This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3124073, IEEE Internet of Things Journal

Blockchain-enabled Trust Management Model for the Internet of Vehicles

Zhigang Yang, *Member, IEEE,* Ruyan Wang, Dapeng Wu, *Senior Member, IEEE,* Boran Yang, and Puning Zhang, *Member, IEEE,*

***Abstract*—The high-speed movement of nodes and the burstiness of interactions in the Internet of Vehicles pose huge challenges to the trusted vehicle collaboration and data sharing. Aiming at the disadvantages of existing authentication mechanisms and trust management models for connected vehicles, this paper proposes a trust management model enabled by blockchain to ensure the traceability, non-tampering, unforgeability, and transparency of vehicular interactions. The proposed trust management model leverages Dirichlet distribution, reputation regression, and revocation punishment to objectively and accurately reflect the trust status of vehicles. Simulation results on real-world datasets show that the proposed trust management model advantageously improves the accuracy of malicious vehicle detection and the attack resistance of connected vehicles.**

***Index Terms*—Internet of Vehicles; Blockchain; Trust Management; Dirichlet Distribution; Reputation Regression**

I. Introduction

Internet of Vehicles (IoV) has emerged from the deep integration of 5g, AI, big data, and other cutting-edge technologies [1]–[3] with the century-old automobile industry. IoV is not only changing the traditional automobile industry but also bringing a new service model and business ecology to people. A broad platform is provided by IoV for intelligent vehicles to interact with each other, enabling the moving vehicles to communicate and cooperate with each other. Valuable information during vehicle driving can be integrated through the collaborations of vehicles, which not only helps the vehicles to obtain the most current road conditions but also enhances the vehicle's capabilities in areas such as Environment Sensing, Computational Decision Making, and Control Execution [4].

This work was supported in part by the National Natural Science Foundation of China under grants 61871062, 61771082 and 61901071, in part by the Natural Science Foundation of Chongqing of China under grant cstc2020jcyj-zdxmX0024, in part by the University Innovation Research Group of Chongqing of China under grant CXQT20017, and in part by the Innovation and Entrepreneurship Demonstration Team of Yingcai Program of Chongqing, China under grant CQYC201903167. (*Corresponding author: Dapeng Wu.)*

Z. Yang is with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications Chongqing, Chongqing 400065, School of Artificial Intelligence, Chongqing University of Arts and Sciences, Chongqing 402160, Advanced Network and Intelligent Connection Technology Key Laboratory of Chongqing Education Commission of China, Chongqing Key Laboratory of Ubiquitous Sensing and Networking, China (e-mail: ayzg163@163.com).

R. Wang, D. Wu, B. Yang, and P. Zhang are with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Advanced Network and Intelligent Connection Technology Key Laboratory of Chongqing Education Commission of China, Chongqing Key Laboratory of Ubiquitous Sensing and Networking, Chongqing 400065, China (e-mail: wangry@cqupt.edu.cn, wudp@cqupt.edu.cn, bryangphd@163.com,zhangpn@cqupt.edu.cn).

However, the inherent characteristics of IoV, such as dynamic topology, high-speed mobility, and openness, bring serious security and privacy challenges [5], [6]. Existing researches focus on establishing secure communication channels against external attacks to ensure communication security [7]. However, in the internal IoV, the collaborations between vehicles are very frequent and mostly in the form of Vehicle-to-vehicle (V2V) communication. Due to the contingency and randomness of the encounter between familiar vehicles, most V2V-based collaborations occur between unfamiliar vehicles. But the lack of a necessary trust base between unfamiliar vehicles makes the authenticity and reliability of the shared information doubtful. Incorrect information will interfere with driving, even cause accidents and threaten human life. Therefore, how to establish an objective, fair and reliable trust management model for vehicle collaboration in V2V scenarios is an issue that needs to be addressed. The following requirements must be met in the trust management model: (1) Malicious service history can be traced to urge the servers to improve service quality. (2) Malicious review history can be traced to urge the reviewers to make fair and objective reviews of services. To meet the above requirements and provide a trusted communication environment for collaborating vehicles, most of the existing studies use the public-key cryptography system to verify the identity of the vehicle to ensure communication security. However, the frequent processes of authentication and encryption waste a lot of computing and communication resources [8] and do not satisfy the burstiness and low latency requirements of inter-vehicle communications. And most of the traditional authentication technologies can only defend against external attacks, but can not resist internal attacks from certified vehicles. Besides, unauthenticated vehicles cannot participate in inter-vehicle collaboration, even if they have a high level of collaboration capability and credibility, which greatly reduces resource utilization.

The trust mechanism based on social networks reflects the trust relationship between people and has the properties of measurability, subjectivity, and transferability. The combination of trust mechanisms with the above properties and IoV applications makes it possible to use measurable reputation values as an important indicator for vehicle collaboration establishment to compensate for the disadvantages of traditional authentication cryptography. The reputation value of a vehicle is calculated based on the historical ratings that it gives others or others give it. The two vehicles preparing to cooperate evaluate the possibility of successful interaction according to each other's reputation value, and make a decision whether to

cooperate or not. A vehicle with a good reputation means it has a good behavior history. The higher the reputation value of a vehicle, the more likely other vehicles are to collaborate with it. So, potentially collaborative vehicles enable trusted real-time collaboration without going through a cumbersome authentication process. From the perspective of IoV managers, the introduction of a trust mechanism enables them to obtain the reputation of each vehicle in the network and remove vehicles with malicious behavior characteristics in a timely manner. Besides, compared with the traditional wireless networks, trust management IoV is more urgent for IoV. Most of the data transmitted through traditional wireless networks are entertainment information, and even if the vehicle transmits false information, it will not affect road traffic or personal safety. However, for V2V communication in IoV, the interactive information between vehicles involves environmental sensing, vehicle priority management, and traffic optimization control, etc., which is directly related to vehicle driving decision-making and driver's life safety.

The existing trust management model of social networks mainly includes two kinds [9]: centralized trust architecture and distributed trust architecture. In the centralized architecture, the central server is responsible for storing and processing the trust data of all nodes. When a vehicle wants to know the credit value of other vehicles, it needs to send a request to the central server. Due to the high-speed mobility of vehicles, the central server located in the cloud often cannot meet the delay requirements of the IoV. At the same time, the central server is not only expensive to maintain, but also an easy target of attackers. Once the central server or trunk line fails, it will cause serious consequences. To overcome the defects of the centralized model, some researchers adopt distributed architecture to implement trust management. In the distributed architecture, the storage and management of trust data are usually completed by the vehicle itself, which reduces the number of interaction times between the vehicles and the network facilities, improves the transmission efficiency, and solves the problem of a single point of failure of the centralized server. However, considering the limitation of the vehicle's resources and the interests of the vehicle itself, the trust database maintained by a vehicle alone is often not completely reliable. And due to the high-speed mobility of vehicles, the contingency and randomness of encounters, and the sudden of interactions, the failure probability of interconnection communication between vehicles objectively exists. Besides because it is difficult to establish and maintain a stable social circle based on the geographical area, the collaboration between vehicles presents weak social characteristics. Therefore, it is not possible to completely copy the traditional trust mechanism that builds trust networks based on direct trust and indirect trust.

