A Trust Assessment Mechanism of the IoV Based on Multi-factor Analytic Hierarchy Process

Peng-Shou Xie, Xin Tong, Hong Wang, Ying-Wen Zhao, Tao Feng, and Yan Yan
(Corresponding author: Xin Tong)

School of Computer and Communications & Lanzhou University of Technology
No. 36 Peng jia ping Road, Lanzhou, Gansu 730050, China
Email: 2505156603@qq.com

(Received July 25, 2021; Revised and Accepted Jan. 28, 2022; First Online Apr. 9, 2022)

Abstract

The impact of multiple factors on the trust of vehicle nodes is considered comprehensively in this paper, a trust assessment mechanism for the Internet of Vehicles is proposed. For multi-application scenarios, the analytic hierarchy process is used to quantify the degree of influence of each factor on vehicle trust in different application scenarios; initial trust is added to prevent vehicle cold start; Bayesian approach is improved based on the same quality of service strength, dynamic trust decay and malicious event influence; cosine similarity is employed to optimize recommendation trust weights, and weighted to establish global Roadside Unit trust. The effectiveness of this evaluation mechanism in portraying node behavior, identifying malicious nodes, and suppressing malicious recommendation behavior is verified by simulation experiments. The experiments show that this paper has advantages in recommendation trust evaluation accuracy and vehicle interaction success rate compared with other methods.

Keywords: Analytic Hierarchy Process; Cosine Similarity; Internet of Vehicles; Multi-Factor; Trust Assessment Mechanism

1 Introduction

The main purpose of Internet of Vehicles (IoV) is to improve road safety and reduce traffic congestion [6]. In recent years, with the rapid development of in-vehicle technologies, control technologies, wireless communication technologies, Internet of Things and information physical systems, the IoV has become an important research area [16]. However, the open network environment and diverse system resources of the Iov are prone to false information, rapid changes in network topology, and unreliable message propagation [25, 27–29], leading to threats to Iov security. Therefore, there is an urgent need to establish a reliable trust assessment mechanism for mutual communication between Iov vehicles to ensure a trusted communication environment and the security and stability of the network [19].

For IoV security-related applications, it is a very important task to ensure that the communication entities meet the trust requirements. In the trust assessment of wireless sensor networks, a fully mediated approach using node internal resources to assess node-level trust is proposed, which enables nodes to assess their own trust level [4]. In response to the traditional static trust model that cannot effectively create trust relationships between vehicles and cannot quickly and dynamically handle frequent vehicle interactions in the network topology, a novel trust model is established from initialization, service demand discovery, distributed evaluation and authentication, and trust transformation by improving trust chains and trustworthy computing theory [26]. For the traditional trust approach is not adapted to the cloud environment with dynamic attribute changes, an evidence-based trust model is proposed, this model uses various attributes of cloud services as evidence factors, it outperforms other models in terms of accuracy and efficiency [5]. To address the lack of objectivity and accuracy of the trust assessment model of wireless sensor network nodes, some researchers have improved the trust assessment model by combining trust management mechanism, trust factors, fuzzy sets and DS evidence theory to improve the security of the network [30]. Some researchers propose a multi-parameter trust calculation method which observes and detects malicious behavior of nodes based on time series theory [12]. There are also researchers who trustevaluate based on clusters and blockchains [11, 24]. In electric vehicle networks [21], researchers used maximum neighbor distance and access trees to improve the efficiency of trust assessment and reduce the whole transmission hops for trust assessment, thus extending the lifetime of the network. In in-vehicle self-organizing networks a method based on Hidden Markov Model for vehicle trust evaluation was proposed to improve the efficiency of trust updates and queries [15]. In the trust assessment of cloud services, researchers build a model based on weight and gray correlation analysis and use rough set theory and analytic hier-

archy process for direct trust by forming a comprehensive trust together with recommended trust [22]. The above-mentioned references on trust assessment of the IoV lacks consideration of Roadside Unit (RSU) in node assessment, and the trust features in recommended trust differ significantly from the evaluated entities, and the identification of malicious nodes needs further enhancement.

In order to correctly and effectively identify malicious nodes and provide trust support for vehicle interaction, this paper proposes a multi-factor trust evaluation mechanism based on hierarchical analysis. The trust of multiple factors of the vehicle is evaluated: including initial trust, direct trust, recommended trust, RSU global trust, and finally the adaptive weights of each factor are obtained by hierarchical analysis according to the application scenario, so as to aggregate and get the comprehensive trust value. The rest of this paper is organized as follows: Section 2 introduces the IoV network framework and trust assessment framework. In the framework of trust assessment, the problems existing in each module and research ideas are described in detail. Section 3 introduces the trust evaluation method in each module in detail. Section 4 shows the simulation experiment configuration environment and the results and analysis.

2 Trust Assessment Framework of the IoV

2.1 Network Framework of IoV

The IoV refers to a mobile communication network that combines wireless communication technology with a vehicle network and provides value-added services to vehicle users based on the social relationship between vehicles that communicate with each other. The IoV can continuously monitor and share road and traffic conditions. The main components of the IoV are vehicles embedded in On-board units (OBU), RSU, communication components including Radio frequency antenna antennas and processing units, and telecommunication networks, such as satellite communications.

The main communication technologies are our c-ellular vehicle networking [2] and IEEE802.11p. Th-ere are three main communication modes [13], Interv-ehicle communication (V2V), Vehicle-to-road-side com-munication (V2I), Interroad-side communication (I2I).

V2V: in this mode of communication vehicles with another vehicle with the help of OBU in every vehicle. In this communication mode, vehicle to vehicle communication with each other with wireless technology.

V2I: in this mode of communication, vehicles will communicate with the roadside communication equipment RSU. Furthermore, in this mode, a direct wireless communication link is established between vehicle and infrastructure units located around the road.

I2I: in this mode, communication RSU communicates with another RSU and core network, for example, 5G, satellite, or wired telecommunication system.

