Hindawi
Mobile Information Systems
Volume 2021, Article ID 7611619, 16 pages
https://doi.org/10.1155/2021/7611619

Research Article

Hierarchical Hybrid Trust Management Scheme in SDN-Enabled VANETs

Ming Mao, Peng Yi, Tao Hu, Zhen Zhang, Xiangyu Lu, and Jingwei Lei

People's Liberation Army Strategic Support Force Information Engineering University, Zhengzhou 450001, China

Correspondence should be addressed to Ming Mao; maoming12345@163.com

Received 20 May 2021; Revised 13 July 2021; Accepted 6 August 2021; Published 17 August 2021

Academic Editor: Vishal Sharma

One of the principal missions of security in the Internet of Vehicles (IoV) is to establish credible social relationships. The trust management system has been proved to be an effective security solution in a connected vehicle environment. The use of trust management can play a significant role in achieving reliable data collection and dissemination and enhanced user security in the Internet of Vehicles. However, due to a large number of vehicles, the limited computing power of individuals, and the highly dynamic nature of the network, a universal and flexible architecture is required to realize the trust of vehicles in a dynamic environment. The existing solutions for trust management cannot be directly applied to the Internet of Vehicles. To ensure the safe transmission of data between vehicles and overcome the problems of high communication delay and low recognition rate of malicious nodes in the current trust management scheme, an efficient flow forwarding mechanism of the RSU close to the controller in the Software-Defined Vehicular Network is used to establish a hierarchical hybrid trust management architecture. This method evaluates the dynamic trust change of vehicle behavior based on the trust between vehicles and the auxiliary trust management of the infrastructure to the vehicle, combined with static and dynamic information and other indicators. The proposed trust management scheme is superior to the comparative schemes in resisting simple attacks, selective misbehavior attacks, and time-dependent attacks under the condition of ensuring superior real-time performance. Its overall accuracy is higher than that of the baseline scheme.

1. Introduction

Software-Defined Network (SDN) adopts the idea of separation of control plane and data plane, and through the use of perfect interfaces (such as the southbound interface of OpenFlow protocol), it has played a great role in the increasingly complex structure of data center and wired network. At the same time, in the wireless and mobile network-related fields, research on Software-Defined Wireless Network (SDWN) [1] has also made progress. Researchers adjust and expand the SDN and SDWN architecture and related concepts to build Software-Defined Vehicular Network (SDVN) to meet the exclusive characteristics of VANETs (Vehicular Ad Hoc Networks) and improve the performance of vehicle communication networks. Jiacheng et al. [2] pointed out that SDN is a powerful innovative solution, which improves the dynamic characteristics of VANET and ITS (Intelligent Transport System) applications by encouraging the flexibility of network management and the large-scale unified optimization of abstraction. In the future, innovative development of 5G VANET must rely on cloud computing, SDN, and fog computing to meet the new requirements of the continuous development and change of ITS.

As shown in Figure 1, in SDVN architecture, the control layer uses the northbound interface (NBI) to connect with the application layer, and the application layer implements services such as traffic management, location prediction, and security. The SDN controller tracks the status of the data plane elements and programs the southbound interface (SBI) through its predefined application to inject forwarding rules into the data plane. The most commonly used SBI is OpenFlow. The data plane consists of an upper data plane and a lower data plane. The upper data plane includes

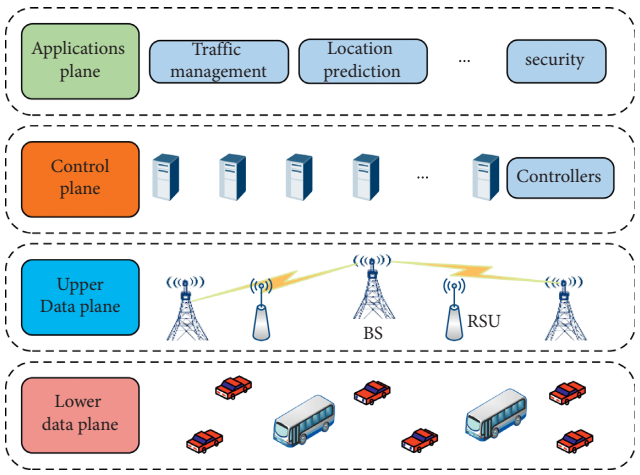


Figure 1: Software-Defined Vehicular Network.

OpenFlow switches, routers, and wireless access infrastructure, namely, roadside unit (RSU), base station (BS), etc. The lower data plane is composed of onboard units (OBUs), that is, the vehicle is equipped with OBU as the terminal user. In this structural system, the specific decisions of the control plane can be conveyed to a single OBU, which promotes fine-grained control, greater scalability, and programmability.

Vehicle communication security issues have consistently been the focus of the SDVN, including availability, authenticity, confidentiality, integrity, and non-repudiation. For example, if a vehicle sends a message that there is congestion somewhere on the road, should other vehicles consider this information to be correct and take corresponding measures? To meet the above requirements, with the help of cryptographic methods, many mechanisms have been proposed to prevent VANET from security attacks. The management scheme based on cryptography has been applied to VANET's message authentication [3, 4]. Although the cryptography-based management scheme has numerous advantages, due to the limited computing power of the OBU, cryptography-based methods are prone to introduce excessive delays to complete all necessary checks. In addition, the verification of messages from unknown vehicles involves the exchange of public certificates, which results in higher message overhead. These methods mainly rely on traditional cryptography-based solutions and have not yet fully resolved the dynamic and distributed behavior of vehicle networks. In addition, encryption technology cannot deal with internal attackers. It is obvious that in a VANET environment, it may be extremely challenging to reduce network management overhead, protect privacy, and implement low-latency communication and intelligent resource management.

Compared with cryptographic methods, the solution architecture based on the trust model (TM) is semi-centralized or distributed. Therefore, it can work independently of the data exchange center in the case of high-mobility network. Trust metric is described as the confidence coefficient that a when node performs certain operations to another node [5]. This operating information is based on information about events (for instance, accidents) between two vehicles and is exchanged through two communication modes, namely, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In critical applications such as hazard warnings, receiving nodes need to ensure their authenticity and trustworthiness before responding to received messages. Once the information is received, trust is calculated based on various factors, including previous interactions, neighbors' suggestions, and statistics related to the history of the event. However, since VANET involves highly maneuverable and diverse vehicles and very frequent topology changes, trust between adjacent vehicles is created in a very short time interval [6]. Therefore, it is also very challenging and difficult to calculate and evaluate trust based on various factors within a limited time.

The current trust management architecture mainly includes infrastructure-based shared management and vehicle self-organization management (as shown in Figure 2). Infrastructure-sharing trust management systems [7, 8] usually deploy vehicle trust management structures above the infrastructure. It realizes the sharing and management of trust information through infrastructure, and it usually needs to set up certificate authorities (CAs) to realize vehicle certification by satisfying a series of trust requirements, including certification, integrity, non-repudiation, etc. The disadvantage of this architecture system is that CAs must be completely credible, and in the event of malicious attacks, they may combine with malicious vehicles to deceive honest vehicles. In addition, the architecture must ensure that all vehicles are within the coverage of the RSU to guarantee the real-time transmission of trust information. In the vast rural areas and suburbs, it is difficult to ensure that vehicles can always meet the RSU coverage service.

Another trust management architecture is a self-organizing vehicle distributed trust management scheme [9–11]. This scheme can realize the trust management of the vehicle through the trust information interaction between the vehicle itself and the vehicle without considering the central authorization and certification CAs. The advantage of self-organizing trust management architecture is that it can acquire trust value in a short time because the trust knowledge it acquires comes from its own and neighbor vehicles' recommendations. Therefore, it can adapt to the highly dynamic changes of the VANET architecture. Its disadvantages are as follows. (1) Due to the dynamic inherent high variability of the VANET structure, similar to a social network, it cannot completely rely on its own existing trust to obtain accurate trust management for new requests from existing vehicles. (2) Since the vehicle adopts a self-organizing trust management method, it is unable to obtain comprehensive trust information, so the trust result obtained may be one-sided and sometimes even wrong. VANET is a decentralized open system. If it does not rely on the infrastructure, peers can join or exit the network at any time. If the neighbor is interacting with the vehicle now, there is no guarantee of interacting with the same vehicle in the future.

The main contributions of this paper are as follows.

