IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 16, 2020, accepted March 23, 2020, date of publication March 30, 2020, date of current version April 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2983994

An Efficient and Secure Data Transmission Mechanism for Internet of Vehicles Considering Privacy Protection in Fog Computing Environment

WENJUAN ZHANG[1] **AND GANG LI**[2]

[1]Institute of Information Security, Zhoukou Normal University, Zhoukou 466001, China
[2]School of Road and Bridge Engineering, Xinjiang Vocational and Technical College of Communications, Ürümqi 831401, China

Corresponding author: Wenjuan Zhang (wdwyyx158@163.com)

This work was supported in part by the Henan Department of Science and Technology Research Project under Grant 182102311126, and in part by the Henan Education Department Natural Science Research Project under Grant 16A520106.

ABSTRACT Aiming at the problems for existing data transmission mechanisms in Internet of vehicles, such as real-time performance, high efficiency of computing tasks, vehicle data privacy, etc., this paper proposes an efficient and secure data transmission mechanism for Internet of vehicles considering privacy protection in fog computing environment. Firstly, this paper proposes a system model and main message attack model for Internet of vehicles in fog computing environment, and designs a data transmission system based on privacy protection to improve data transmission efficiency in Internet of vehicles and protect the privacy information of vehicle users. Then, the task allocation and data aggregation mechanism of privacy protection is proposed in the crowd-sensing model based on the assistance of fog nodes, and the location prediction method based on social infection theory is used to predict the vehicle location for better allocating network resources. Finally, for the selfishness of end users in Internet of vehicles, selfish node incentive mechanism based on Robin Steiner bargaining game model is proposed to encourage selfish nodes to perform data transmission and reduce time delay. Operational network environment simulation software is used to carry out experiments. The experimental results show that when malicious nodes and selfish nodes exist in the Internet of Vehicles, the proposed method has stronger competitiveness in resisting attacks and improving the efficiency of message transmission compared with other methods, which can achieve efficient and secure data transmission.

INDEX TERMS Fog computing, Internet of Vehicles, privacy protection, location prediction, game theory, selfish node incentive mechanism, data aggregation mechanism.

I. INTRODUCTION

As an important part of social infrastructure, the safety and efficiency of urban transportation networks have a direct impact on urban development and people's daily lives. With the rapid development of wireless communication technologies, sensing technologies, mobile computing and automation control technologies, The concept of Internet of Vehicles (IoV) came into being and became an indispensable component in the realization of Intelligent Transportation System (ITS) and autonomous driving [1], [2], which is highly valued by the government, academia and industry. IoV technologies are based on the coordinated communication between cars and cars, cars and people, cars and roads, cars and clouds (platforms), enabling data transmission and information intercommunication between cars and all systems. It supports a variety of applications in IoV based on the transmission of car driving information, road state information, traffic warning information, and mobile services [3].

There are two main factors for the rapid development of IoV. On the one hand, there is an urgent need for improving the safety and efficiency of road traffic management systems [4]. With the continuous acceleration of urbanization, the number of urban vehicles has also increased dramatically. As a result, this results in transportation, economic and environmental issues, including huge economic costs such as traffic congestion and accidents, environmental pollution and destruction [5]. On the other hand, the demand for mobile

The associate editor coordinating the review of this manuscript and approving it for publication was Honghao Gao.

data and high-speed mobile Internet services are increasing sharply on the road. The network connection solution based on IoV can not only satisfy the requirements of mobile data, but also enrich security-related applications such as online diagnosis, intelligent anti-theft and tracking. And the servers of these applications are in internet cloud [6], [7]. However, the guarantee of node data transmission quality in IoV, as a prerequisite to achieve various application services, is one of the key issues studied by researchers in various countries [8].

While ensuring efficient and reliable wireless data transmission in IoV, more and more attention has been paid to the communication security and privacy issues of IoV [9], [10]. Since the security and privacy protection of IoV itself will directly affect the personal and property safety of participants such as drivers, passengers and car owners, information security and privacy protection are issues that must be resolved before IoV is actually deployed and applied.

However, the IoV environment has its own particularities, which is quite different from the Internet and Internet of Things. Thus, the security mechanisms applicable to traditional networks are not well applicable to this dynamic self-organized multi-hop wireless network, and the traditional network architectures are not suitable for the dynamic, flexible and efficient scenario of IoV [11]. And as the development of IoV becomes more and more intelligent, the connected equipment are more and more diversified, the required service functions are becoming more and more abundant, the more new risk problems faced by IoV are increasing. There are many types of information attacks in IoV, such as eavesdropping, tampering, forgery, privacy leaks, node capture and replication, witches and other forms of attack [13]. Besides, there is an urgent need to study the security mechanism for information security problem of IoV. On the basis of ensuring the safe and efficient transmission of IoV information, IoV technologies can play more uses in the safe operating environment and better realize the functions of IoV [14], [15]. Therefore, the research on information security mechanism for IoV becomes the focus of current scholars' research, which has high theoretical research value.

II. RELATED RESEARCH

The Internet of Things contains a large number of terminal equipment. Most of them have only limited computing, storage, and communication capabilities, hence they need to rely on cloud platforms to enhance node information processing capabilities [16]. Mobile cloud computing can provide powerful computing and storage capabilities for terminals, however, the high latency of data processing from remote cloud center to end users is not suitable for the application scenario of IoV where real-time application demand is strong. For this reason, the concept of fog computing is proposed. It transforms the association of cloud services with networks to connect users' near-end computing or storage resources to networks, which can significantly reduce transmission delay and jitter [17]. Fog computing is recognized as a key technology for real-time interaction of the Internet of Things (such as IoV). Reference [18] designed an efficient load forecasting mechanism for IoV, which offloaded the computing tasks through fog nodes. Considering vehicle delay, location information and scalability, reference [19] proposed an intelligent IoV architecture based on collaborative fog computing. Its goal is to process the multi-source data generated for IoV in a distributed manner. However, research on vehicle fog computing at home and abroad is still in its infancy, which cannot guarantee the privacy of users and prevent intrusion by illegal users [20].