Trusted authority (TA): Trusted authority is the heart of the IoV system.The primary responsibility is registering the RSUs,OBUs,and vehicles.Secondary responsibilities include ensuring safety management through vehicle identity verification,user identification and OBU identification,and assigning initial trust to the vehicle.

RSU: these are communication-based units installed near highways, which transmit useful information to vehicles that came in the radio range of RSU. They are connected to a central network with means of wired or wireless. The network framework of the IoV is shown in Figure 1.

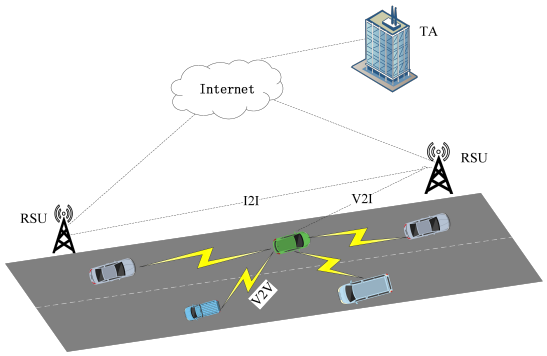

Figure 1: Internet of Vehicles network framework

2.2 Trust Evaluation Framework of the IoV

Trust is a subjective behavior. Vehicle nodes can choose which nodes to cooperate with. In the IoV, messages are filtered through mutual trust evaluation between vehicles. The trust assessment framework in this paper consists of the following modules. Initial Trust Module; Direct Trust Module; Recommended Trust Module; RSU Trust Module. Since vehicles can only interact when a trust value is available, the initial trust value setting provides the trust basis for direct vehicle interaction. The calculation of the direct trust value also provides the basis for the calculation of the recommended trust and RSU fusion trust. The proposed framework studies the computational approach between several trust modules. The dynamic weights of each module are calculated by the analytic hierarchy process, and then combined and weighted to obtain the comprehensive trust value.The trust evaluation framework is shown in Figure 2.

The problem analysis and research ideas of each module are described as follows.

A. Initial Trust Module

In the IoV, when a newly added vehicle node communicates with other vehicle nodes, other vehicle nodes cannot find the trust value to authenticate the new vehicle node, so a cold start problem occurs [8].

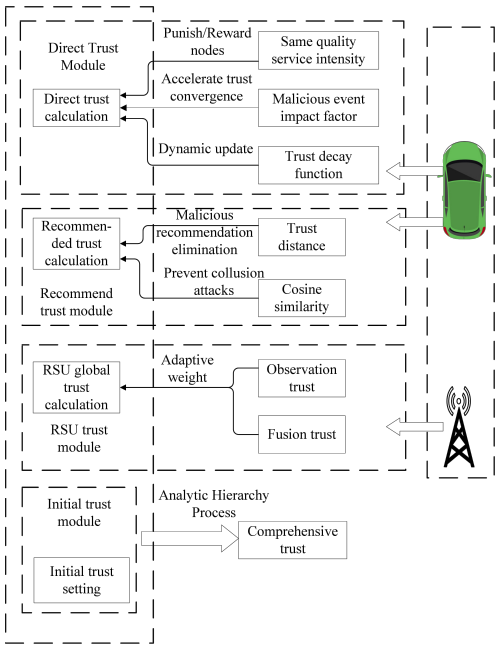

Figure 2: Trust evaluation framework

To address the above issues, the research idea of this paper is: Because newly registered vehicles do not have historical interaction data records, the legitimacy of the vehicle cannot be judged, so newly registered vehicles cannot have a high trust value. Therefore, the initial trust can be set to 0.1-0.4 according to the vehicle safety related attributes, which can effectively solve the problem of cold start (trust value = 0). Vehicle safety related attributes include: vehicle type, vehicle ID, whether there is security hardware support, etc.

B. Direct Trust Module

The main problems in direct trust assessment are as follows.

1) In most direct trust assessment methods based on Beta distribution, static decay factors are employed to achieve the decay of historical trust, but it is difficult to guarantee the validity of trust assessment;
2) Trust is built slowly during the node interaction. Ceteris paribus, trust value increases slowly due to good behavior and decreases quickly due to malicious behavior;
3) In the IoV, the quality of service of vehicle nodes may be affected when they are affected by non-intrusive factors such as signal interference. If the impact of non-intrusive factors is ignored and causes failed interactions, it will not be able to effectively distinguish malicious nodes from nodes with occasional abnormal behavior;

Taking into account the above problems, the research ideas of this paper are as follows.

1) Considering the time factor of direct trust [14], a dynamic trust decay function is designed to combine the historical trust value of the node with the latest observation value to realize the dynamic update of the direct trust value;
2) To increase the influence of malicious events, the effect of malicious events is introduced in this paper to quickly converge the trust value to within the trust threshold, thus speeding up the detection of malicious nodes;
3) To better characterize the behavior of nodes, effectively distinguish malicious nodes, and avoid malicious nodes from participating in cooperation, this paper designs the same quality service intensity evaluation factor to evaluate the overall behavior of nodes in the continuous monitoring cycle, and according to the same quality of nodes in the monitoring cycle Service intensity punishes nodes that continue to provide malicious services or motivates legitimate nodes;

C. Recommend Trust Module

The main problems with the recommended trust node calculation are as follows.

1) Malicious recommendations from malicious nodes;
2) Complex calculations required in the recommendation delivery process;
3) Malicious nodes are prone to perform malicious recommendations after obtaining high trust ratings from evaluation nodes by providing good services, which reduces the accuracy of recommendation trust calculation;

Considering the above problems, the research ideas are as follows.

1) To reduce malicious recommendations and improve the honesty of recommendations, trust distance is used in the computation of recommendation trust to exclude some malicious recommendation nodes;
2) To reduce the complicated calculation caused by recommendation transmission, this paper only considers the recommendation opinions of neighboring nodes within one hop of the subject;
3) Optimizing the weight calculation of recommendation trust using cosine similarity, reduce the situation that the trust characteristic of the malicious recommendation node is quite different from the evaluation entity, to improve the accuracy and reliability of the trust evaluation;

D. RSU Trust Module

The RSU acts as a roadside unit to detect the various states of the vehicle nodes, and when a vehicle

enters the communication range of the RSU the vehicle transmits the acquired trust value to the RSU. then the RSU fuses the trust of other vehicle nodes about a certain vehicle node. Therefore, RSU trust considers two aspects.