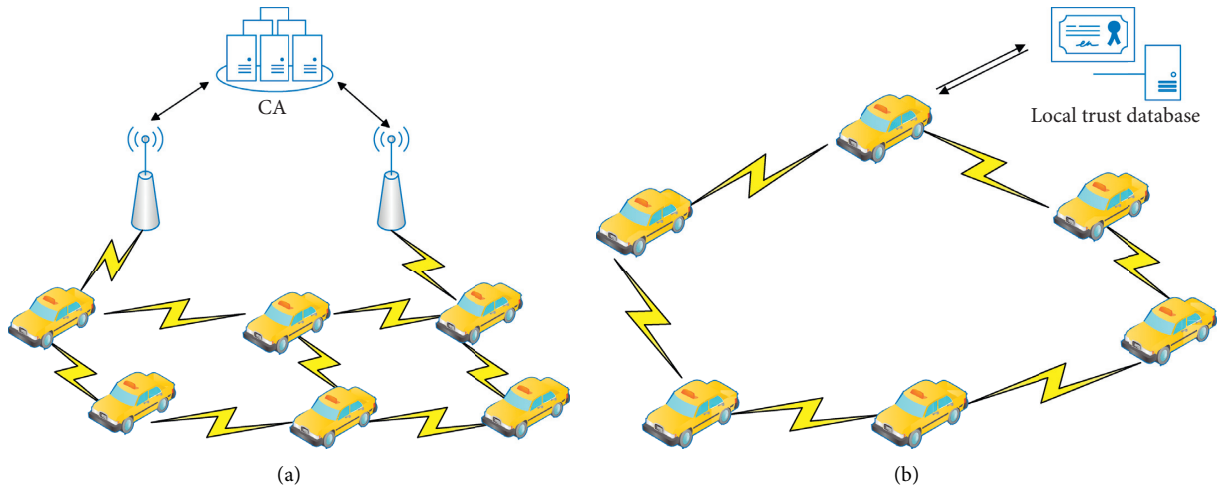


Figure 2: (a) Infrastructure-based trust management architecture. (b) Vehicle-based distributed trust management architecture.

First, a hierarchical hybrid trust management system (HHTM) is proposed, which can conduct a wide range of trust management assessments according to the different environments in which the vehicle is located. If the vehicle is within the coverage area of the RSU, it performs a hybrid trust management evaluation. If the vehicle is not within the coverage area of the RSU, it can still perform distributed trust management evaluation to realize the trust management of the vehicle.

Secondly, according to the characteristics of high mobility of vehicles, the subjective trust between vehicles is calculated according to the local trust database of vehicles, and the recommended trust between vehicles is calculated according to the interactive information between the vehicles and neighbors, to complete the calculation of the trust metric between vehicles. The concept of similarity is utilized to calculate the similarity between the vehicle information in the infrastructure trust table and the message sending vehicle, and the calculation of the infrastructure trust value is realized by combining the distance coefficient of the infrastructure. Meanwhile, we design algorithms to realize the calculation of vehicle hybrid trust value.

Finally, a dynamic simulation environment is established for extensive simulation experiment analysis, which verifies that the robustness of the proposed scheme against node attacks is significantly better than that of the existing schemes.

2. Related Work

The existing literature proposes various solutions to realize trust management and evaluate the trustworthiness and authenticity of the transmitted messages in VANET. A vehicle's trust in information can be calculated based on various factors, including the neighbours' opinions, the reputation of the vehicle, and their past interactions with communication vehicles [12]. Based on the above goals, trust management models are roughly divided into three categories, namely, data-oriented, entity-oriented, and combined trust models [13, 14].

2.1. Data-Oriented Trust Models (DTMs). In this model, "data" are regarded as an important part of the TM, where the trust in the message (data) is calculated based on the opinions generated by neighboring vehicles or the historical interactions between peers.

Raya et al. [15] proposed a DTM that uses Bayesian Inference (BI) and Dempster–Shafer Theory (DST) to evaluate evidence about events received from the neighborhood. The TM consists of three main stages. Firstly, the evaluator node (EvN) accumulates reports generated by neighboring vehicles. Secondly, EvN assigns weights to the received reports according to the spatiotemporal characteristics of the event. Finally, EvN forwards these reports to the decision logic module and uses BI and DST for trust calculation. The limitation of this technology is that it calculates trust based on the received data of EvN, which is inefficient for high-mobility networks.

Gazdar et al. [16] adopted a layer-based analysis method. The vehicle continuously evaluates the credibility of the received data based on its direct experience. In this TM, each participating vehicle is evaluated for trust, and its main purpose is to identify highly trusted vehicles and dishonest vehicles based on the exchanged data. Each vehicle maintains a trust table for its neighbors. The trust value of messages received from trusted vehicles will increase, while for malicious vehicles, it will decrease. Since this technology only involves the direct experience of participating vehicles, it is very effective in identifying malicious vehicles.

Wu et al. [17] proposed a centralized trust modeling framework for data evaluation by taking advantage of the RSU. On RSU, trust is calculated based on two factors: (1) observation and (2) feedback. The vehicle generates observation results for detected events and their credibility. The credibility depends on the distance to the event, the maximum message detection rate, and the number of sensors that detect the event. Then, the observation results are shared with the RSU, which updates the list of recently observed events. RSU evaluates the credibility of the received observations by using the ant colony optimization algorithm to perform trust calculations on the received observations.

Updated trust information is distributed by RSU together with nearby vehicles. Because this method relies too much on infrastructure, it cannot be applied in suburban and remote rural areas.

Gurung et al. [18] proposed an information-oriented trust model that enables each individual vehicle to assess the credibility of a potentially large number of messages received in VANET without relying on any infrastructure support, such as RSUs or central servers. The proposed trust model "RMCV" takes into account several factors that affect message credibility, including message content similarity, content conflict, and message routing path similarity. The RMCV scheme consists of two main parts: (1) message classification and (2) information-oriented trust pattern.

2.2. Entity-Oriented Trust Models (ETMs). In ETM, the credibility of the entity (vehicle) is evaluated. This method relies on providing recommendations from the sender to EvN's neighbors to identify dishonest nodes in the legitimate vehicle pool.

Khan et al. [19] made extensive use of the cluster-based technology and first chose the cluster head (CH), and it is responsible for evaluating the trust in the network. In this TM, CH implements a watchdog mechanism in which nearby vehicles will provide reports on vehicles that behave abnormally. If such vehicles are detected, CH will notify the trusted authority (TA) responsible for revoking these vehicles to maintain the trusted network. The disadvantage of this scheme is that the communication overhead caused by the message exchange by the CH reduces the efficiency of the entire network.

Yang [20] proposed a TM by using the similarity mining method to calculate the trust degree. After receiving the message from the vehicle, EvN calculates the similarity between the received messages based on the Euclidean distance and the trust of the sending vehicle. Since trust is obtained by EvN using Euclidean local distance, this TM cannot provide any global information about message similarity.

In order to quickly and accurately distinguish malicious or selfish nodes that spread false or fake messages throughout the network, Mármol and Pérez [21] proposed an infrastructure-based trust and reputation model, namely, TRIP. The model calculates reputation scores based on recommendations given by other vehicles and RSU. The decision in this model is based on fuzzy logic and probability.

2.3. Combined Trust Models (CTMs). CTM aggregates the attributes of entity-oriented and data-oriented trust management schemes, where node trust is calculated based on the trust evaluation of the received message.

Ahmed and Tepe [22] proposed a CTM whose logic-based trust calculation is used to identify nodes that inject false information into the network. In this TM, when neighboring vehicles share messages, EvN can identify the credibility of the event. Once the true event is determined, this information is used to classify the behavior of the sender node as legitimate or malicious. EvN calculates trust through weighted voting and a logical trust function. The TM can effectively identify dishonest vehicles that spread false information. However, the main limitation of this TM is its reliance on weighted voting, which may be biased when dishonest vehicles are in the majority.

To enhance user privacy in the network, Chen and Wei [23] proposed a beacon-based CTM that combines the characteristics of ETM and DTM. The trust level is calculated in two steps. First, it establishes entity trust based on the received beacon. Then, the data trust will be calculated based on various reasonableness checks to identify and revoke dishonest vehicles and their malicious content. The TM is highly dependent on the Public Key Infrastructure (PKI) and the central authority for trust evaluation, and adding it to each forwarded message will cause greater overhead.

Shrestha and Nam [24] proposed a CTM to calculate the trust in vehicles in a completely distributed manner. First, it evaluates the vehicle's trustworthiness and then calculates the trustworthiness of the information. The model uses a clustering algorithm to achieve trust. In this algorithm, honest and dishonest vehicles are divided into two separate groups to identify the credibility of neighboring nodes. Next, the modified threshold random walk algorithm is used to evaluate EvN's trust in the received message. The main disadvantage of this scheme is that it assumes that the distribution of dishonest nodes in the network is even. In VANET, malicious tools are randomly distributed throughout the network. This assumption may be incorrect.

The core element of the IoV is the vehicle, and trust management is based on data interaction. The credible data transmission between vehicles is carried out by the vehicle as a relay. Therefore, trust management around data and the vehicle is inseparable. We propose a hierarchical hybrid trust management mechanism (HHTM), which includes management of vehicle trust information shared between infrastructures and the management of trust information between vehicles. Because this method not only uses the infrastructure to share the management trust value but also takes into account the calculation of the self-organizing management trust value between vehicles, the flexibility of this structure allows it to overcome the low accuracy and the real-time problem of trust information that the vehicle may encounter during trust management.

