the continuous trajectory segments covered by the onboard sensors of both vehicles during sharing, denoted as $SIM_{i\to j}$:

$$SIM_{i\to j} = \tau_1 S_{spd} + \tau_2 S_{dirc}, \tag{3}$$

where S_{spd} represents the velocity similarity of the trajectory; S_{dirc} represents the direction similarity of the trajectory; and their weights in the trajectory similarity are τ_1 and τ_2, respectively, with $\tau_1 + \tau_2 = 1$.

The similarities of velocity and direction are calculated using the cosine similarity formula:

$$S_j^i = \sum_{k=1}^{n} c_k^i c_k^j \Big/ \left(\sqrt{\sum_{k=1}^{n} (c_k^i)^2} \sqrt{\sum_{k=1}^{n} (c_k^j)^2}\right), \tag{4}$$

where c_k^i represents the velocity or direction in the trajectory of vehicle node i; c_k^j represents the velocity or direction in the trajectory of vehicle node j; and k represents the number of trajectory points in a similar trajectory segment during the information sharing process between the two vehicles.

1. Direct Opinion Weights

The final direct weight is obtained by taking the weighted average of the three factors in from equation 1 to equation 3:

$$\delta_{i\to j} = \rho_1 F_{i\to j} + \rho_2 TIM_{i\to j} + \rho_3 SIM_{i\to j}, \tag{5}$$

where the direct opinion weight parameters are ρ_1, ρ_2, ρ_3, with $\rho_1 + \rho_2 + \rho_3 = 1$.

4.1.2 Event Validity Based on Growth Curve Function

1. Growth Curve Function

The growth curve function is a class of mathematical functions used to describe the developmental process of things. Generally, the development process is similar to the biological development process, which includes three stages: initiation, development, and maturity, with different development speeds at each stage. In the initial stage, the change is slow; in the development stage, the change accelerates; and in the maturity stage, the change slows again. The curve of the development process drawn according to the development rules of these three stages is usually called a growth curve or logistic growth curve. This curve has been widely used to describe and predict various fields of technical and economic development. There are many mathematical growth curve models, among which the Gompertz and Pearl models are the most widely used. In reference [33], the Gompertz model was employed to calculate and update the reputation values. In contrast, reference [34] utilized the Piel model, incorporating the difference between positive and negative events for reputation value calculation. Consequently, this study refers to these publications and adopts a weighted average of negative event counts in conjunction with the Piel model for reputation calculation.

2 Event Effectiveness

Event effectiveness indicates that in the reputation value calculation, the weights of positive and abnormal events are different. The weight of the negative events decreased as the number of negative feedbacks increased, whereas that of the positive events increased as the number of negative feedbacks increased. In this study, the weighted sum of negative event numbers is used, and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

according to the Piel growth curve function, the effectiveness of negative event θ is obtained, whereas the effectiveness of positive event $1-\theta$ is:

$$\begin{cases} \theta = \mu / 1 + e^{Err_{x\to j}} \\ Err_{x\to j} = \dfrac{1}{\sum\limits_{x\in X}\delta_{x\to j}} \sum\limits_{x\in X}\delta_{x\to j} err_{x\to j} \end{cases}, \tag{6}$$

where μ is the adjustment factor of the growth curve, which determines the value range of θ. $Err_{x\to j}$ is the weighted average of the abnormal event numbers; X represents the set of vehicle nodes that have interacted with vehicle node; $\delta_{x\to j}$ represents the direct opinion weight between two vehicle nodes; and $err_{x\to j}$ represents the number of abnormal events in the interaction between the two vehicle nodes.

3 Direct Opinions Based on Event Effectiveness

Through the effectiveness of negative and positive events, the weighted vehicle node pairs' positive event number $\alpha^{\theta}_{i\to j}$ and the weighted vehicle node pairs' negative event number $\beta^{\theta}_{i\to j}$ were obtained:

$$\begin{cases} \alpha^{\theta}_{i\to j} = (1-\theta)\alpha_{i\to j} \\ \beta^{\theta}_{i\to j} = \theta\beta_{i\to j} \end{cases}, \tag{7}$$

where represents the number of positive events between vehicle nodes, and represents the number of negative events between vehicle nodes.