1) Various state attributes of the vehicle. As the trajectory of the vehicle changes, trust can be transmitted between RSUs in real-time. As an observer, the RSU will make a trust assessment of the various states of the vehicle;
2) A report on the trust value of a vehicle node to other vehicle nodes;

Considering the above problems, the research ideas are as follows.

1) Considering the different effects of different state attributes in the node trust calculation process, assign relevant values and weights to vehicle-related state attributes;
2) RSU integrates the trust value reported by other vehicles on a certain vehicle;

3 Trust Evaluation Method of IoV

3.1 Direct Trust Assessment

The validity of the trust record of the target vehicle node changes dynamically with the increase of time. The trust record that is far away from the current transaction time has a weaker ability to react to the current attributes of the node, while the nearest trust record is relatively more able to reflect the current node attributes and behavioral intentions.

To make more reasonable use of historical records, the distance between the moment of trust record generation and the current moment is adopted to measure the decay of trust records in the historical trust sequence, and accordingly improve the trust decay method based on the length of time window. Meanwhile, a decay rate adjustment factor is added to control the decay rate in different application scenarios and when nodes perform different cooperative behaviors. Accordingly, the trust decay function shown in Formula (1) is used to express the timeliness of trust.

$$FR(\alpha, t_i) = e^{-\alpha \cdot L(t-t_i)}. \tag{1}$$

Among them, α and $L(t-t_i)$ are two independent variables. α is the rate adjustment factor, and $0 < \alpha \leq 1$, which can be adjusted according to actual application scenarios. $L(t-t_i)$ is a time update function that represents the distance from the current moment t when the ith historical record occurred, and t_i is the moment when the ith interaction of the node was generated.

3.1.1 Same Quality Service Intensity Calculation

In order to better portray node behavior and avoid malicious nodes from participating in cooperation, this paper penalizes nodes that continue to provide malicious services or incentivizes legitimate nodes based on the sustained intensity of the same quality service during the monitoring period [10]. The proportion of the number of successful and failed interaction services generated by the evaluated node to the total number of interaction services in the monitoring cycle is the same quality service persistence intensity of the node, $F_B^c(c = r, p)$. F_B^p is the penalty factor of the evaluated node B, and F_B^r is the reward factor. F_B^c is calculated as Formula (2) [20].

$$F_B^{\mathrm{c}} = \frac{service_B^{type}}{service_B^{su} + service_B^{fa}}. \tag{2}$$

Among them, $type = su, fa$. $service_B^{su}$ and $service_B^{fa}$ are respectively the number of successful and failed interactive services provided by the evaluated node B during the monitoring period.

3.1.2 Direct Trust Calculation

In the Bayesian theory-based trust assessment method, if the state probability density function is known to be$P(\theta)$, then the probability density function is expressed as in Formula (3).

$$P(\theta) = \frac{\Gamma(u+f+2)}{\Gamma(u+1)\Gamma(f+1)}\theta^u(1-\theta)^f. \tag{3}$$

where $\theta \in [0, 1]$ and $\Gamma(\cdot)$ is the gamma function. θ is the probability that the subject node observes that the guest node is a normal node, and the recent successful interactions of the nodes are denoted as u, and the failed interactions are denoted as f. In this paper, a successful interaction means that the guest node successfully forwards the information it receives, and the opposite is considered as a failed interaction.

According to the above formula to predict future events, the probability of the next interaction success can be regarded as the expectation of the beta distribution, as shown in Formula (4).

$$P = E(\beta(u+1, f+1)) = \frac{u+1}{u+f+2} \tag{4}$$

The above formula is the expectation of future behavior. Referring to the definition of trust, it can be used to express the trust evaluation of node A to node B, as shown in Formula (5).

$$T_d = \frac{u_{AB}+1}{u_{AB}+f_{AB}+2} \tag{5}$$

The malicious event impact factor η is introduced in this paper to improve the original Bayesian model and increase

the impact of malicious events. The corrected A-to-B trust assessment value is shown in Formula (6).

$$T_d = \frac{u_{AB} + 1}{u_{AB} + \eta f_{AB} + 2} \tag{6}$$

Where η is a constant and $\eta > 1$, each vehicle node in the network has a trust information table, which is used to record the direct trust value of the vehicle node that has interacted with it. The calculation method is derived from the above formula.

Remember the success sequence of A and B historical interaction is $u'_{AB}(u'^{t1}_{AB}, u'^{t2}_{AB}, ..., u'^{tn}_{AB})$, and the failed interaction sequence is $f'_{AB}(f'^{t1}_{AB}, f'^{t2}_{AB}, ..., f'^{tn}_{AB})$. Among them, u'_{AB} and f'_{AB} are updated according to the following rules.

If node B provides a successful interactive service, the observation values obtained this time is $(u'^{pr}_{AB}, f'^{pr}_{AB}) = (1, 0)$. After A interacts with B i times, u_{AB} is updated by u'_{AB} as shown in Formula (7).

$$u_{AB} = \sum_{i=1}^{n} FR(\alpha, t_i) \cdot u'^{ti}_{AB} + F^r_B \cdot u'^{pr}_{AB} \tag{7}$$

If node B provides a failed interactive service, the observed values obtained this time is $(u'^{pr}_{AB}, f'^{pr}_{AB}) = (0, 1)$. After A interacts with B i times, f_{AB} is updated with Formula (8).

$$f_{AB} = \sum_{i=1}^{n} FR(\alpha, t_i) \cdot f'^{ti}_{AB} + F^p_B \cdot f'^{pr}_{AB} \tag{8}$$

3.2 Recommended Trust Assessment

3.2.1 Malicious Recommendations Elimation

In order to prevent unreasonable recommendations, this paper introduces the concept of "trust distance" to preclude malicious recommendations in order to effectively resist collusive attacks by malicious vehicle nodes. Assume that there are N recommended nodes$k_1, k_2, ..., k_i, ..., k_N$ within one hop of node A that have direct interaction with B, where the node k_i is the most trusted recommended node of node A, the direct trust value of k_i to B is the trust reference value T_{refer},and d is the trust distance threshold. As the trust distance threshold is too large or too small to effectively identify malicious nodes, it has been verified that the trust distance threshold in this paper is set to 0.2.The trust distance of recommended node and to node B can be calculated by Equation (9).

$$Dis(k_j, k_i) = |T_{d(k_j,B)}| - T_{d(k_i,B)} \tag{9}$$

Among them, $T_{d(k_j,B)}$ and $T_{d(k_i,B)}$ are the direct trust values of and to B respectively.The specific pseudocode to exclude malicious recommendations node is shown in Algorithm 1.

