Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3537771, 10 pages
https://doi.org/10.1155/2022/3537771

*Research Article*

# Auto-Adaptive Trust Measurement Model Based on Multidimensional Decision-Making Attributes for Internet of Vehicles

**Deshuai Yin**[1] **and Bei Gong**[2]

[1] *Beijing Institute of Technology, Beijing 100081, China*
[2] *Beijing Key Laboratory of Trusted Computing, Beijing University of Technology, Beijing 100124, China*

Correspondence should be addressed to Bei Gong; gongbei@bjut.edu.cn

Received 31 October 2021; Revised 21 December 2021; Accepted 26 January 2022; Published 21 February 2022

Academic Editor: Li Zhu

As an important branch and application of the Internet of Things (IoT), the Internet of Vehicles (IoV) has the characteristics of wide distribution and dynamic connection. The current research on trust measurement and management in IoV, to some degree, solved vehicles reliability and QoS issues, but these models still have some drawbacks, like insufficient adaptability to the dynamic changes of the context. Therefore, this paper proposes an adaptive trust measurement model for IoV based on multidimensional decision-making attributes. The model not only takes full advantage of the central static trust management role of the local organization but also implements a distributed self-governing mechanism to tackle the dynamic trust management issues. In the process of trust management, the model allows vehicles to handle the trust evaluation according to the service preferences, and vehicles can select some or all of the attributes from the multidimensional trust decision attribute list. For the recommendation trust evaluation, vehicles can select those vehicles which have similar service preferences from the vehicle candidate list. When computing the recommendation trust, the recommendation trust dispersion model is used to handle evaluation bias problems. The method of information entropy is introduced to tackle the weight adaptation problem when computing comprehensive trust evaluation. The simulation results and analysis show that the model can detect and recognize the malicious vehicles in the network and mitigate the risk that malicious vehicles provide the service to normal vehicles.

## 1. Introduction

With the application of various connected devices and the rise of intelligent driving technology, IoV has become an important choice for people to travel intelligently [1]. It allows the vehicle to perceive the road information and vehicle information in the process of moving, and with the aid of intelligent information processing technology for analysis and processing, it provides safe, intelligent, efficient traffic services, while improving the efficiency of road traffic. However, the IoV networking and topology features are highly dynamic, such as the ad hoc networking method and flexible connection method. Moreover, the links among vehicles are open, and the computing power and resources of vehicles are different. Traditional cryptography-based security schemes can guarantee authenticity, confidentiality, and integrity, but their theoretical assumptions—that the authenticated entity must be credible—are no longer valid. With the development of attack technology, attackers can control vehicles with legal status and secret keys in the network [2], so that they can launch any type of internal network attacks and even endanger the life of the passenger. Therefore, only relying on cryptography-based security mechanisms cannot completely solve the security problems of the IoV.

Trust management has become a new mechanism to solve the security problems of the IoV and has become a research hotspot in recent years. The trust management mechanism has the characteristics of dynamic, real-time resistance to internal attacks; flexible application and deployment; and multidimensional evaluation. Cho's [3] review of trust modeling and quantification described different understanding levels of trust in different fields from political, economic, and sociological aspects. Mike et al. [4] correlated trust with risk and threat and established a direct connection between trust and risk through trust research in multiple contexts. Alshehri and Hussain [5] proposed a trust management model based on fuzzy logic, which can efficiently detect malicious nodes involved in the Internet of Things environment, but the dynamic and universal adaptability of the model is insufficient. Liu [6] added factors such as personality preference similarity and interactive environment context to the definition of trust in a mobile distributed environment. Xie and Wei [7] proposed a node dynamic trust evaluation method (IDTEM) for the Internet of Things, which can better characterize node behavior and suppress malicious recommendations, but it needs to distinguish in detail the cooperation methods between devices in specific application scenarios, and the versatility is poor. Pawar et al. [8] proposed a mechanism to calculate the reputation of cloud service providers and described the uncertainty of trust more accurately based on evidence.

In recent years, the research on trust modeling is mainly divided into two parts according to the entities that bear the responsibility of trust computing, namely, centralized trust modeling and distributed trust modeling. Centralized trust modeling includes a reputation center to collect trust evaluation information, calculate entity reputation values, and provide reputation query services for network entities. Mohsenzadeh et al. [9] proposed a trust model based on fuzzy mathematics according to the success and failure interactions between cloud entities on the basis of trust attributes and semantics, but the accuracy of discrimination is low. Su et al. [10] proposed a game-based IoT terminal node trust evaluation model and algorithm, which manages the reputation of each node more dynamically and efficiently, but it relies too much on the reputation feedback of the reputation management intermediary station. Centralized trust modeling has the shortcomings of single point failure and poor node scalability. At present, it is mainly used in scenarios such as e-commerce websites and shopping websites. Distributed trust modeling is born to adapt to distributed networks. The IoV has the characteristics of distributed networks and is especially suitable for dynamic networks. Aiming at distributed trust modeling, Li et al. [11] proposed an opportunistic network security routing decision-making method based on a trust mechanism, which relies on the message carrying method to realize the collection of evidence chains and uses a trust vector with signature and time stamp to trust the node and to provide effective feedback. Wu [12] proposed a blockchain-based peer-to-peer network trust model, namely, ChainTrust, which determines the weight of indirect trust according to the reliability of the indirect trust of the evaluation node in the network, which has high flexibility, universality, and performance, but the model granularity is relatively coarse. You et al. [13] corrected the reliability of recommended nodes based on the feedback of interaction satisfaction, but their evaluation process relied too much on local storage and could not be effectively applied to scenarios without local storage, such as cross-domain and unfamiliar node interactions. Jiang et al. [14] proposed a distributed wireless sensor network trust model. This model considers communication trust, energy trust, data trust, and other factors in the calculation process of direct trust and defines trust reliability and familiarity. However, this model has certain limitations in determining the weight of direct trust and recommendation trust. Lu et al. [15] improved the Eigen-Trust model and used evolutionary game theory to model peer entities and transaction behavior, which more accurately reflected the actual situation. Jayasinghe et al. [16] extended the method of establishing trust based on entity reputation, experience, and knowledge to the trust evaluation of data items and proposed an effective modular hybrid trust framework. Truong et al. [17] clarified the concept of trust in the social IoT ecosystem, using third-party opinions, experience, and direct observation as three trust indicators to establish a reliable social network between owner-based entities, but its practicality is not strong.