Subsequently, according to the evidence-mapping operator of subjective logic, a direct opinion is obtained $\omega_{i\to j} = (T_{i\to j}, D_{i\to j}, I_{i\to j})$:

$$\begin{cases} T_{i\to j} = (1-I_{i\to j})\dfrac{\alpha^{\theta}_{i\to j}}{\alpha^{\theta}_{i\to j} + \beta^{\theta}_{i\to j}} \\ D_{i\to j} = (1-I_{i\to j})\dfrac{\beta^{\theta}_{i\to j}}{\alpha^{\theta}_{i\to j} + \beta^{\theta}_{i\to j}} \\ I_{i\to j} = 1 - \ln(1+SIM_{i\to j}) \end{cases}. \tag{8}$$

4.1.3 Direct Opinion Combination Based on Three Weights and Event Validity

Subsequently, based on the TWSL algorithm [28,29] and considering the direct opinion weight, the direct combined opinion $\omega^{dir}_{j} = (T^{dir}_{j}, D^{dir}_{j}, I^{dir}_{j})$ is obtained:

$$\begin{cases} T^{dir}_{j} = \dfrac{1}{\sum\limits_{x\in X}\delta_{x\to j}} \sum\limits_{x\in X}\delta_{x\to j} T_{x\to j} \\ D^{dir}_{j} = \dfrac{1}{\sum\limits_{x\in X}\delta_{x\to j}} \sum\limits_{x\in X}\delta_{x\to j} D_{x\to j} \\ I^{dir}_{j} = \dfrac{1}{\sum\limits_{x\in X}\delta_{x\to j}} \sum\limits_{x\in X}\delta_{x\to j} I_{x\to j} \end{cases}, \tag{9}$$

where X represents the set of vehicles that interact with vehicle node j.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

4.2 Indirect Combined Opinions

The blockchain stores direct interaction information between vehicles in the system. It is necessary to obtain indirect opinion paths using an algorithm and calculate the indirect combined opinions using an indirect weight formula.

4.2.1 Indirect Opinion Path Search Algorithm Based on Depth-First Search

Using an indirect opinion path search algorithm based on Depth-First Search (DFS), we can obtain the required indirect opinions for the discount operator using subjective logic. The algorithm process is as follows:

Algorithm 1: Indirect Opinion Path Search Algorithm

```
Initialization
Input: Opinion set G of nodes, Complete set of nodes V, Target node Vt.
Output: All indirect opinion paths Ws reaching the target node Vt.
for all element Vs    //Consider nodes in set V, excluding Vt, as source nodes Vs
    Ws=[];              //Define the path set Ws for Vs.
    Opinion_Walk(G,Vs,Vt)      //Recursively search for vehicles that have interactions
     if Vs≠Vt and G[Vs]!=[]
       W←Vs;                    //Add qualifying nodes to the path W
     for node in G[Vs]
      if node not in W and len(W)<3
         Opinion_Walk(G,node,Vt);
       if len(W)==3 and Vs==Vt   //If an indirect path is found, add it to the path set Ws
         Ws←W;                  //Add qualifying nodes to the path W
       end if
      end if
    end for
    end if
end for
END
```

4.2.2 Indirect Combined Opinions Based on Discount Operator and Indirect Weights

Calculate indirect opinions based on all indirect opinion paths obtained in the previous subsection and the discount operator using subjective logic. We then computed the combined indirect opinions based on indirect weights.