3. Vehicle Trust Management Model

Alioua et al. [25] pointed out that to ensure that the installation time of flow rules can meet the low-latency requirements of applications for most vehicles' safety in dense networks like HetVNet (Heterogeneous Vehicular Network), the SDN controller must be installed at the edge of the network, the closest network location to the vehicle. Since the RSU acts as an OpenFlow switch in some locations, this trust solution uses the centralized and efficient flow forwarding mechanism of the RSU and the control plane to set the upper trust management plane at the RSU layer. The upper trust management plane includes trust query, trust calculation, trust update, and blacklist upgrade

functions (as shown in Figure 3). The lower trust management plane depends on the trust management of the vehicle itself, which makes full use of the characteristics of the vehicle's high mobility to ensure that trust information is updated in real time.

The main abbreviations used in this paper are summarized in Table 1. The complete hierarchical hybrid trust management model and its calculation process are shown in Figure 4. After vehicle i receives the message from vehicle j, it calculates the trust between vehicles and inquires the trust based on the infrastructure of the vehicle respectively. The trust calculation between vehicles is divided into two parts: ST and RT, and the trust opinion of infrastructure is IT. After calculating the above value, we can get the hybrid trust value HT. Finally, the system judges whether the value meets the evaluation criteria that have been set, so as to determine whether the node is credible.

3.1. Inter-Vehicular Trust Calculation. The trust between vehicles includes subjective trust and recommendation trust. The subjective trust is determined by the vehicle's existing social knowledge to calculate the vehicle's subjective trust value of the vehicle that receives the interactive information, and the recommendation trust requires the information receiving vehicle (EvN) to calculate the vehicle recommendation trust based on the interactive information from the message sending vehicle.

3.1.1. Inter-Vehicular Subjective Trust (ST). The subjective trust model is concentrated on the social relationship between vehicles. The EvN calculates the trust value of the vehicle network by applying existing trust rules created based on social relationships. To quantify this social relationship, the following two main social indicators are used.

(1) Inter-Vehicular Subjective Trust Weight (STW). Existing vehicle information mainly communicates to cloud services and RSUs. Since the transmission distance of the vehicle is identified, we believe that the EvN has low credibility for receiving messages sent from vehicles over a long distance crossing multiple RSU coverage. The distance between vehicles can be used to intuitively determine the weight of the subjective credibility of vehicles. We use DIS_{ij} to denote the Euclidean distance between node i and node j and utilize $\mathrm{COV}_{\mathrm{RSU}}$ to denote the coverage radius of RSU. We define the subjective trust weight (STW) of a vehicle based on the distance between vehicles as follows:

$$\mathrm{STW} = \begin{cases} 1, & \text{if } 0 < \mathrm{DIS}_{ij} \le 2\mathrm{COV}_{\mathrm{RSU}}, \\ 0.75, & \text{if } 2\mathrm{COV}_{\mathrm{RSU}} < \mathrm{DIS}_{ij} \le 3\mathrm{COV}_{\mathrm{RSU}}, \\ 0.5, & \text{if } 3\mathrm{COV}_{\mathrm{RSU}} < \mathrm{DIS}_{ij} \le 4\mathrm{COV}_{\mathrm{RSU}}, \\ 0.25, & \text{if } \mathrm{DIS}_{ij} > 4\mathrm{COV}_{\mathrm{RSU}}. \end{cases} \quad (1)$$

(2) Original Trust of Vehicle (OTV). In the decentralized trust system, each vehicle stores a local trust database (LTD), which records the trust information generated by the original vehicle interaction data. It also contains legitimate and illegitimate interaction information generated by vehicle interaction. First, we define LEG_{ij} to represent the number of legitimate interaction messages from vehicle j that vehicle i has received and MAL_{ij} to represent the number of illegitimate interaction messages from vehicle j that vehicle i has received. Then, the original trust of the vehicle OTV_{ij} can be expressed as follows:

$$\mathrm{OTV}_{ij} = \frac{\mathrm{LEG}_{ij}}{\mathrm{LEG}_{ij} + \mathrm{MAL}_{ij}} * \left(1 - \frac{1}{\mathrm{LEG}_{ij} + 1}\right). \quad (2)$$

The subjective trust of a vehicle is a trust association established on a social basis. After the vehicle receives the sender's information, it first queries whether the trust information of the sending vehicle exists in the LTD. If it

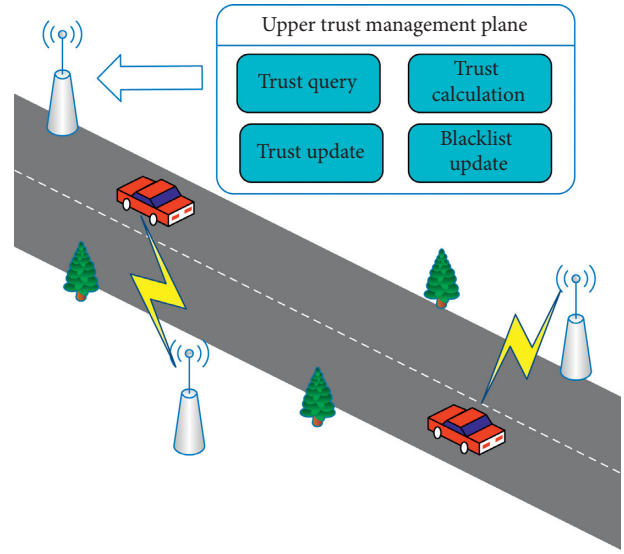


Figure 3: Upper trust management plane.

Table 1: Abbreviations.

Abbreviation	Description
RSU	Roadside unit
BS	Base station
OBU	Onboard unit
TM	Trust model
CA	Certificate authority
DTM	Data-oriented trust model
ETM	Entity-oriented trust model
CTM	Combined trust model
EvN	Evaluator node (information receiving vehicle)
ST	Inter-vehicular subjective trust
STW	Subjective trust weight
OTV	Original trust of vehicle
RT	Inter-vehicular recommendation trust
RW	Role-based trust weight
NT	Neighbor trust
SP	Trust opinion of neighbors
DC	Distance coefficient of RSU
sim_i^j	Similarity between node i and node j
IT	Infrastructure trust
HT	Hybrid trust

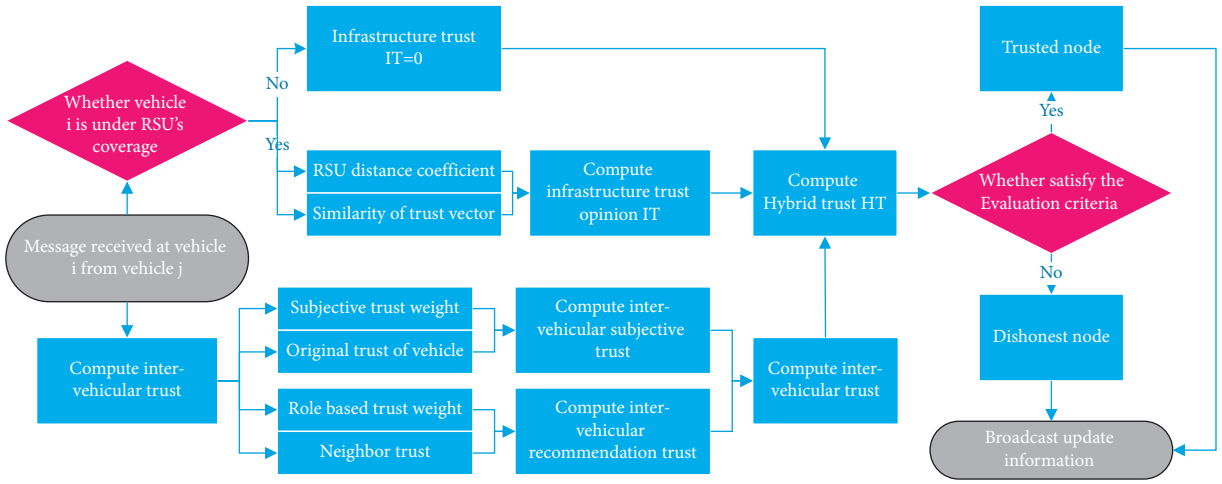


Figure 4: Hierarchical hybrid trust management model.

exists, it directly calculates the OTV. If it does not exist, then assign an initial value OTV_{ini} to it and update this value as the original trust in the vehicle trust table.

(3) Subjective Trust Calculation. The subjective trust of the vehicle can be obtained by multiplying the STW of the vehicle with the OTV:

$$ST = STW * OTV_{ij}. \tag{3}$$

3.1.2. Inter-Vehicular Recommendation Trust (RT). Due to the high mobility of VANET, the two vehicles cannot always maintain direct communication. Therefore, the trust between the vehicles must be obtained indirectly by relying on the cognition of the data and information of other neighboring vehicles. If the vehicle has never interacted with the information sending vehicle before, then the trust suggestions received by the vehicle from other neighboring vehicles will become the only evaluating variable for evaluating the trust value of the information sending vehicle.