Taking the trust given by A's most trusted recommended node k_i as a reference, if the distance between other nodes k_j and its trust is less than the threshold d , it means that node k_j can be used as a recommended node for A. Otherwise, it is considered as a malicious node and k_j is deleted in the recommended node.

In Algorithm 2, find the most trusted recommended node k_i of node A , and z is the total length of the direct trust table of node A.

Algorithm 1 Malicious recommendation node elimination

```
Begin
Find node k_i among the recommended of node A
T_refer ← T_d(k_i,B)
Dis_(k_j,k_i) ← |T_d(k_j,B) − T_refer|(j = 1, 2, ..., N&j ≠ i)
if Dis_(k_j,k_i) < d then
    keep k_j
else
    delete k_j
end if
End
```

Algorithm 2 search k_i

```
Begin
Input Trust table of node A
T_d(A,k_i) ← T_d(A,k_1)
For j=2 to z
if T_d(A,k_j) > T_d(A,k_i) then
    T_d(A,k_i) ← T_d(A,k_j)
end if
End For
Return k_i
End
```

3.2.2 Recommended Trust Calculation

After the malicious recommendation node exclusion algorithm excludes some of the malicious recommendations, the remaining n recommendation nodes can be represented as $K_i(i = 1, 2, ..., n)$. If there is no direct interaction experience between A and B, when calculating the trust value of A to B, the trust value of the recommended node to B is required. In the traditional trust model, the trust value of the node is used as the weight, as shown in Formula (10).

$$T_r(A, B) = \sum\nolimits_{i=1}^{n} T_d(A, K_i) T_d(K_i, B) \tag{10}$$

Where $T_d(A, K_i)$ is the direct trust value of A to K_i , and $T_d(K_i, B)$ is the direct trust value of K_i to B. This means that the higher the trust value of node A to K_i , the more important its recommendations are. However, this algorithm ignores the possibility of collusion attacks, so that malicious nodes can gain a higher trust value through camouflage and spread malicious resources to normal nodes. Therefore, it is inappropriate to use the trust value of A versus K_i as the weight. Therefore,

this paper uses similarity as the weight to calculate the recommended trust value of A versus B.

When calculating the trust value of A to B , A has no direct interaction experience with B , and the trust value of B needs to be calculated indirectly through the trust value of recommender K_i to B . The recommender K_i in this paper is obtained from the communication list of vehicle B stored in RSU.

The score similarity characterizes the similarity of the scores of node A and node K_i.This paper uses cosine-based similarity to measure the similarity between two vectors [17], let nodes A and K_i rate the same set of items, and then the cosine similarity is calculated according to Formula (11).

$$Sim(A,K_i)=\frac{|\sum_{j=1}^{m} r_{aj}r_{sj}|}{\sqrt{\sum_{j=1}^{m}(r_{aj})^2}\sqrt{\sum_{j=1}^{m}(r_{sj})^2}} \tag{11}$$

The score vectors of the successful transaction rate of m vehicles by node A and node K_i within a period of t are represented as $r_a = [r_{a1}, r_{a2}, ..., r_{am}]$ and $r_s = [r_{s1}, r_{s2}, ..., r_{sm}]$ respectively. Among them,$Sim \in [0,1]$. The larger the value of Sim , the higher the score similarity between the two nodes, which means that the scores of A and K_i on other nodes of the network are more consistent. r_{aj} is the successful transaction rate score of vehicle node A for the jth vehicle. It represents the ratio of the number of successful interactions between node A and j in the interaction history to the total number of interactions with node j.

The n advisers K_i feedback their trust value $T_d(K_i,B)$ to B, A uses the similarity $Sim(A,K_i) \in [-1,1]$ between himself and K_i as the weight to calculate the trustworthiness of A's recommendation on B, as in Formula (12).

$$T_r(A,B)=\sum_{i=1}^{n} Sim(A,K_i)T_d(K_i,B) \tag{12}$$

3.3 RSU Trust Assessment

The selection of RSU transfer trust attributes should be able to fully reflect the activity characteristics of vehicle nodes in the network, and accurately describe the real-time behavior of the vehicle. For example, the vehicle's moving speed, signal power, and the vehicle's participation in network communications. This may be a traffic violation when the vehicle is moving faster than the normal range compared to the surrounding vehicles. The low signal power of vehicles participating in normal communication, or deliberately discarding some messages or not participating in the network communication of message forwarding, may lead to the decline of vehicle trust level. The vehicle-related attributes are expressed as in Formula (13).

$$csa=[csa^1, csa^2, ..., csa^x] \tag{13}$$

Where x is the number of relevant attributes of the vehicle. Considering that different trust attributes play different roles in the process of node trustworthiness calculation, different trust weight is defined for each trust attribute, and the weight is defined as in Formula (14).

$$\omega_{csa}=[\omega_{csa}^1, \omega_{csa}^2, ..., \omega_{csa}^{\mathrm{x}}] \tag{14}$$

And $\sum_1^{\mathrm{x}} \omega_{csa}=1$, then the observed trust value of the evaluated vehicle B is as in Formula (15).

$$OT_B=\sum_1^{\mathrm{x}} csa\omega_{csa} \tag{15}$$

RSU can obtain the integrated trust value of the vehicle by fusing the trust value report of all other vehicles on the vehicle, as shown in Formula (16).

$$FT_B=[\prod_{i=1}^{s} T_d(A,B)^{\frac{1}{s}}] \tag{16}$$

Where s represents the number of vehicles that have estimated the trust value of vehicle B and $T_d(A,B)$ represents the direct trust value of vehicle A to vehicle B.