To sum up, most of the existing trust research focuses on solving the trust problem in specific application scenarios and does not consider that normally in IoV there are two networking methods, that is, static and dynamic. Most of the above-mentioned papers handle the trust measurement in a dynamic networking environment and do not take identity authentication, deliberate modification of key software, and hardware components into consideration. In addition, if one trust measurement model relies too much on the distributed self-operation mechanism, the vehicles with limited computational and energy constraints can hardly participate in mutual trust evaluation. Therefore, it is necessary to make the best of the role of central trust management when evaluating the trust. At the same time, the current research of many domestic and foreign scholars mainly focuses on the trust model suitable for communication transmission technology [18] or one specific network. There is a lack of trust models designed for one network with massive heterogeneous vehicles. Furthermore, in current exiting trust models, the aspects which may have an impact on trust evaluation, such as vehicles attributes, weight of coefficients, and other factors, are not considered enough. Current models either give too little consideration to the attributes that affect trust evaluation or lack consideration of the fairness and consistency of mutual evaluation among vehicles, resulting in a decrease in the fairness of trust and an increase in vulnerability from malicious vehicle attacks [19].

In response to the above drawbacks, this paper proposes a novel trust measurement model, which makes the best of advantages of both central trust management and distributed trust management. The trust evaluation is based on the multidimensional decision-making attributes of the vehicles, and the model is also auto-adaptive. This trust measurement model allows the trustor vehicles to take multiple factors into consideration when computing the trust value, such as package forwarding rate and package repetition rate. The model solves the problem of insufficient adaptability of traditional quantitative models to the dynamic changes of the IoV. The method to calculate the direct trust value fuses the historical statistical trust record and subjective interaction satisfaction to enhance the objectivity of the direct trust measurement. Once getting the direct trust result and recommendation trust result, the model introduces the information entropy to smoothen the weights of these two trust measurement factors, and the introduction of the information entropy further improves the dynamic adaptability of the model. At the end of this paper, the model is simulated by experiments. The experiment proves that the model can effectively solve the problem of vehicle trust measurement in IoV, even in the environment of massive heterogeneous devices with huge computing capacity span and dynamic changes in network topology. In addition, the model has the ability to automatically adapt to different IoV.

The rest of this paper is organized as follows. In Section 2, the application environment and fundamental definitions are given, and the proposed trust model is also introduced. Direct trust measurement is studied in Section 3, and Section 4 details the calculation of the recommendation trust measurement. Section 5 describes how to handle the total trust measurement. Section 6 presents the simulation experiments and the analysis of the results. Section 7 concludes the paper and discusses the future work.

## 2. Application Environment and Fundamental Definition

*2.1. Application Environment Network Model.* This article assumes that the set of IoV nodes in an area is $\{\beta_1, \beta_2, \ldots, \beta_n\}$, and for generality, these nodes may belong to different organizations. Since the IoV nodes tend to have multilevel tasks in the actual operation process, the sequence of nodes $\beta_{\pi 1}, \beta_{\pi 2}, \ldots, \beta_{\pi m} (m \geq 1)$ with the highest computing resources, network resources, energy, and neutral position can take the role of the IoV security management center (assuming that these nodes are unconditionally trustworthy). In view of the fact that IoV networks may belong to different organizations which may be in a state of competition or even hostility, normally one IoV node joins one network dynamically or statically on the basis of the organization. Suppose the number of organizations $(I_1, I_2, \ldots, I_m)$ in this area is $m$, $\{\beta_{i1}, \beta_{i2}, \ldots, \beta_{im}\} \subseteq \{\beta_1, \beta_2, \ldots, \beta_n\}$ is one set belonging to the organization $I_i$, and $\beta_{i\pi}$ is one node with a management role. The trust of nodes set $\{\beta_{i1}, \beta_{i2}, \ldots, \beta_{im}\}$ is measured by $\beta_{i\pi}$, and $\beta_{i\pi}$ in each organization is evaluated by the nodes with a management role in this area.

As shown in Figure 1, this network model defines a three-layer structure of ordinary nodes, organizational management nodes, and domain management nodes, which assumes that the domain management nodes are unconditionally trustworthy. The organization management node maintains the node trust matrix and conducts node management by obtaining the trust evaluation between nodes, removing dangerous nodes, and recommending service nodes, while regularly broadcasting the information of nodes joining the organization through static identity verification in the organization. After the node interaction is completed, the ordinary node transmits the interaction satisfaction data to the organizational management node.

This paper first assumes that the node with a central management role is trustworthy, and the nodes to be evaluated are those nodes with management roles in the organization $(I_1, I_2, \ldots, I_m)$. The nodes without management roles inside one organization can evaluate each other, and this paper only describes this situation. The trust evaluation result can be used for the following: (1) the trustor node selects the node that can provide the required service in the organization; (2) once the trustor node finishes the trust evaluation, it reports the result to the node with a management role, and the management node can use this result, together with other trust results from other nodes, to measure the trust of all nodes in the organization and conduct some management work like removing malicious nodes.

Figure 2 depicts the node trust measurement procedure:

Combine static trust decision factors and dynamic trust decision factors to get multidimensional decision factors, calculate direct trust metric based on multidimensional decision factors and subjective interaction and historical interaction satisfaction, compute recommended trust metric based on interest similarity and recommended trust dispersion, combine direct trust computing and recommended trust computing to get total node trust value, and realize trust assessment based on node trust value. According to the trust assessment result, node interaction is carried out; trust feedback is carried out according to the node interaction result; malicious nodes are found and excluded; and the trustworthiness of the car network node group is ensured.

*2.2. Direct Trust Measurement Model.* Suppose the number of the nodes deployed in one organization is $n$. Assume $\beta_i$ is trustor node and $\beta_j$ is the node to be evaluated, that is, the target node.