(1) Role-Based Trust Weight (RW). According to the different social attributes of the vehicle, the trust basis of the vehicle is also different. Based on the social role to which the vehicle belongs, we divide the role of vehicle (RV) as follows:

RW_1: authoritative vehicles, such as law enforcement department, prisons, police, and so on.

RW_2: vehicles of specific companies, such as TV stations, newspapers, banks, and so on.

RW_3: local vehicles familiar with traffic conditions, such as freight drivers on fixed routes, commuters, taxi drivers, and so on.

RW_4: ordinary roles (all roles except the above three roles).

Assign the corresponding trust weight to each role type:

$$RW = \begin{cases} 1, & \text{if } RV_i \in RW_1, \\ 0.9, & \text{if } RV_i \in RW_2, \\ 0.8, & \text{if } RV_i \in RW_3, \\ 0.7, & \text{if } RV_i \in RW_4. \end{cases} \tag{4}$$

(2) Neighbor Trust Calculation (NT). The trustworthiness of the neighbor depends on the trust opinions of the neighboring vehicles of vehicle i on vehicle j. Define the trustworthiness of the neighbor of vehicle i to vehicle j as follows:

$$NT_{ij} = \left[\prod_{N}^{\forall k \in \text{Neigh}(i)} \left(OTV_{ik} * SP_{kj} \right)^{1/2} \right]^{1/N}. \tag{5}$$

The trustworthiness calculation of neighbor j includes the trust score of vehicle j by vehicle k in the one-hop neighbor node set Neigh (i). Among them, OTV_{ik} is the original trust of vehicle k in vehicle i, and SP_{kj} is the indirect score of vehicle k on vehicle j. The following describes how to obtain the recommender j's score.

(3) Trust Opinion of Neighbors (SP). For the EvN, the more the neighbor nodes receive the message of vehicle j, the higher the credibility of the message. At the same time, the packet delivery rate reflects the reliability of information transmission, so a high delivery rate can also enhance the trust of the EvN to the information sending vehicle. Therefore, we should increase the trust score for vehicles that meet the conditions and reduce the trust score for vehicles that do not meet the conditions. SP_{ij} consists of two parts: the proportion of the number of vehicles in the neighboring vehicles that received messages of vehicle j and the packet delivery rate of the message sending vehicle to the neighboring vehicles. Use ROV_{ij} to denote the proportion of the number of the neighbor vehicle set Neigh (i) receiving vehicle j's messages. If it is greater than or equal to the threshold ROV_{thre}, increase the reward factor λ; otherwise,

subtract the penalty factor μ. QOD_{ij} represents the packet delivery rate to node i during the packet transmission process of node j. If it is greater than or equal to the delivery rate threshold $\mathrm{QOD}_{\mathrm{thre}}$, the reward factor λ is increased; otherwise, the penalty factor μ is subtracted. It can be seen that the range of ROV_{ij} and QOD_{ij} is from 0 to 1. The definition of SP_{ij} is as follows:

$$\mathrm{SP}_{ij} = \frac{1}{2} * \frac{\mathrm{ROV}_{ij} * \mathrm{QOD}_{ij}}{\mathrm{ROV}_{ij} + \mathrm{QOD}_{ij}}. \tag{6}$$

(4) Recommendation Trust Calculation. We can get inter-vehicular recommendation trust as follows:

$$\mathrm{RT} = \mathrm{RW} * \mathrm{NT}_{ij}. \tag{7}$$

We use Algorithm 1 to calculate the trust value between vehicles.

3.2. Calculation of the Infrastructure Trust Opinion

3.2.1. Distance Coefficient of RSU (DC). The trust management mechanism of the RSU has higher requirements for the time delay. The closer the RSU to the vehicle that sent the original message, the more detailed the vehicle message that can be obtained. Therefore, the distance between the sending vehicle and the RSU for trust management has also become an important criterion. The distance coefficient (DC) is expressed as follows:

$$\mathrm{DC}_{ij} = \frac{\sum_{r=1}^{|R|} \mathrm{DIS}_{rj} - \mathrm{DIS}_{ij}}{\sum_{r=1}^{|R|} \mathrm{DIS}_{rj}}, \tag{8}$$

where R represents the set of RSUs that received the original message of sending vehicle j. It can be seen that the closer the estimated RSU is to the sending vehicle, the greater the DC of the RSU to vehicle j is.

3.2.2. Similarity Calculation. To improve the trustworthiness accuracy of the infrastructure to the message sending vehicle, the concept of similarity metrics is used to measure the trust measurement opinion of the RSU to the vehicle [26]. Reference [27] uses cosine-based similarity to judge the similarity of two vectors. The cosine similarity or cosine metric calculates the similarity between two vectors in the inner product space by determining the cosine of the angle between them. This index is widely used for information retrieval and text mining [28]. Each trust level can be regarded as a vector in a k-dimensional space. If the node does not evaluate other nodes, the default rating is used. We define the similarity measure as sim_i^j. Assuming it is an n-dimensional normalized vector, we express the similarity as follows:

$$\mathrm{sim}_i^j = \frac{\sum_{k=1}^{n} \mathrm{TV}_k^i * \mathrm{TV}_k^j}{\sqrt{\sum_{k=1}^{n} \left(\mathrm{TV}_k^i\right)^2} * \sqrt{\sum_{k=1}^{n} \left(\mathrm{TV}_k^j\right)^2}}, \tag{9}$$

where TV_k^i and TV_k^j represent the kth dimension of the normalized vector of node i and node j, respectively. Since the value of this vector cannot be negative, the similarity value range is between 0 (dissimilar) and 1 (completely similar). After the infrastructure receives the similarity calculation instruction, it will calculate the similarity of the interest preferences of the vehicle j that sends the message and the vehicle i in the trust table of the infrastructure. The greater the similarity value is, the closer the interest preferences are between them and the more likely it is to be accepted as a trusted node.

3.2.3. Infrastructure Trust Value (IT). The trust value management of IT can be realized between the infrastructure RSUs, and the trust upgrade information about the upper trust management plane can be updated synchronously. By combining the RSU distance coefficient and the similarity between the computing nodes, the trust calculation of the infrastructure for the vehicle can be expressed by the following formula:

$$\mathrm{IT} = \mathrm{DC}_{ij} * \mathrm{sim}_i^j. \tag{10}$$

3.3. Hybrid Trust Calculation (HT). In VANET, the ultimate global hybrid trust calculation should include the trust between vehicles and the trust between vehicles and infrastructure. Owing to the complementary role of infrastructure in trust management, trust between vehicles is more important than trust in infrastructure. Therefore, if n is used to represent the number of vehicle interactions and $1/(n+1)$ is used as the adjustment factor, it can ensure that the trust between vehicles gets more weight. Then, the hybrid trust can be obtained by the following formula:

$$\mathrm{HT} = \left[\left(1 - \frac{1}{n+1}\right) * \sqrt{\mathrm{ST} * \mathrm{RT}}\right] + \left[\frac{1}{n+1} * \mathrm{IT}\right]. \tag{11}$$

We use Algorithm 2 to represent the complete vehicle hybrid trust calculation process.

4. Simulation and Performance

To test the performance of the proposed scheme, in this section, we first introduce the relevant attack models and explain the tools and parameter settings used in the simulation environment. Secondly, we define evaluation indicators to evaluate the accuracy of HHTM, and finally, we carry out the comparative analysis of experimental results under different schemes.

4.1. Attack Models. The trust management model is mainly to spread trustworthy information in the IoV, so this paper mainly notes the following malicious attacker model to evaluate the performance of HHTM.

4.1.1. Simple Attacks (SAs). The attacker acts as a receiver where messages are deliberately discarded or delayed, thereby preventing legitimate vehicles from receiving safety

Input LTD, OTV, vehicle ID, ROV_{ij}, QOD_{ij}
Output ST, RT
if vehicle i receives interactive information from vehicle j then
  Calculate the distance between nodes and obtain the STW value according to equation (1)
  Check the local trust database (LTD) of vehicle i
  if $ID_j \in LTD_i$ then
    Search OTV_{ij}
  else
    Take OTV_{ini} as the OTV value of vehicle i to vehicle j
  end if
  Upgrade the OTV information of vehicle i
  Calculate the ST of vehicle j using equation (3)
  if $ROV_{ij} \geq ROV_{thre}$ then
    $ROV_{ij} \longleftarrow ROV_{ij} + \lambda$
  else
    $ROV_{ij} \longleftarrow ROV_{ij} - \mu$
    if $QOD_{ij} \geq QOD_{thre}$ then
      $QOD_{ij} \longleftarrow QOD_{ij} + \lambda$
    else
      $QOD_{ij} \longleftarrow QOD_{ij} - \mu$
    end if
  end if
  Use equation (6) to calculate the trust score SP between vehicles
  Calculate the value of NT according to the value of SP_{ij} using equation (5)
  Determine the role type of vehicle j and use equation (4) to find RW
  Use equation (7) to calculate the RT of vehicle i to vehicle j
end if

Algorithm 1: Inter-vehicular trust calculation.