3.3.1 RSU Global Trust Calculation

The RSU global trust is obtained through observation trust and fusion trust, as shown in Formula (17).

$$T_{RSU}=\frac{\mathrm{x}}{s+\mathrm{x}}OT_B+\frac{s}{s+\mathrm{x}}FT_B \tag{17}$$

The weight of observation trust and fusion trust is adaptively obtained from the number of relevant attributes and the number of evaluated vehicles.

3.4 Comprehensive Trust Calculation Based on Analytic Hierarchy Process

The hierarchical analysis method decomposes the goal-related influencing factors and uses the decision maker's experience to compare multiple factors in two to arrive at the relative importance; it combines qualitative analysis with quantitative analysis to quantify the level of importance among multiple factors. Hierarchical analysis can be used in the program to determine the specific weights of each factor in trust assessment in a more reasonable and scientific way [23].

3.4.1 Weight Calculation Method

1) Build a hierarchical model

   Divide the decision-making goals, consideration factors (decision criteria), and decision objects into the highest level, middle level, and the lowest level according to their mutual relationship, and the multi-factor hierarchical structure model shown in Figure 3 can be obtained.

2) Constructing the judgment matrix

   Comprehensive trust is affected by four factors: initial trust, direct trust, recommendation trust, and

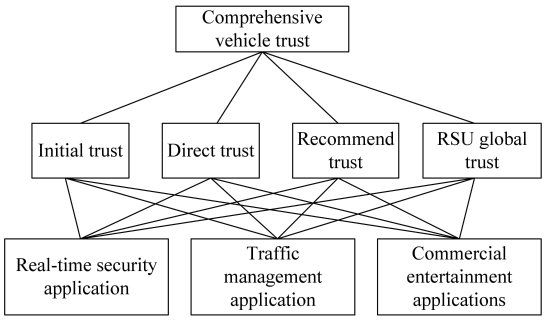

Figure 3: Multi-factor hierarchical structure model

RSU trust. The importance of various scenes relative to the four factors is different, so according to the different actual scenes, the consistent matrix method can be used to compare the importance of these factors relative to the upper layer. Construct multiple judgment matrices using the proportional scaling method as shown in Table 1, as shown in Figure 4.

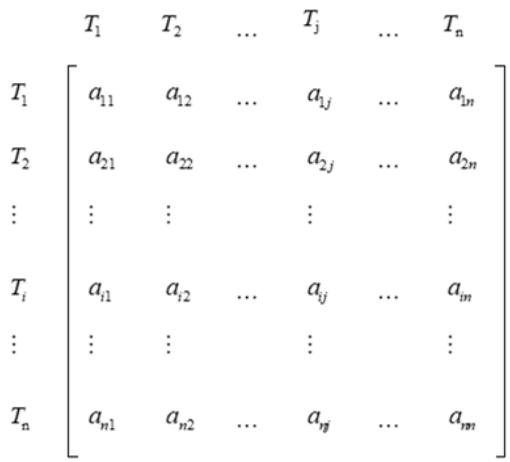

Figure 4: Judgment matrix

3) Judgment matrix solution and consistency check

Use the sum-product method to solve the matrix. The calculation is as follows: divide each item in the matrix by the sum of each item in the column of the item, standardize the matrix, use formula $b_{ij} = a_{ij}/\sum_{j=1}^{n} a_{ij}$; take the average of each row of the new matrix, Get the weight $w_i = \sum_{j=1}^{m} b_{ij}/m$ of each factor. When constructing the judgment matrix, there may be logical errors. For example, A is more important than B, B is more important than C, but C is more important than A. Therefore, it is necessary to use the consistency test to check whether there is a problem. Because we calculate the importance of the scene in the upper layer of trust factors, we adopt the hierarchical single ordering and the consistency test. The calculation steps are as follows: Calculate the maximum eigenvalue $\lambda_{\max} = \sum_{i=1}^{n} A_i/(nw_i)$ of each matrix A; Calculate the consistency index $CI = \frac{\lambda_{\max}-n}{n-1}$; the closer the CI is to 0, the more satisfactory the consistency, and the larger the CI, the more serious the inconsistency. The random consistency index RI is obtained by checking Table 2 from the order n of the matrix. Calculate the consistency ratio: $CR = \frac{CI}{RI}$. Generally, when the consistency ratio $CR < 0.1$, the degree of inconsistency of the matrix is considered to be within the allowable range. If the consistency is satisfactory, the consistency test is passed, and the corresponding weight vector obtained at this time is available. The element a_{ij} of the judgment matrix is given by Santy's 1-9 scale method, as shown in Table 1.

Calculation by the analytic hierarchy process, the weights of initial trust, direct trust, recommendation trust, and RSU trust in different scenarios can be determined, and the weights are set as w_1, w_2, w_3, and w_4 respectively.

Table 1: Random consensus indexesl

n	RI
1	0
2	0
3	0.58
4	0.90
5	1.12
6	1.24

3.4.2 Comprehensive Trust Calculation Method

After a certain cycle, the comprehensive trust of the vehicle is calculated as in Formula (18).

$$T_{total} = w_1 IT + w_2 T_d + w_3 T_r + w_4 T_{RSU} \tag{18}$$

After the trust calculation, it is assumed that the message receiver decides to receive the message sender's information. After the message is received, it needs to give feedback on whether the information is true or not. If the number of inauthentic messages over some time is greater than or equal to half of the number of communications, the vehicle is considered to be a malicious vehicle. To reduce the storage burden of the vehicle, the vehicle will periodically clean up the vehicle trust values that have been in place for too long [3, 9].