Due to personal privacy protection is particularly important in the data distribution mechanism of IoV, a lot of research has been carried out on privacy protection schemes in IoV. They are roughly divided into three categories: anonymous schemes, cryptographic schemes and signature schemes. Among them, there are mainly three types of authentication protocols based on cryptosystems [21]: authentication system based on Public Key Infrastructure (PKI), Identity-based Encryption (IBE) and authentication system based on Certificateless Public Key Cryptography (CL-PKC). Reference [22] proposed a certificate-based authentication system, and designed a two-factor authentication mechanism based on smart cards. It provides anonymous authentication and location privacy policies, but cannot support vehicle-to-vehicle communication. Reference [23] proposed an identity-based authentication scheme. This solution is based on a bilinear pairing algorithm, supports batch authentication and has low computational energy consumption. However, this scheme cannot resist forgery attacks. Attackers can forge a legitimate vehicle identity and send false information to the IoV that cannot be detected. Reference [24] proposed an identity-based fast authentication scheme, which can reduce computing energy consumption, which supports batch authentication and privacy protection. However, this scheme relies heavily on secure communication channels. In the secret key distribution process, each secret key needs to be transmitted to users by a secure communication channel, otherwise it will cause a large area of user key leakage.

In addition, the real-time and reliable propagation of various messages cannot be separated from connected network systems in IoV. Connectivity determines the performance of entire networks. With regard to the research on the connectivity of IoV, with the joint efforts of scholars at home and abroad, preliminary results have been achieved. Reference [25] studied the multi-hop transmission based on relay technology and used multi-hop communication to transmit information to vehicle nodes outside the range of vehicle one-hop communication. It reduces transmission cost while expanding the vehicles' connectivity range, enabling information to be transmitted to further vehicles. Reference [26] evaluated the connectivity probability between vehicles under the Nakagami fading channel model and proposed that cooperation between vehicles can improve the connectivity of vehicle networks. However, too much vehicle cooperation can also cause interference. With the development of 5G communication technologies, IoV will integrate more types of

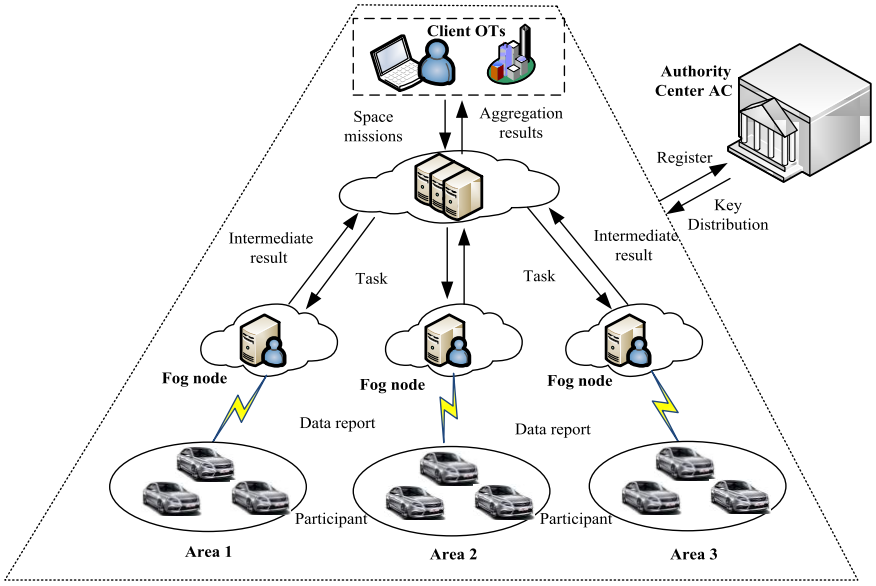

FIGURE 1. Overall framework of the proposed method.

networks and emerging technologies to provide high-quality connectivity. While ensuring the connectivity of IoV, it is necessary to reduce the response delay and energy consumption of networks to improve service performance. Reference [27] discussed the service delays in forwarding routing. In order to reduce the energy consumption of systems, the choice of delay metric was considered. Reference [28] proposed various topology control algorithms focusing on interference constraints and delay reduction. Most studies have reduced energy consumption by improving technical issues within the network. Few studies also consider the use of external conditions to reduce network energy consumption, so as to reasonably select relay nodes.

Due to the problems of poor real-time performance, low transmission efficiency and threats to users' privacy for the existing data transmission mechanism in IoV, this paper proposes an efficient and secure data transmission mechanism for IoV that considers privacy protection in the fog computing environment. The main innovations of this paper are summarized as follows:

1) In order to alleviate the load of terminal equipment and improve the transmission efficiency of IoV, an IoV system model in fog computing environment is proposed. It offloads the computing load of terminal equipment to fog nodes, which reduces system overhead.

2) In crowd-sensing model based on the assistance of fog nodes, a privacy-based task assignment and data aggregation mechanism is proposed. It uses a secure addition aggregation protocol to verify the integrity of data and ensure data security.