Input DIS, TV, HT_{thre}
Output HT
if vehicle i receives interactive information from vehicle j then
  Use Algorithm 1 to solve the ST and RT of the vehicle
  if Vehicle i is within the coverage of RSU then
    Calculate DC_{ij} using equation (8)
    Calculate sim_i^j using equation (9)
    Calculate IT using equation (10)
  else
    $IT = 0$
  end if
  Calculate HT using equation (11)
end if
if $HT \geq HT_{thre}$ then
  Confirm that vehicle j is a trusted vehicle
  Continue to receive interactive information from vehicle j
else
  Confirm that vehicle j is a dishonest vehicle
  Discard the interaction request information of the vehicle
end if
Upgrade the trust management information of vehicle j in the LTD of vehicle i
Broadcast the trust management upgrade information of vehicle i

Algorithm 2: Hybrid trust calculation.

messages promptly. Due to the sensitive nature of the messages involved in the IoV, discarding safety messages can make a huge impact on the network. The attacker may use selfish behavior to manipulate the infected node so that it will not follow normal network protocol and provide necessary services for other nodes. For example, they will not

forward data packets or spread route discovery requests. However, when the node is requested about the credibility of other nodes, it will not provide any false trust opinions.

4.1.2. Selective Misbehavior Attacks (SMAs). In this attack, malicious nodes provide false information to some nodes while providing normal information to other nodes. Attackers have inconsistent behavior patterns for different nodes, which will make the trust management between different nodes inconsistent and increase the difficulty of detection.

4.1.3. Time-Dependent Attacks (TDAs) [29]. Attackers use random patterns in the network to produce intelligent behavior. The attacker will initially act as a legitimate node in a short period to obtain the trust of vehicles in the network. The attacker can only start malicious behavior after gaining the trust of other vehicles and being a part of the legitimate network. In the attack mode, the attacker will share false messages and ratings with neighboring vehicles.

4.2. Simulation Setup. To facilitate the simulation, we used Veins [30], an open source platform widely used in vehicle network simulation. Veins is constructed by two mainstream simulators: traffic simulator SUMO [31] and discrete-time simulator OMNET++ [32]. Through the traffic control interface, events triggered by OMNET++ can deliver response instructions to SUMO to change vehicle paths and other information. We select part of the real road network in Zhengzhou City, Henan Province (as shown in Figure 5), as the simulated road network, with a topological area of $3\,\text{km} \times 3\,\text{km}$, and use SUMO to construct the initial road network (as shown in Figure 6). We randomly place 10 RSUs in the road network, and all vehicles are equipped with wireless communication standard protocol IEEE 802.11p. The system deploys one controller, and the infrastructure is connected to the controller through an Ethernet interface.

To ensure the reliability of the experimental results, 30 random experimental seeds have been carried out for each experimental scene and the average value has been taken. Table 2 provides details on the parameters used in the experimental environment. Since we believe that credibility is difficult to establish and easy to be destroyed, we set $\mu = 10\lambda$. To avoid the cold start problem [33], we set both HT_{thre} and OTV_{ini} to 0.5. The probabilities of malicious behaviors of the three malicious node attacks are all set to 0.5.

4.3. Evaluation Metrics. Since the weighted voting method has been widely used in many previous wireless network trust management schemes [15, 34], we use the weighted voting method as a baseline method when evaluating the performance of the HHTM scheme.

We utilize the following three parameters to evaluate the accuracy of the HHTM scheme: precision (P) and recall (R), which are widely used in machine learning and information retrieval to evaluate accuracy [35]. In this paper, we use both P and R to evaluate the accuracy of the proposed scheme for identifying dishonest nodes in VANET. F-score (F) is the weighted average of P and R values, used to reflect the overall accuracy of the trust management model. The parameters are defined as follows:

$$P = \frac{\text{number of truly malicious nodes caught}}{\text{total number of dishonest nodes caught}},$$

$$R = \frac{\text{number of truly malicious nodes caught}}{\text{total number of truly malicious nodes}}, \tag{12}$$

$$F = \frac{2 * P * R}{P + R}.$$

4.4. Result Analysis. As shown in Figure 7(a), the precision values of HHTM at different number of nodes are higher than those of the baseline method. As the node density continues to increase, its value exceeds by 90%. This is because when the total number of honest nodes increases, the trust evaluation node is more likely to receive real data from other nodes. Figures 7(b) and 7(c) show that the HHTM scheme is also superior to the baseline method in terms of recall value and F-score value. Similarly, when the node density is high, the value exceeds by 90%.

Figure 8 shows the changes of P and R values during SA. When the number of malicious nodes is small, the precision and recall of the two schemes are better. As the number of malicious nodes increases, the P and R values of the two schemes have both declined to a certain extent. It can be seen that the difference between the two schemes is not obvious. This is because SAs only maliciously discard or delay information and do not spread false trust opinions, so they are less destructive than other attacks.

Figure 9 shows the changes of P and R values during SMA. It can be seen that the P and R values of the baseline method are significantly lower than those of HHMT. When the number of malicious nodes reaches 40%, the P and R values of HHMT are 12.7% and 11% higher than those of the baseline method, respectively. This is because the baseline method relies on weighted voting, so the recognition of nodes with inconsistent trust management is reduced.

Figure 10 indicates the changes of P and R values during TDA. Because the attacker uses intelligent behavior to initiate attacks intermittently, the values of P and R of HHTM are lower than those of the above two attacks. However, opposed to the baseline method, HHTM still shows good response capabilities due to the adoption of a hierarchical trust management strategy. When the number of malicious nodes reaches 40%, the P and R values of HHTM are 13.8% and 12.2% higher than those of the baseline method, respectively.

For different levels of security incidents, the trust threshold requirements are also different, such as setting a higher threshold for the determination of road traffic accidents to ensure the reliability of the event. We compare the detection rate and F-score value of the HHTM scheme with EBT [36] and AATMS [37] when the threshold is different to confirm the performance difference between the different schemes.

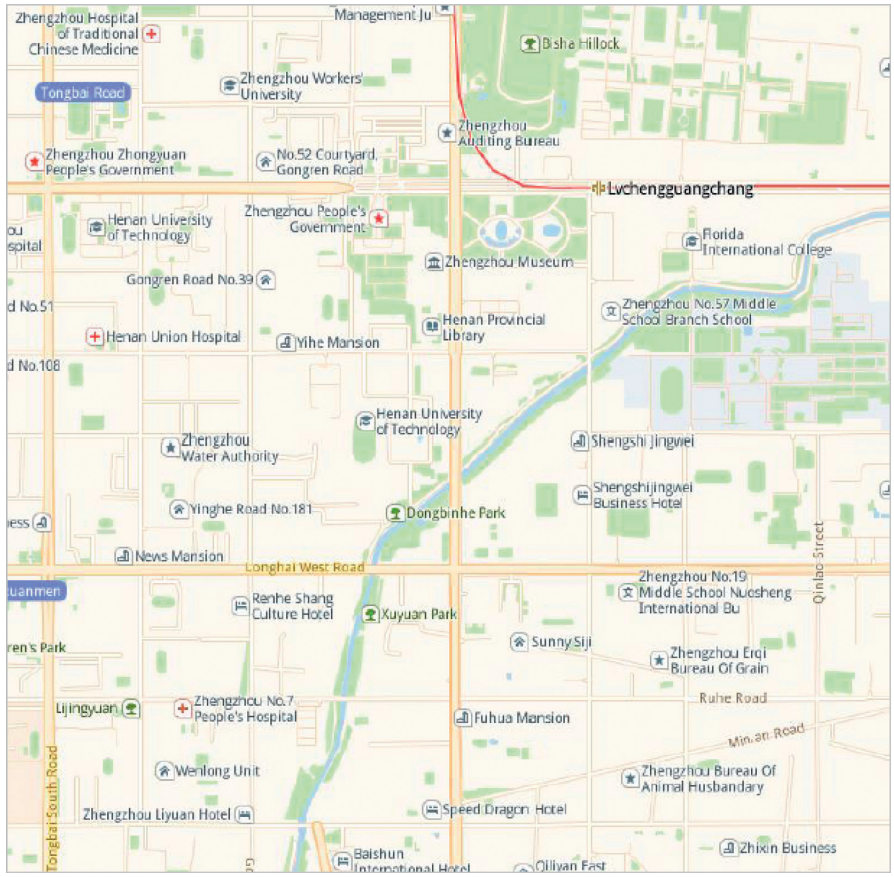


Figure 5: Extracted city map.

Figure 6: Initial road network model.

