Simulation Modelling Practice and Theory 120 (2022) 102627

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Blockchain and deep learning based trust management for Internet of Vehicles

Shujuan Wang [a], Yingnan Hu [a], Guanqiu Qi [b,*]

[a] School of Information Engineering and Automation, Kunming University of Science and Technology, Yunnan, 650500, China
[b] Computer Information Systems Department, State University of New York at Buffalo State, Buffalo, NY 14222, USA

ARTICLE INFO

Keywords:
Internet of Vehicles
Trust management
Blockchain
Deep learning

ABSTRACT

Internet of Vehicles (IoVs) works as the most advanced component of Intelligent Transportation Systems (ITSs). In IoVs, vehicles are able to communicate with nearby vehicles or RoadSide Units (RSUs). Traffic safety and efficiency can be provided by collecting and uploading real-time traffic information through vehicles, as well as broadcasting information by RSUs. However, there may be malicious vehicles in the network uploading false information, which will lead to serious traffic problems. To alleviate this problem, a trust management system based on blockchain technology is proposed in this paper. In this system, vehicles in the network firstly collect information about their surroundings and then upload valid information to nearby RSUs. To prevent malicious vehicles from uploading false messages, this paper designs a deep learning based verification model to calculate the trustworthiness of uploaded messages, and to further obtain the credibility scores of vehicles using the calculated results, and detect malicious vehicles accordingly. Moreover, a public blockchain framework is proposed and a Proof-Of-Trust (POT) consensus algorithm is designed. Vehicles are motivated to report true and valid information, and are penalized for uploading false data under this framework. Simulation results show that this mechanism can effectively detect malicious vehicles and motivate unfamiliar vehicles to upload true and reliable information to achieve trust management in the open and dynamic vehicular network environments.

1. Introduction

Nowadays, the number of people owning private cars keeps climbing drastically due to the fast development of the automobile industry and the ever-growing transportation needs of people [1,2]. While facilitating people's journey to go everywhere, it also causes severe problems that may jeopardize the safety and efficiency of transportation systems. For example, traffic congestions are frequently reported on the main roads of big cities, especially in the morning and evening peaks, or in bad weathers. Traffic efficiency is greatly degraded once congestion occurs. Moreover, traffic accidents occur constantly and result a great loss on lives and properties. How to enhance the traffic efficiency and to improve the transportation safety so that people can enjoy the convenience brought by the technology development of automobile industry without endangering their lives and properties, is the most vital problem to be resolved at this stage. Luckily, with the development of wireless communication technology, sensor network technology and intelligent transportation technology [3,4], etc., Internet of Vehicle (IoV) emerges as a potential way to solve the problem.

* Corresponding author.
E-mail addresses: shujuanwang0703@126.com (S. Wang), qig@buffalostate.edu (G. Qi).

https://doi.org/10.1016/j.simpat.2022.102627

Available online 27 June 2022

IoV is a self-organized, open structured inter-vehicle communication network, which provides varied data access services for vehicles in high-speed moving state, supporting Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications for information interaction. IoV is designed for guaranteeing the safety of vehicle driving, and providing high speed data communication, intelligent traffic management and in-car entertainment [5–8]. For IoV, it is essential to disseminate true and accurate information related to critical events, such as traffic jams and accident reports. However, in a dynamic IoV environment with the presence of malicious vehicles, false and inaccurate messages may be delivered, thus causing serious security problems. For example, a malicious vehicle shares a false traffic update message stating that a roadway is normal, but it is actually under construction. Drivers who receive the false message may not pay enough attention to the roadway situation and cause traffic stops or accidents very likely. Therefore, it is crucial to guarantee that vehicles will upload correct and valid information. Unfortunately, due to the characteristics of IoV, such as high-speed moving vehicles, dynamically changing topologies, randomness of vehicles movement and open network environment [9], the communication relationships between vehicles or vehicles and RoadSide Units (RSUs) are temporary and unreliable, leading to the lack of trustworthiness between vehicles or between vehicles and administration center. It is challenging to verify the truthfulness and correctness of uploaded messages timely so that optimal management and driving decisions can be made. As a result, how to motivate vehicles to upload useful and correct information, and to prevent malicious vehicles to upload false messages, is becoming the most important and urgent issue to be resolved for realizing safe and efficient transportation in IoV.

Trust Management (TM) [10] is seen as an effective measure to address this issue. The existing trust management approaches are divided into centralized [11] and distributed models [12]. The centralized model processes and stores the data uploaded by vehicles on a central processor, e.g., a cloud repository. However, with the increasing number of vehicles, a central processor may need to process tens of millions of data at the same time, which can cause great latency and is far from adequate for time-sensitive management and control(like traffic jam control, accident alert, etc.). The distributed model of trust management is performed on the vehicle or RSU, which largely reduces the burden of interaction with the server and ultimately improves the efficiency of the system . Multiple vehicular nodes, which are highly possible strangers for each other, are involved in the distributed TM process. The existing distributed TM models usually rely on the endorsement of vehicle nodes for each other to verify the truthfulness of uploaded messages [13], yet the endorsement of vehicular nodes may not be updated timely to adapt to the situation. Moreover, if it does updated timely, the process requires a large number of information interaction between multiple vehicles, which poses a great challenge to the time-varying and easily interrupted channels between high-speed moving vehicles, and increases the communication overhead and complexity markedly. As a result, how to design a distributed TM model that can realize efficient and effective trust management for IoV with timeliness and low overhead, is another challenge to be resolved in providing safe and efficient transportation in IoV.

In recent years, blockchain has received a lot of attention from researchers [14–16] and has promising applications in various fields [17–19]. Blockchain is a distributed ledger technology introduced by Satoshi Nakamoto [20]. It converges the concepts of multiple theories, such as cryptography, game theory, distributed systems, and communication technologies. Blockchain has properties such as decentralization, immutability, traceability, and anonymity [21], which makes it inherently suitable for distributed trust management in IoVs. Due to its anonymity, it enables vehicles to upload messages anonymously, which effectively ensures the privacy and security of vehicles. At the same time, its tamper-evident nature effectively prevents hackers from tampering with the content of uploaded data. When a malicious vehicle uploads false information, the traceability characteristic of blockchain can track the true identity of the vehicle, which greatly reduces the possibility of a vehicle to upload false messages and solves the above-mentioned problem.

In this paper, we focus on the design of a blockchain-based distributed trust management strategy with timeliness and low overhead. Particularly, a deep learning model is cleverly incorporated into the overall strategy. The deep learning model is used to get the trustworthiness of the content of the message uploaded by a vehicle based on multiple characteristics, such as location, speed, time, as well as the type of vehicle, familiarity of the vehicle (whether it often drives on this road), and the credibility of the vehicle when the message is uploaded, etc.. When the model is successfully established, once a vehicle uploads a traffic-related message in the coverage area of an RSU, the RSU can determine the authenticity of the message and broadcast this message to the surrounding vehicles in a very short time to take effective measures for fast response and damage control.

The main contributions of this work are as follows.