3) Selfish nodes are less considered in the existing data transmission mechanism of IoV, and they have a greater impact on the system. Therefore, the selfish node incentive mechanism of Robbins-Stein bargaining game model based on game theory is proposed to encourage selfish nodes to perform data transmission, thereby reducing system time delay and energy consumption.

III. SYSTEM MODEL AND ATTACK MODEL

A. SYSTEM MODEL

The IoV system in fog computing environment includes: awareness platform (also known as crowdsourcing platform / server, referred to as Server), data collectors / task owners (TOs), a series of fog nodes, participation vehicles and an authority center (AC), as shown in Figure 1.

The specific entities in the system are described as follows:

Awareness platform / crowdsourcing server Server: Service provider, providing data aggregation services for TOs. That is, after receiving the encrypted tasks of TOs, awareness platform assigns the tasks to fog nodes in the corresponding sensing area. And when users submits the awareness data, awareness platform and fog nodes jointly calculate the encrypted aggregation results, and return aggregated cipher text to TOs [29], [30].

Data collectors / task owners TOs: task publishers, which may be individuals, enterprises or other organizations. TOs want to obtain the perceptual data aggregation information in a certain perceptual area. Due to its limited perception and computing capabilities, it is necessary to outsource aggregation tasks to the awareness platform. It also provides some compensation information to encourage users to participate in tasks.

Fog nodes: They are deployed at the edge of networks and close to mobile equipment terminals as a relay node for mobile terminals and awareness platforms. That is, each fog node covers a geographical area, it is responsible for task

assignment and data collection in that area. After collecting the encrypted data submitted by users in the area, fog nodes and awareness platforms cooperate to calculate the aggregation results and send them to awareness platforms for further processing. Besides, when fog nodes receive users' awareness data, they can detect invalid data sent by external attackers.

Participants / Users: A mobile user who carries mobile equipment. Mobile users utilize GPS and other equipment to freely collect awareness data according to the requirements of tasks. To protect data privacy, data needs to be encrypted before it is submitted to fog nodes.

Authority center AC: trusted third party. AC is responsible for initializing the entire system, registering all entities and assigning keys to each entity. After the initialization phase, AC can choose to be online or offline according to whether it supports new users to join the system. If new users are allowed to join the system, AC needs to stay online, but will not participate in the task assignment and data aggregation process.

B. ATTACK MODEL

In the system model, it is assumed that there are three kinds of nodes: legal nodes, selfish nodes and malicious nodes. Legal nodes fully cooperate with the message transmission process. Selfish nodes tend to transmit data with nodes that have a closer social relationship. Malicious nodes attack the system to gain profits and disrupt the network order. Three types of attacks are considered, as shown in Figure 2.

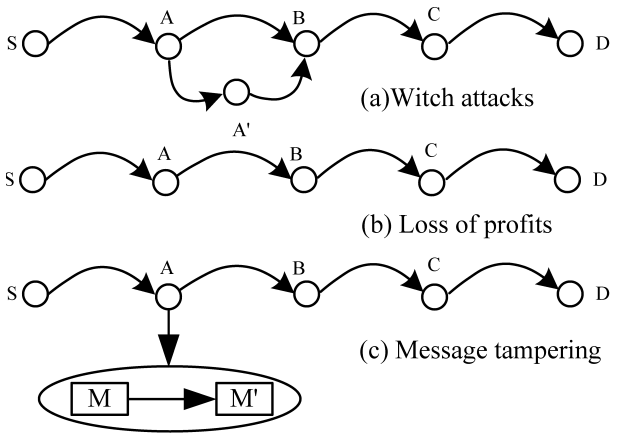

FIGURE 2. Three attack models.

1) Sybil attack: A malicious node can obtain additional profits by forging virtual nodes on the path of message transmission. Node A forges node A' and places A' between itself and node B. Then all rewards received by node A' will belong to node A.

2) Packet loss profits attack: In order to get rewards, the attacker can pretend to be willing to pass messages to other nodes. When the message is received, it is discarded. Attacker A drops the message before it delivers it to the next-hop node B.

3) Message tampering attack: The attacker tampers with the content of messages, thereby misleading the behavior of destination nodes. In addition, the node reward message sent by cloud server may be tampered to facilitate the attacker to gain more benefits. Attacker A modifies message M into message M' and sends it to other nodes.

Moreover, three aspects of privacy are considered in the proposed attack model [31]: data, social attribute and transaction privacy. The packet loss profits attack will leak users' data privacy, the message tampering attack will lead to the leakage of data and transaction privacy information. The Sybil attack conflicts with privacy protections, since the better the information is protected, the easier it is for attackers to launch Sybil attacks. In addition, if a legal node communicates with a witch node, attribute-based privacy information is easily leaked by the mobile prediction phase [32]. Besides, fog nodes can send passive attacks to obtain vehicle privacy information, and can also collaborate with malicious nodes to obtain data during the message transmission phase.

IV. DATA TRANSMISSION SYSTEM DESIGN BASED ON PRIVACY PROTECTION

In order to improve the transmission efficiency of messages in IoV and protect the privacy information of vehicle users, a data transmission system based on privacy protection is designed. In the two-tier structure of cloud system model, a message transmission mechanism based on privacy protection is proposed. The mechanism consists of three parts, namely mobile prediction, message processing and node incentive protection mechanism. When a node generates a message, it needs to find a transmission path for the message to reach the destination node. The mobile prediction module can efficiently and securely find a suitable next-hop routing node for a message. The message processing module combines attribute-based encryption policies with the routing process to protect users' data privacy [33]. The node incentive protection module records the relay node's reward to local cloud server in an encrypted manner and is used to protect the transaction privacy information of vehicles.