It can be seen from Figure 11 that the higher the trust threshold, the lower the detection rate. The proposed trust management scheme is superior to the comparison scheme in terms of detection rate. When the trust threshold is set to 0.9, the detection rate of HHTM is still above 20%. It can be seen from Figure 12 that with the increase of the trust

Table 2: Simulation parameters.

Parameter	Value
Simulation area (km × km)	3 × 3
Simulation time (sec)	800
Number of vehicles	25, 50, 100, 200
Location of vehicles	Random
Num. of attackers (%)	10, 20, 30, 40, 50
MAC protocol	IEEE 802.11p
ROV_{thre}	0.5
QOD_{thre}	0.5
HT_{thre}	0.5
OTV_{ini}	0.5
Reward factor λ	0.01
Penalty factor μ	0.1

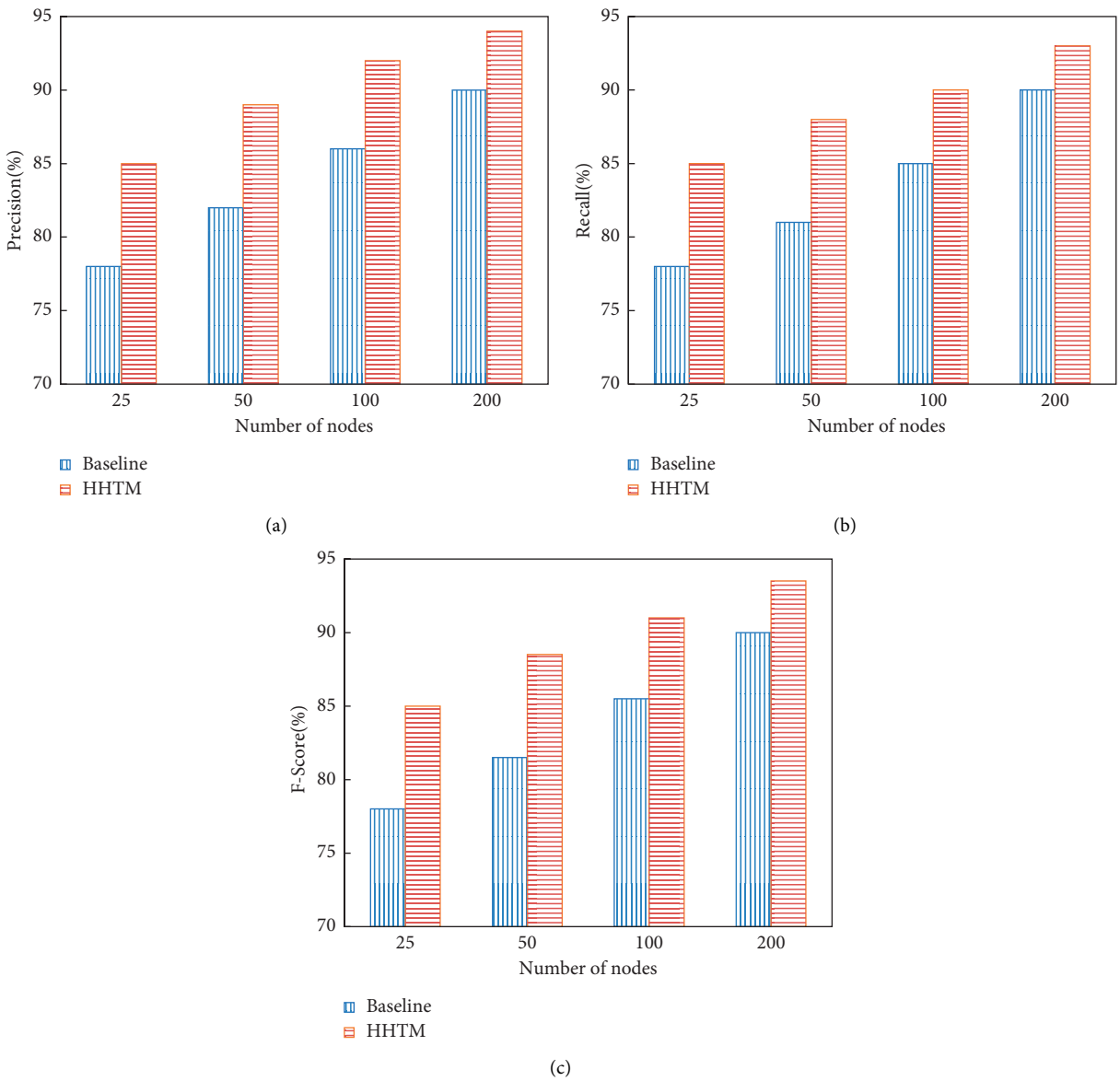


Figure 7: (a) Precision at different number of nodes. (b) Recall at different number of nodes. (c) *F*-score at different number of nodes.

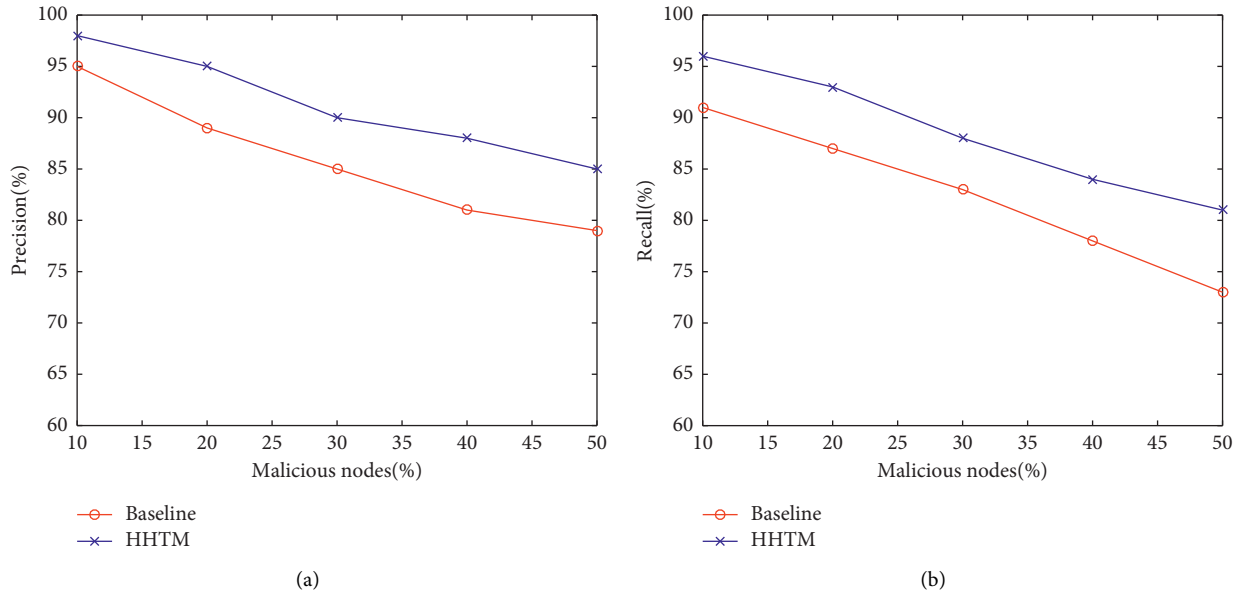


Figure 8: (a) P value during SA. (b) R value during SA.

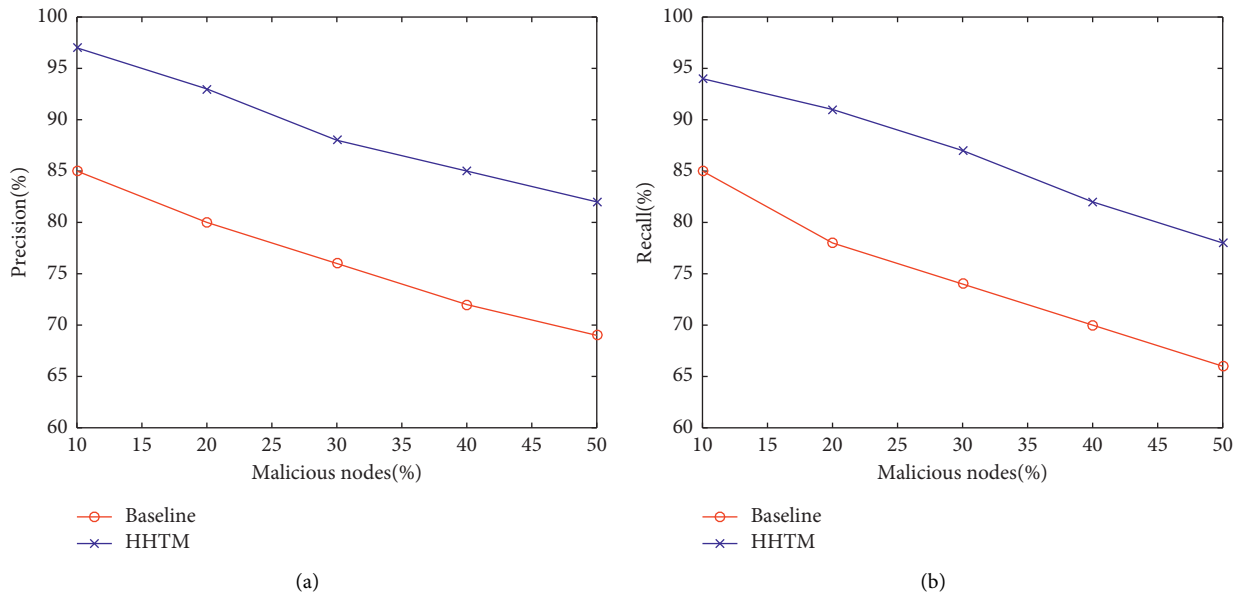


Figure 9: (a) P value during SMA. (b) R value during SMA.

threshold, the F-score decreases continuously. When the trust threshold reaches 0.8, the F-score of all schemes decreases significantly. At the same time, the F-score of the proposed scheme is always better than that of the contrast schemes.