4.2.3 Indirect Opinions Based on Discount Operator

After determining the opinion path using the indirect opinion-path search algorithm, the discounted opinion definition based on the indirect path can be calculated using the discount operator. Let the opinion of node A on node B be $\omega_{A\to B}=(T_{A\to B},D_{A\to B},I_{A\to B})$ and the opinion of node B on node C be $\omega_{B\to C}=(T_{B\to C},D_{B\to C},I_{B\to C})$. The indirect opinions of both nodes C is defined as $\omega_C^{A:B}=(T_C^{A:B},D_C^{A:B},I_C^{A:B})$:

$$\begin{cases} T_C^{\mathrm{A:B}}=T_{A\to B}T_{B\to C} \\ D_C^{\mathrm{A:B}}=T_{A\to B}D_{B\to C} \\ I_C^{\mathrm{A:B}}=D_{A\to B}+I_{A\to B}+\mathrm{T}_{A\to B}I_{B\to C} \end{cases}. \tag{10}$$

4.2.4 Indirect Weights

The indirect weights $\delta_C^{A:\mathrm{m}}$ are obtained according to the weight transfer formula in reference as

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

$$\delta_C^{A:m} = \frac{T_{A\to m}\delta_{m\to C}}{\sum_{n\in N} T_{A\to n}\delta_{n\to C}}, \tag{11}$$

where m represents the intermediate nodes that meet the serial relationship and N represents the vehicle node set meeting the serial relationship obtained by the indirect opinion path search algorithm.

4.2.5 indirect combined opinions

Based on indirect opinions and indirect weights, the weighted average was used to obtain the indirect combined opinion $\omega_C^{ind} = (T_C^{ind}, D_C^{ind}, I_C^{ind})$:

$$\begin{cases} T_C^{ind} = \dfrac{\sum_{n\in N}\sum_{m\in M} \delta_C^{\mathrm{n:m}} T_C^{\mathrm{n:m}}}{\sum_{n\in N}\sum_{m\in M} \delta_C^{\mathrm{n:m}}} \\ D_C^{ind} = \dfrac{\sum_{n\in N}\sum_{m\in M} \delta_C^{\mathrm{n:m}} D_C^{\mathrm{n:m}}}{\sum_{n\in N}\sum_{m\in M} \delta_C^{\mathrm{n:m}}} \\ I_C^{ind} = \dfrac{\sum_{n\in N}\sum_{m\in M} \delta_C^{\mathrm{n:m}} I_C^{\mathrm{n:m}}}{\sum_{n\in N}\sum_{m\in M} \delta_C^{\mathrm{n:m}}} \end{cases}, \tag{12}$$

where N and M represent the vehicle node set that satisfies the serial relationship obtained by the indirect opinion path search algorithm, and $\delta_C^{n:m}$ represents the indirect weight obtained from the serial relationship.

4.3 Fusion of Opinions and System Reputation Value

By using the fusion operator of the subjective logic trust model, direct and indirect opinions are combined to obtain the final system opinion. Suppose that the system's direct combined opinion on node C is $\omega_C^{\mathrm{dir}} = (T_C^{\mathrm{dir}}, D_C^{\mathrm{dir}}, I_C^{\mathrm{dir}})$, and the indirect combined opinion on node C is $\omega_C^{ind} = (T_C^{ind}, D_C^{ind}, I_C^{ind})$. The fusion opinion on node C is derived from both and is denoted as $\omega_C^{\mathrm{dir,ind}} = (T_C^{\mathrm{dir,ind}}, D_C^{\mathrm{dir,ind}}, I_C^{\mathrm{dir,ind}})$:

$$\begin{cases} \mathrm{T}_C^{\mathrm{dir,ind}} = (T_C^{\mathrm{dir}} I_C^{ind} + T_C^{ind} I_C^{\mathrm{dir}}) / k \\ D_C^{\mathrm{dir,ind}} = (D_C^{\mathrm{dir}} I_C^{ind} + D_C^{ind} I_C^{\mathrm{dir}}) / k \\ I_C^{\mathrm{dir,ind}} = (I_C^{\mathrm{dir}} I_C^{ind}) / k \\ k = I_C^{\mathrm{dir}} + I_C^{ind} - I_C^{\mathrm{dir}} I_C^{ind} \end{cases}. \tag{13}$$