For the message transmission process, the operation of entire system is described as follows: When node v_i meets node v_j, node v_i is based on Security Multiparty Computation (SMC) by comparing Ego Betweenness and Contact Delay Estimation to determine whether v_j is suitable as a next hop relay node. When node v_i moves to the range covered by the signal of fog node c_l, node v_i first encrypts the local message through a symmetric encryption algorithm. Then it uses attribute-based encryption algorithms to encrypt the keys of the symmetric encryption algorithm. At the same time, fog node c_l verifies the report information uploaded by node v_i and calculates the reward of each relay node. Fog node c_l re-encrypts the key uploaded by nodes and periodically synchronizes information with the remote cloud (Server).

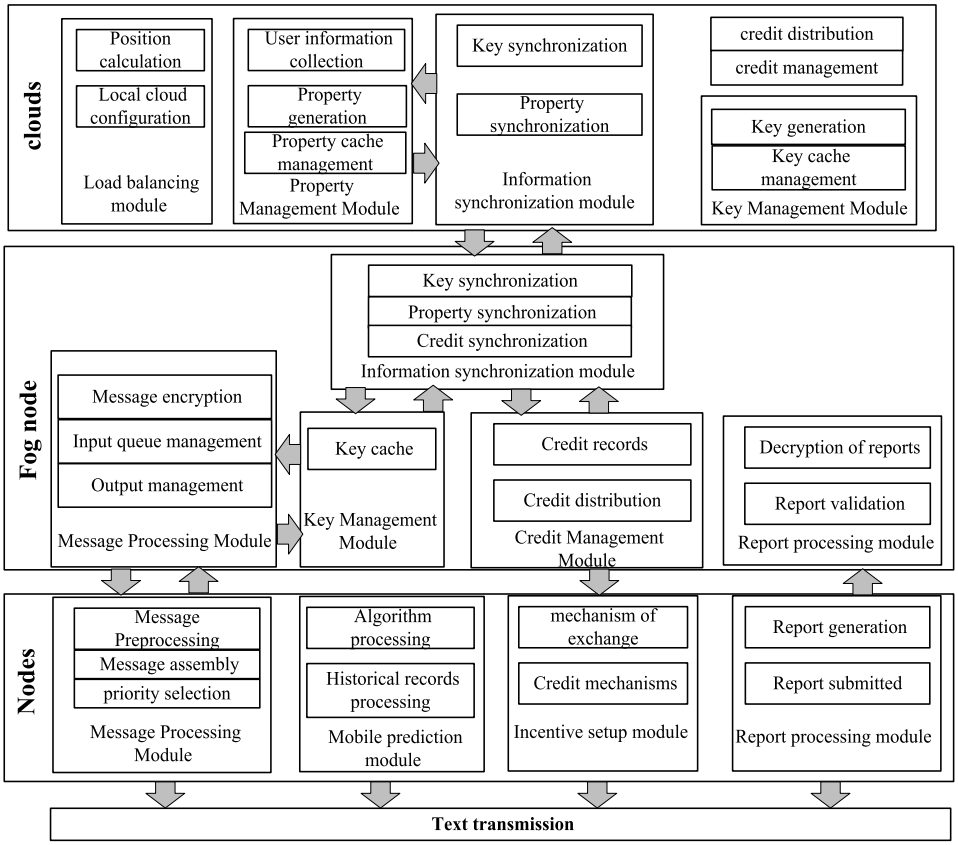

FIGURE 3. System model based on two-tier cloud server.

A. SYSTEM MODEL BASED ON TWO-TIER CLOUD SERVER

Cloud computing is considered an effective means of offloading. The terminal equipment can offload the computing load to fog nodes to improve its performance. At the same time, a third-party trusted institution can authorize some of its functions to fog nodes. This can overcome the shortcomings that nodes cannot communicate directly with third-party trusted institutions due to the instability of wireless links and the high cost of cellular communication. The established system architecture based on two-tier cloud server is shown in Figure 3. It has the following advantages: 1) Offloading the computing load of terminal equipment to fog nodes can alleviate the load of terminal equipment. 2) The robustness of the system is enhanced. If one fog node fails, others can still guarantee the normal operation of system. 3) The terminal equipment uses wireless communication technologies to send and receive messages for reducing the users' overhead.

The remote cloud includes five modules: load balancing module, property management module, key management module, information synchronization module and credit management module. The load balancing module balances the load between fog nodes by placing fog nodes in a suitable place. The property management module manages its property information obtained from the vehicle registration information. The key management module manages the keys involved in system. The information synchronization module is responsible for synchronizing the information between the remote cloud and fog nodes. The credit management module is responsible for the credit update and maintenance of all vehicles in the management system [34].

Each fog node includes five parts: message processing module, credit management module, report processing module, key management module and information synchronization module [35]. The message processing module can encrypt messages for nodes, the credit management module is used to manage the credit value of corresponding nodes. The report processing module is used to verify the report message uploaded by destination nodes and provide the reward list to the credit management module. The key management module manages the conversion key of vehicles and can provide it to other required modules. The information synchronization module is responsible for regularly performing information synchronization with the remote cloud.

Each terminal equipment includes four functional modules: message processing module, mobile prediction module, incentive setup module and report processing module. The message processing module pre-processes messages that need to be transmitted, including message and key encryption processing. The mobile prediction module establishes a mobile prediction model and guides nodes to reasonably

select the next hop routing node. The incentive setup module encourages users to transmit data and records the virtual currency obtained by vehicles according to the adopted incentive mechanism. The report processing module is responsible for generating the recorded vehicle reward report message and adding it to the end of messages to be transmitted [36].