Blockchain, the underlying technology that drives Bitcoin, is essentially a distributed, tamper-proof ledger that is decentralized, tamper-proof, and transparent [10]. The advantages of blockchain itself bring new ideas to distributed data storage and management and become an effective method to solve the above problems. The traditional blockchain disperses the data storage and maintenance functions to multiple nodes in the network and ensures the consistency of the data by each node through the distributed consensus method [11]. Therefore, the data interaction between nodes and nodes can be completed without the participation of third-party organizations. However, this consensus approach has high communication and computing costs and is not applicable for the IoV scenario in which the vehicles are moving at high speed. Based on the above considerations, the paper proposes a blockchain-enabled trust management model for IoV. The main contributions of this paper can be summarized as follows.

(1) Aiming at the disadvantages of traditional centralized trust and distributed trust, a layered architecture based on the trust management model enabled by blockchain is proposed for the IoV to realize traceability, non-tampering, unforgeability, and transparency of V2V trust records.

(2) A trust management model that combines Dirichlet, reputation regression, and punishment revocation mechanisms is proposed. The model considers the possibility of communication failure, improves the sensitivity of malicious behavior detection, and reduces the number of normal vehicles judged as malicious ones.

(3) The simulation results show that the trust management method with multiple ratings proposed in this paper can greatly avoid misclassifying normal vehicles as malicious vehicles and protect the interests of normal vehicles. And it is effective in resisting simple attacks, slander attacks, and strategic attacks.

The rest of this paper is organized as follows. Section 2 analyses related work and section 3 introduces the system and adversary models. In section 4, the blockchain-enabled V2V collaboration model is proposed. The trust management model is proposed in section 5. Simulation results are presented in section 6. Finally, section 7 concludes the paper.

II. Related Work

This section reviews the relevant literature on authentication technology, centralized trust management model, and decentralized trust management model implementations in vehicular networking.

The openness of wireless communication channels and the lack of effective means of verification in IoV make it easy for attackers to control the communication link and deliver false messages by forging identities. Therefore, to protect normal vehicles from false messages sent by malicious ones, authentication techniques are used to verify the identities of vehicles. Bayat et al. [12] use elliptic curves and bilinear pairings to construct signatures to conceal the legitimate message sender while preventing impersonation signature attacks and enabling traceability of malicious messages. However, due to the computational complexity of bilinear pairings, it is not applicable to IoV. Some studies have used elliptic curve cryptosystem to construct lightweight secure authentication protocols that reduce the computational complexity of the signature and authentication process while providing conditional privacy protection. For example, Lo et al. [13] achieved the secure verification of transport messages between vehicles and infrastructure, and the scheme also supports a batch verification mechanism; He et al. [14] achieved an efficient batch verification mechanism with reduced time and communication

overhead. To reduce the computational and time overhead incurred by Roadside Unit (RSU) authentication, Liu et al. [15] proposes a Proxy-based Authentication Scheme (PBAS) using distributed computing that supports simultaneous authentication of multiple identities and reduces the time consumed in the authentication process. The above authentication schemes are effective in ensuring the trustworthiness of individual users and the reliability of the transmission environment, there are still some issues: (1) Frequent authentication and encryption which require the amount cost of key management and huge storage space for message traceability, waste a lot of computation and communication resources, leading to inefficiency and high latency of message interactions. So, these schemes are not applicable for IoV with highly dynamic changes in network topology. (2) Identity authentication does not guarantee the correctness and integrity of messages, cannot resist malicious attacks from internal legitimate users. (3) Unauthenticated users cannot participate in collaboration, resulting in a waste of efficient resources.

The trust management model of IoV uses trust value to evaluate the user credibility and the trust relationship between users. The users make decisions according to trust value to ensure the reliability of collaboration objects and messages. In IoV, a centralized trust management model is usually used. It means that all trust data are stored and processed at a central institution. To reduce the risk of anomalies and malicious behaviors in IoV, Mhlbauer et al. [16] proposed a VANETs system, which centrally calculates the reputation and dynamically updates the reputation by vehicles periodically interacting with certification authorities and traffic control agencies. Yao et al. [17] proposed two trust models, a weight-based dynamic vehicle-centric trust model based on the type of application and the authority level of the nodes, and a lightweight data-centric trust model using experience and utility theory to help detect false messages. To balance user privacy and vehicle information reliability, Pham et al. [18] proposed ALRS secure connectivity scheme to verify anonymized vehicle identities and obtain trust values. It can achieve untraceability and hide internal information from unauthorized users. Besides, the ATMS context-aware trust management model is designed to estimate the trustworthiness of the received message according to the credibility level of the sender.

The decentralized trust management model in IoV is usually adopted blockchain technology to realize point-to-point collaboration. Due to the complex IoV network structure and high mobility, the messages shared between vehicles are not always reliable. Zhang et al. [19] proposed a blockchain-based trust management model in IoV, which can detect vehicles sending false messages and reduce their reputation values according to the punishment mechanism. The blockchain-based data storage system can prevent attackers from tampering with the reputation value stored in RSU, and the complete reputation value calculation scheme is formalized to solve the credibility calculation issues. Because of the untrusted environment, it is difficult for vehicles to evaluate the credibility of the messages they receive. Javaid et al. [20] proposed a blockchain-based IoV protocol that uses a Physical Unclonable Function (PUF), certificates, and dynamic Proof of Work (dPoW) consensus algorithm smart contract. It can distinguish registered vehicles from malicious vehicles by managing the list of registered vehicles. Fan et al. [21] proposed a secure and verifiable data sharing scheme to realize one-to-many data sharing. The data access strategies adopted blockchain to achieve user self-authentication and cloud non-repudiation. In addition, a strategy hiding scheme is proposed to protect the sensitive information contained in the access strategy. Yang et al. [22] proposed a new blockchain-based trust management model for vehicle networks. Vehicles can use Bayesian inference models to verify received messages from neighboring vehicles and give a rating based on the verification results. It enables RSU to update and share the trust value of different vehicles in a distributed manner. Kang et al. [23] used alliance chains and smart contracts to realize the secure storage and sharing of data in IoV, effectively preventing unauthorized data access. Fernandes et al. [24] proposed a decentralized reputation system to analyze the trust value of vehicles in VANET, and identify the existence of malicious nodes through the use of reputation lists, direct reputation, indirect reputation, and voting schemes, resisting collusion attack.