The measurable trust factors for $\beta_i$ to $\beta_j$ are $\Omega_1(\beta_i, \beta_j), \Omega_2(\beta_i, \beta_j), \ldots, \Omega_k(\beta_i, \beta_j)$; $k$ is the number of the measurable trust factors; then, the measurable set is $\Omega = \{\Omega_1(\beta_i, \beta_j), \Omega_2(\beta_i, \beta_j), \ldots, \Omega_k(\beta_i, \beta_j)\}$, where each value ranges from 0 to 1. Each item in the set is measurable, $\delta_l$ is the weighted coefficient for each item in the set, and $\delta_l$ satisfies the following conditions:

$$\begin{gathered} 0 \leq \delta_l \leq 1, \\ \sum_{l=1}^{k} \delta_l = 1. \end{gathered} \tag{1}$$

Suppose $M(\beta_i, \beta_j, t)$ is the subject interaction satisfaction function of node $\beta_i$ to node $\beta_j$ at time $t$; this function can be described as below:

$$M(\beta_i, \beta_j, t) = \sum_{l=1}^{k} \delta_l \Omega_l(\beta_i, \beta_j). \tag{2}$$

By computing the value of the function $M(\beta_i, \beta_j, t)$, we can obtain the specific satisfaction degree of the subject

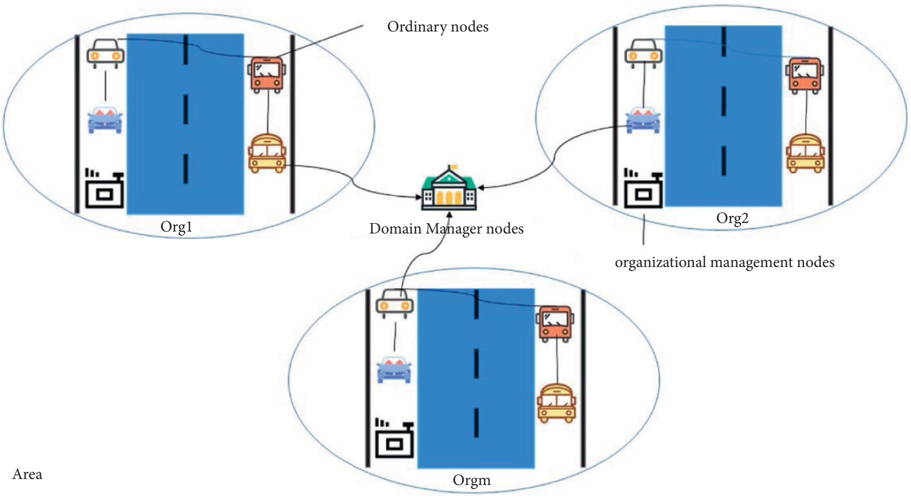

Figure 1: Trust measurement network model.

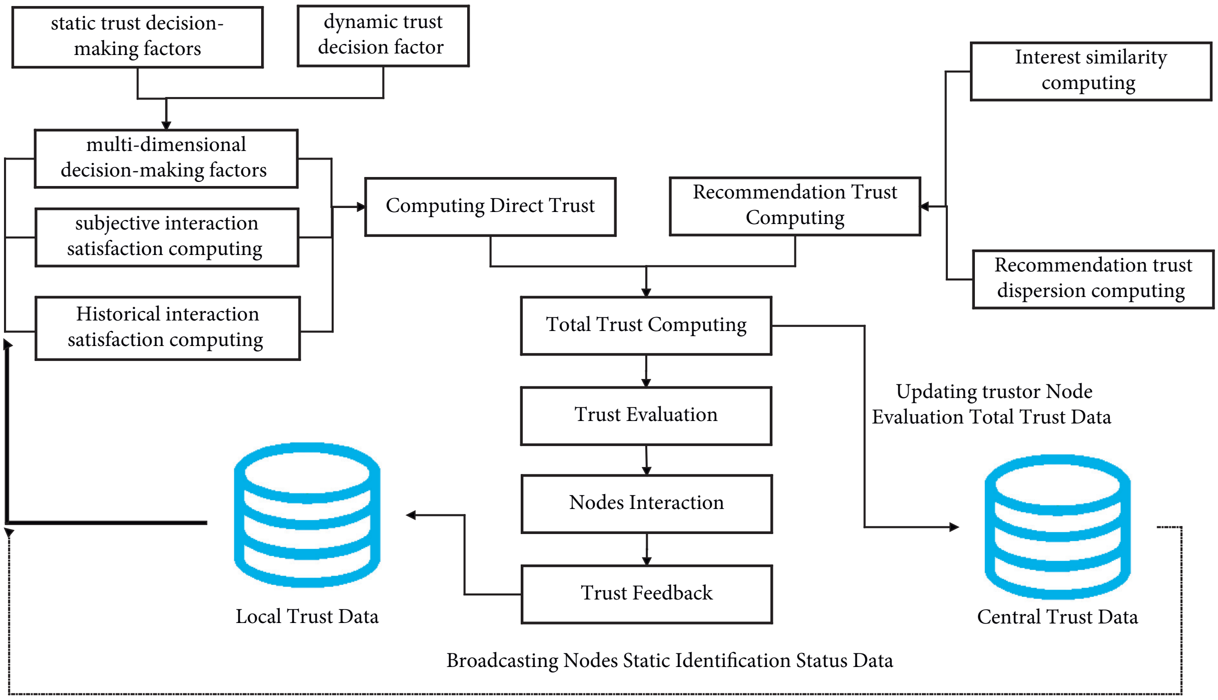
static trust decision-making factors
dynamic trust decision factor
multi-dimensional decision-making factors
subjective interaction satisfaction computing
Historical interaction satisfaction computing
Computing Direct Trust
Recommendation Trust Computing
Interest similarity computing
Recommendation trust dispersion computing
Total Trust Computing
Trust Evaluation
Nodes Interaction
Trust Feedback
Updating trustor Node Evaluation Total Trust Data
Local Trust Data
Central Trust Data
Broadcasting Nodes Static Identification Status Data

Figure 2: Trust measurement diagram based on multidimensional decision-making attributes.

interaction, and the detailed computing method can be seen in Section 3. In this paper, the $M(\beta_i, \beta_j, h)$ is used to indicate the historical record of subjective interaction satisfaction, and $M_t(\beta_i, \beta_j, t)$ is used for direct trust measurement function.