In summary, based on the subjective logic algorithm, the final system reputation value for vehicle E_c is

$$E_c = T_C^{\mathrm{dir},ind} + \gamma I_C^{\mathrm{dir},ind}, \tag{14}$$

Here, γ is a given constant given by vehicles, which indicates the uncertainty effect level on reputation for vehicles. This constant can be set as 0.5 by default [29].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

5. Simulation and Results

5.1. System Setup

In this study, the performance of the proposed MSMWSL scheme is evaluated using a real-world Chongqing taxi dataset provided by Chongqing China Transport Telecommunications and Information Technology Co., Ltd. This dataset comprises the movement trajectories of approximately 1000 urban taxis over a month and mainly includes data such as latitude, longitude, speed, direction, and time. This study randomly selects 100 taxis as examples. In urban areas, vehicles typically follow familiar routes within specified time periods such as similar trajectories from home to work during the day. In the en route, vehicles can perceive road conditions within approximately a 200-meter range using equipment such as radar and sensors [35]. Consequently, vehicles can share this data to receive rewards or access this information to facilitate safe and convenient driving.

Malicious vehicles temporarily behave normally in the initial stages to gain the trust of other vehicles. This study assumes that after the detection period begins, they exhibit abnormal behavior. To identify these vehicles, the system periodically calculates their reputation values, and prohibits vehicles with reputation values below a certain threshold from accessing the network. We compared the proposed MSMWSL subjective logic algorithm with the TWSL and SL algorithms. The initial reputation values of all vehicles are represented by $E_0 = 0.6$.

5.2 Simulation experiment parameters

The parameter settings for the simulation experiment are shown in Table 1.

Table 1. Simulation experiment parameters table

Parameter Name	Value
Vehicle Count	100
Message Frequency	[5,10] times/cycle
Timeliness Parameter	$\eta = 10, \varepsilon = 1.05$
Trajectory Similarity Weight	$\tau_1 = 0.5, \tau_2 = 0.5$
Direct Opinion Weight	$\rho_1 = 0.3, \rho_2 = 0.3, \rho_3 = 0.4$
Pearl Growth Curve Function Adjustment Factor	μ=0.8

5.3 Simulation Results and Analysis

As shown in Figure 3, ten malicious vehicles were randomly selected for reputation updates during the observation period, and all vehicles interacted randomly with other vehicles. The figure shows that the reputation values of all malicious vehicles were below the initial reputation value of 0.6. Additionally, the reputation values of the malicious vehicles under the MSMWSL and TWSL algorithms were all below the reputation threshold. Notably, the reputation values of the malicious vehicles under the MSMWSL algorithm were significantly lower than those under the TWSL and SL algorithms. This is because the MSMWSL algorithm considers various factors such as event validity and the three weights of direct opinions, and integrates both direct and indirect opinion sources. This allows the system to calculate reputation more accurately, thereby identifying malicious vehicles more quickly.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

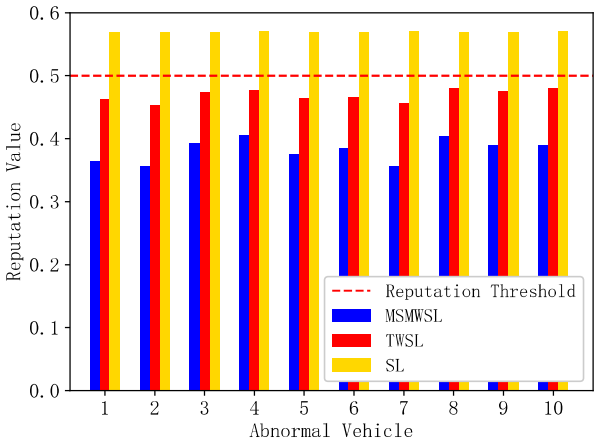

Figure 3. Comparison of reputation values of ten abnormal vehicles under four algorithms.