Figure 13 shows the impact of the delay on the trust management scheme under the three types of attacks. It can be observed that in the SA, the end-to-end delay of the three schemes is not much different. In the SMA, with the increase of malicious nodes, the delays of the three schemes are comparable. When the number of malicious nodes is 50%, the delay of HHTM is reduced by 38.6% and 25.2% compared with EBC and AATMS, respectively. In the TDA, when the number of malicious nodes exceeds 30%, the delay of EBC increases significantly. It shows that this scheme has no advantage in dealing with TDAs. In the three attack modes, the delay of HHTM is better than that of the comparison schemes.

In summary, compared with other solutions, HHTM has achieved better results in resisting the attacks of the three models and can better deal with a higher proportion of malicious nodes.

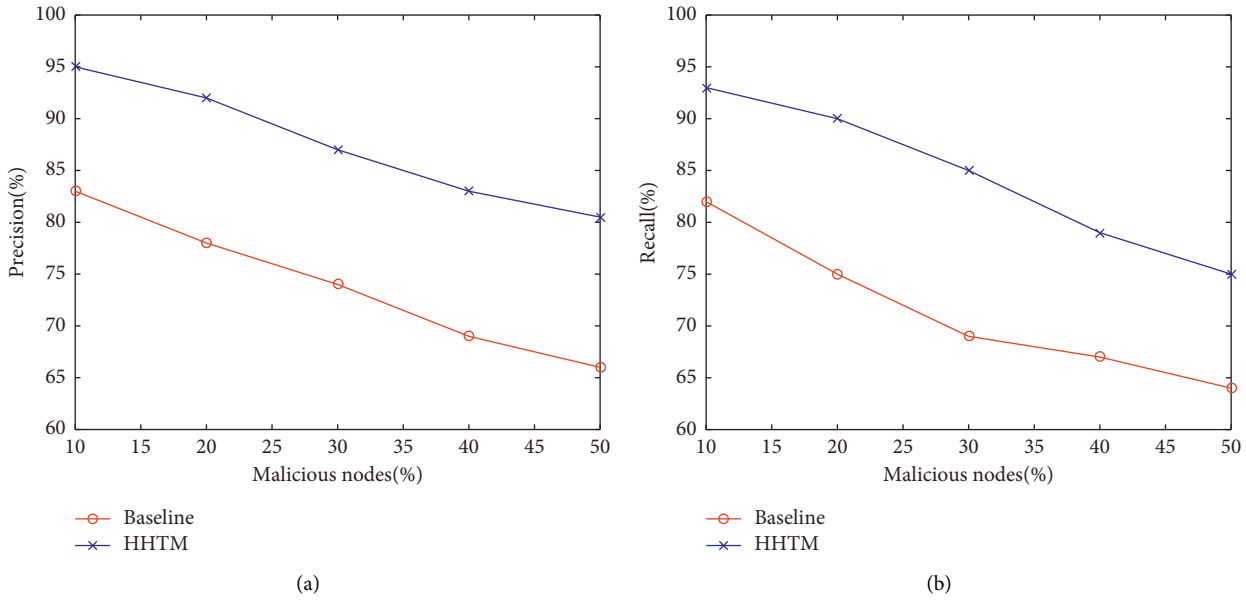


Figure 10: (a) P value during TDA. (b) R value during TDA.

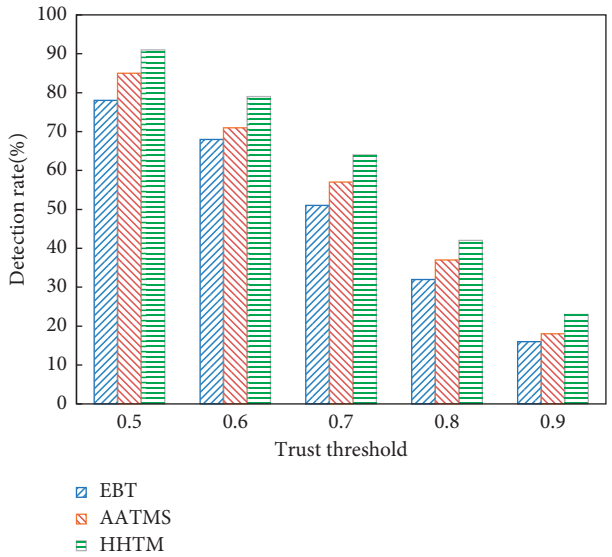


Figure 11: The impact of trust threshold on detection rate.

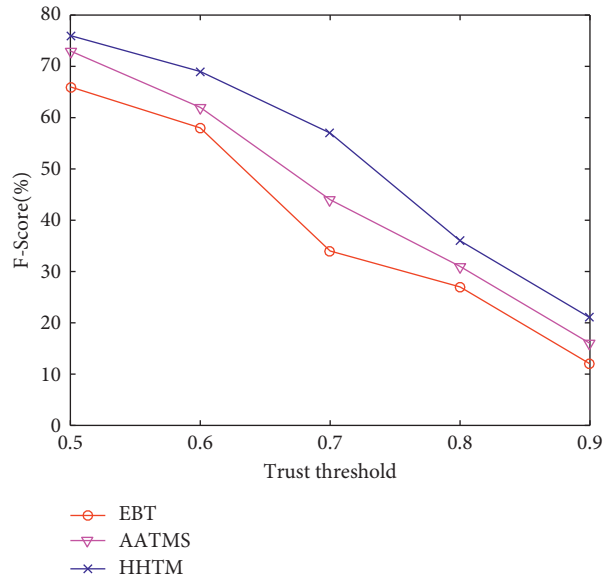


Figure 12: The impact of trust threshold on *F*-score.

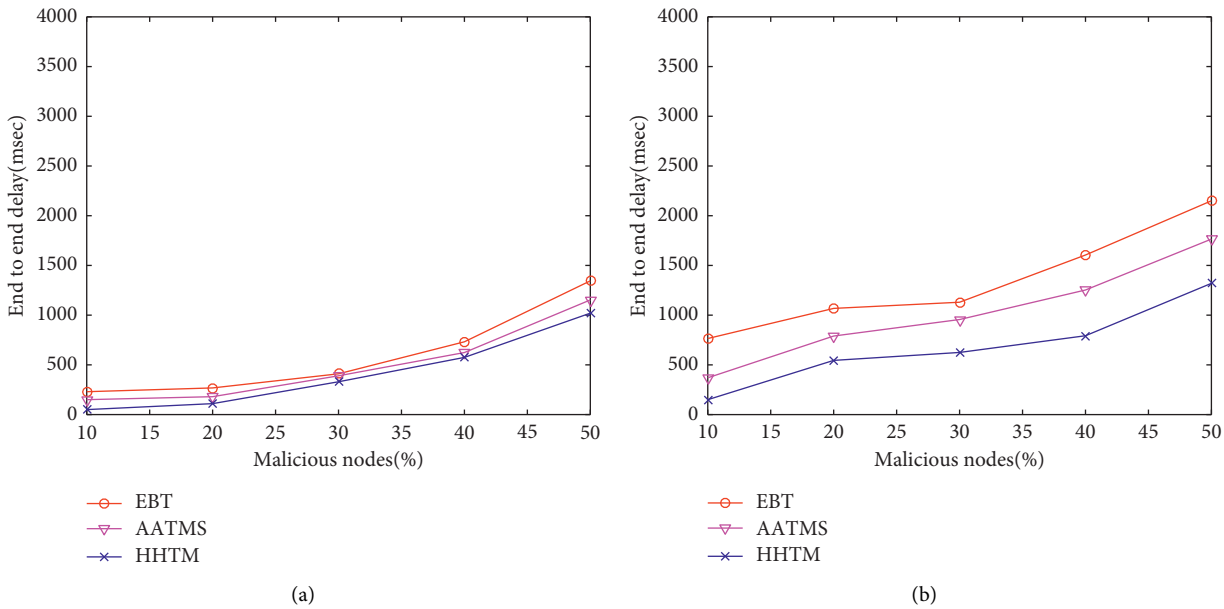
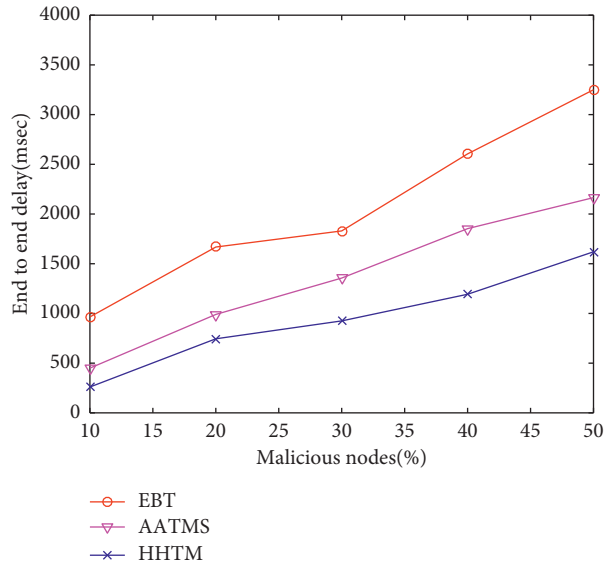