The instability of the wireless channel caused by the high-speed mobility of vehicles makes the collaboration between vehicles have a certain failure probability. The binary classification method of traditional trust management is not suitable for IoV collaboration with objective failure probability. In addition, traditional trust management needs to calculate the direct trust value and indirect trust value between nodes. Direct trust is the probability of successful interaction inferred from the historical interaction between nodes, while the calculation of indirect trust often requires global direct trust information. In traditional trust management, the trust value updating consumes a lot of resources, and it is difficult to guarantee the authenticity of indirect trust.

III. System Model

A. System Model

Inspired by the collaboration architecture of cloud-edge-client [3], the trust management model of IoV enabled by blockchain is divided into three layers: data storage layer, edge application layer, and data transmission layer, as shown in Fig. 1. And the function of each layer is as follows:

The data storage layer contains the certification authority (CA) center, the cloud. The CA Center is responsible for verifying the real identity of the RSUs and the vehicle owners, and for issuing, managing, and destroying the keys. The legitimacy and timeliness of review records are verified by the cloud in this layer. The verified records are packed and stored on the blockchain, which can be used for subsequent reputation traceability, achieving traceability, non-tampering, unforgeability, and transparency of collaboration records.

The edge application layer provides various services, such as information service (real-time and high-precision map navigation), traffic safety (smart intersection), media service (multimedia distribution), automatic driving (vehicle status detection), etc. It conducts security analysis on the services requested by vehicles and provides low delay service.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3124073, IEEE Internet of Things Journal

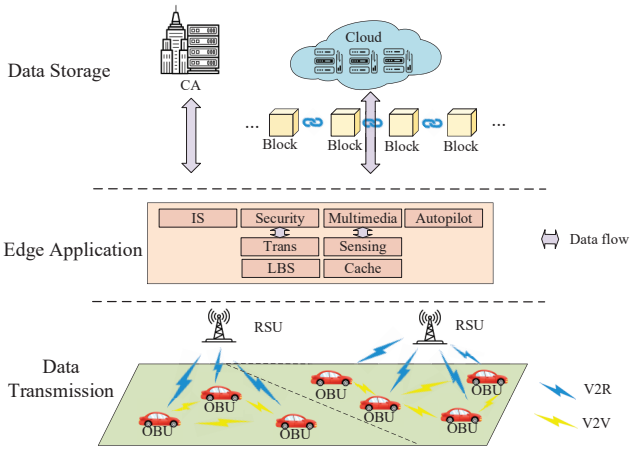


Fig. 1. System Model.

Data transmission layer contains vehicles, Roadside Unit (RSU), and On Board Unit (OBU). The main interaction styles include V2V and Vehicle to Roadside (V2R). V2V focuses on the establishment of trusted collaboration channels between vehicles, and V2R emphasizes the establishment of relevant service request and response channels.

B. Attack Model

The IoV faces many malicious threats while developing rapidly, and the threats from the inside are the most difficult to prevent. Malicious vehicles in the IoV will destabilize the network in many ways, affect the normal operation of the RSU and the vehicle decision-making, and destroy the cornerstone of trust in the IoV. The main attack models considered in this paper are as follows:

(1) Simple attack: attackers provide malicious services to other vehicles in the IoV, such as sending wrong messages or wrong calculation results, which affect the decisions of other vehicles.

(2) Slander attack: after receiving services from other vehicles, the malicious vehicle will give the server an evaluation that is contrary to the actual service quality, causing the reputation of the server to be abnormally reduced, making it untrustworthy by other vehicles, and enhancing the malicious vehicles discourse on the network right.

(3) Strategic attack: in order to avoid detection, cunning malicious vehicles will adopt intermittent malicious behaviors. They may use a lower attack frequency to implement simple attacks or slander attacks, which not only achieves the purpose of the attack but also increases the difficulty of bad vehicle detecting.

IV. Blockchain-enabled V2V collaboration

Decentralized blockchain application usually adopts consensus mechanism to ensure the consistency and fairness of system operation. However, the consensus mechanism will waste a lot of resources and time, making the system performance poor, and the decentralized system architecture is vulnerable to Sybil attack and unable to meet the requirements of high-speed mobility of the vehicle and low latency. Therefore, this paper does not adopt a completely decentralized architecture and consensus mechanism but uses blockchain technology to limit the capability of the central server (cloud) so that the central server cannot obtain non-essential privileges, and ensure the traceability, non-tampering, unforgeability, and transparency of rating records while fully safeguarding user privacy.

In the system proposed in this paper, vehicles and RSU will be registered in the certification center, and service requesters in the IoV will rate the servers after accepting the services provided by them, and the rating levels are divided into three levels: positive, neutral (offline disconnection for unknown reasons, etc.), and negative. The main symbols used in the paper are as shown in Table I. The specific collaboration process is as follows:

Step 1: Key distribution. The CA center assigns a pair of keys to each RSU and multiple pairs of keys to each vehicle: one pair for communication between friends, one pair for anonymous collaboration, and the rest for backup.

Step 2: Request for collaboration. Supposing that vehicle v_A intends to collaborate with the surrounding vehicles. If there is no friends of v_A nearby, v_A obtains the information of the surrounding vehicles through the nearest RSU R and calculates the reputation values of nearby vehicles. Then, v_A randomly selects a suitable vehicle (i.e. vehicle v_B) for collaboration according to the distances (see Section V-D) and reputation values of nearby vehicles.

Step 3: Response. If v_B agrees to provide services to v_A and sends service provision evidence to v_A. If v_B rejects the service or response times out, the collaboration cannot be established.

Step 4: Collaboration confirmation. v_A sends collaboration confirmation evidence to v_B. Then, v_A and v_B establish collaboration.

Step 5: Service evaluations. At the end of the collaboration, v_A rates v_B and sends the service provision evidence and service evaluation evidence to the cloud via local MEC sever.

Step 6: Record on the chain. The cloud verifies the legitimacy and timeliness of the service provision evidence and service evaluation evidence, and periodically packs the verified records into the chain.

Step 7: Evaluation timeout. If v_A fails to give v_B a rating within the required time, v_B will upload service provision evidence and collaboration confirmation evidence, and then the cloud will give a positive rating by default.

TABLE I
Main symbols used in the paper

Notation	Description
v_A	The vehicle which requests for service.
v_B	The vehicle which responses the request of v_A.
R	The RSU that communicates with v_A
K_A, K_B	Public keys of v_A and v_B.
Hash( )	A hash function.
$\text{Signature}_X(\text{C})$	Sign content C with X's private key.
$x \parallel y$	Element x concatenates to y.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3124073, IEEE Internet of Things Journal

The collaboration flow chart is shown in Fig.2 and involves dedicated concepts explained as follows.