As shown in Figure 4, during the observation period, ten normal vehicles were randomly selected for reputation updates, with vehicles interacting randomly with each other. In the figure, the reputation values of all normal vehicles are above the initial reputation value of 0.6. Moreover, the calculated results of the MSMWSL algorithm were generally higher than those of the TWSL and SL algorithms. This is because all reputation calculation values are sufficiently weighted by various factors, allowing vehicles to choose vehicles with higher reputations intuitively when sharing information. This also indicates that, while quickly lowering the reputation values of malicious vehicles, the MSMWSL algorithm still performs well in evaluating the reputation of normal vehicles.

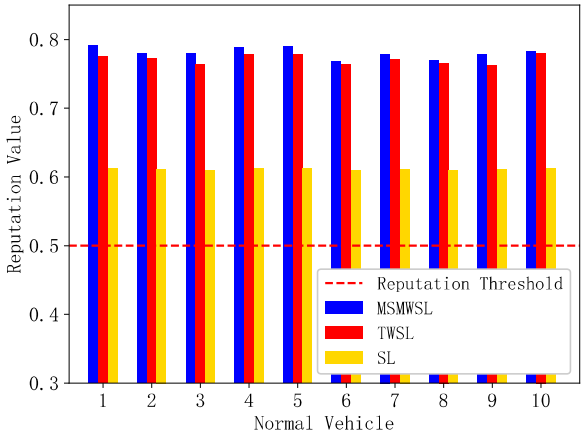

Figure 4. Comparison of reputation values of ten normal vehicles under four algorithms.

The change in the reputation value of an abnormal vehicle with the number of detection cycles is shown in Figure 5. Initially, this abnormal vehicle tended to provide high-quality data to other vehicles to gain trust in the system. However, during the detection window, the vehicle's reputation value gradually decreases owing to abnormal behavioral events. As shown in the figure, the reputation value of the abnormal vehicles under the MSMWSL and TWSL algorithms declined significantly faster than that under the SL algorithm. After the first detection cycle, the reputation values calculated by the MSMWSL algorithm decreased below the reputation threshold of 0.5, and the MSMWSL algorithm's value was lower than that of the TWSL algorithm. However, the values for the TWSL and SL algorithms remained above the reputation threshold. Eventually, in all detection cycles, the reputation value of the abnormal vehicles calculated using the MSMWSL algorithm was

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

significantly lower than that calculated using the other algorithms. Overall, the MSMWSL algorithm outperformed the other algorithms and exhibited higher detection efficiency for abnormal vehicles.

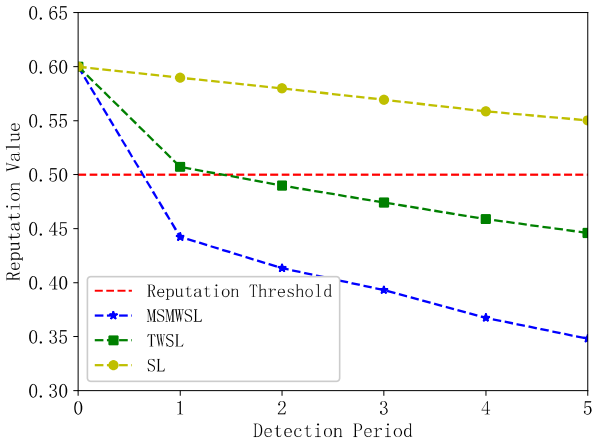

Figure 5. Change of abnormal vehicle reputation value with detection period under four algorithm.

During the observation period, 30 abnormal vehicles were randomly selected for reputation updates, and their detection rates were compared using the two algorithms and six reputation threshold values, as shown in Figure 6. This figure illustrates a comparison of the abnormal vehicle detection rates within the same detection cycle for the MSMWSL and TWSL algorithms. It is evident from the figure that under different threshold values, the MSMWSL algorithm has higher detection rates for abnormal vehicles than the TWSL algorithm. With a reputation threshold of 0.39, the detection rate of the MSMWSL algorithm for abnormal vehicles reached 80%, and increased to 100% when the threshold was 0.43. By contrast, the TWSL algorithm has detection rates of 20% and 70% for abnormal vehicles at reputation thresholds of 0.45 and 0.47, respectively, and reaches 100% when the threshold is 0.49.