Figure 13: Continued.



(c)

Figure 13: (a) End-to-end delay during SA. (b) End-to-end delay during SMA. (c) End-to-end delay during TDA.

5. Conclusions

In VANET, a safe and attack-free environment is essential for the transmission of trusted messages between the vehicle and the infrastructure. However, because VANET involves a variety of different application environments, it is a very challenging task to ensure the trust foundation in each environment when an attacker penetrates the network and pollutes the network with fake information. A robust TM architecture should be established to achieve vehicle and message verification.

In this article, with the help of SDVN's fast flow forwarding mechanism, a trust management scheme named HHTM is proposed to evaluate the credibility of vehicles and traffic data in VANET. In the HHTM scheme, the trustworthiness of the EvN is modeled and evaluated as two independent indicators, namely, the trust between vehicles and the trust between nodes and infrastructure. Among them, it focuses on the use of the inter-vehicular trust to evaluate whether the received node data are credible and to what extent. On the other hand, we use the node-infrastructure trust to strengthen the trust of vehicles sending data in VANET. Extensive experiments are carried out to verify the robustness of the proposed trust management scheme. The experiment results show that compared with the comparative schemes, the proposed HHTM scheme can accurately assess the credibility of nodes and data in VANET and deal with various malicious attacks.

Based on the realization of the trust management of the Internet of Vehicles, in order to strengthen the data transmission security of the Internet of Vehicles, future work should be aimed at establishing security mechanism for vehicular data sharing. At the same time, the fine-grained access control of the Internet of Vehicles is also a direction worth studying.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (nos. 61802429, 61872382, and 61521003) and the National Key R&D Program of China (nos. 2018YFB0804002, 2019YFB1802505, 2019YFB1802501, 2019YFB1802502, and 2020YFB1804803).

References

[1] N. A. Jagadeesan and B. Krishnamachari, "Software-defined networking paradigms in wireless networks: a survey," *ACM Computing Surveys*, vol. 47, no. 2, pp. 1–11, 2015.

[2] C. Jiacheng, Z. Haibo, Z. Ning, Y. Peng, G. Lin, and S. Xuemin, "Software defined Internet of vehicles: architecture, challenges and solutions," *Journal of Communications and Information Networks*, vol. 1, no. 1, pp. 14–26, 2016.

[3] C. Y. Yeun, "Security protocol model for ubiquitous networks," US patent, 2006.

[4] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: a robust and privacy-preserving reputation management scheme for pseudonym enabled VANETs," *International Journal of Distributed Sensor Networks*, vol. 2016, Article ID 6138251, 15 pages, 2016.

[5] J. Grover, M. S. Gaur, and V. Laxmi, "Trust establishment techniques in VANET," *Wireless Networks and Security*, Springer, Berlin, Germany, pp. 273–301, 2013.

[6] F. Li and Y. Wang, "Routing in vehicular Ad Hoc networks: a survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.

[7] S. Park, B. Aslam, and C. C. Zou, "Long-term reputation system for vehicular networking based on vehicle's daily commute routine," in *Proceedings of the 2011 IEEE Consumer Communications and Networking Conference (CCNC'11)*, pp. 436–441, Las Vegas, NV, USA, January 2011.

[8] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: a reputation-based global trust establishment in VANETs," in *Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS'13)*, pp. 210–214, IEEE, Xi'an, China, September 2013.

[9] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Networking and Applications*, vol. 7, no. 3, pp. 229–242, 2014.

[10] W. Bamberger, J. Schlittenlacher, and K. Diepold, "A trust model for intervehicular communication based on belief theory," in *Proceedings of the 2nd IEEE International Conference on Social Computing (SocialCom'10)*, pp. 73–80, IEEE, Minneapolis, MN, USA, August 2010.

[11] X. Hong, D. Huang, M. Gerla, and Z. Cao, "SAT: situation-aware trust architecture for vehicular networks," in *Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture, MobiArch'08*, pp. 31–36, Seattle, WA, USA, August 2008.

[12] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: a trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.

[13] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[14] F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A comparative analysis of trust models for safety applications in IoT-enabled vehicular networks," in *Proceedings of the 2019 Wireless Days (WD)*, Manchester, UK, 2019.

[15] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proceedings of the IEEE 27th Conference on Computer Communications (INFOCOM)*, April 2008.

[16] T. Gazdar, A. Belghith, and H. Abutair, "An enhanced distributed trust computing protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, 2018.

[17] A. Wu, J. Ma, and S. Zhang, "RATE: a RSU-aided scheme for data-centric trust establishment in VANETs," in *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing*, September 2011.

[18] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," *Network and System Security*, Springer, Berlin, Germany, pp. 94–108, 2013.

[19] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," in *Proceedings of the 2014 International Conference on Information and Communication Technologies (ICICT)*, pp. 965–972, Elsevier, Chengdu, China, December 2014.

[20] N. Yang, "A similarity based trust and reputation management framework for VANETs," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, pp. 25–34, 2013.

[21] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.

[22] S. Ahmed and K. Tepe, "Using logistic trust for event learning and misbehaviour detection," in *Proceedings of the IEEE 84th Vehicular Technology Conference (VTC-Fall)*, September 2016.

[23] Y.-M. Chen and Y.-C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153–163, 2013.

[24] R. Shrestha and S. Y. Nam, "Trustworthy event-information dissemination in vehicular ad hoc networks," *Mobile Information Systems*, vol. 2017, Article ID 9050787, 16 pages, 2017.

[25] A. Alioua, S.-M. Senouci, S. Moussaoui, H. Sedjelmaci, and A. Boualouache, "Software-Defined heterogeneous vehicular networks: taxonomy and architecture," in *Proceedings of the 2017 Global Information Infrastructure and Networking Symposium (GIIS)*, Saint Pierre, France, 2017.

[26] C. Piao, J. Zhao, and J. Feng, "Research on entropy-based collaborative filtering algorithm," in *Proceedings of the 2007 IEEE ICEBE*, Hong Kong, China, October 2007.

[27] J.-M. Chen, T.-T. Li, and J. Panneerselvam, "TMEC: a trust management based on evidence combination on attack-resistant and collaborative Internet of vehicles," *IEEE Access*, vol. 7, pp. 148913–148922, 2019.

[28] A. Singhal and I. Google, "Modern information retrieval: a brief overview," *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, vol. 24, no. 4, pp. 35–43, 2001.

[29] H. Xia, S.-s. Zhang, Y. Li, Z.-k. Pan, X. Peng, and X.-z. Cheng, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7108–7120, 2019.

[30] Veins, "Vehicles in network simulation, the open source vehicular simulation framework," 2018, http://veins.car2x.org.

[31] M. Behrisch, L. Bieker, J. Erdmann et al., "SUMO-simulation of urban mobility: an overview," in *Proceedings of the 3rd International Conference on Advances in System Simulation*, Barcelona, Spain, 2011.

[32] OMNET, "OMNET++: discrete event simulator," 2018, https://omnetpp.org/.

[33] L. H. Son, "Dealing with the new user cold-start problem in recommender systems: a comparative review," *Information Systems*, vol. 58, pp. 87–104, 2016.

[34] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[35] J. Davis and M. Goadrich, "The relationship between precision-recall and ROC curves," in *Proceedings of the ACM 23rd International Conference on Machine Learning*, Pittsburgh, PA, USA, 2006.

[36] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile Ad Hoc vehicular networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 3, pp. 407–420, 2011.

[37] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: an anti-attack trust management scheme in VANET," *IEEE Access*, vol. 8, pp. 21077–21090, 2020.