B. MESSAGE TRANSMISSION MECHANISM BASED ON PRIVACY PROTECTION

There are three types of communication in the system: communication between terminal equipment; communication between terminal equipment and fog nodes; communication between fog nodes and remote clouds. When a node is ready to exchange data with another node, the mobile prediction module analyzes their historical encounter information. If the meeting node is suitable for message transmission, the ordering sub-module in message module prioritizes the messages to be sent in the local cache. The incentive setup module implements corresponding incentive mechanism to increase the participation of nodes. At the same time, the report processing module records the transaction price finally negotiated by the two nodes and forms a report message, and places the report at the end of messages to be transmitted. When nodes moves into the coverage of a fog node signal, nodes can communicate with fog nodes to pre-process the messages that need to be sent and obtain corresponding rewards.

The fog node synchronizes information with the remote cloud by synchronization management module, including the users' registration information and the generated conversion key. When a vehicle joins the network for information registration for the first time, remote cloud's property management module converts the vehicles' input into attribute information. The key management module generates various keys according to property information generated by vehicles.

V. PROPOSED DATA FORWARDING MECHANISM

A. POSITION PREDICTION

In this paper, we first use second-order Markov to build a vehicle movement model for position prediction. Then the large-scale trajectory data is compressed to obtain a consistent subset of the trajectory dataset. Furthermore, a vehicle similarity calculation method based on moving trajectory is proposed, and a vehicle group with high similarity to the measured vehicle is found in the trajectory data subset. Finally, the movement model of the vehicle group is used to modify the results of position prediction.

In the mobile environment, system records its movement data through the mobile equipment of vehicles, that is, location information at various times. The location information may be absolute location information (such as GPS coordinates) or relative location information (connected AP location information instead of mobile equipment location information). The system uses the user's current mobile data or historical data to build mobile model, and then uses the mobile model to predict the user's next location.

Suppose there are n cars in current scene, and the set of cars is $U = \{u_1, u_2, \cdots, u_i, \cdots, u_n\}$. There are m locations in current scene, and the location set $L = \{l_1, l_2, \cdots, l_m\}$ is set. Assume that the collected user movement data is initialized to $D = \{D_1, D_2, \cdots, D_n\}$, where $D_i\,(d_1, d_2, \cdots)$ contains all the movement data of vehicles in this scene. The proposed method combines the movement trajectories of vehicles under test and the changes that vehicles under test may make under the influence of a strongly correlated vehicle group, which obtains the prediction results. In addition, the Markov chain model is used to model the vehicle's movement data to obtain a vehicle state transition matrix. And among all vehicles, C_i, $C_i\,\{u\,|u \in U\}$ consisting of k u_i whose trajectory is most similar to vehicles under test are selected. Synthesize the state transition matrix of each vehicle in u and C_i to get the movement prediction model of u_i.

The proposed method uses second-order Markov chain model to model the vehicle movement data. $X = \{X_1, X_2, \cdots, X_M\}$ is the current state of vehicles in the model, m is the number of states, and X_i is the two consecutive locations in the movement trajectory. $Y = \{Y_1, Y_2, \cdots, Y_n\}$ is the set of transition states, and n is the total number of states. Then the state transition matrix is:

$$p_i = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mn} \end{pmatrix} \tag{1}$$

In the formula, $p_{mn} = \frac{q_{mn}}{q_m}$ is the probability that the vehicle departs from X_m to Y_n, where q_{mn} is the number of times the vehicle departs from X_m to Y_n, and q_m is the total number of visits to various locations.

Vehicle trajectory similarity calculation. First, the vehicle's movement data is converted into trajectory data, which is $Traj_i = \left\{(l, t_d)_t, \cdots\right\}$, where t_d is the dwell time of location l. Then, the trajectory set $Traj = Traj_1 \cup Traj_2 \cup \cdots \cup Traj_n$ is segmented to obtain vehicle u_i trajectory segment set $Tr_i = \{trace_1, \cdots, trace_n\,|trace_i \in L\}$. The global trajectory segment set $Tr_{total} = Tr_1 \cup \cdots \cup Tr_n$ is obtained by merging all vehicle trajectory segments. Suppose that Tr_{total} has a total of m elements, number all its segments, and convert Tr_i to an m dimensional vector $V_i = \{v_1, v_2, \cdots, v_m\}$, where v_i corresponds to the track segment labeled i in Tr_{total}. The similarity of any two vehicles u_i and u_j in the vehicle set can be expressed as $count\left(v_i \wedge v_j\right)$, the number after the statistical operation is 1, the larger the number, the higher the similarity of vehicle trajectories.

The location prediction method in mobile scene is shown in Figure 4. First, the data fusion component collects real-time information of the vehicles connected by each AP, converts them into vehicle movement data $d\,(uid, t, l)$, and stores them in a local database. Trajectory location prediction (TLP) algorithms retrieve vehicle movement data from a database to establish vehicle location prediction model, and stores the established model. When an external service sends a location prediction request for the vehicle u_i to TLP,

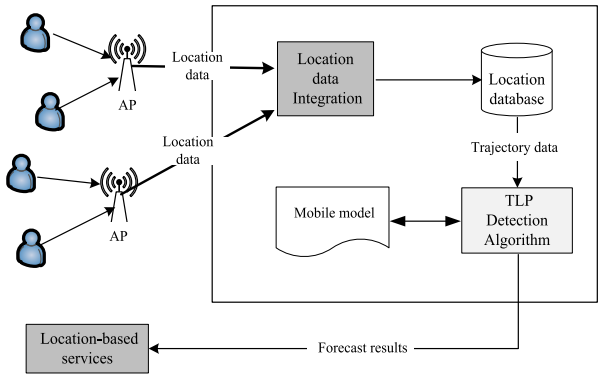

FIGURE 4. Proposed position prediction algorithm.