*2.3. Recommendation Trust Reliability Measurement Model.* The recommendation trust reliability describes the reliability of the trust evaluation of the recommendation node to the target node. The recommendation trust reliability calculation is mainly affected by two factors: one is the honesty of the recommendation node and the reference value of the recommendation trust it provides; the other is the trustor node's trust evaluation of the recommendation node. Therefore, this paper defines the recommendation trust measurement reliability of $\beta_k$ to target node $\beta_j$ as follows:

$$R\left(\beta_k, \beta_j, t\right) = \mathrm{Sim}\left(\beta_i, \beta_k\right) * \left(1 - \rho_k\right) * M_t\left(\beta_k, \beta_j, t\right). \quad (3)$$

Among them, $\mathrm{Sim}(\beta_i, \beta_k)$ is the service preference similarity between the recommendation node $\beta_k$ and trustor node $\beta_i$, and $\rho_k$ is the recommendation node's evaluation dispersion of the target node $\beta_j$ relative to all the recommendation nodes.

*2.4. Total Trust Measurement Model.* The essence of the total trust calculation process is to integrate the effective information of multiple evaluation indicators to make a more objective comprehensive evaluation of the target node. Information entropy can reflect the degree of disorder of information. Therefore, the index weight can be automatically adjusted according to the difference between direct and recommended trust to realize adaptive weight distribution, so as to make full use of effective information to solve the limitation of empirical weight. The total trust measurement is calculated using the following equation:

$$M_{\text{total}}\left(\beta_i, \beta_j, t\right) = \gamma_t M_t\left(\beta_i, \beta_j, t\right) + \gamma_{rt} M_{rt}\left(\beta_i, \beta_j, t\right), \tag{4}$$

where $\gamma_t$ and $\gamma_{rt}$ are the direct trust and recommendation trust information entropy, respectively, and Section 5 shows more specific contents.

## 3. Direct Trust Measurement

Suppose that $\{\beta_1, \beta_2, \ldots, \beta_n\}$ represents the Internet of Vehicles nodes that have interactive behaviors in the network environment. The direct trust of a node is the quantified trust evaluation value calculated by the trustor node with reference to the interaction result; however, the interaction result is comprehensively calculated by fusing multidimensional trust evaluation factors.

*3.1. Selection of Multidimensional Decision-Making Factors.* The research on trust mechanism is divided into two directions: policy-based trust mechanism and reputation-based mechanism. The former usually uses a complete cryptographic system to verify the identity of nodes to ensure the security of the Internet of Vehicles. It is a relatively static trust management mechanism. The reputation-based trust mechanism evaluates the trustworthiness of nodes through interactions among nodes, which is a dynamic trust management mechanism. This paper combines these two methods by selecting trust decision factors from both static and dynamic perspectives. Therefore, this method satisfies both static and dynamic networking requirements and avoids the following trust issues of the Internet of Vehicles: (1) the problem that nodes can launch any kind of internal network attacks after concealing their identity and obtaining authentication; (2) the problem that a node is able to obtain and provide services without performing identity authentication when joining the network dynamically.

*3.1.1. Selection of Static Trust Decision-Making Factors.* The organizational management node can select static $m$-dimensional factors as below:

$$\Omega_S = \left(\Omega_s^1, \Omega_s^2, \ldots, \Omega_s^m\right). \tag{5}$$

The $m$-dimensional static trust factors can include the following:

(1) Whether the nodes pass the authentication phase.

(2) Whether the critical hardware components have been replaced or hacked, such as key computing chips and power management chips.

(3) Whether key software components are invaded or changed, such as core software boot program, security chain checking program, operating system core, and critical data collection and processing programs.

For the convenience of experimental simulation, this paper only uses one static trust factor, that is, whether the node's identity is authenticated, and defines the related weight of the trust factor as follows:

$$\delta_{\Omega_s^1} = \begin{cases} 0.5, & \text{if node } \beta_i \text{ joins the network staticly,} \\ \dfrac{1}{k}, & \text{if node } \beta_i \text{ joins the network dynamicly and } k \text{ indicates the total direct trust factors.} \end{cases} \tag{6}$$

The trust measurement factor $\Omega_0(\beta_\pi, \beta_i)$ is defined as below:

$$\Omega_0(\beta_\pi, \beta_i) = \begin{cases} 1, & \text{if node } \beta_i \text{ passes authentication or dynamicly joins network,} \\ 0, & \text{if node } \beta_i \text{ fails to pass authentication.} \end{cases} \tag{7}$$

The organization management node periodically broadcasts node identity verification information to other nodes in the organization, so that trustor nodes can obtain effective information during the trust evaluation phase, in which the trustor node performs the trust evaluation on the node that provides services, that is, the trustee node.

*3.1.2. Dynamic Trust Decision Factor Selection.* The dynamic trust decision factors are defined as follows:

$$\Omega_D = \left(\Omega_D^1, \Omega_D^2, \ldots, \Omega_D^l\right). \tag{8}$$

Among them, the trust evaluation factors based on the dynamic behavior of nodes may include the following aspects:

(1) Data package forwarding rate: During nodes interaction, the trustor node requests $N$ data packages forwarding service from the trustee node, and the latter forwards $n(n \leq N)$ data packets. After the trustee node completes the service, the trustor node evaluates the behavior of the node based on the data packet forwarding rate.

(2) Data package repetition rate: The data package repetition rate is also an important reference indicator for judging whether the behavior of a node is abnormal. When the data package repetition rate is low, the node tends to be credible. Its satisfaction degree regarding the service of forwarding data package will decrease when the repetition rate increases. As the repetition rate gradually approaches or is greater than the tolerable repetition rate threshold, the possibility of abnormal behavior of a node becomes bigger, and this node is more likely to be identified as a malicious node.