4 Experiment and Result Analysis

4.1 Experimental Environment

The simulation environment configuration is as follows:

Table 2: "1-9" proportional scaling method

Scaling	Meaning
1	Indicates that two factors have the same importance compared to each other
3	Indicates that one factor is slightly more important than the other when compared to the two factors
5	Indicates that one factor is significantly more important than the other when compared to the two factors
7	Indicates that one factor is strongly more important than the other when compared to the two factors
9	Indicates that one factor is more extremely important than the other when compared to the two factors
2,4,6,8	The median of the above two adjacent judgments
Reciprocal	The comparison of factor i and j is judged as a_{ij} , and the judgment of factor j and i is judged as $a_{ji} = 1/a_{ij}$

Software: By using veins [18] as the V2V open-source framework and OMNET++ (as a network simulator) and SUMO (as a traffic simulator). Use SUMO to generate vehicle motion status files, and OMNET++ queries and dispatches vehicle motion status through TraCI.Hardware: Intel(R) Core i7-10510U CPU @1.80 GHZ processor, 16GB RAM. NVIDIA GeForce MX250 graphics display. Microsoft Windows 10 Professional operating system.

There are three main types of malicious vehicle node behavior introduced in the network: selfish nodes that do not send information, nodes that send false information and nodes that deliberately drop packets.Netedit is used to generate road network files,the experimental simulation parameter settings in this paper are shown in Table 3.

Table 3: Simulation parameters

Parameter Parameter	The values used in the simulation
Road length	1000m
Number of lanes	6
Required speed	40m/s
Frequency	V2V 5.9GHz
Packet size	200 bytes
Transmission rate	6Mbps
MAC protocol	IEEE802.11p
Network protocol	IEEE1609.4

4.2 Result Analysis

With the increase of malicious nodes, this paper compares the direct trust value of using Bayesian without considering the malicious factor [7] with the direct trust value of considering the malicious factor in this paper. The experimental results are shown in Figure 5.

Figure 5 shows that when the proportion of malicious nodes keeps increasing, the direct trust degree value with

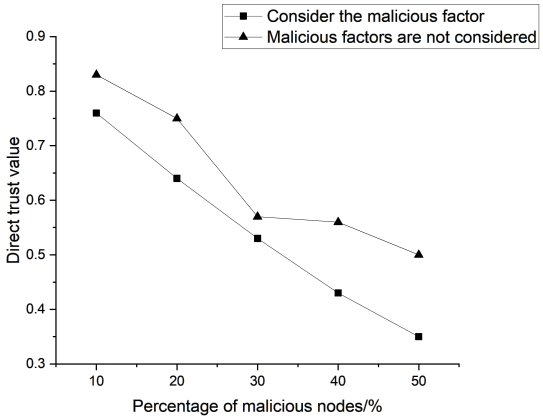

Figure 5: Comparison of whether to consider malicious factors

malicious factor considered decreases at the fastest rate. It can be seen that the calculation of the direct trust degree value of malicious factor being considered in this paper can better portray the node behavior and quickly identify malicious nodes.

To verify whether the direct trust value in this paper can better reflect the behavior of nodes and effectively identify malicious nodes, the direct trust calculation method in this paper is compared with the traditional Bayesian method in different time periods. To simulate the changes of direct trust degree values in different time periods, the direct trust degree values of nodes are calculated by setting the time period t from 0 to 20 minutes when the target nodes provide normal services. At t from 20 to 40 minutes,10% of malicious nodes are configured to randomly generate discarded packets to calculate the direct trust degree value of the nodes, and the experimental results are shown in Figure 6.

Figure 6 shows that with the accumulation of time after adding malicious nodes, the direct trust value of this paper decreases at the fastest rate and is lower than the

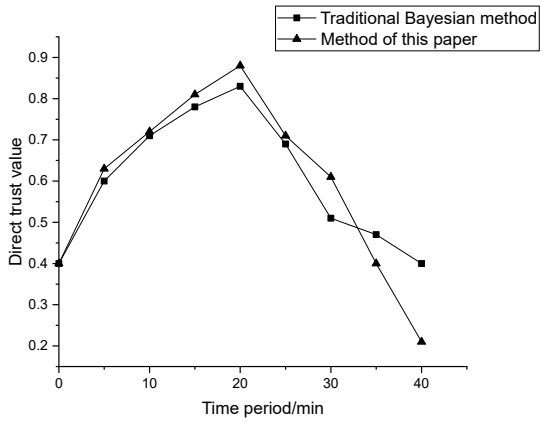

Figure 6: Changes in the value of direct trust

direct trust value obtained by traditional Bayes after 33 minutes. This shows that the direct trust degree calculation in this paper can better characterize the node behavior and identify malicious nodes quickly.

To evaluate the effectiveness of adding the malicious referral node exclusion algorithm to the recommendation trust calculation, this paper compares the packet loss rate of the network before and after adding the malicious referral node exclusion algorithm. The packet loss rate is the ratio of the total number of packets lost by the receiving node to the total number of packets sent by the sending node. The packet loss rate is compared between two groups of experiments, one without the malicious recommendation node exclusion algorithm and the other with the malicious recommendation node exclusion algorithm, where the excluded nodes are no longer added to the network. The simulation time is set to 5min, 10min, 15min, 20min, 25min and 30min. The experimental results are shown in Figure 7.

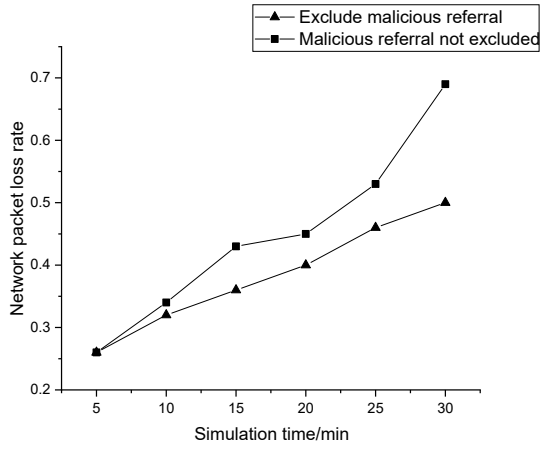

Figure 7: Comparison of network packet loss rate

As can be seen in Fig. 7, the network packet loss rate in different periods after adding the malicious recommendation node exclusion algorithm is significantly lower than the network packet loss rate without adding the malicious recommendation node exclusion algorithm. It shows that the malicious recommendation exclusion algorithm is added to exclude some of the malicious recommendation nodes, which makes the network packet loss rate decrease compared with that before the malicious recommendation exclusion algorithm is added, and also proves the effectiveness of the malicious recommendation exclusion algorithm.