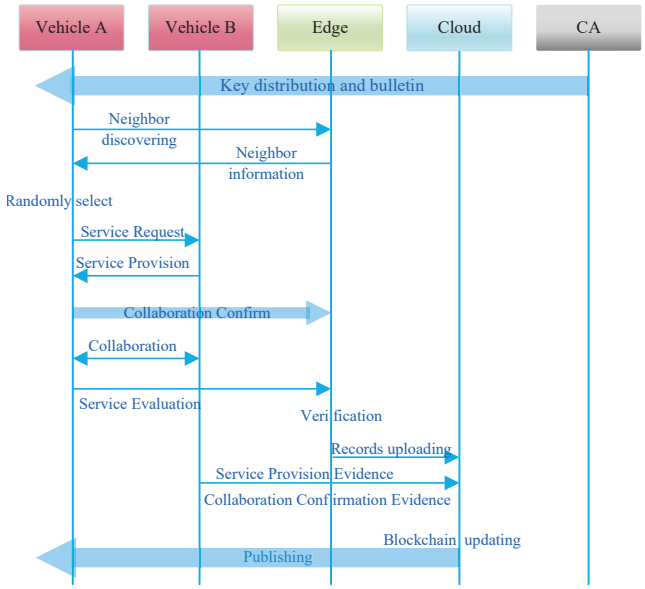


Fig. 2. Collaboration Flow Chart.

The evidence of service request. It is presented by the service requestor to the server. It includes the service requestor public key K_A, service type (ST), request time (RT), request serial number (RSN), request content (RC), and signature. The signature generation rule is as follows.

$$sig_{A1} = \text{Signature}_A\left(\text{Hash}\left(\text{ST} \parallel \text{RT} \parallel \text{RSN}\right)\right) \quad (1)$$

The evidence of service provision. It is presented by the server to the service requestor. The service delivery evidence mainly includes the service requestor public key K_B, ST, RT, service provision time (SPT), service serial number (SSN), signature sig_{A1} and sig_B. The signature generation rule is as follows.

$$sig_B = \text{Signature}_B(\text{Hash}(sig_{A1} \parallel \text{SPT} \parallel \text{SSN})) \quad (2)$$

The evidence of collaboration confirmation. It is provided by the service requestor to the server and local MEC server, including evidence of service provision, collaboration confirm time (CCT), signature sig_{A2} and signature sig_R. The collaboration confirmation evidence should be sent to the server and local MEC server at the same time. If the local MEC server does not receive the collaboration confirmation evidence, the server can refuse to provide service.

$$sig_{A2} = \text{Signature}_A\left(\text{Hash}\left(sig_B \parallel \text{CCT}\right)\right) \quad (3)$$

$$sig_R = \text{Signature}_{RSU}\left(\text{Hash}\left(\text{sig}_{A1} \parallel sig_B \parallel sig_{A2}\right)\right) \quad (4)$$

The evidence of service evaluation. Evidence of service evaluation sent by service requester to local MEC server, including evidence of collaboration confirmation, the rating of service (RS) and signature sig_{A3}.

$$sig_{A3} = \text{Signature}_A\left(\text{Hash}\left(\text{SSN} \parallel \text{RS}\right)\right) \quad (5)$$

The collaboration record packaging. The evidences received by the cloud from the service requesters (or the server) are packed after verification. The packetization includes K_A, K_B, ST, RT, RSN, SPT, SSN, CCT, RS, sig_{A1}, sig_{A2}, sig_R, sig_{A3} (if any), sig_B, the time of MEC server received the evaluation, and the MEC server signature, etc.

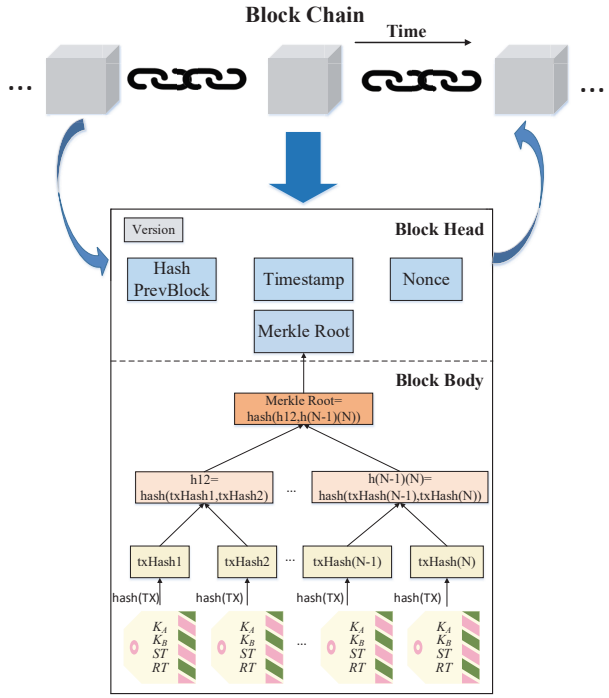


Fig. 3. Records store in blockchain.

V. TRUST MANAGEMENT MODEL

A. Trust Management Based on Dirichlet

The Dirichlet distribution is a conjugate prior for the multinomial distribution, and is an extension of the beta distribution in the high-dimensional distribution. In this paper, the trust model based on Dirichlet distribution considers the diversity of ratings, including positive, neutral, and negative ratings, instead of only including positive and negative ratings.

Let the service rating c contain K categories, $\boldsymbol{\pi} = (\pi_1, \ldots \pi_k, \ldots, \pi_K)$ be a probability vector, where π_k is the probability of obtaining the k-th category rating, such that $p(c = k) = \pi_k$. Considering that c obeys the categorical distribution, there is

$$\pi_k > 0 \ , \sum_k^K \pi_k = 1 \quad (6)$$

$$p(c|\boldsymbol{\pi}) = \prod_{k=1}^K \pi_k^{\delta(c,k)} \quad (7)$$

where $\delta(c, k)$ is the indicator function, such that

$$\delta(c,k) = \begin{cases} 1 & c = k \\ 0 & else \end{cases} \quad (8)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3124073, IEEE Internet of Things Journal

Let $\mathbf{c} = \{c_1, \ldots, c_N\}$ denote the N ratings satisfying the independently identically distribution (IID).

$$p(\mathbf{c}|\boldsymbol{\pi}) = \prod_k^K \pi_k^{N_k} \tag{9}$$

$$N_k = \sum_{i=1}^N \delta(c_i, k) \tag{10}$$

Let $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_K]$ be the concentration hyperparameter, where α_k is a virtual count for the k-th category, before seeing the rating vector $\mathbf{c}$.

$$p(\boldsymbol{\pi}|\boldsymbol{\alpha}) = \frac{1}{B(\boldsymbol{\alpha})} \prod_{k=1}^K \pi_k^{\alpha_k - 1} \tag{11}$$

$$\boldsymbol{\pi}|\boldsymbol{\alpha} \sim \mathbf{Dir}(\boldsymbol{\pi}|\boldsymbol{\alpha}) \tag{12}$$

where $B(\boldsymbol{\alpha})$ is the multivariate beta function for normalization

$$B(\boldsymbol{\alpha}) = \frac{\prod_{i=1}^K \Gamma(\alpha_i)}{\Gamma\left(\sum_{k=1}^K \alpha_k\right)} \tag{13}$$