(3) Data package integrity: If the node tampers with the content of the data package passed, the credibility of the node will be reduced.

(4) Service response time: This factor is used to describe the response time consumed when the trustor node requests service from the trustee node.

(5) Transmission delay time: If the transmission delay time for forwarding the data package is less than the threshold value specified by the system, the credibility level of the node, which provides data package forwarding service, is considered to be at a good level; otherwise, this node has the tendency to be regarded as one malicious node aiming to attack the network.

(6) The remaining energy of the node: Due to the resource limitation of the IoV node, the node may not be able to provide requested data package forwarding services or other services because the energy of this node is near to exhaustion. In order to avoid judging such normal nodes as malicious nodes, the remaining energy of the node should be taken into consideration when handling the trust evaluation. The node detects its own remaining energy, records it, and broadcasts the maximum energy and remaining energy to other nodes in the network if necessary. The impact of the node's remaining energy will be quantified as the remaining energy influence factor.

*3.2. Subjective Interaction Satisfaction Computing.* The subjective interaction satisfaction refers to the evaluation made by the trustor node based on the multidimensional attributes after it finishes interacting with the trustee node. According to the source of satisfaction data in trust calculation, it is divided into subjective interaction satisfaction and historical interaction satisfaction. The value range of satisfaction is [0, 1], where 0 means totally dissatisfied and 1 means very satisfied. The subjective interaction satisfaction at time $t$ can be calculated by the trustor node using (1) and (2) after the trustee node completes the service requested by the trustor node. The following equation shows how to calculate this value.

$$M\left(\beta_i, \beta_j, t\right) = \sum_{u=1}^{l+m} \delta_u \Omega_u\left(\beta_i, \beta_j\right). \tag{9}$$

Subjective satisfaction is the subjective behavior of nodes, and the different node has different preferences for multidimensional decision-making attributes. Therefore, considering the node's own interest preferences, the evaluation value of each trust aspect has a different impact on the total trust evaluation; the impact is represented by the weighted coefficient for each trust aspect; and this weighted coefficient shows the level of interest preference, for example, the weight $\delta_i$ shows the level of interest preference of $i^{th}$ aspect.

*3.3. Historical Interaction Satisfaction Computing.* After the trustor node finishes calculating the subjective interaction satisfaction to the trustee node, the trustor node will store the calculated satisfaction result and update the historical interaction satisfaction record. The historical interaction satisfaction record of the node $\beta_j$ recorded by the trustor node $\beta_i$ is as follows:

$$M_{\text{history}}\left(\beta_i, \beta_j\right) = \left(M_1\left(\beta_i, \beta_j, t_1\right), M_2\left(\beta_i, \beta_j, t_2\right), \ldots, M_n\left(\beta_i, \beta_j, t_n\right)\right). \tag{10}$$

In addition, the following equation defines how the historical interaction satisfaction is calculated:

$$M\left(\beta_i, \beta_j, h\right) = \sum_{k=1}^{n} \left(\frac{\eta_k}{\sum_{l=1}^{n} \eta_l} * M_k\left(\beta_i, \beta_j, t_k\right)\right), \tag{11}$$

and $\eta_k$ is the weighted time-related coefficient and is defined as below:

$$\eta_k = e^{-\lambda * L(t - tk)}. \tag{12}$$

$\lambda$ is the rate adjustment factor, and its scope is $0 < \lambda < 1$. $\lambda$ can be adjusted according to actual context. $L(t - t_k)$ is the time update function, which represents the distance of the $k^{\text{st}}$ historical trust record from the current time.

*3.4. Direct Trust Computing.* Direct trust value can be calculated by fusing subjective interaction satisfaction and historical interaction satisfaction, that is,

$$M_t\left(\beta_i, \beta_j, t\right) = \xi M\left(\beta_i, \beta_j, t\right) + (1 - \xi) M\left(\beta_i, \beta_j, h\right), \tag{13}$$

where $\xi (0 < \xi \leq 1)$ is the adjustable parameter and presents the weight of subjective interaction satisfaction; this parameter indicates the importance of the latest interaction of node $\beta_i$ with $\beta_j$, and this parameter can be set by the trustor node each time it interacts with the trustee node.

## 4. Recommendation Trust Measurement

The recommendation trust measurement is affected by two factors: the trust measurement of the recommendation node to the target node and the trustor node's evaluation of the recommendation node. When handling the selection of the recommendation nodes in this paper, several aspects are taken into consideration: (1) select the node that has the same or similar service preference between the recommendation node and the trustor node; (2) the node to be evaluated and the recommendation node have actually interaction records in history. It can be seen from (3) that the reliability of the trust measurement of the recommendation node to the target node consists of three parts, namely, the service preference similarity between the recommendation node and the trustor node, the recommendation trust dispersion degree of the recommendation node with respect to all the recommendation nodes to the target node, and the direct trust value of the recommendation node to the target node. This section details how these three parts are calculated.

*4.1. Service Interest Similarity Computing.* This paper calculates the similarity of service preferences between recommendation node and trustor node according to (14), that is, according to the dynamic trust decision factor in Section 3, and the service preference similarity between two nodes is calculated according to the cosine similarity. The service preference is initialized when the system is running and stored in the trusted memory of the node. The manufacturer needs to update it online through the key. The higher the similarity value is, the closer the service preferences between the two nodes are, and the more meaningful the recommendation trust is.

$$\mathrm{Sim}\left(\beta_i, \beta_k\right) = \frac{\sum_{j=1}^{l}\left(\delta_j^i * \delta_j^k\right)}{\sqrt{\sum_{j=1}^{l} \delta_j^{i\,2}} * \sqrt{\sum_{j=1}^{l} \delta_j^{k\,2}}}. \tag{14}$$

*4.2. Recommendation Trust Dispersion Computing.* Suppose that $\overline{M_t\left(\beta, \beta_j, t\right)}$ is the direct trust expectation from all the recommendation nodes and $M_t\left(\beta_k, \beta_j, t\right)$ is used to indicate the direct trust value of the recommendation node to the target node $\beta_j$; then, the dispersion can be calculated as below.