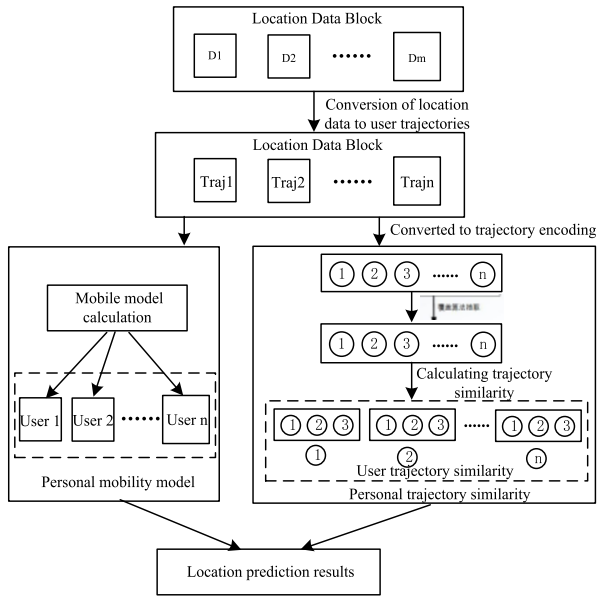

FIGURE 5. Processing flow of TLP algorithm.

TLP transfers location prediction model of u_i, and outputs prediction results to the external service after calculation.

The proposed TLP algorithm is a location prediction method based on social infection theory. In the big data environment, this algorithm predicts vehicle movements and corrects the prediction results of nodes by the movement law of group. The processing flow of TLP algorithm is shown in Figure 5.

First, all vehicle movement data is obtained, the trajectory data $Traj_i$ of each vehicle is obtained after conversion. Next, scan $Traj_i$ to get the state set X, Y, and then get the state transition matrix p_i. Next, TLP uses the coverage idea to extract a consistent subset U_{sub} of vehicles, and calculates the similarity between vehicle trajectory data of $Traj_i$ and U_{sub} to obtain the vehicle trajectory similarity group C_i. Integrate the state transition information of p_i and vehicles with similar trajectories to obtain the vehicle position prediction model $P\_predict_i$. When TLP receives a request for external service location prediction, it returns the predicted location lp to the external service according to $P\_predict_i$.

B. DATA PRIVACY PROTECTION

Based on crowd-sensing model for the assistance of fog nodes, this paper proposes a privacy aware task allocation and data aggregation (PTAA) mechanism. PTAA includes five phases: system initialization, task generation and distribution, data collection and aggregation, decryption of aggregation results, and the selection of updates to aggregation results according to task requirements.

1) System initialization: This phase is performed on AC side and includes two sub-steps: Setup, entity registration and key distribution. First, AC generates system parameters in Setup, and then responsible for registering the system entities and assigning them the appropriate keys.

When each entity registers, AC selects the random number $s \in Z_p^*$ as server's private key, and calculates $S = g^s$ as the public key. For each data collector (TO) o_j and participant P_i, AC executes $KeyGen\ (sp)$ algorithm and generates a key pair (sk_j, pk_j) , (sk_i, pk_i). Moreover, AC randomly selects $p_i \in Z_p^*$ as the private key of fog node f_i, and calculates the public key g^{p_i}. Select a random number $\alpha_i \in Z_p^*$ and calculate $A' = (g^{\alpha})^{1/\alpha}$. AC sends α to all fog nodes and A' to Server.

2) Task generation and distribution: At this stage, TO generates aggregate statistics tasks and sends them to Server. Server performs the task privacy protection allocation process with the assistance of fog nodes. Suppose there are m TOs in the system, and it is written as $O = \{o_1, o_2, \cdots, o_m\}$. In the process that TO $o_i \in O$ obtains the data aggregation results in a sensing area, in order to protect the privacy of tasks, o_i selects two random numbers $r_1, r_2 \in Z_p^*$ and encrypts task $\upsilon_i = (\upsilon_i^c, \upsilon_i^o, \upsilon_i^l, \upsilon_i^t)$ in the following way:

$$c_1 = \left(\upsilon_i^c \left\| \upsilon_i^o \right\| \upsilon_i^l \| \upsilon_i^t \right) e\,(S,h)^{r_1}\, G^{r_2}, c_2 = h^{r_1}, c_3 = A^{r_2} \tag{2}$$

where υ_i^c is the task content, υ_i^o is the aggregate statistical operation, υ_i^l and υ_i^t are the perceived position / area and task expiration time respectively. G^{r_i} is a multiplicative cyclic group, $G = e\,(g, h)$. In order not to reveal the exact perceived position of task υ_i, o_i replaces υ_i^l with a fuzzy sensing area υ_i^r and sends message $< c_1, c_2, c_3, \upsilon_i^r, \sum pk_i >$ to server.