According to formulas (8) and (10), there is

$$p(\boldsymbol{c}, \boldsymbol{\pi}|\boldsymbol{\alpha}) = \frac{1}{B(\boldsymbol{\alpha})} \prod_{k=1}^K \pi_k^{\alpha_k + N_k - 1} \tag{14}$$

Consider the probability density function of $\mathbf{Dir}(\boldsymbol{\pi}|\boldsymbol{\alpha} + \mathbf{c})$ as follows:

$$\frac{1}{B(\boldsymbol{\alpha} + \mathbf{c})} \prod_{k=1}^K \alpha_k^{\alpha_k + N_k - 1} \tag{15}$$

$$\begin{aligned} p(\mathbf{c}|\boldsymbol{\alpha}) &= \int_\pi p(\mathbf{c}, \boldsymbol{\pi}|\boldsymbol{\alpha}) \\ &= \frac{B(\boldsymbol{\alpha} + \mathbf{c})}{B(\boldsymbol{\alpha})} \int_\pi \frac{1}{B(\boldsymbol{\alpha} + \mathbf{c})} \prod_{k=1}^K \pi_k^{\boldsymbol{\alpha}_k + N_k - 1} \\ &= \frac{B(\boldsymbol{\alpha} + \mathbf{c})}{B(\boldsymbol{\alpha})} \end{aligned} \tag{16}$$

Therefore,

$$\begin{aligned} p(\boldsymbol{\pi}|\boldsymbol{\alpha}, \mathbf{c}) &= \frac{p(\mathbf{c}, \boldsymbol{\pi}|\boldsymbol{\alpha})}{p(\mathbf{c}|\boldsymbol{\alpha})} \\ &= \frac{1}{B(\boldsymbol{\alpha} + \mathbf{c})} \prod_{k=1}^K \alpha_k^{\alpha_k + N_k - 1} \end{aligned} \tag{17}$$

$$\boldsymbol{\pi}|\boldsymbol{\alpha}, \mathbf{c} \sim \mathbf{Dir}(\boldsymbol{\pi}|\boldsymbol{\alpha} + \mathbf{c}) \tag{18}$$

Its marginal distribution is,

$$\pi_1|\boldsymbol{\alpha}, \mathbf{c} \sim \mathbf{Dir}(\pi_1|\alpha_1 + N_1, \alpha_2 + N_2 + \ldots + \alpha_K + N_K) \tag{19}$$

$$E(\pi_1|\boldsymbol{\alpha} + \mathbf{c}) = \frac{\alpha_1 + N_1}{\sum_{k=1}^K \alpha_k + \sum_{k=1}^K N_k} \tag{20}$$

Considering prior knowledge $\boldsymbol{\alpha}$, the mathematical expectation of the k-th category rating is,

$$E(\pi_k) = \frac{\alpha_k + N_k}{\sum_{i=1}^K \alpha_i + \sum_{i=1}^K N_i} \tag{21}$$

B. Reputation regression

Newton's law of cooling establishes the functional relationship between temperature and time, constructing an exponential decay process, and is often used in the ranking of popular articles. In our model, service rating has freshness. The fresher the rating, the more accurately the current reputation of the vehicle can be reflected. The importance of rating decays exponentially with time. In this paper, the cloud packs a block every 5 minutes and stores all the collaboration records received in the previous 5 minutes, which is called an epoch.

The total number of k-class ratings obtained by a vehicle in the m-th epoch is denoted as $r_k(m)(m \geq 1)$, whose residual heat in $n\,(m \leq n)$ epoch is $r_k(n, m) = r_k(m)\, h_k(n - m)$, where $h_k(n) = e^{-\beta_k n}$ is the decay function of the k-th rating, β_k is the exponential decay factor. Then in the n-th epoch of interaction, the effective number (namely afterheat) of the k-th ratings is:

$$\begin{aligned} N_k(n) &= \sum_{m=1}^n r_k(n, m) \\ &= \sum_{m=1}^n r_k(m) h_k(n - m) \\ &= \sum_{m=1}^n r_k(m) e^{-\beta_k(n-m)} \end{aligned} \tag{22}$$

The mathematical expectation of obtaining a k-th rating in the next interaction is:

$$E(\pi_k(n)) = \frac{\alpha_k + N_k(n)}{\sum_{i=1}^K \alpha_i + \sum_{i=1}^K N_i(n)} \tag{23}$$

If a vehicle has not received any ratings or rated any servers for a long time, its reputation will gradually regress to the initial value, that is $E(\pi_k(0)) = \frac{\alpha_k}{\sum_{i=1}^K \alpha_i}$.

C. Punishment Revocation Mechanism

The malicious vehicles referred to in this paper include malicious reviewers and malicious servers, and bad reputations include bad reviewer reputations and bad server reputations. According to the history of positive, neutral, and negative rating records of a vehicle, the bad reputation of the vehicle is calculated as the basis for whether the vehicle should be punished. When the bad reputation of a vehicle is higher than the blocking threshold, it will be judged as a malicious vehicle, which will be blocked by the system and cannot request or provide services. As time goes on, its bad reputation gradually decreases. When the bad reputation of a malicious vehicle is less than the comeback threshold, the system will revoke the punishment and allow it to come back to the IoV. But once its bad reputation is higher than the blocking threshold, it will be judged as a malicious node again. Each time a vehicle is judged as a malicious node, its comeback chances will be reduced by 1. The malicious vehicles with 0 comeback chances are not allowed to come back to the IoV, even their bad reputation is lower than the comeback threshold. The chance of comeback can be increased to prevent misjudgment of unfortunate normal vehicles and give malicious vehicles a chance to correct.

D. Weighted Random Sampling Based on Distance

Once a vehicle intends to request service, it will randomly select a server from the normal vehicles based on the distance. Let the distance between a candidate vehicle and the service requester be $r\,(r < r_{max})$, where r_{max} is the maximum distance allowed to request service. Considering that the power of the electromagnetic wave signal is inversely proportional to the square of the distance [25], and the perceived strength of the signal has logarithmic characteristics, we set the weight of the candidate vehicle as $lg\,(r_{max}/r)^2$. Then the service requester randomly selects a vehicle from all candidates as a server according to their weights. The detailed description is shown in Algorithm I.