$$\rho_k = \frac{M_t\left(\beta_k, \beta_j, t\right) - \overline{M_t\left(\beta, \beta_j, t\right)}}{\sum_{l=1}^{n}\left(M_t\left(\beta_l, \beta_j, t\right) - \overline{M_t\left(\beta, \beta_j, t\right)}\right)}. \tag{15}$$

*4.3. Recommendation Trust Measurement Computing.* After getting the recommendation trust reliability of node $\beta_k$ to node $\beta_j$, which is indicated with $R\left(\beta_k, \beta_j, t\right)$, the recommendation trust of the target node is calculated as follows:

$$M_{rt}\left(\beta_i, \beta_j, t\right) = \sum_{l=1}^{n} \frac{R\left(\beta_l, \beta_j, t\right)}{\sum_{l=1}^{n} R\left(\beta_l, \beta_j, t\right)} * M_t\left(\beta_l, \beta_j, t\right). \tag{16}$$

## 5. Total Trust Measurement

The total trust measurement calculation process is to fuse the direct trust value and the recommendation trust value and is a comprehensive trust evaluation of the trustee vehicle. It can be seen from (4) that after getting the direct trust value and the recommendation trust value, their respective weights have a direct impact on the result of the comprehensive trust measurement.

Information entropy can reflect the degree of disorder of information. Therefore, the index weight can be adjusted according to the difference between direct and recommended trust by implementing the information entropy during total trust computing. The introduction of information entropy solves the problem of the limitation of setting the weight empirically thanks to the auto-adaptive feature of information entropy. The following equation shows how to calculate the information entropies for direct trust and recommendation trust.

$$\begin{aligned} H\left(M_t\left(\beta_i, \beta_j, t\right)\right) &= -M_t\left(\beta_i, \beta_j, t\right)\log M_t\left(\beta_i, \beta_j, t\right) - \left(1 - M_t\left(\beta_i, \beta_j, t\right)\right)\log\left(1 - M_t\left(\beta_i, \beta_j, t\right)\right), \\ H\left(M_{rt}\left(\beta_i, \beta_j, t\right)\right) &= -M_{rt}\left(\beta_i, \beta_j, t\right)\log M_{rt}\left(\beta_i, \beta_j, t\right) - \left(1 - M_{rt}\left(\beta_i, \beta_j, t\right)\right)\log\left(1 - M_{rt}\left(\beta_i, \beta_j, t\right)\right). \end{aligned} \tag{17}$$

The following equation shows how the auto-adaptive weight parameters for direct and recommendation trust are calculated.

Table 1: Simulation parameter setting.

| Parameter | Value |
|---|---|
| Number of vehicle nodes | 100 |
| Static decision-making factor | 0~1 |
| Dynamic decision-making factors | 0~1 |
| Node preference | $\delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5 + \delta_6 = 1$ |
| Interaction success rate | 0 |
| Trust threshold | 0.5 |

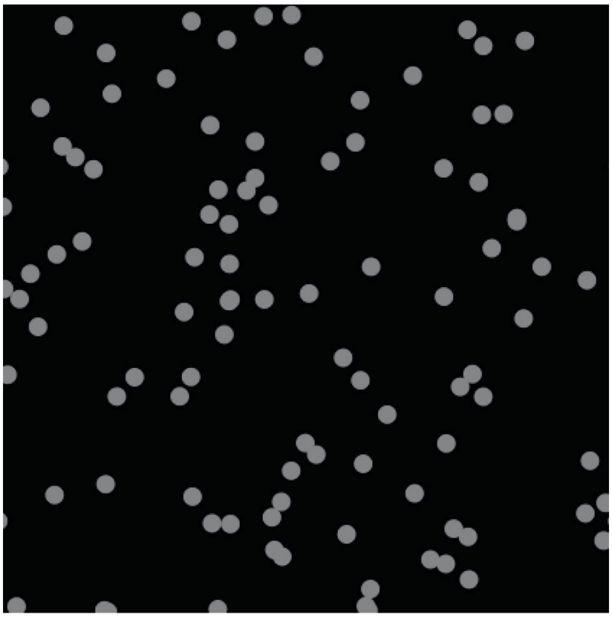

Figure 3: Initial status of the IoV.

$$\gamma_t = \frac{\left(1-\left(H\left(M_t\left(\beta_i,\beta_j,t\right)\right)/\log H\left(M_t\left(\beta_i,\beta_j,t\right)\right)\right)\right)}{\left(\left(1-\left(H\left(M_t\left(\beta_i,\beta_j,t\right)\right)/\log H\left(M_t\left(\beta_i,\beta_j,t\right)\right)\right)\right)+\left(1-\left(H\left(M_{rt}\left(\beta_i,\beta_j,t\right)\right)/\log H\left(M_{rt}\left(\beta_i,\beta_j,t\right)\right)\right)\right)\right)},$$
$$\gamma_{rt} = \frac{\left(1-\left(H\left(M_{rt}\left(\beta_i,\beta_j,t\right)\right)/\log H\left(M_{rt}\left(\beta_i,\beta_j,t\right)\right)\right)\right)}{\left(\left(1-\left(H\left(M_t\left(\beta_i,\beta_j,t\right)\right)/\log H\left(M_t\left(\beta_i,\beta_j,t\right)\right)\right)\right)+\left(1-\left(H\left(M_{rt}\left(\beta_i,\beta_j,t\right)\right)/\log H\left(M_{rt}\left(\beta_i,\beta_j,t\right)\right)\right)\right)\right)}. \tag{18}$$

Finally, the total trust value is calculated as follows:

$$M_{\text{total}}\left(\beta_l,\beta_j,t\right) = \gamma_t M_t\left(\beta_i,\beta_j,t\right) + \gamma_{rt} M_{rt}\left(\beta_i,\beta_j,t\right). \tag{19}$$

## 6. Experimental Simulation and Result Analysis

To evaluate the credibility metric model proposed in this paper, the Windows 10 operating system is utilized as the simulation platform, and an IoV simulation network is built by using the NetLogo simulator. In the scheme of this article, there are three types of nodes in the IoV network, which are vehicle nodes, organizational management nodes, and domain management nodes. The target nodes to be evaluated are mainly vehicle nodes, and the management node is only responsible for the evaluation and management of vehicle nodes. Therefore, this simulation model mainly focuses on the interaction and evaluation between vehicles in a single organization. The detailed experimental parameters simulated in this section are shown in Table 1.