By setting up different proportions of malicious nodes in the simulated environment, the accuracy rate of the recommended trust is calculated in this paper and the EigenTrust method. The accuracy rate of recommended trust = detection of real malicious nodes / detection of untrusted nodes. The experimental results are shown in Figure 8.

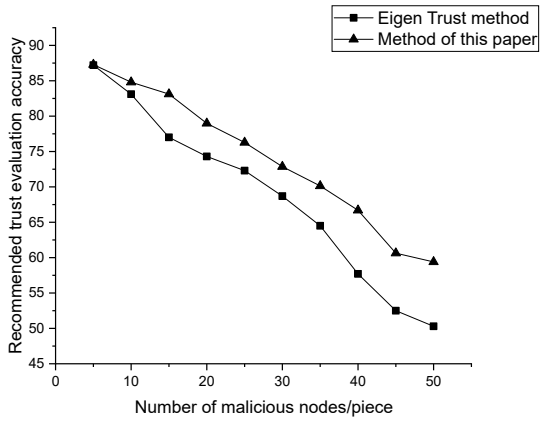

Figure 8: Comparison of recommended trust evaluation accuracy

Figure 8 shows that when the density of malicious nodes continues to increase, it can be seen that the accuracy of the recommendation trust evaluation in this paper is always higher than that of the EigenTrust method.

To test the overall performance of the trust evaluation in this paper, the experiment compared the trust evaluation mechanism of this paper with the EigenTrust method and the success rate of vehicle interaction under different malicious node ratios in the References [1]. Let the ratios of malicious nodes be 5%, 10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%, 55%. The experimental results are shown in Figure 9.

Figure 9 shows that when the proportion of malicious nodes is 15%-60%, the vehicle interaction success rate of the trust mechanism in this paper is higher than that of the other two models. It can be seen that the trust mechanism in this paper has certain advantages in the success rate of interaction.

5 Conclusion

The presence of malicious nodes in IoV can seriously affect network communication and may even cause incalculable

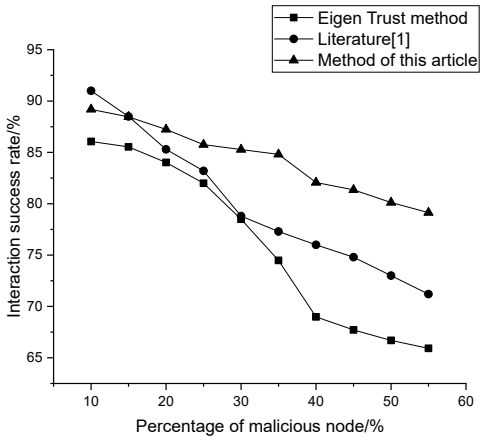

Figure 9: Comparison of recommended trust evaluation accuracy

consequences if a large number of malicious nodes invade and send shared false information once they exist. The trust assessment mechanism proposed in this paper integrates four trust factors from initial trust, direct trust, recommended trust, and RSU global trust regarding the trust assessment of vehicle nodes. The analytic hierarchy process is used to quantify the degree of influence of each factor and different application scenarios on vehicle trust. This trust assessment mechanism can detect and exclude some malicious referrals and also provides a basis for vehicle information reception and decision making, thus ensuring a trustworthy environment for vehicular communication. To solve the cold start problem, an initial trust module is added; to accelerate the rapid convergence of trust values of vehicle nodes, a malicious event impact factor is introduced to improve Bayes; to reduce malicious recommendation behavior, trust distance is used to exclude malicious recommendations from some malicious nodes; to effectively prevent the possibility of collusion attacks, cosine similarity is adopted as the weight of recommendation trust. In addition, to give full play to the role of RSU in trust evaluation, the influence of observed trust and fused trust on vehicle nodes in RSU is considered comprehensively. The research in this paper focuses on the evaluation of interaction information, and the next step will be to consider more influencing factors on node behavior, including node processing capabilities and specific application scenarios. In this paper the possibility of collusion attacks is considered, in the future, more complex and more possible attacks are considered in our plan to explore the resilience of the proposed mechanism.

Acknowledgments

This research is supported by the National Natural Science Foundations of China under Grants No.61862040, No.61762059 and No.6176 2060.The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

References

[1] F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A comparative analysis of trust models for safety applications in iot-enabled vehicular networks," in *IEEE Wireless Days*, pp. 1–8. IEEE, 2019.

[2] S. Z. Chen, J. L. Hu, Y. Shi, L. Zhao, and W. Li, "A vision of c-v2x: technologies, field testing, and challenges with chinese development," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3872–3881, 2020.

[3] T. Cheng, G. C. Liu, Q. Yang, and J. G. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 652–663, 2019.

[4] S. S. Desai and M. J. Nene, "Node-level trust evaluation in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2139–2152, 2019.

[5] S. Deshpande and R. Ingle, "Evidence based trust estimation model for cloud computing services," *Internation Journal of Network Security*, vol. 20, no. 2, pp. 291–303, 2018.

[6] H. El-Sayed, S. Zeadally, M. Khan, and H. Alexander, "Edge-centric trust management in vehicular networks," *Microprocessors and Microsystems*, vol. 84, p. 104271, 2021.

[7] H. El-Sayed, S. Zeadally, and D. Puthal, "Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks," *Vehicular Communications*, vol. 24, p. 100227, 2020.