Algorithm 1 Weighted Random Sampling Based on Distance

Input:
Maximum distance allowed to request for collaboration $r_{\max}$;
Longitude and latitude (x_0, y_0) of service requester v_0;
Longitude and latitude (x_i, y_i) of a candidate server $v_i (1 \leq i \leq M)$
output:
Sequence number of selected server s;

```
Initialize B_0 = 0
for i ∈ 1, ..., M do
    r_i ← sqrt((x_i − x_0)^2 + (y_i − y_0)^2)
    w_i ← lg(r_max / r_i)^2
end for
W ← Σ_{i=1}^{M} w_i
Randomly selecting a number t from [0, C)
for i ∈ 1, ..., M do
    B_i = B_{i−1} + w_i
    if t < B_i then
        s ← i
        Return
    end if
end for
```

E. Security and Privacy Analysis

The cloud, local MEC server, and other vehicles can't obtain the real identity of the user, but they can de-anonymize the user by tracking its public keys to get its trajectory information. To prevent identity tracking, each vehicle has multiple pairs of spare keys. Once the vehicle owner suspects that the current public key is tracked, he can apply to CA to change the key pair and inherit the reputation value obtained by the previous pair of keys. The process of updating the key pair is confidential to the cloud, and the cloud cannot associate the user's new identity with the old one. Therefore, the user's identity is confidential to the cloud, local MEC servers, and other vehicles. The cloud is responsible for adding the records to the blockchain. Each collaboration record requires the signatures of the cloud, RSU, requester, and server. Although the cloud is the manager of the blockchain, due to the characteristics of the hash function, it cannot delete or change any records in blockchain, nor can the local MEC server and vehicles. In short, the proposed trust management model has the characteristics of anonymity, traceability, non-tampering, unforgeability, and transparency.

VI. Simulation Analysis

A. Simulation Settings

From the perspective of service provision, the vehicles are classified as normal servers and malicious servers; from the perspective of service review, the vehicles are classified as normal reviewers and malicious reviewers. Considering the reality, in this paper, normal servers (normal reviewers) may also be malicious reviewers (malicious servers).

Normal servers provide services honestly and normal reviewers give evaluations honestly. Malicious servers provide malicious services with probability b and malicious reviewers give malicious evaluations with probability c. In other cases, they provide services or give evaluations as normal ones.

However, considering the instability of the V2V communication channel, even if the server is not malicious, V2V communication still has a failure probability. Therefore, the servers are rated by the reviewers in three categories: positive (successful collaboration), neutral (failed communication), and negative(failed collaboration). Table II shows the probabilities that a server receives positive, neutral, and negative ratings in different situations.

TABLE II
THE PROBABILITY DISTRIBUTION OF THREE CATEGORY RATINGS

	Normal server	Malicious server
Normal reviewer	$[1-a, a, 0]$	$[(1-b)(1-a), (1-b)a, b]$
Malicious reviewer	$[(1-c)(1-a), (1-c)a, c]$	$[(1-c)(1-b)(1-a), (1-c)(1-b)a, b+c-bc]$

A 24-hour taxi GPS dataset collected in Chongqing in 2017 is employed in simulations. After preliminary processing, we get a spatio-temporal dataset of 11,980 vehicles with 288-time points. For the convenience of calculation, we only calculate the Euclidean distance of two vehicles in the longitude and latitude coordinate system, not the geographical distance between them. The Euclidean distance r between vehicles V_1 and V_2 is defined as follows.

$$r = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{24}$$

where (x_1, y_1) and (x_2, y_2) are the latitude and longitude coordinate pairs of vehicles V_1 and V_2.

Table III shows the parameter description and settings involved in this paper.

B. Simulation results analysis

The trust model of comparison is the Beta Distribution based Trust Model (BDTM). In BDTM, the servers are rated by the reviewers only in two categories: positive (successful collaboration) and negative (unsuccessful collaboration). This means that a failed communication between the two collaborators is also treated as an unsuccessful collaboration and the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3124073, IEEE Internet of Things Journal

TABLE III
PARAMETER SETTINGS IN THE SIMULATION

Parameter	Description	Value
a	Probability of communication failure	0.3
b	Attack probability of malicious reviewer	0.2
c	Attack probability of malicious server	0.2
P_{mr}	Proportion of malicious reviewers	0.15
P_{ms}	Proportion of malicious servers	0.15
Pr	Probability of requesting collaboration	0.3
$r_{\max}$	Maximum coordinate distance	0.0015
$[\alpha_1, \alpha_2, \alpha_3]$	Concentration hyperparameter	$[1, 1, 1]$
$[\beta_1, \beta_2, \beta_3]$	Heat decay factor of positive, neutral, and negative reviews	$[0.1, 0.15, 0.1]$
Nchance	Comeback chance	3
Nepoch	Collaboration epochs	250

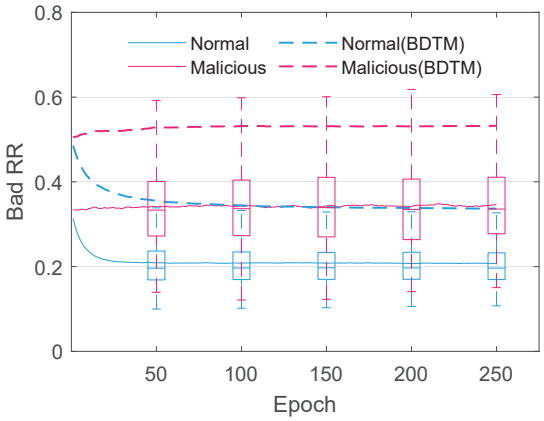
server will receive a negative rating. For the sake of fairness, both BDTM and our model work in the blockchain-enabled V2V collaboration system. Due to the particularity of the blockchain-enabled trust management model, direct trust and indirect trust are not used in the simulations.

1) Bad Reputations: At the beginning of the experiment, both the malicious vehicles and the normal vehicles had the same reputation, but with the increase of the experiment epochs, their reputation diverged. This experiment compares the malicious detection sensitivity of our model and BDTM without using the punishment mechanism. Since BDTM only supports negative and positive ratings, the neutral rating is regarded as a negative rating in BDTM. Fig. 4 shows the changing trend in the bad reputation of normal vehicles and malicious vehicles under our model and BDTM.

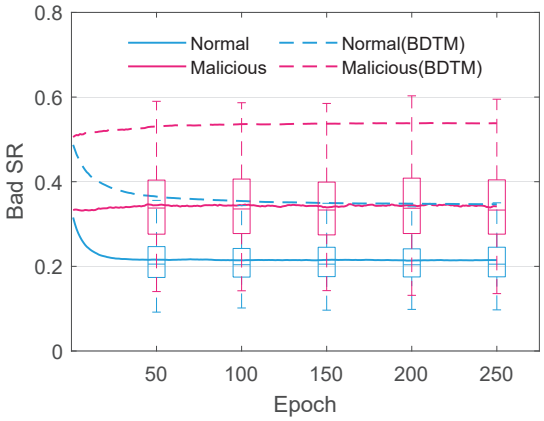
Fig. 4-a shows the changing trend of bad reviewer reputation (RR). The blue solid line (blue dotted line) and the red solid line (red dotted line) represent the average bad RR of normal reviewers and malicious reviewers in our model (BDTM). For the same type of vehicles, BDTM has a higher bad RR than ours, because BDTM regards communication failures as malicious behaviors, which will increase the probability of normal reviewers being misjudged as malicious reviewers. As the number of cooperation epochs increases, the gap between the mean bad RR of malicious nodes and normal nodes gradually increases and tends to stabilize. Although the distinction between malicious vehicles and normal vehicles in BDTM is more obvious than our model, it does not mean that BDTM is more suitable for malicious vehicle identification. The accuracy of malicious vehicle identification will be analyzed in the simulation of malicious vehicle identification. In addition, our model stabilizes faster than BDTM, which shows that our model has more advantages in the speed of malicious detection.