(i) To resolve the problem that normal vehicle nodes usually lack enthusiasm to upload messages since it consumes a certain number of their limited resources, whereas malicious nodes upload false messages to harm the IoV on purpose, this paper proposes a distributed trust management mechanism in which truthful vehicle nodes are motivated to upload authentic and useful traffic-related messages to increase their credibility scores, which will favor them to compete in the mining process and to get certain reward at last. Meanwhile, the proposed TM mechanism penalizes malicious vehicles which upload false messages through decreasing their credibility scores. Messages sent by vehicles with low credibility scores are more likely to be verified as false information to protect the system. Moreover, vehicles that have credibility scores lower than a threshold are not allowed to send any message in the network, and their true identities can be traced to take administrative measures accordingly.

(ii) To realize effective and efficient trust management for IoV with timeliness and low overhead, this paper presents a blockchain-based TM mechanism in which vehicles meet certain criteria are qualified to participate in the mining process. Every time a vehicle uploads a traffic-related message, the information is verified quickly by an RSU and the vehicle's credibility score will be updated according to the verification result. Moreover, a Proof-of-Trust (PoT) algorithm is designed based on the Proof-of-Stake (PoS) consensus algorithm. The designed PoT algorithm helps vehicles with high credibility scores to win in the mining process. A block is then generated by the winning vehicle to record this transaction and then broadcasted to all vehicles in the IoV.

(iii) To achieve fast and reliable authenticity verification for uploaded messages, and to keep the communication overhead low, this paper applies the emerging deep learning technology to the overall mechanism. The deep learning model is pre-trained and is deployed on RSUs. Upon receiving a message, an RSU can verifies the trustworthiness of this message based on various attributes (e.g., vehicle type, familiarity, speed, location, etc.) and the reporting vehicle's historical behavior, to quickly determine whether this message is valid and useful for instant traffic management and control. Moreover, RSUs can spot malicious vehicles with the support of this proposed deep learning model, thus prevent them from further harming the system.

(iv) Theoretical analysis and simulation results show that the designed mechanism can effectively recognize false information and identify malicious vehicles in IoVs, and achieve efficient and low overhead trust management, which is very meaningful for the realization of various intelligent transportation applications in IoVs.

The rest of this paper is organized as follows: Section 2 summarizes the related works, Section 3 describes the system model specifically. Section 4 explains the designed TM mechanism in details. We evaluate the performance of the proposed mechanism in Section 5, and give specific analysis both from theoretical aspect and simulation results. Finally, Section 6 concludes this paper.

2. Related works

2.1. Trust management systems for IoVs

In IoVs, trust management systems are designed for motivating vehicles to upload true and valid information, establishing trust interactions between unfamiliar vehicles, and distinguishing truthful nodes from malicious ones. TM mechanisms generally use incentives and penalties to manage vehicles to upload true messages. In this section, we review the research progress on trust management systems for IoVs in recent years.

Classically, the trust level of a vehicle is calculated indirectly by getting evaluations from the vehicle's neighbors, and vice versa [13]. Li et al. [22] proposed a reputation-based announcement scheme for VANETs. Vehicles broadcast messages to their neighbors and neighbors report feedback to a reputation server. The reputation server then aggregates the feedback to generate the reputations and propagate them. However, this scheme uses a centralized trust management model that is no longer well adapted to the increasing number of vehicles in IoVs. Raya et al. [23] designed a data-centric distributed trust approach for VANETs. Once a vehicle receives reports from others, it calculates the trust level of each report as evidence. Reports that are related to the same event are merged and the reliability of the event is judged using a decision scheme that is based on Bayesian inference and weighted voting. However, this scheme requires each vehicle to conduct the calculation and decision processes, which consume a number of computing and communication resources of vehicles, thus limiting its effectiveness and adaptability.

Rawat et al. [24] used a hybrid approach to calculate vehicle trust level. It not only uses the information received by neighboring vehicles to determine the message trust level, but also combines the received signal strength (RSS) for distance calculation and the geographic location (location coordinates) of the vehicle to measure the trust level of the received message, to further obtain the trust level of the vehicle. However, with the presence of malicious vehicles, the reliability of this model is far from satisfying the requirements. Hussain et al. [25] suggested email-based social trust to build and manage data-level trust. The main drawbacks of data-centric trust model are latency and data sparsity. Large amounts of data from separate sources may contain redundant information, which will increase latency or overwhelm important information. Li and Song [26] proposed a trust management model that can be implemented under the different attack models. It utilizes the trust assessment of information exchanged by multiple neighboring vehicles. However, this model is implemented under the premise that it does not consider vehicle density in a vehicle-dense environment. In [27], the authors proposed a hybrid framework to manage trust and privacy of vehicles. In this, nodes evaluate the trustworthiness of received events by considering the entity reputation of the sender. However, this paper only achieves a balance in terms of vehicle privacy and security, and the trust management aspect for specific vehicles is not considered in the presence of a larger number of malicious vehicles.

In summary, existing works of trust management usually rely on collecting neighboring vehicles' evaluations to calculate the reliability of a vehicle/message. However, this requires frequent information interactions between vehicles, when the number of vehicles is large, the evaluation gathering could consumes a huge portion of bandwidths and degrades the transmission performance. Furthermore, it is difficult to find malicious node or false message timely since the evidence collecting also introduces significant delay into the network. Besides, malicious nodes may not only upload false information but also give false evaluation on other vehicles, which makes it more difficult to make correct calculation of vehicles' trust levels, nor to make precise decisions based on the calculation results.

2.2. Blockchain-based trust management system for IoVs

Youssef et al. [28] proposed an optimized link state based routing protocol to address the repetitive process in trust management. It uses blockchain to provide a distributed, secure and tamper-proof framework for all vehicles in the network. However, this work mainly addresses the resource wastage problem of repeatedly detecting malicious vehicles and does not optimize the way of detecting malicious nodes. In [29], a blockchain-based trust management model is proposed to obtain aggregated packets which use neighboring vehicle's witness information as signatures to return to the vehicle. RSU collects the aggregated packets from vehicles within its communication range to assess the trustworthiness of the information and update the reputation value of the vehicle using a logistic regression algorithm. It is also combined with an anonymous aggregated vehicle announcement protocol to protect the

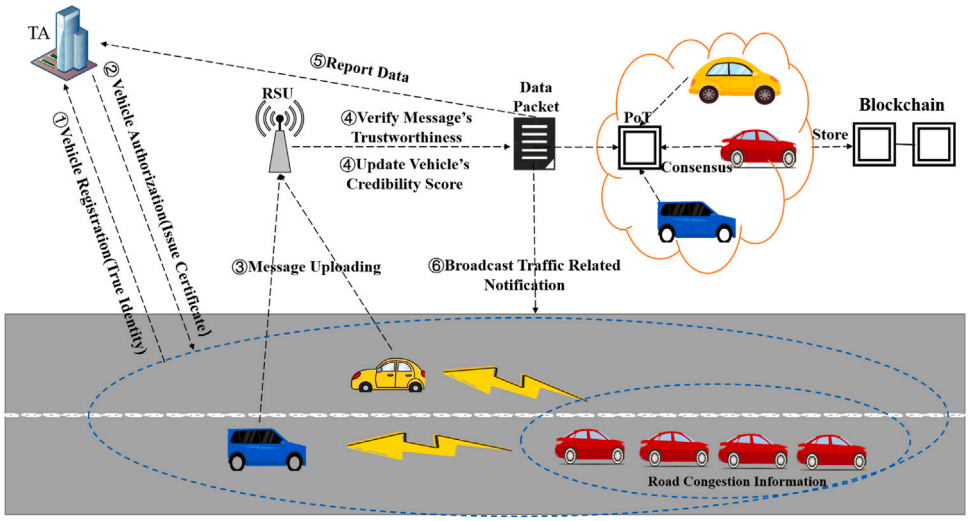

Fig. 1. System model.