After receiving the above message, Server assigns a series of tasks $\Gamma = \{\upsilon_1, \upsilon_2, \cdots, \upsilon_m\}$ to the corresponding fog node set $\Im = \{f_1, f_2, \cdots, f_k\}$ according to υ_i^r. For each candidate fog node $f_j \in \Im_i$, based on the dual nature, there is $\varphi_j = e\,(g^{p_j}, h^{r_1})^s = G^{p_j \cdot r_1 \cdot s}$. Server sends $< i, c_1, c_1', \varphi_j, \sum pk_i, \upsilon_i^o >$ to f_j, and f_j uses its private key p_j and the secret α sent by AC to decrypt to obtain the specific task requirements:

$$\upsilon_i^c \left\| \upsilon_i^o \right\| \upsilon_i^l \| \upsilon_i^t = \frac{c_1}{c_1^{1/\alpha} \cdot \varphi_j^{1/p_j}} \tag{3}$$

Then, f_j broadcasts decrypted task requirements to the local participants and grants task permissions to the participants by issuing task secrets.

3) Data submission and aggregation: In order to protect perceived data privacy and resist external attacks, participants encrypt the data and send it to the corresponding fog nodes. At the same time, participants also attached some verification information to prove their authority to participate in the task (authorized participants) and the integrity of data. After fog nodes are successfully verified, it cooperates with the server to perform statistical aggregation on all sensed data according to the task aggregation operation requirements. Throughout the aggregation process, neither fog nodes nor Server knows the perception data submitted by each participant.

Assume that when performing task υ_j, participant P_i gets perceptual data d_i. To protect the confidentiality of data, P_i first chooses a random number r_i and encrypts the data with its public key pk_i to obtain $\mu_i = [d_i + r_i]_{pk_i}$. Then, P_i uses the task secret X_j as the key, generates a hash message verification code $h_i = HMAC_{X_j}(j|\mu_i|r_i|t_i)$, and sends the message $M =< j, \mu_i, r_i, h_i >$ to the corresponding fog node f_j under the pseudonym $H(pk_i)$. After receiving the message sent by the local participant, f_j verifies the integrity of messages. That is, $h' = HMAC_{X_j}(j|\mu_i|r_i|t_i)$ is calculated based on the secret X_j of the j task. If $h' = h_i$, the message has not been tampered with.

Then, with the help of Server, f_j aggregates all valid data according to υ_j^o. In the data aggregation phase, the data transmitted between F and Server are summed and aggregated to ensure the integrity of data. The Secure Additive Aggregation (SSA) protocol is shown in Algorithm I.

Algorithm 1 Secure Addition Aggregation Protocol SSA

Input: $f_j(\lambda_1, \sum pk_i)$, Server$(\lambda_2, \sum pk_i)$
Output: $[\sum_{P_i \in N} d_i]_{\sum pk_i}$
Fog node f_j
1: **for**all $P_i \in N$ **do**
2: $\mu_i' \leftarrow PSD1(\mu_i, \lambda_1)$
3: Send $< \mu_i, \mu_i' >$ to Server
4: **end for**
5: // Server
6: **for**all $P_i \in N$ **do**
7: $\mu_i'' \leftarrow PSD2(\mu_i, \mu_i', \lambda_1)$
8: **end for**
9: $S \leftarrow \sum_{P_i \in N} \mu_i''$
10: Compute $[S]_{\sum pk_i}$
11: Send $[S]_{\sum pk_i}$ to f_j
12: //Fog node f_j
13: Compute $R \leftarrow \sum_{P_i \in N} r_i$, $[R]_{\sum pk_i}$
14: $[\sum_{P_i \in N} d_i]_{\sum pk_i} \leftarrow [S]_{\sum pk_i} \cdot \left([R]_{\sum pk_i}\right)^{N-1}$

4) Data decryption: After obtaining the cipher text of aggregated results, each fog node $f_j \in \Im_i$ sends the cipher text result to Server. If multiple fog nodes are assigned task υ_j, Server needs to further aggregate the cipher text results of multiple fog nodes. After receiving the encrypted aggregation result, o_i uses private key θ_{oi} and random number ξ_i, and decrypts to obtain the clear text of final aggregation results.

C. SELFISH NODE INCENTIVE MECHANISM

In IoV with people as the carrier of terminal equipment, since network nodes have limited resources and different social relationships, they often show selfishness. The selfishness of nodes in IoV is usually divided into two types: personal selfishness and social selfishness. For the existence of selfish nodes, many researchers have adopted corresponding incentive mechanisms to promote selfish node collaboration. The selfish node incentive mechanism used in the proposed method is a Robbins-Stern bargaining game model based on game theory.

Map the data forwarding process between selfish nodes to each other as a Robbins-Stern bargaining game model. The process of providing forwarding data service between the node carrying the forwarded data and nodes that needs to meet as a bargaining game to satisfy the benefits of both parties. Among them, the game product is to provide forwarding services between nodes. The node carrying the forwarding data acts as a consumer, since it needs to buy a cooperative forwarding service from the forwarding node, and it is represented by B. The forwarding node that provides the forwarding service serves as the seller and is represented by S. Consumers and sellers take turns to propose the ratio of revenue sharing at different times until the transaction is completed or failed. Thus, the selfish node incentive mechanism is established using virtual currency.

There are many factors that affect the selfishness of nodes in IoV, including:

1) Remaining survival time of data carried by nodes: For consumers, the price paid is related to the remaining survival time of data. That is, the longer the remaining survival time, the smaller the consumer B's willingness to purchase forwarding service from sellers, thereby affecting the efficiency of information forwarding to destination nodes. The remaining lifetime of node i for data d is:

$$T_{i,d}^r = \frac{T_{TTL}^d - T_c}{T_{TTL}^d} \tag{4}$$

where T_{TTL}^d is the total TTL for forwarding data d, T_c is the time it takes for data d to be forwarded to node i. $T_{i,m}^r$ is the ratio of remaining TTL of data d to the total TTL.