Fig. 4-b shows the changing trend of bad server reputation (SR). Since Fig. 4-b is highly similar to Fig. 4-a, the analysis result will not be repeated here.

2) Malicious vehicle identification: This experiment compares the performance of our model and BDTM on malicious vehicle identification. The punishment mechanism and punishment revocation mechanism are used in our model, and the blocking threshold is set to 0.5, and the comeback threshold



(a) Bad reviewer reputation



(b) Bad server reputation

Fig. 4. The bad reputation of normal or malicious vehicle.

is set to 0.35. Once the bad RR or the bad SR of a vehicle exceeds the blocking threshold, the vehicle is judged as a malicious vehicle. If the bad RR and the bad SR of the vehicle judged to be malicious are lower than the comeback threshold, and its comeback chance is not 0, the vehicle rejoins the IoV. In BDTM the blocking threshold is set to 0.465. Since the reputation regression and punishment revocation mechanisms are not used in BDTM, a normal vehicle that is misjudged as malicious is unable to rejoin the IoV. In order to better observe the changing trend of the bad reputation of malicious vehicles, the BDTM model in this experiment still does not adopt the punishment mechanism.

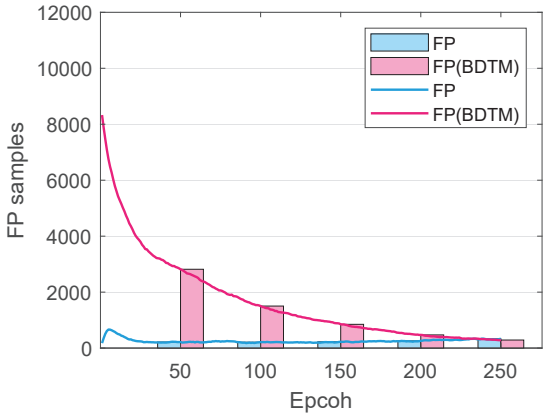
Fig. 5-a shows the number of false-positive vehicles in our model and BDTM. The blue curve (bar) represents false positive (FP) vehicles in our model, and the red curve (bar) represents FP vehicles in BDTM. The FP vehicles of our model reached a maximum of 663 at Epoch 5, then slowly declined, and fluctuated between 150 and 300 after Epoch 22. Since the failed communication is treated as the unsuccessful collaboration in BDTM, more than 8,300 vehicles are FP at Epoch 1, and then FP number declines rapidly as the number of epochs increased. Approaching Epoch 250, the number of FP vehicles in BDTM is comparable to that of our model.

Fig. 5-b shows the number of false-negative vehicles in

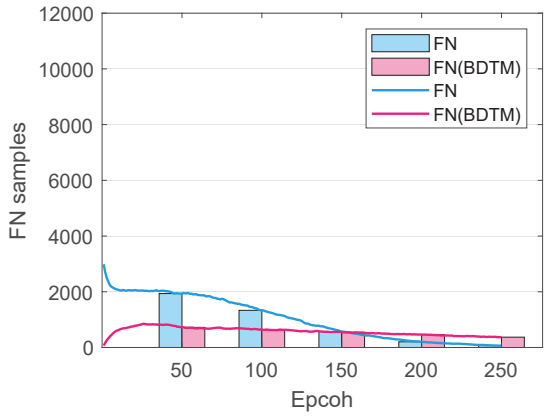
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3124073, IEEE Internet of Things Journal

our and BDTM models. The blue curve (bar) represents false negative (FN) vehicles in our model, and the red curve (bar) represents FN vehicles in BDTM. The number of FN vehicles in BDTM reaches the peak value 852 at Epoch 30, then slowly drops to 370 at Epoch 250. The number of FN vehicles in our model reaches the peak value 2987 at Epoch 1, and then gradually declines, reaching parity with BDTM at Epoch 150 and dropping to 69 vehicles at Epoch 250. When the number of the epoch is small, the malicious vehicle recall rate in BDTM is higher than the one in our model, but this is at the cost of a large number of normal vehicles misjudge as malicious ones (namely, low precision rate). With the increase of the number of experimental epochs, the recall rate of malicious vehicles in our model gradually increases while maintaining a high precision rate. At Epoch 150, it catches up with the recall rate in BDTM, and then excesses it. In reality, both good reputations and bad reputations need to be accumulated slowly, so we need a longer observation process to discover the malicious vehicles. In short, our model far outperforms BDTM at the precision of malicious vehicle identification, and the number of misjudged normal vehicles is always maintained at a very low level, which effectively protects the enthusiasm of normal vehicles to participate in the collaboration. And with the increase of the experimental epoch, our model has gradually surpassed BDTM in recall rate, so that the malicious vehicles with strong confusion are not hidden, ensuring the stability of IoV.

3) Collaborative vehicle and collaboration success rate: This experiment compares the number of vehicles participating in collaboration and the success rate of collaboration in our model and BDTM, as shown in Fig. 6. Considering the excessive number of FP vehicles in BDTM before Epoch 150, the punishment mechanism is adopted after Epoch 150 in BDTM. The rest of the parameter settings are the same as last experiment. The blue (red) curve and bar represent the number of collaborative vehicles in our model (BDTM), and the proportion of them to all vehicles. The blue (red) curve with squares indicates the success rate of collaboration, namely the ratio of the number of successful collaborations to the total number of collaborations. Since the punishment mechanism is not considered before Epoch 150, the number of collaborative vehicles in BDTM before Epoch 150 is more than that of our model, but it drops sharply after Epoch 150, nearly 800 less than that of our model. This is because BDTM kicks a large number of FP vehicles out of the IoV, resulting in fewer vehicles participating in the collaboration than our model. Both collaboration success rates of our model and BDTM slowly rise with the increase of the number of collaboration epochs. Before Epoch 150, BDTM was slightly lower than our model due to not kicking out malicious vehicles. Although the ratio of malicious vehicles is nearly 30%, the probability of launching an attack is low (20%), so there is not much difference between the success rates of BDTM and ours after Epoch 150. After Epoch 150, the success rates of two models are very close, fluctuating around 70%. Considering that the communication failure probability is set at 30% in this paper, and the collaboration success rate of 70% is the limit. Since BDTM does not use the reputation regression mechanism,



(a) FP



(b) FN

Fig. 5. FP and FN vehicles.

its sensitivity to malicious behaviors is much lower than our model. Therefore, BDTM must adopt strict measures, such as reducing the threshold value of malicious vehicle identification, which leads to a large number of misjudgments. Even the punishment mechanism is launched at Epoch 150, the number of misjudged malicious vehicles is nearly 800 more than ours. And our model can take the punishment mechanism at the beginning of the experiment, rather than Epoch 150. This means that our model can identify malicious vehicles more timely and accurately, and better protect the rights and interests of normal vehicles.