privacy of vehicles. However, this model does not consider the case of fewer vehicles, where there may be insufficient neighboring vehicles that have witnessed the event, leading to performance degradation and errors. In [30], the authors proposed a blockchain-based trust management scheme for Vehicle Crowdsourcing Networks (VCNs) using trust evaluation model to achieve accurate vehicle trust assessment. Yang et al. [31] used a Bayesian inference model to verify messages sent by neighboring vehicles and to generate a rating for each vehicle. With these ratings, RSU can determines malicious vehicles. However, the accuracy of this model may be biased if there are too many malicious nodes. El Sayed et al. [32] studied a hierarchical trust management system for a network of vehicles. The system employs trust assessment, trust propagation, and trust aggregation steps to derive the trustworthiness of each vehicle. However, its hierarchical design requires repeated propagation of data, which can result in large communication overhead.

In summary, most of the existing blockchain-based trust management is based on neighboring vehicles evaluating the content of a vehicle's propagated messages to get aggregated packets. Then the RSU is used to evaluate the aggregated packets to get the reputation value of the vehicle, and store the result to the blockchain. However, in networks with a large number of malicious vehicles, the evaluation of neighboring vehicles may be inaccurate. In addition, it should also be considered that the use of neighboring vehicles for vehicle evaluation is not suitable in the case of low traffic hours (e.g., early morning) or remote locations with few vehicles.

3. System model

In this section, we describe the focused system model. As shown in Fig. 1, the focused system model is mainly composed of three element: TA, Vehicle, and RSU.

(1) *Traffic Authority (TA):* We consider TA as a fully trusted entity, and each node entering the IoV must provide its real information (including its identity information) to TA to get a valid certificate. When a vehicle uploads a message to a RSU, it firstly needs to check whether the vehicle's certificate is real and valid, and only when the certificate is valid, the RSU will acknowledges the message. A RSU will sends a packet to TA after each data reporting event. The packet contains critical information, including the complete reported data, vehicle's credibility score and so on. TA maintains a table which stores the attributes of each vehicle, and updates the credibility score of a vehicle accordingly every time it receives a packet from RSUs.

(2) *RSU:* RSUs are fixed nodes, which are usually arranged at intersections and have sufficient resources for data processing, storage, and communication. Vehicles can exchange messages with RSUs through V2I communications, while RSUs share and update data with each other through wired links. After receiving a message, a RSU analyzes the message using the proposed Deep Learning (DL) model, to verify the truthfulness of the message, as well as the reliability of the vehicle. The trustworthiness of the message and the credibility score of the reporting vehicle will be calculated and updated according to the DL model. After then, the RSU will broadcasts the reported message, along with attributes that associate with the message, such as the verification result, the updated credibility score of the uploading vehicle, etc., to all vehicles within its coverage, and to RSUs that are connected with it. Upon receiving a packet from a neighboring RSU, a RSU will broadcasts this packet immediately to vehicles within range. Meanwhile, the RSU will also sends the packet to TA so that TA can stores the event and updates related attributes, such as the vehicle's credibility score and so on.

(3) *Vehicles:* Vehicles are the most common nodes in IoVs, which are loaded with On-Board Units (OBUs) with certain processing, communication, and storage capabilities. Vehicles are encouraged to report instant traffic situation to RSUs when they are driving on the roads. (e.g. traffic accidents, road condition information, and service information, etc.). Vehicles can get high credibility scores through honestly uploading traffic information, as well as low credibility scores by cheating the network. High credibility score will help vehicles to win the mining process and to finally get some reward, while low credibility score may revoke the certificate of vehicles and prevent them from uploading any messages further. A vehicle keeps its credibility score locally and updates it accordingly upon receiving a packet from a RSU.

The goal of the proposed mechanism is to achieve trust management in IoVs, so that the cost of uploading a false message is greater than that of uploading a true message, thus ensuring the trustworthiness of vehicles. As Fig. 1 shows, each vehicle enters the network needs to register with TA, and TA will issue a certificate for each vehicle after administrative check. When an event occurs, multiple nearby witness vehicles will send messages regarding this event to the nearest RSU. The RSU firstly checks a vehicle's credibility score, and only when the credibility score is higher than the "listening threshold" (TH_1), the uploaded message will be processed. The RSU then run the deep learning-based truthfulness verification model to check the authenticity and validity of the content of the messages. The trustworthiness of a message, as well as the credibility score of the reporting vehicle, are calculated by this model. After the verification, the RSU will generates a packet, containing the original reported data, as well as the attributes that describe the message uploading event, such as the verification result, the updated credibility score of the vehicle, etc., to broadcast to all vehicles within its coverage (through wireless links), to RSUs that are connected with it (through wired links), and to TA. RSUs will further broadcast this packet to all vehicles within range. As a result, all vehicles in the network can receive this packet in a short time. Upon receiving this packet, a vehicle can look over the traffic related information in this packet to make better driving decisions. Moreover, in the following mining process, once a vehicle has won the bookkeeping right, it can generates a block based on the data in the received packet, and earns a certain amount of credits from it.

A RSU will periodically checks vehicles within its' coverage. If a vehicle's credibility score is lower than the "reporting threshold" (TH_2), the RSU will report this vehicle to TA, and initiates the certificate revoking process. A vehicle with credibility score lower than the threshold is considered as malicious and its certificate is revoked by TA to prevent it from sending any message that may harm the network.

4. Specific mechanism design

In this section, we introduce the designed mechanism in detail.

As illustrated in Fig. 1, the trust management mechanism works on the basis of evaluating behaviors of vehicles and making proper actions according to the evaluations. The mechanism consists of three main parts: (1) Vehicle Authorization, (2) Message Uploading and Verification, and (3) Event Record.

4.1. Vehicle authorization

When a vehicle enters the IoV, it is required to register with the network by sending its critical information, including its true identity, to TA. If the vehicle passes administrative check, TA will issue a certificate to the vehicle to qualify it to send messages in the network. Meanwhile, TA will also assign a pseudonym on the vehicle so that the vehicle can exchange data using the pseudonym instead of its real identity, to realize privacy-preserving communications. The mapping between the vehicle's pseudonym and its true identity is confidentially stored at TA.

4.2. Message uploading and verification

All registered vehicles can upload traffic-related messages in the IoV. However, considering that there may be malicious vehicles in the network that upload false information to confuse RSUs, effective measures should be taken to guarantee that only true and valid information is disseminated in the network.