This is because the MSMWSL algorithm can reduce the reputation values of misbehaving vehicles more rapidly under different thresholds than other algorithms, allowing for faster differentiation between abnormal and normal vehicles. Consequently, this algorithm can effectively eliminate potential security threats and enhance the safety of information sharing within a network.

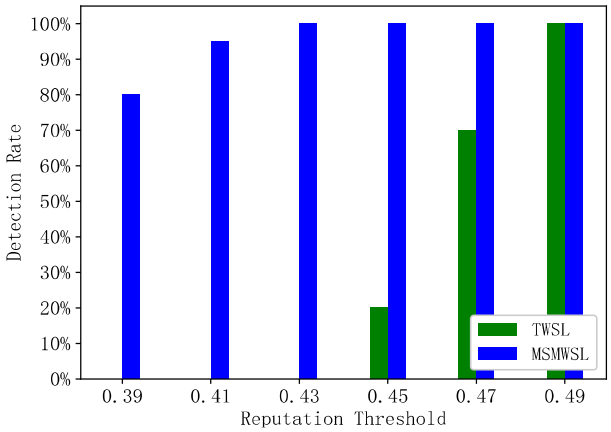

Figure 6. Abnormal vehicle detection rates of two algorithms under different reputation thresholds.

The changes in the detection rates of 30 randomly selected abnormal vehicles for reputation updates during the observation period under different reputation thresholds in the MSMWSL

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 April 2023 doi:10.20944/preprints202304.0449.v1

algorithm are shown in Figure 7. It should be noted that the higher the reputation threshold, the stronger is the ability to differentiate abnormal vehicles.

At a reputation threshold of 0.47, the MSMWSL algorithm achieved a 95% detection rate for abnormal vehicles in the first detection cycle, and reached 100% in the second cycle. When the reputation threshold was 0.45, the MSMWSL algorithm had an identification rate of 70% for abnormal vehicles in the first detection cycle, which increased to 100% in the second cycle. With a reputation threshold of 0.43, the MSMWSL algorithm attained an 80% identification rate for abnormal vehicles in the second detection cycle and achieved 100% detection in the third cycle. At a reputation threshold of 0.41, the MSMWSL algorithm achieved an 85% identification rate of abnormal vehicles in the third detection cycle. When the reputation threshold was 0.39, the MSMWSL algorithm achieved a 70% identification rate for abnormal vehicles in the fourth detection cycle.

In summary, when the reputation threshold is lower than the typical value of 0.5, the MSMWSL algorithm can achieve a high detection rate for abnormal vehicles. This is attributed to the MSMWSL algorithm proposed in this study, which considers various factors and integrates multisource information. This allows for the rapid identification of abnormal vehicles in each detection cycle under different reputation values, thereby enhancing the overall defensive capabilities of the system against abnormal vehicles.

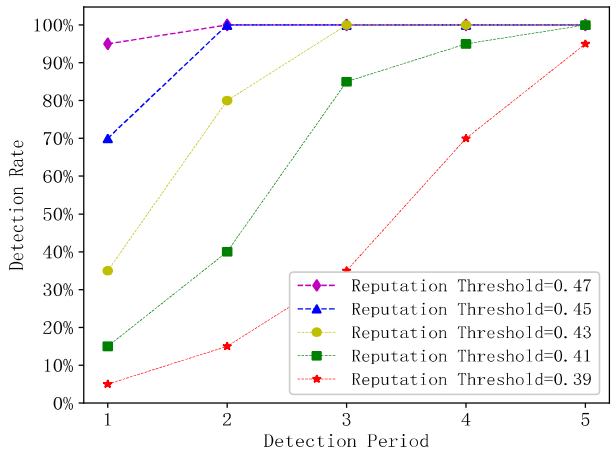

Figure 7. Detection rate of anomalous vehicles varies with cycle under varying reputation thresholds.