VII. Conclusion and Future Work

In this paper, we proposed the blockchain-enabled trust management model, exploiting the hierarchical architecture of blockchain to realize open, fair, and credible trust management. Our proposed trust management model involves Dirichlet distribution, reputation regression, and revocation punishment to adapt to the complex and dynamic communication environment of IoV, to more objectively and accurately evaluate the trust status of connected vehicles, to better protect the rights and interests of these vehicles, and to ensure the friendly and sustainable vehicular cooperation. Finally, the simulation results on real-world datasets show the reliability

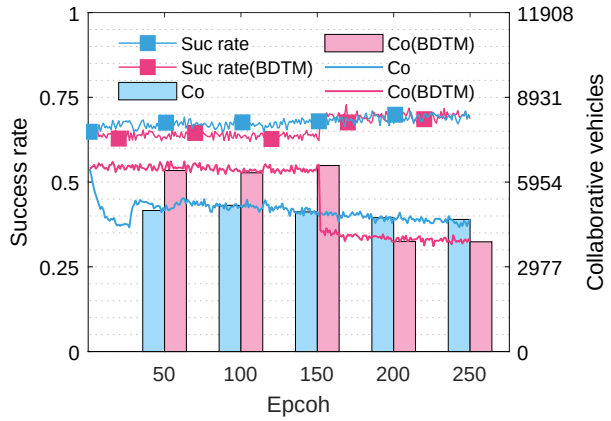


Fig. 6. Collaboration times and success rates.

and superiority of our proposed trust management model. For future work, we will introduce the reward mechanism into our model and explore our model to the other areas, such as crowd sensing and social internet of things.

REFERENCES

[1] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, "Channel state information prediction for 5g wireless communications: A deep learning approach," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 227–236, 2018.

[2] D. Wu, R. Bao, Z. Li, H. Wang, H. Zhang, and R. Wang, "Edge-cloud collaboration enabled video service enhancement: A hybrid human-artificial intelligence scheme," *IEEE Transactions on Multimedia*, 2021.

[3] D. Wu, X. Han, Z. Yang, and R. Wang, "Exploiting transfer learning for emotion recognition under cloud-edge-client collaborations," *IEEE Journal on Selected Areas in Communications*, 2020.

[4] C. Luo, S. Guo, S. Guo, L. T. Yang, G. Min, and X. Xie, "Green communication in energy renewable wireless mesh networks: Routing, rate control, and power allocation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3211–3220, 2014.

[5] J. Xiong, R. Bi, M. Zhao, J. Guo, and Q. Yang, "Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 24–30, 2020.

[6] D. Yu, Z. Zou, S. Chen, Y. Tao, B. Tian, W. Lv, and X. Cheng, "Decentralized parallel sgd with privacy preservation in vehicular networks," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2021.

[7] Z. Yang, R. Wang, D. Wu, and D. Luo, "Utm: A trajectory privacy evaluating model for online health monitoring," *Digital Communications and Networks*, 2020.

[8] P. Zhang, X. Li, D. Wu, and R. Wang, "Edge-cloud collaborative entity state data caching strategy towards networking search service in cpss," *IEEE Transactions on Industrial Informatics*, 2020.

[9] D. Wu, Z. Yang, B. Yang, R. Wang, and P. Zhang, "From centralized management to edge collaboration: A privacy-preserving task assignment framework for mobile crowd sensing," *IEEE Internet of Things Journal*, 2020.

[10] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[11] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404818300890

[12] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for vanets with batch verification," *Wireless networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[13] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2015.

[14] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[15] Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Transactions on vehicular technology*, vol. 64, no. 8, pp. 3697–3710, 2014.

[16] R. Mühlbauer and J. H. Kleinschmidt, "Bring your own reputation: A feasible trust system for vehicular ad hoc networks," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 37, 2018.

[17] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in vanets," *Ad Hoc Networks*, vol. 55, pp. 107–118, 2017.

[18] T. N. D. Pham and C. K. Yeo, "Adaptive trust and privacy management framework for vehicular networks," *Vehicular Communications*, vol. 13, pp. 1–12, 2018.

[19] H. Zhang, J. Liu, H. Zhao, P. Wang, and N. Kato, "Blockchain-based trust management for internet of vehicles," *IEEE Transactions on Emerging Topics in Computing*, 2020.

[20] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 815–11 829, 2020.

[21] K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li, and Y. Yang, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5826–5835, 2020.

[22] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[23] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2018.

[24] C. P. Fernandes, I. de Simas, E. R. de Mello, and M. S. Wangham, "Rs4vanets-a decentralized reputation system for assessing the trustworthiness of nodes in vehicular networks," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2015, pp. 268–273.

[25] D. Yu, Y. Zou, J. Yu, Y. Zhang, F. Li, X. Cheng, F. Dressler, and F. C. Lau, "Implementing the abstract mac layer in dynamic networks," *IEEE Transactions on Mobile Computing*, vol. 20, no. 5, pp. 1832–1845, 2021.

Zhigang Yang received his M.S. degrees in 2006 from Chongqing University of Posts and Telecommunications, where he is currently pursuing the Ph.D. degree. He is an associate professor with Chongqing University of Arts and Sciences. His research interests include edge computing, network security and privacy.

Ruyan Wang received his Ph.D. degree in 2007 from the University of Electronic and Science Technology of China. He is the Dean of School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications. He is the recipient of the Danian Huang Team from the Ministry of Education of the People's Republic of China. His research interests include network performance analysis and multimedia information processing.

Dapeng Wu received his Ph.D. degree in 2009 from the Beijing University of Posts and Telecommunications, Beijing, China. Now, he is a professor at the Chongqing University of Posts and Telecommunications, Chongqing, China. He authored more than 100 publications and two books. He is the inventor and co-inventor of 28 patents and patent applications. His research interests are in social computing, wireless networks, and big data. Prof. Wu serves as TPC Chair of 10th Mobimedia and program committee member for numerous international conferences and workshops. He served or is serving as an Editor or/and Guest Editor for several technical journals, such as IEEE IoT, Elsevier Digital Communications and Networks, ACM/Springer Mobile Network and Applications. He is a senior member of the IEEE.

Boran Yang received his B.S. and M.S. degrees in 2013 and 2016 from Chongqing University of Posts and Telecommunications, where he is currently pursuing the Ph.D. degree. His research interests include edge computing, edge resource sharing and network security.

Puning Zhang received his Ph.D. degree in 2017 from the Beijing University of Posts and Telecommunications, Beijing, China. Now he works as a lecturer in School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China. His research interests include Internet of Things search and Deep Learning.