When a vehicle notices something that is worth to report, such as traffic accident, congestion, uneven pavement, missing gully cover, etc., it can send a message to the nearest RSU to report this event. If the information is true, the RSU can take proper actions based on the information to realize smart traffic management and control. For example, if the vehicle reports an accident honestly, the RSU can broadcasts emergency alert to all vehicles nearby to avoid secondary accidents.

The mechanism takes two steps to make sure the uploaded message will not brings any harm to the network. Firstly, the RSU will check the credibility score of an uploading vehicle once it receives a reporting message. If the credibility score is lower than the "listening threshold", this message is discarded without any further process, and the reporting event will be recorded later in the blockchain. Secondly, if the credibility score is higher than the threshold, indicating that this vehicle may be honest, the RSU then uses the pre-trained deep learning model to further verify the authenticity of the message, as well as the truthfulness of the vehicle.

In this work, we design a Fully Connected Network (FCN) to verify the authenticity of a uploading message by calculating the message content trustworthiness, and to further verify the truthfulness of the vehicle through calculating the credibility score of this vehicle. The structure of the proposed FCN is shown in Fig. 2. The FCN includes an input layer, three hidden layers and an output layer. The first and second hidden layers contain 100 neurons respectively and the third hidden layer contains 50 neurons.

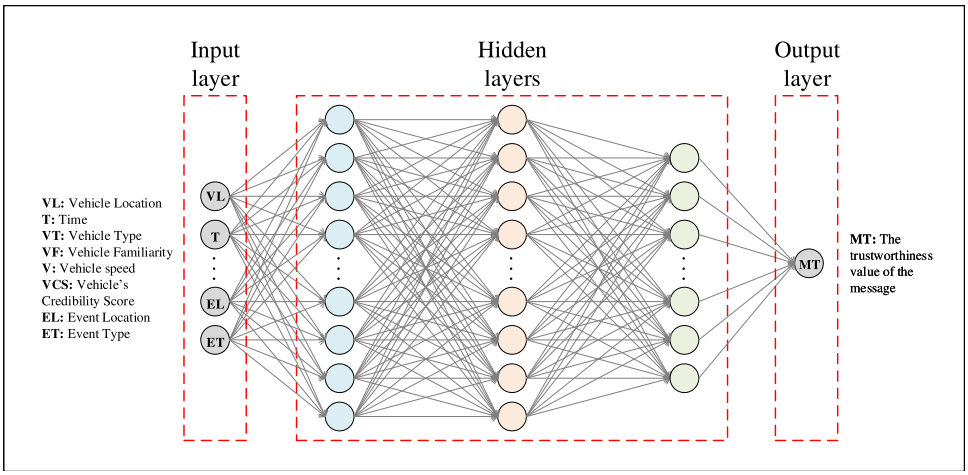

Fig. 2. Structural diagram of the fully connected neural network.

Table 1
The input parameters of the FCN.

Input	Description
Vehicle location	The x coordinate of the vehicle when uploading information.
Vehicle location	The y coordinate of the vehicle when uploading information.
Time	The time when the vehicle uploads information.
Vehicle type	Different types of vehicles (e.g. private cars, buses, police cars, etc.).
Vehicle familiarity	Does this vehicle often drives this road?
Vehicle speed	Speed of the vehicle when uploading messages.
Vehicle's credibility score	The credibility score of the vehicle when uploading the message.
Event location	The x coordinate of the spot where the event occurs.
Event location	The y coordinate of the spot where the event occurs.
Event type	Different message types (regular, emergency, etc.).
Output	The trustworthiness value of the message.

The input layer sends the input data to the FCN, and the hidden layer outputs the trustworthiness of the uploaded message. The selected input features are: (1) the location of the vehicle when the message is uploaded and the location of the spot reported in the message. The distance difference between these two can help to determine whether the traffic event occurred within the visible range of the vehicle. (2) The time period when the vehicle uploaded the message. When the vehicle uploads the message at the time of peak hours, the information is relatively reliable; if it happens in the early morning, the event described in the message is less likely because of the low flow of people and vehicles. (3) The type of the vehicle. If a vehicle is a public vehicle, for example, a police car, bus, ambulance and etc., it is more likely that the message uploaded by it is authentic. (4) Familiarity of the vehicle. If a vehicle often drives on this road, then the traffic information it uploads about this road is relatively reliable. (5) The driving speed of the vehicle. If a vehicle runs in a high speed, there is no good chance for the driver to observe details in the surroundings, lowering the trustworthiness of messages it uploads. The specific input information sent to the network for prediction is shown in Table 1.

Before entering the FCN, the data shall be processed to prevent the influence of too large or too small value on the performance of FCN. Specifically, the location information of the vehicle and the location information of the event need to be processed according to formula (1),

$$l_n = \frac{l_{in} - l_{min}}{l_{max} - l_{min}} \tag{1}$$

where, l_{in} represents the raw data of the position coordinates of the reporting event or the position information of the reporting vehicle, l_{min} and l_{max} represent the minimum and maximum value of the position coordinates of the reported vehicle and the reported event within the simulation range, respectively. Under the action of formula (1), numbers of a larger order of magnitude will be mapped between 0 and 1.

Since the maximum value of the speed is much smaller than the value of the coordinate, the speed can be directly preprocessed according to the reciprocal of formula (2).

$$v_n = \frac{1}{v_m} \tag{2}$$

where v_m is the original data and v_n is the input value of speed for the FCN.

Table 2
The structure of the suggested FCN.

Number of layer	Calculation formula	Matrix size	Bias size	Activate function	Output size
1	$y_1^n = W_1 x_i^n + b_1$	$W_1 \in \mathbb{R}^{100 \times 10}$	$b_1 \in \mathbb{R}^{100}$	ReLU	$y_1^n \in \mathbb{R}^{100 \times 1}$
2	$y_2^n = W_2 y_1^n + b_2$	$W_2 \in \mathbb{R}^{100 \times 100}$	$b_1 \in \mathbb{R}^{100}$	ReLU	$y_2^n \in \mathbb{R}^{100 \times 1}$
3	$y_3^n = W_3 y_2^n + b_3$	$W_3 \in \mathbb{R}^{50 \times 100}$	$b_3 \in \mathbb{R}^{50}$	Sigmoid	$y_3^n \in \mathbb{R}^{50 \times 1}$
4	$y_o^n = W_4 y_3^n + b_4$	$W_4 \in \mathbb{R}^{1 \times 50}$	$b_4 \in \mathbb{R}^{1}$	Sigmoid	$y_0^n \in \mathbb{R}^{1 \times 1}$

The 10 input parameters, such as the reporting vehicle's location, type, familiarity, speed, credibility score and etc., are arranged into vectors x_m^n, where n represents that x_m^n is the N_{th} input vector in the batch. x_m^n will be used as the input of the FCN network and return the trustworthiness value of the uploaded message y_o^n, where n indicates that y_o^n is the N_{th} output in one batch. Specifically,

$$y_o^n = F\left(x_i^n\right) \tag{3}$$

where, $F(\cdot)$ means the proposed FCN model whose structure is shown in Table 2.