6. Conclusions

To address trust and security risks in the data-sharing process of IoV, this paper proposes a secure, blockchain-assisted reputation management scheme. First, it employs a VEC model to address issues such as limited vehicle resources and task latency. It then leverages the consortium blockchain technology to establish a blockchain network among edge servers, ensuring the security and authenticity of data storage at a reasonable cost. Next, to defend against malicious attacks from abnormal vehicles and prevent a group of such vehicles from unfairly influencing the reputation of the target vehicle through biased feedback, the method utilizes asymmetric encryption techniques provided by the blockchain to prevent vehicles from being continuously identified and attacked. Moreover, when calculating reputation values, this study employs a subjective logic trust model to compute reputation values based on feedback events during the car-sharing process, taking into account factors such as familiarity, timeliness, and trajectory similarity to sufficiently weight opinions. The discount and fusion algorithms of the subjective logic trust model are then used to obtain a reputation value that combines direct and indirect opinions, improving the multisource nature and accuracy of the reputation value calculation. Finally, to counteract false message attacks and prevent abnormal vehicles from broadcasting false messages that disrupt other vehicles, this study calculates the effectiveness of both positive and negative events using historical interaction

records and a Piel model based on growth curve functions, in addition to considering multi-source opinions. By weighting the interaction events with the effectiveness of the two types of events, the vehicle reputation calculation becomes more precise.

In conclusion, this study achieved accurate reputation calculations and ensured high-quality data sharing. Using the proposed algorithm, the system can identify and eliminate the security risks posed by abnormal vehicles, and vehicles can efficiently select the best data providers. The experimental results demonstrate that this method has significant advantages in terms of improving the detection rate of abnormal vehicles and ensuring the security of data sharing.

Author Contributions: Formal analysis and writing—original draft preparation, JunQuan Gong; writing—review and editing, JunQuan Gong and Qian Liu; Funding acquisition, Qilie Liu and Qian Liu; supervision, Qilie Liu and Qian Liu. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No.KJZD-K201900605), Doctoral "through train" scientific research project of Chongqing (sl202100000307), the Doctoral Initial Funding of Chongqing University of Posts and Telecommunications under Grant A2021-195(E012A2021195), and the Youth Project of Chongqing Municipal Education Commission Science and Technology Research Program(KJQN201900639, and KJQN202200645

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Zhou H, Xu W, Chen J, et al. Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities[J]. Proceedings of the IEEE, 2020, 108(2): 308-323.
2. Vishwakarma L, Das D. SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain[J]. Vehicular Communications, 2022, 33: 100429.
3. Jiang T, Fang H, Wang H. Blockchain-based internet of vehicles: distributed network architecture and performance analysis[J]. IEEE Internet of Things Journal, 2019, 6:4640-4649.
4. Mollah M B, Zhao J, Niyato D, et al. Blockchain for the internet of vehicles towards intelligent transportation systems: a survey[J]. IEEE Internet of Things Journal, 2020, 8(6): 4157-4185.
5. De Souza A B, Rego P A L, Carneiro T, et al. Computation offloading for vehicular environments: a survey[J]. IEEE Access, 2020, 8: 198214-198243.
6. Shen B, Xu X, Qi L, et al. Dynamic server placement in edge computing toward internet of vehicles[J]. Computer Communications, 2021, 178: 114-123.
7. Liu L, Chen C, Pei Q, et al. Vehicular edge computing and networking: a survey[J]. Mobile Networks and Applications, 2021, 26: 1145-1168.
8. Brehon Grataloup L, Kacimi R, Beylot A L. Mobile edge computing for V2X architectures and applications: a survey[J]. Computer Networks, 2022, 206: 108797.
9. Bai X, Chen S, Shi Y, et al. Collaborative task processing in vehicular edge computing networks[C]. International Conference on Hot Information-Centric Networking, Nanjing, China, 2021: 92-97.
10. Xie R, Tang Q, Wang Q, et al. Collaborative vehicular edge computing networks: architecture design and research challenges[J]. IEEE Access, 2019, 7: 178942-178952.
11. Xu X, Huang Q, Zhu H, et al. Secure service offloading for internet of vehicles in SDN-enabled mobile edge computing[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(6): 3720-3729.
12. Mostafa A. VANET Blockchain: a general framework for detecting malicious vehicles[J]. Journal of Communications, 2019, 14(5): 356-362.
13. Najafi M, Khoukhi L, Lemercier M. Decentralized prediction and reputation approach in vehicular networks[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(7): e4456.
14. Hbaieb A, Ayed S, Chaari L. A survey of trust management in the internet of vehicles[J]. Computer Networks, 2022, 203: 108558.
15. Cui J, Zhang X, Zhong H, et al. RSMA: reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(4): 6417-6428.
16. Shrestha R, Bajracharya R, Nam S Y. Centralized approach for trustworthy message dissemination in VANET[C]. IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, China, 2018: 1-5.