In this experiment, the number of vehicle nodes is 100, and the status of all vehicle nodes will be randomly reset to the default state, as shown in Figure 3. Then, each vehicle randomly interacts with other vehicles and conducts trust evaluation of the interacting vehicles; during the running period, some vehicles are marked as trusted node and others are recognized as untrusted nodes. For vehicle nodes whose trust value is too low, the organizational management node will reset it.

The trust evaluation model in this experiment is mainly through the combination of direct trust measurement and recommended trust measurement. Therefore, as the system runs, the evaluation accuracy of the entire system will become higher and higher, and the trust of untrusted vehicles

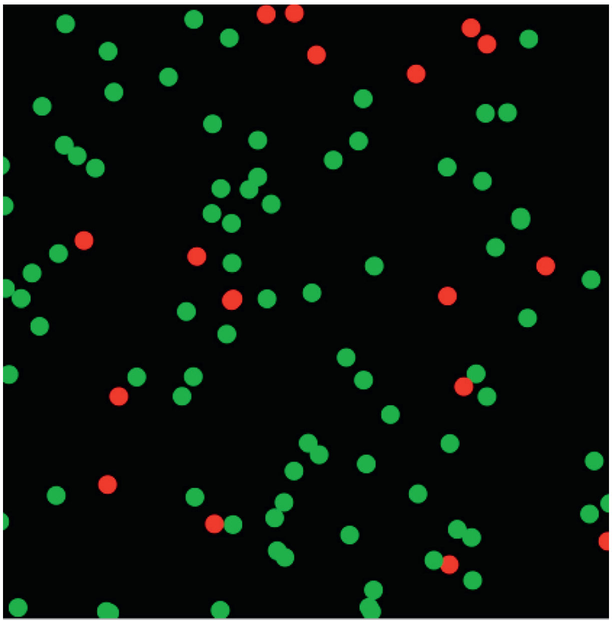

Figure 4: The interaction procedure of IoV.

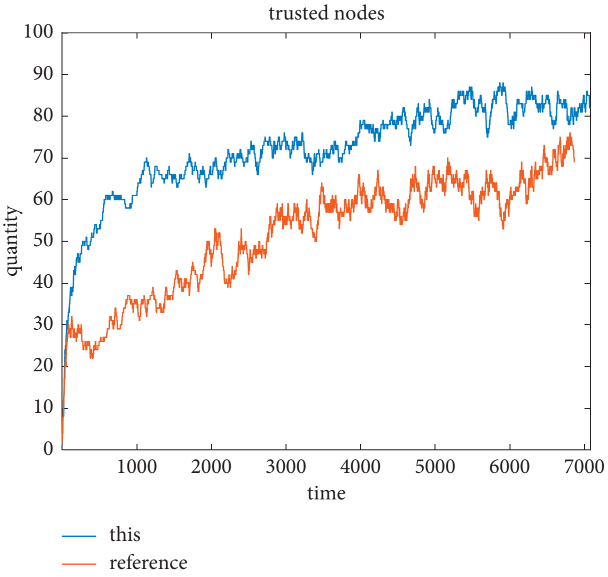

Figure 5: Evolution of the number of trusted vehicle nodes.

will gradually decrease until it is managed by the organization. When the untrusted vehicle is reset or kicked off from the network, the entire IoV tends to be trusted, as shown in Figure 4. At the same time, this experiment is compared with Liu's trust measurement scheme [6], and the detailed IoV changes as the simulation network runs are as follows.

As shown in Figure 5, in the same IoV environment, the increased speed of trusted vehicle nodes in this paper is comparable to that of the references at the beginning, but with the mutual trust evaluation process of the vehicles in the network, the solution in this paper is effective for trusted vehicles. The evaluation becomes more and

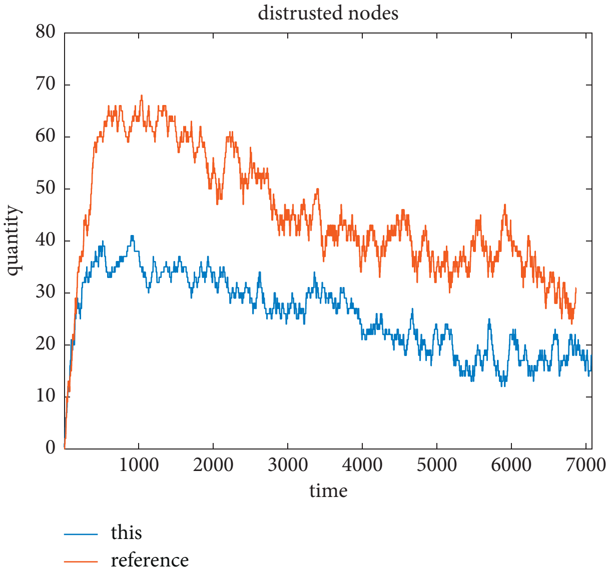

Figure 6: Evolution of the number of untrusted vehicle nodes.