Under the constraint of loss function shown in (4), the FCN model will adjusts the parameters of the network under the mechanism of back propagation,

$$L\left(w_{1\sim4}, b_{1\sim4}\right) = \frac{1}{N}\sum_{n=0}^{N}\left(y_i^n - y_o^n\right)^2 \tag{4}$$

where y_i^n is the label of the trustworthiness of the uploaded message. Follow the pipeline of FCN and the optimization networks in (4), the regression of the trustworthiness value of the uploaded message can be achieved.

By running the FCN-based verification model, the trustworthiness of the uploaded message is calculated. The RSU then determines whether the message is true by comparing the calculated trustworthiness with a trust threshold (TH_3). The message is determined as true if its trustworthiness is higher than TH_3. Otherwise the message is considered as false. After then, the newly calculated trustworthiness value of the uploaded message is used as another input parameter, along with the input parameters in Table 1, to be input into the FCN network to calculate the credibility score of the reporting vehicle. The reporting vehicle's credibility score is updated after the calculation. As a result, the RSU will broadcasts the content in the message, as well as the attributes that describe the message uploading event, including the vehicle's ID, location, reporting time, trustworthiness of the message, credibility score of the vehicle, and so on, to vehicles in the region and other RSUs. TA will also receive a copy of this packet so that intelligent traffic management and control can be realized. Upon receiving the packet, RSUs will further broadcast this packet to all vehicles within range, so that every vehicle in the area can receive the packet successfully in a short time. The received packet is useful for vehicles to understand the latest traffic and road conditions, and also for them to get prepared to record the event.

4.3. Event record

For each reporting event, a specific vehicle gets an updated credibility score, which will have strong impact on its behavior and treatment received from the network. Moreover, the valid messages uploaded by truthful vehicles contain important traffic-related data that have potential value for subsequent vehicles to query. As a result, it is worth to make record for each reporting event, in consideration of discriminating truthful vehicles from malicious ones, as well as providing valid and quick traffic-related information query service for vehicles.

In this work, we propose to use a public chain on the vehicles to record each uploading event. Public chain is chosen over consortium chain for two main reasons. On one hand, public chain is able to promote as many as possible vehicles to participate in the traffic related message uploading process, so that RSUs and TA can receive sufficient information for intelligent control and management. On the other hand, using a public chain, every authorized vehicle in the network can easily access the blocks and obtain the traffic related information, so that transportation efficiency can be improved. Particularly, we design a Proof-Of-Trust (POT) consensus algorithm, which favors vehicles with high credibility scores in the mining process. It determines the miners based on the credibility score of the vehicles. The higher the credibility score is, the bigger the chance that the vehicle will get to bookkeeping. This modified version of the POS algorithm makes the public blockchain perform better compared to the traditional public blockchain that uses POW, and it can handle a large number of vehicles uploading blocks faster.

4.3.1. Public chain-based trust model

The typical blockchain model consists of three main components: (a) transactions for message uploading, (b) credibility score ledger to record vehicles' credibility scores, and (c) consensus algorithm to update the distributed ledgers. In this work, the transaction data includes the information of uploading vehicle, event time, message content, the calculated message trustworthiness, and the corresponding measure taken by the RSU. The credibility score ledger is used to record the updated credibility score of the vehicle, after each verification. This system uses the credibility score to determine which vehicles are malicious, and record every message uploading event in the network for further investigation and administration. In the mean time, by storing the reported messages' contents on the blockchain, vehicles can access the information easily and use them to make better driving decisions. Due to the lack of centralized management in IoVs, the consensus process must be performed in a decentralized manner at the vehicle level. Several consensus algorithms exist in the literature, the most commonly used algorithms are Proof of Work (POW) and Proof of

Table 3
Main symbols.

$V \rightarrow TA$	A vehicle V sends a message to TA
ID_V	V's true identity information
Sig_V, Cer_V	Signature of V, Certificate of V
$E_{K_N^P}(m)$	Data m encrypted by the public key of N
K_N^P, K_N^S	Public key of N, private key of N
$D_{K_N^S}(m)$	Data m decrypted by the private key of N

Share (POS). POW validates transactions by the node with the highest computational capacity, which does not apply to the resource-limited IoV environment. POS selects the richest node as the validator, which is well adapted to the resource-limited environment. This system uses the POT consensus algorithm, which is a modified POS consensus algorithm. It uses the credibility scores of vehicles as shares in the consensus algorithm, so that the vehicles with higher credibility scores within the RSU communication range have more chances to be miners to generate blocks.

4.3.2. Smart contract

Smart contracts allow trusted transactions to be executed without a third party, which saves time, reduces costs, and makes transactions traceable and irreversible [33]. Table 3 summarizes the meaning of all symbols used in this section.

The smart contract design and execution are introduced as follows.

a. *Vehicle Registration & Authorization:* A vehicle V sends the real identity information about itself to the TA to register with the network when it firstly enters the network. Upon receiving the registration request, TA will run a validity check on V and issues a certificate to V so it can send messages in the network, i.e.,

$$V \rightarrow TA : content = ID_V \tag{5}$$

$$TA \rightarrow V : content = Cer_V \tag{6}$$

b. *Event Report & Message Upload:* When the vehicle finds traffic information worth reporting(such as traffic congestion, road icing, etc.), it uploads traffic message to the nearest RSU. The public key of the RSU is used to encrypt the message, i.e.,

$$V \rightarrow RSU : content = E_{K_{RSU}^P}(traffic\ data) \tag{7}$$

c. *Truthfulness Verification:* After receiving the message, the RSU uses its private key K_{RSU}^S to decrypt the message and then check the uploading vehicle's credibility score. If the score is higher than TH_1, the RSU initiates the FCN-based verification process, to calculate the trustworthiness value of the message, and update the credibility score of the vehicle, respectively.

$$RSU : content = D_{K_{RSU}^S}(traffic\ data) \tag{8}$$

d. *Result Processing & Transaction Settlement:* If the calculated trustworthiness value of the message is greater than the trust threshold TH_3, the message is true. Otherwise, it is false.
RSU uses its private key to encrypt the verified traffic data and packages the vehicle information, traffic information and processing results (trustworthiness value, credibility score) updated in previous steps as event attributes, and sends them to all vehicles within its communication range, RSUs and TA, i.e.,

$$RSU \rightarrow TA, V, RSU : content = E_{K_{RSU}^S}(event\ attributes\ \&\ traffic\ data) \tag{9}$$

After receiving the packet, all vehicles in the IoV can use the RSU's public key K_{RSU}^P to decrypt the packet and obtain the corresponding data. The mining competition starts and vehicles with credibility scores that are above the "mining threshold" (TH_4) are allowed to compete for the mining. The higher the vehicle's credibility score is, the higher chance it will have to generate the block and update the ledger.

The vehicle that wins in the mining process will pack the event attributes into a block, broadcasts it across the network, and uploads it to the chain after getting the consensus of other miners, and get a certain number of virtual currency reward.