[8] Z. El-Yebdri, S. M. Benslimane, F. Lahfa, M. Barhamgi, and D. Benslimane, "Context-aware recommender system using trust network," *Computing*, no. 1, pp. 1–19, 2021.

[9] T. L. Gao, T. Li, R. Jiang, M. Yang, and R. Zhu, "Research on cloud service security measurement based on information entropy," *Internation Journal of Network Security*, vol. 21, no. 6, pp. 1003–1013, 2019.

[10] G. A. Ghazvini, M. Mohsenzadeh, R. Nasiri, and A. M. Rahmani, "A new multi-level trust management framework (mltm) for solving the invalidity and sparse problems of user feedback ratings in cloud environments," *The Journal of Supercomputing*, vol. 77, no. 3, pp. 2326–2354, 2021.

[11] Z. G. He, "Multi-parameter and time series based trust for iot smart sensors," *Internation Journal of Network Security*, vol. 22, no. 4, pp. 589–596, 2020.

[12] V. S. Janani and M. S. K. Manikandan, "An outlook on cryptographic and trust methodologies for clusters based security in mobile ad hoc networks," *Internation Journal of Network Security*, vol. 20, no. 4, pp. 746–753, 2018.

[13] M. H. Junejo, A. H. A. Rahman, R. A. Shaikh, K. M. Yusof, I. Memon, H. Fazal, and D. Kumar, "A privacy-preserving attack-resistant trust model for

internet of vehicles ad hoc networks," *Scientific Programming*, vol. 2020, no. 2, pp. 1–21, 2020.

[14] T. Li, A. F. Liu, N. N. Xiong, S. B. Zhang, and T. Wang, "A trustworthiness-based vehicular recruitment scheme for information collections in distributed networked systems," *Information Sciences*, vol. 545, no. 12, pp. 65–81, 2021.

[15] H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in vanets," *Journal of Parallel and Distributed Computing*, vol. 151, no. 2, pp. 61–69, 2021.

[16] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K. Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157–4185, 2020.

[17] S. O. Ogundoyin and I. A. Kamil, "A fuzzy-ahp based prioritization of trust criteria in fog computing services," *Applied Soft Computing*, vol. 97, p. 106789, 2020.

[18] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata. *Veins: The open source vehicular network simulation framework*, Recent Advances in Network Simulation, pp. 215–252. Springer, 2019.

[19] B. Su, C. H. Du, and J. Huan, "Trusted opportunistic routing based on node trust model," *IEEE Access*, vol. 8, no. 99, pp. 163077–163090, 2020.

[20] S. R. Tong, B. Z. Sun, X. L. Chu, X. R. Zhang, T. Wang, and C. Jiang, "Trust recommendation mechanism-based consensus model for pawlak conflict analysis decision making," *International Journal of Approximate Reasoning*, vol. 135, pp. 91–109, 2021.

[21] T. Wang, H. Luo, X. X. Zeng, Z. Y. Yu, A. F. Liu, and A. K. Sangaiah, "Mobility based trust evaluation for heterogeneous electric vehicles network in smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1797–1806, 2020.

[22] Y. B. Wang, J. H. Wen, X. B. Wang, B. M. Tao, and W. Zhou, "A cloud service trust evaluation model based on combining weights and gray correlation analysis," *Security and Communication Networks*, vol. 2019, no. 1, pp. 1–11, 2019.

[23] L. B. Wen, "Security evaluation of computer network based on hierarchy," *Internation Journal of Network Security*, vol. 21, no. 5, pp. 735–740, 2019.

[24] P. S. Xie, X. Q. Wang, X. J. Pan, Y. F. Wang, T. Feng, and Y. Yan, "Blockchain-based trust evaluation mechanism for internet of vehicles nodes," *Internation Journal of Network Security*, vol. 23, no. 6, pp. 1065–1073, 2021.

[25] H. Z. Zhao, Q. G. Chen, W. Shi, T. L. Gu, and W. Y. Li, "Stability analysis of an improved car-following model accounting for the driver's characteristics and automation," *Physica A: Statistical Mechanics and Its Applications*, vol. 526, p. 120990, 2019.

[26] H. Z. Zhao, D. H. Sun, H. Yue, M. Zhao, and S. Cheng, "Dynamic trust model for vehicular cyber-physical systems," *Internation Journal of Network Security*, vol. 20, no. 1, pp. 157–167, 2018.

[27] H. Z. Zhao, D. X. Xia, S. H. Yang, and G. H. Peng, "The delayed-time effect of traffic flux on traffic stability for two-lane freeway," *Physica A: Statistical Mechanics and its Applications*, vol. 540, p. 123066, 2020.

[28] H. Z. Zhao, H. Yue, T. L. GU, C. H. Li, and D. Zhou, "Low delay and seamless connectivity-based message propagation mechanism for vanet of vcps," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3385–3402, 2021.

[29] H. Z. Zhao, H. Yue, T. L. Gu, and W. Y. Li, "Cps-based reliability enhancement mechanism for vehicular emergency warning system," *International Journal of Intelligent Transportation Systems Research*, vol. 17, no. 3, pp. 232–241, 2019.

[30] J. H. Zhu, "Wireless sensor network technology based on security trust evaluation model," *International Journal of Online Engineering*, vol. 14, no. 4, pp. 211–226, 2018.

Biography

Peng-shou Xie was born in Jan. 1972. He is a professor and a supervisor of master student at Lanzhou University of Technology. His major research field is Security on Internet of Things. E-mail: xiepsh_lut@163.com

Xin Tong was born in Aug. 1995. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 2505156603@qq.com.

Hong Wang was born in Oct. 1995. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 2967589625@qq.com

Ying-Wen Zhao was born in Feb. 1996. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 1075224210@qq.com

Tao Feng was born in Dec. 1970. He is a professor and a supervisor of Doctoral student at Lanzhou University of Technology. His major research field is modern cryptography theory, information security . E-mail: fengt@lut.cn

Yan Yan was born in Oct. 1980. She is a associate professor and a supervisor of master student at Lanzhou University of Technology. Her major research field is privacy protection, multimedia information security. E-mail: yanyan@lut.cn