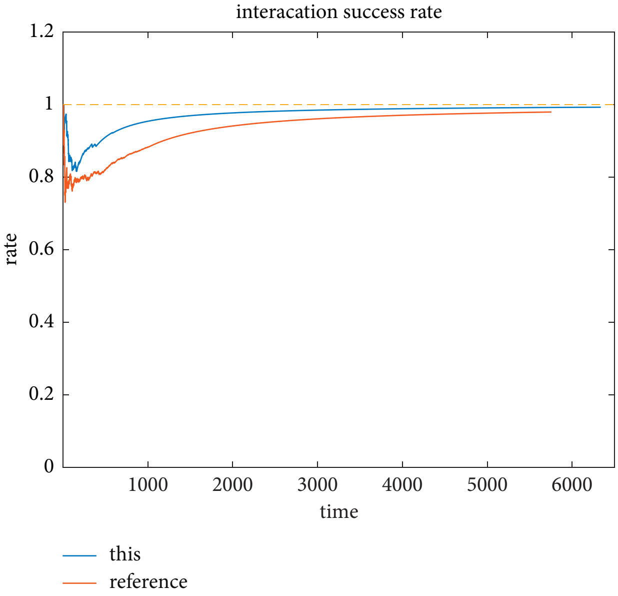

Figure 7: Evolution of the interaction success rate.

more accurate, and finally, when the entire IoV becomes stable, the number of trusted vehicles is more than that of the reference model.

As shown in Figure 6, in the same IoV environment, the number of untrusted vehicle nodes in this scheme is less, and the reduction speed is faster. When the IoV tends to be stable, the number of untrusted vehicle nodes is also less.

As shown in Figure 7, in the same IoV environment, the nodes of this scheme have a higher success rate in the interaction process. With the continuous evolution of the IoV environment, the interaction success rate of this scheme tends to approach 1 earlier.

## 7. Conclusion

In view of the insufficient consideration of the networking modes of the IoV, the characteristics of vehicles, and the multidimensional decision-making attributes of trust modes in the existing research, this paper proposes a novel model making the best of advantages of both central trust management and distributed trust management, that is, the auto-adaptive trust measurement based on multidimensional decision-making attributes. This model allows the evaluation vehicle to consider multiple decision attributes such as the vehicle's packet forwarding rate and packet repetition rate in the direct credibility measurement, and the model solves the problem of insufficient adaptability of the traditional quantitative model in the environment with dynamic changes. The adoption of methods such as direct trust measurement, indirect trust measurement, and information entropy smoothing of vehicles improves the efficiency and credibility of trust evaluation and, at the same time, enhances the dynamic adaptability of the model. The model proposed in this paper still has shortcomings, such as the lack of detailed quantification of each decision attribute, and the quantification of trust reliability caused by the difference in the number of hops between the recommendation trust vehicles and evaluation vehicles. In the future, according to the development trend of the IoV technology, the decision-making attributes in the network environment will be optimized to improve the trust evaluation model of the vehicles.

## Data Availability

No data were used to support this study.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This research work was supported by the National Key R&D Program of China (Grant number: 2019YFB1406303).

## References

[1] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, "Cognitive internet of vehicles," *Computer Communications*, vol. 120, pp. 58–70, 2018.

[2] Y. Li, L. Zhu, and H. Wang, "A cross-layer defense scheme for edge intelligence-enabled CBTC systems against MitM attacks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2286–2298, 2020.

[3] J.-H. Cho, "A survey on trust modeling," *ACM Computing Surveys*, vol. 48, no. 2, 2015.

[4] S. Mike, C. Gianluca, and M. Ken, "Trust Modelling in 5G mobile networks," in *Proceedings of the Workshop on Security in Softwarized Networks: Prospects and Challenges (SecSoN' 18)*, pp. 14–19, New York, NY, USA, August 2018.

[5] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)," *Computing*, vol. 12, pp. 1–28, 2018.

[6] Z. Q. Liu, *Research on Key Issues of Trust Modeling in Mobile Distributed Environment*, Xi'an University of Electronic Science and Technology, Xian, China, 2017.

[7] L. X. Xie and R. X. Wei, "A dynamic trustworthiness assessment method for Internet of Things nodes," *Computer Applications*, vol. 3, pp. 2597–2603, 2019.

[8] P. S. Pawar, M. Rajarajan, and S. K. Nair, "Trust model for optimized cloud services," in *Proceedings of the Ifip International Conference on Trust Management*, pp. 97–112, Berlin, Germany, May 2012.

[9] A. Mohsenzadeh, H. Motameni, and M. J. Er, "Retraction note to: a new trust evaluation algorithm between cloud entities based on fuzzy mathematics," *International Journal of Fuzzy Systems*, vol. 18, pp. 659–672, 2019.

[10] Z. L. Su, W. B. Jiang, and Q. D. Qiu, "A game based IoT terminal unfamiliar node trust evaluation model and algorithm," *Information Security and Technology*, vol. 7, pp. 87–92, 2016.

[11] F. Li, Y. L. Shi, and ChenZ, "A trust-based approach to secure routing decisions for networks of opportunity," *Software Journal*, vol. 29, pp. 2829–2843, 2018.

[12] D. Y. Wu, Q. Li, and X. Yu, "A peer-to-peer network trust model based on blockchain," *Computer science*, vol. 46, pp. 138–147, 2019.

[13] J. You, J. L. Shangguan, and S. K. Xu, "Distributed dynamic trust management model based on trust reliability," *Journal of Software*, vol. 28, pp. 2354–2369, 2017.

[14] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[15] K. Lu, J. Wang, and M. Li, "An Eigentrust dynamic evolutionary model in P2P file-sharing systems," *Peer-to-Peer Networking and Applications*, vol. 9, no. 3, pp. 599–612, 2016.

[16] U. Jayasinghe, A. Otebolaku, and T. W. Um, "Data centric trust evaluation and prediction framework for IoT," in *Itu Kaleidoscope: Challenges for A Data-Driven Society*, pp. 27–29, IEEE, Nanjing, China, 2017.

[17] N. B. Truong, T. W. Um, and B. Zhou, "From personal experience to global reputation for trust evaluation in the social internet of things," in *Proceedings of the Global Communication (GLOBECOM), Singapore*, pp. 4–8, IEEE, New York, NY, USA, December 2017.

[18] L. Zhu, H. Liang, and H. Wang, "Joint security and train control design in blockchain empowered CBTC system," *IEEE Internet of Things Journal*, 2021.

[19] L. Zhu, Y. Li, and F. R. Yu, "Cross-layer defense methods for jamming-resistant CBTC systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, 2020.