17. Lai C, Zhang K, Cheng N, et al. SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 18(6): 1559-1574.
18. Shen M, Lu H, Wang F, et al. Secure and efficient blockchain-assisted authentication for edge-integrated Internet-of-Vehicles[J]. IEEE Transactions on Vehicular Technology, 2022, 71(11): 12250-12263.
19. Jain S, Ahuja N J, Srikanth P, et al. Blockchain and autonomous vehicles: recent advances and future directions[J]. IEEE Access, 2021, 9: 130264-130328.
20. Chen C, Wu J, Lin H, et al. A secure and efficient blockchain-based data trading approach for internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2019, 68(9): 9110-9121.
21. Cui J, Ouyang F, Ying Z, et al. Secure and efficient data sharing among vehicles based on consortium blockchain[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(7): 8857-8867.
22. Yang Z, Yang K, Lei L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE internet of Things Journal, 2018, 6(2): 1495-1505.
23. Jøsang A, Gray E, Kinateder M. Simplification and analysis of transitive trust networks[J]. Web Intelligence and Agent Systems: An International Journal, 2006, 4(2): 139-161.
24. Audun Jsang. Subjective logic: a formalism for reasoning under uncertainty[M]. Springer, 2018: 7-288.
25. Xu S, Guo C, Hu R Q, et al. Blockchain-inspired secure computation offloading in a vehicular cloud network[J]. IEEE Internet of Things Journal, 2021, 9(16): 14723-14740.
26. Liu Y, Li K, jin Y, et al. A novel reputation computation model based on subjective logic for mobile ad hoc networks[J]. Future Generation Computer Systems, 2011, 27(5): 547-554.
27. Alemneh E, Senouci S M, Brunet P, et al. A two-way trust management system for fog computing[J]. Future Generation Computer Systems, 2020, 106: 206-220.
28. Huang X, Yu R, Kang J, et al. Distributed reputation management for secure and efficient vehicular edge computing and networks[J]. IEEE Access, 2017, 5: 25408-25420.
29. Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2018, 6(3): 4660-4670.
30. Kang J, Xiong Z, Niyato D, et al. Securing data sharing from the sky: Integrating blockchains into drones in 5G and beyond[J]. IEEE Network, 2021, 35(1): 78-85.
31. Zhang Haibo,BIAN Xia,XU Yongjun,XIANG Shengting,HE Xiaofan. Blockchain-assisted vehicle reputation management method for VANET[J]. Journal of Xidian University, 2022, 49(4): 49-59.
32. Zhou Z, Wang B, Dong M, et al. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 50(1): 43-57.
33. Wang D, Zhang L, Huang C, et al. A privacy-preserving trust management system based on blockchain for vehicular networks[C]. IEEE Wireless Communications and Networking Conference, Nanjing, China, 2021: 1-6.
34. Liu H, Zhang P, Pu G, et al. Blockchain empowered cooperative authentication with data traceability in vehicular edge computing[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4221-4232.
35. Yan Shi, Peng Mu-gen, Wang Wen-bo. Integration of Communication, Sensing and Computing: the Vision and Key Technologies of 6G[J]. Journal of Beijing University of Posts and Telecommunications, 2021, 44(4): 1-11.