If the updated credibility score is lower than the "reporting threshold" (TH_2), the RSU uploads the corresponding vehicle's information to TA. TA finds the real information of the corresponding vehicle and revokes the certificate of the vehicle. Vehicles without certificates will not be able to upload messages in IoV as well as request for traffic information.

5. Performance evaluation

5.1. Simulation analysis

5.1.1. Simulation preparation

In this article, we use simulator of urban mobility (SUMO) [34], to get a real-time map of Manhattan from OpenStreetMap (OSM) [35]. This map contains the real-time operation of vehicles in Manhattan at a certain moment. Fig. 3 shows the map

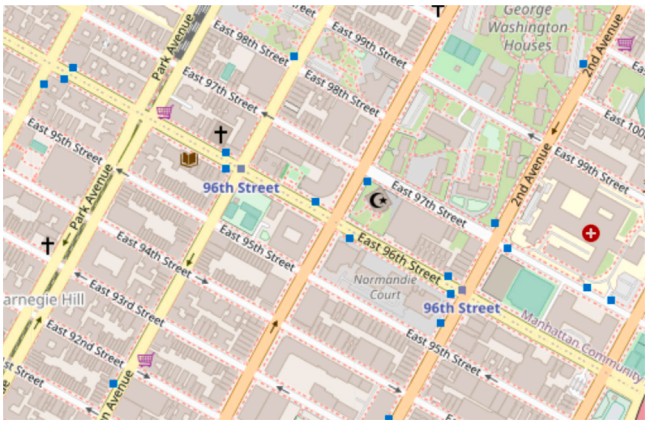

Fig. 3. Manhattan city map.

Table 4
Simulation parameters.

Parameter	Value
Simulation area	4000 × 4000 m
Number of vehicles	50, 100, 200
RSU transmission range	1500 m
Initial placement of vehicles	SUMO traces
Number of malicious vehicles	10%, 15%, 20%, 25%, 30%, 35%, 40%

downloaded and generated by SUMO, which represents a portion of the road network in the city of Manhattan. The size of this map is 4000 m by 4000 m.

With the map obtained by OSM, the operation of the vehicles in the map can be simulated using SUMO, to obtain vehicles' initial motion positions, speeds, IDs, and accelerations. The generated data source was run continuously for 600 s, and it contains vehicles' attribute information such as positions, speeds, IDs, and etc. The original SUMO simulation uses 1000 vehicles to generate a training set containing 20,000 inputs/outputs. The data used are split as 60% training, 20% generalization and 20% validation. A simulation is run using SUMO and all the generated data is output to an .xml file which contains the attributes of vehicles, such as real-time positions, speeds and ID of each vehicle. Python is utilized as the network simulator. The simulation parameters are shown in Table 4. In each simulation run, 50, 100 and 200 vehicles are randomly placed in the simulation area. To detect malicious vehicles more accurately, we keep the number of vehicles in the simulation area constant by adjusting the python data so that if a vehicle leaves the simulation area, a new vehicle is generated accordingly with a new set of attributes, including its initial position, speed, and ID.

We use the following two metrics, namely Precision (P) and Recall (R), to evaluate the performance of the proposed mechanism. The Precision and Recall rate are defined as in Eqs. (10) and (11).

$$P = \frac{Number\ of\ Malicious\ Vehicles\ Detected}{Total\ Number\ of\ Reported\ Malicious\ Vehicles} \tag{10}$$

$$R = \frac{Number\ of\ Truly\ Malicious\ Vehicles\ Detected}{Total\ Number\ of\ Truly\ Malicious\ Vehicles} \tag{11}$$

5.1.2. Simulation results

We use two series of simulations to evaluate the performance of the proposed mechanism from different perspectives, respectively. The first series of simulation aims to evaluate the Precision (P) and the Recall (R) of the system in detecting malicious vehicles from a temporal perspective, as shown in Figs. 4 and 5. The second series of simulations evaluates the performance of the system from the perspective of different percentages of malicious nodes, as shown in Figs. 6 and 7. Each series of simulations has 100 different random runs, which ensures that the initial properties of the vehicles are different from the set malicious nodes each time, and the obtained experimental results are averaged from the 100 simulation results to ensure the accuracy of the experimental data.

Figs. 4 and 5 depict the precision and recall metrics of the system when the ratio of malicious vehicle is set as 20%. The numbers of vehicles that travel in the simulation area are 50, 100 and 200, respectively. Due to the application of deep learning algorithm and blockchain technology, the system obtains high precision and recall rate. In particular, the accuracy and recall rate gradually increase as time increases, and a stable performance is obtained when the system runs for a certain time period (30 s). This is because as the time increases, the fully connected neural network(FCN) deployed inside the RSU can obtain more historical data of the vehicles, thus determining the credibility score and identifying malicious vehicles more accurately. The proposed deep learning

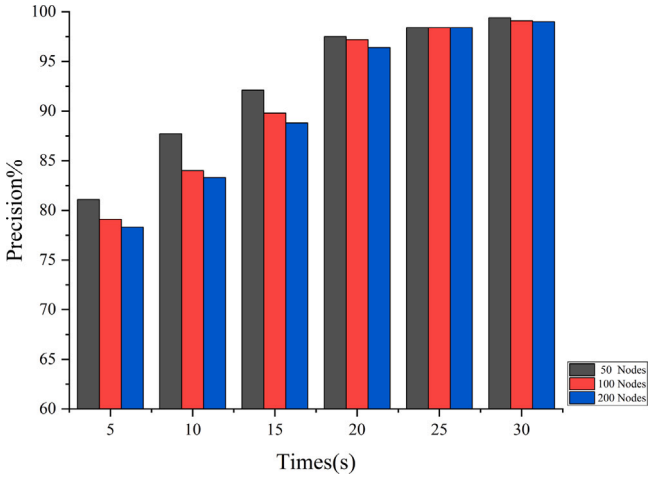

Fig. 4. Performance of precision with different number of vehicles under different time.

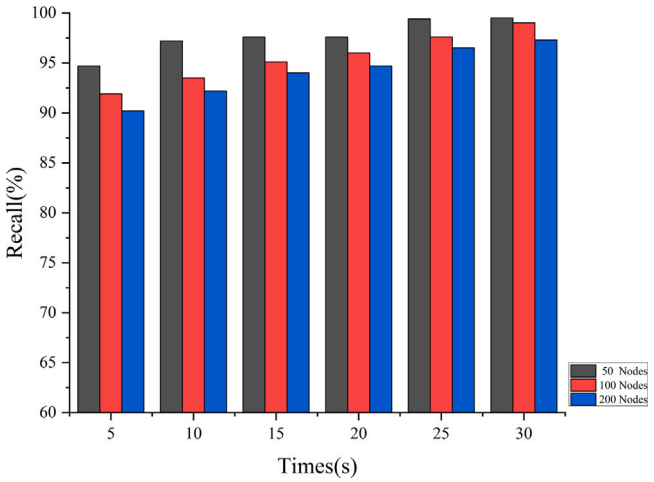

Fig. 5. Performance of recall rate with different number of vehicles under different time.

algorithm works well especially when a large amount of data is available, enabling the system to accurately identify malicious vehicles in the IoVs. Due to the limitation of the computational resources of RSUs, the system performance is higher when the number of vehicles in the network is small than that when the number of vehicles in the network is large. However, we can observe from Figs. 4 and 5 that after the system runs for 30 s, its accuracy and recall rate also stabilizes around 95% as the number of vehicles increases, satisfying our system requirements for detecting malicious vehicles. In addition, the application of blockchain technology will ensure the validity and authenticity of both vehicles and messages, thus resulting in a more accurate trust evaluation and detection of malicious vehicles.

Figs. 6 and 7 shows the precision and recall values for different numbers of nodes under varied malicious node percentages. The numbers of vehicles are set as 50, 100, and 200. It is clear from Figs. 6 and 7 that as the percentage of malicious nodes increases, its accuracy and recall performance decrease accordingly. This is reasonable because the higher the percentage of malicious nodes in the network, the more false messages are received by the RSU. It is also because the FCN model we designed is mainly based on the historical and current information uploaded by the vehicles to determine the trustworthiness of the messages, which makes it difficult to accurately assess the trust of the vehicles and successfully identify all malicious vehicles. However, when the percentage of malicious nodes reaches forty percent, the accuracy still remains around 85% and the recall rate remains around 90%, which proves the good performance of the proposed mechanism. Besides, the application of blockchain technology also ensures that the historical behavior of malicious vehicles can be queried, which helps the FCN algorithm to detect malicious vehicles more accurately. The combination of both technologies ensures the performance of our system.

In conclusion, we can see from Figs. 4 to 7 that the proposed mechanism performs good both with high and low number of nodes, and with a high percentage of malicious vehicles in the network.

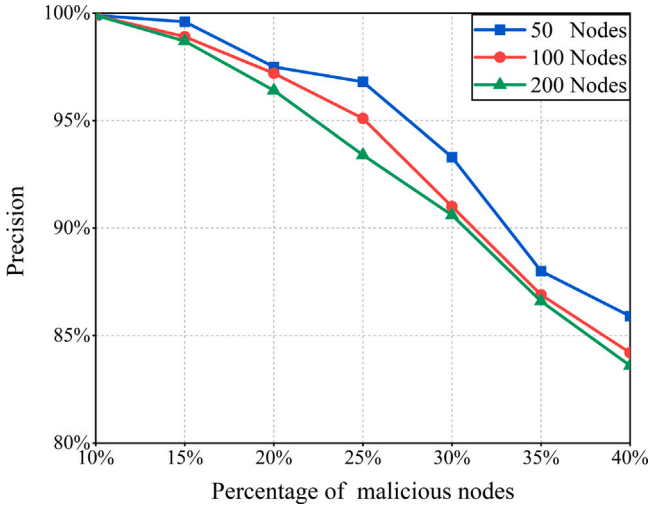

Fig. 6. Performance of precision with different number of vehicles under different malicious vehicle ratios.

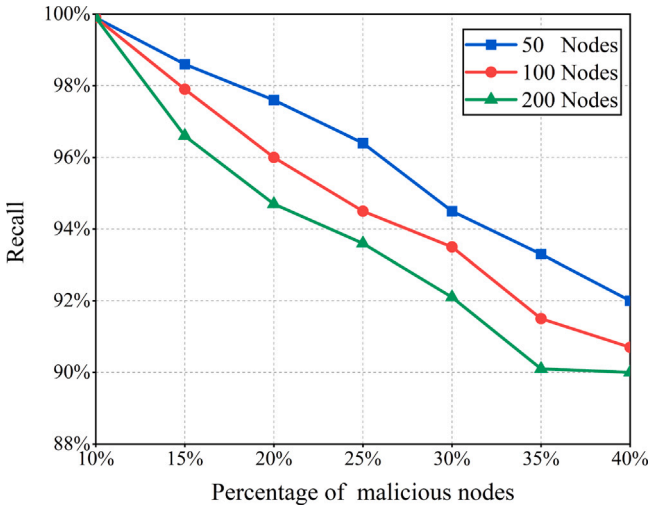

Fig. 7. Performance of recall rate with different number of vehicles under different malicious vehicle ratios.

5.2. Security analysis

Conditional privacy protection: This system provides conditional privacy protection because the identity of malicious vehicles can be disclosed by TA. In the system, each vehicle uses a public address as a pseudonym, which can be retrieved from the blockchain. A TA with superior access can easily find the malicious vehicle based on a stored list that records the relationship between the public address and the vehicle's identity.

Data integrity: In the system, the trust data of the vehicles recorded in the blockchain has been agreed upon with all authorized vehicles. The sequence of blocks are protected by using a hash chain. The hash value of each block is unique and once any content of any block is modified, the hash values of other blocks will be changed. Therefore, if an adversary wants to perform a message modification attack, he needs to not only modify the contents of the current block, but also recalculate the hash values of all blocks. Thus the data integrity is guaranteed.

RSU Compromise Attack: Since RSUs are distributed on the road and sometimes lack protection from network operators, they can be compromised by attackers. However, since this system places the blockchain on vehicles, even if a RSU is briefly compromised and returns the wrong information to vehicles, vehicle can view the data blocks generated based on the information returned to vehicles by other RSUs, to get the correct information and report the compromised data of this RSU to other RSUs, which in turn will be taken care of by the network operator.

6. Conclusion

In this paper, we propose a trust management system for connected vehicles using a combination of blockchain and deep learning techniques. In the proposed system, both vehicles and RSUs will be involved in the trust management process, and calculating the trust level of the information uploaded by vehicles, to help determining the trust degree of vehicles and identify malicious ones accurately. The designed FCN network provides a fast and accurate way to verify the truthfulness of information and to discriminate malicious vehicles from honest ones. Moreover, the public blockchain on vehicles support the system to achieve reliable and smart trust management in the open and dynamic IoV environment. Extensive simulations were conducted to verify and evaluate the performance of the proposed mechanism, and the experimental results show that the system can accurately and effectively assess the trust of nodes, and detect malicious nodes.

Data availability

This research uses the public dataset.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (Grant No. 61962032, 61561029), Yunnan Ten Thousand Talents Plan Young & Elite Talents Project, China, and Yunnan Province Fund for Excellent Young Scholars, China (Grant No. 202001AW070003).

References

[1] F. Tang, Y. Kawamoto, N. Kato, J. Liu, Future intelligent and secure vehicular network toward 6G: Machine-learning approaches, Proc. IEEE 108 (2) (2020) 292–307, http://dx.doi.org/10.1109/JPROC.2019.2954595.
[2] J. Contreras-Castillo, S. Zeadally, J.A. Guerrero-Ibañez, Internet of vehicles: Architecture, protocols, and security, IEEE Internet Things J. 5 (5) (2018) 3701–3709, http://dx.doi.org/10.1109/JIOT.2017.2690902.
[3] Z. Li, X. Yang, Y. Chen, J. Zhang, Application of wireless communication in intelligent distribution network communication technology, in: 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 1879–1883, http://dx.doi.org/10.1109/IWCMC51323.2021.9498881.
[4] S. He, D.H. Shin, J. Zhang, J. Chen, Y. Sun, Full-view area coverage in camera sensor networks: Dimension reduction and near-optimal solutions, IEEE Trans. Veh. Technol. 65 (9) (2016) 7448–7461.
[5] Q. Yao, T. Li, C. Yan, Z. Deng, Accident responsibility identification model for internet of vehicles based on lightweight blockchain, Comput. Intell. (2022) 0824–7935, http://dx.doi.org/10.1111/coin.12529.
[6] X. Chen, H. Zhang, F. Zhao, Y. Hu, C. Tan, J. Yang, Intention-aware vehicle trajectory prediction based on spatial-temporal dynamic attention network for internet of vehicles, IEEE Trans. Intell. Transp. Syst. (2022) 1–13, http://dx.doi.org/10.1109/TITS.2022.3170551.
[7] X. Kong, B. Zhu, G. Shen, T.C. Workneh, Z. Ji, Y. Chen, Z. Liu, Spatial-temporal-cost combination based taxi driving fraud detection for collaborative internet of vehicles, IEEE Trans. Ind. Inf. 18 (5) (2022) 3426–3436, http://dx.doi.org/10.1109/TII.2021.3111536.
[8] C. Song, W. Xu, T. Wu, S. Yu, P. Zeng, N. Zhang, QoE-Driven edge caching in vehicle networks based on deep reinforcement learning, IEEE Trans. Veh. Technol. 70 (6) (2021) 5286–5295, http://dx.doi.org/10.1109/TVT.2021.3077072.
[9] O. Kaiwartya, A.H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, X. Liu, Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects, IEEE Access 4 (2016) 5356–5373, http://dx.doi.org/10.1109/ACCESS.2016.2603219.
[10] Z. Lu, G. Qu, Z. Liu, A survey on recent advances in vehicular network security, trust, and privacy, IEEE Trans. Intell. Transp. Syst. 20 (2) (2019) 760–776, http://dx.doi.org/10.1109/TITS.2018.2818888.
[11] C. Lai, K. Zhang, N. Cheng, H. Li, X. Shen, SIRC: A Secure incentive scheme for reliable cooperative downloading in highway VANETs, IEEE Trans. Intell. Transp. Syst. 18 (6) (2017) 1559–1574, http://dx.doi.org/10.1109/TITS.2016.2612233.
[12] X. Huang, Y. Rong, J. Kang, Z. Yan, Distributed reputation management for secure and efficient vehicular edge computing and networks, IEEE Access 5 (2017) 25408–25420, http://dx.doi.org/10.1109/ACCESS.2017.2769878.
[13] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, Y. Ji, Decentralized trust evaluation in vehicular internet of things, IEEE Access 7 (2019) 15980–15988, http://dx.doi.org/10.1109/ACCESS.2019.2893262.
[14] R. Shrestha, S.Y. Nam, R. Bajracharya, S. Kim, Evolution of V2X communication and integration of blockchain for security enhancements, Electronics 9 (9) (2020) 1338.
[15] T.A. Butt, R. Iqbal, K. Salah, M. Aloqaily, Y. Jararweh, Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions, IEEE Access 7 (2019) 79694–79713, http://dx.doi.org/10.1109/ACCESS.2019.2922236.
[16] Z. Zhu, G. Qi, M. Zheng, J. Sun, Y. Chai, Blockchain based consensus checking in decentralized cloud storage, Simul. Model. Pract. Theory 102 (2020) 101987.
[17] Z. Zheng, S. Xie, H.N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.
[18] S. Li, F. Li, K. Wang, G. Qi, H. Li, Mutual prediction learning and mixed viewpoints for unsupervised-domain adaptation person re-identification on blockchain, Simul. Model. Pract. Theory 119 (2022) 102568.
[19] K. Wang, Z. Liu, Z. Zhu, G. Qi, J. Yao, G. Miao, Formation optimization of blockchain-assisted swarm robotics systems against failures based on energy balance, Simul. Model. Pract. Theory 120 (2022) 102599.
[20] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2084–2123, http://dx.doi.org/10.1109/COMST.2016.2535718.
[21] Khan, Minhaj, Ahmad, Salah, Khaled, IoT Security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. Fgcs 82 (2018) 395–411, http://dx.doi.org/10.1016/j.future.2017.11.022.
[22] Q. Li, A. Malip, K.M. Martin, S.L. Ng, J. Zhang, A reputation-based announcement scheme for VANETs, IEEE Trans. Veh. Technol. 61 (9) (2012) 4095–4108.
[23] M. Raya, P. Papadimitratos, V.D. Gligor, J.P. Hubaux, On data-centric trust establishment in ephemeral Ad Hoc networks, in: IEEE INFOCOM 2008 - the 27th Conference on Computer Communications, 2008, pp. 1238–1246, http://dx.doi.org/10.1109/INFOCOM.2008.180.
[24] D.B. Rawat, G. Yan, B.B. Bista, M.C. Weigle, Trust on the security of wireless vehicular Ad-hoc networking, Ad Hoc Sens. Wirel. Netw. 24 (3–4) (2014) 283–305.

[25] R. Hussain, W. Nawaz, J.Y. Lee, J. Son, J.T. Seo, A Hybrid Trust Management Framework for Vehicular Social Networks, Vol. 9795, Springer International Publishing, 2016, pp. 214–225.
[26] W. Li, H. Song, ART: AN attack-resistant trust management scheme for securing vehicular Ad Hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2016) 960–969.
[27] T. Pham, C.K. Yeo, Adaptive trust and privacy management framework for vehicular networks, Veh. Commun. 13 (2018) 1–12.
[28] Y. Inedjaren, M. Maachaoui, B. Zeddini, J.P. Barbot, Blockchain-based distributed management system for trust in VANET, Veh. Commun. 30 (2021) 100350.
[29] X. Liu, H. Huang, F. Xiao, Z. Ma, A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs, IEEE Internet Things J. 7 (5) (2020) 4101–4112.
[30] D. Wang, X. Chen, H. Wu, R. Yu, Y. Zhao, A blockchain-based vehicle-trust management framework under a crowdsourcing environment, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1950–1955, http://dx.doi.org/10.1109/TrustCom50675.2020.00266.
[31] Z. Yang, K. Yang, L. Lei, K. Zheng, V. Leung, Blockchain-based decentralized trust management in vehicular networks, Vol. 6, no. 2, 2019, pp. 1495–1505. http://dx.doi.org/10.1109/JIOT.2018.2836144.
[32] H.E. Sayed, S. Zeadally, D. Puthal, Design and evaluation of A novel hierarchical trust assessment approach for vehicular networks, Veh. Commun. 24 (2020) http://dx.doi.org/10.1016/j.vehcom.2019.100227.
[33] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.
[34] P. Álvarez López, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, E. Wießner, Microscopic traffic simulation using SUMO, 2018, pp. 2575–2582, http://dx.doi.org/10.1109/JIOT.2018.2836144.
[35] Website, http://www.openstreetmap.org.