2) Node remaining resource ratio: cache and bandwidth resources. The cache resources and bandwidth resources of each node are limited. As more data is stored, the remaining space is gradually reduced. The remaining cache and bandwidth resource ratios are expressed as:

$$S_i^r = \frac{s_i^r}{S_i}, B_i^r = \frac{b_i^r}{B_i} \tag{5}$$

where S_i^r and B_i^r are the remaining cache and broadband resource ratios respectively, s_i^r and b_i^r are the remaining cache space and bandwidth respectively. S_i is the cache space of node i, and B_i is the initial space of node i.

3) Social connection degree: In a network of opportunities with social attributes, nodes will show a certain degree of social selfishness because of different degrees of social connection with each other. Therefore, measuring the degree of social relationship between nodes is also one of factors affecting selfish nodes. The degree of social connection between nodes is described based on Jaccard similarity coefficient between nodes:

$$S_{i,j} = \frac{\sum_{a=1}^{k} z_{i,j}(a) \times J_{i,j}(a)}{\sum_{a=1}^{k} z_{i,j}(a)} \tag{6}$$

If two nodes have the same social property a, then $z_{i,j}(a) = 1$. Jaccard similarity coefficient is:

$$J_{i,j}(a) = \frac{f_{i,a} \cap f_{j,a}}{f_{i,a} \cup f_{j,a}} \tag{7}$$

where $f_{i,a}$ and $f_{j,a}$ are the number of neighbor nodes where node i and node j have the same social property a respectively.

Based on Robbins-Stern bargaining game model, consumer node i carrying data d in the network of chances wants to purchase the forwarding service at a lower price. The seller node j wants to obtain more revenue by providing services. The two sides of game will give the lowest bid for this forwarded data based on maximizing each other's benefits. Due to the existence of selfish nodes, the lowest quote given by consumer B at data d at time t is:

$$P_d^B = VC_B \times \frac{D_d}{\lambda_1 S_B^r + \lambda_2 B_B^r + \lambda_3 T_B^r} \tag{8}$$

where VC_B is the number of virtual currencies of consumer B at time t, D_m is the size of data d, $\lambda_1, \lambda_2, \lambda_3$ is weight coefficient, and the sum is 1.

In the same way, the lowest quotation given by seller S is:

$$P_d^S = VC_S \times \frac{1}{\pi_1 S_B^r + \pi_2 B_B^r} \times \frac{D_d}{S_{S,B}} \tag{9}$$

where VC_S is the number of virtual currencies of consumer S at time t, $S_{S,B}$ is the social connection between the two parties participating in game. π_1, π_2 is a weighting factor that adds up to 1.

In this model, the transaction can only be completed when $P_m^B > P_m^S$. And the two parties allocate the total income Cap by bargaining, and the secondary income is:

$$Cap = P_m^B - P_m^S \tag{10}$$

Since both sides of the game are selfish, they pursue the maximization of their own interests. Consequently, the utility functions of consumer B and seller S are:

$$U_B(x_B) = x_B Cap,\ U_S(x_S) = x_S Cap \tag{11}$$

where x_B and x_S are the proportion of consumers and sellers to the total revenue in game.

Since Robins-Stein bargaining game model has only one sub-game perfect Nash equilibrium, after multiple rounds of bargaining games, the two sides get an equilibrium solution to the game:

$$\begin{aligned} (x_S^*, x_B^*) &= \left(\frac{Cap - \mu_B Cap}{Cap - \mu_B \mu_S Cap}, \frac{\mu_B Cap - \mu_B \mu_S Cap}{Cap - \mu_B \mu_S Cap} \right) \\ \mu_B &= \frac{e^{\delta_B} - e^{-\delta_B}}{e^{\delta_B} + e^{-\delta_B}},\ \mu_S = 1 - \frac{e^{\delta_S} - e^{-\delta_S}}{e^{\delta_S} + e^{-\delta_S}} \end{aligned} \tag{12}$$

where δ_B and δ_S are patience coefficients of consumers and sellers.

The distribution ratio of income has reached equilibrium at this point in the game. Since the bargaining game is a complete information game, the result can be obtained by exchanging tolerance factors between two parties. So there is no need for multiple rounds of bargaining games. At the same time, increasing the number of game rounds in IoV will increase the average delay and affect the data to reach power. By exchanging tolerance factors to obtain an equilibrium solution, network delay and overhead can be reduced.

VI. SIMULATION EXPERIMENT

Operational network environment (ONE) simulation software is used to simulate and analyze the performance of the proposed system and method. The parameters in the simulation experiment are shown in Table. 1. The experiment was run 100 times to calculate the average experiment result.

TABLE 1. Simulation parameter settings.

Simulation parameters	Value
Datasets	INFOCOM06，SIGCOMM09
Simulation time/*h*	94/36
Interface Type	Bluetooth
Transmission mode	External movement
Transmission range	10 meters
Transmission speed	250KB
Cache / message size	5MB/500-1024KB
The number of local cloud	1-8

The following five indicators were used in the experiments to evaluate the performance of proposed method and these methods in reference [23], reference [24], and reference [27]:

1) Average transmission efficiency: The ratio of all messages transmitted to all messages generated in the network. This indicator describes the effective throughput of an efficient data transmission mechanism.

2) Average transmission delay: The average delay from the time a message is generated to the time it is delivered. This indicator describes the latency of an efficient data transmission mechanism.

3) Average transmission cost: the ratio of all replica messages to all delivered messages. This indicator describes the overhead of an efficient data transmission mechanism.

4) Credit value: the average amount of virtual currency obtained by nodes. This indicator describes the node benefits of an efficient data transmission mechanism.

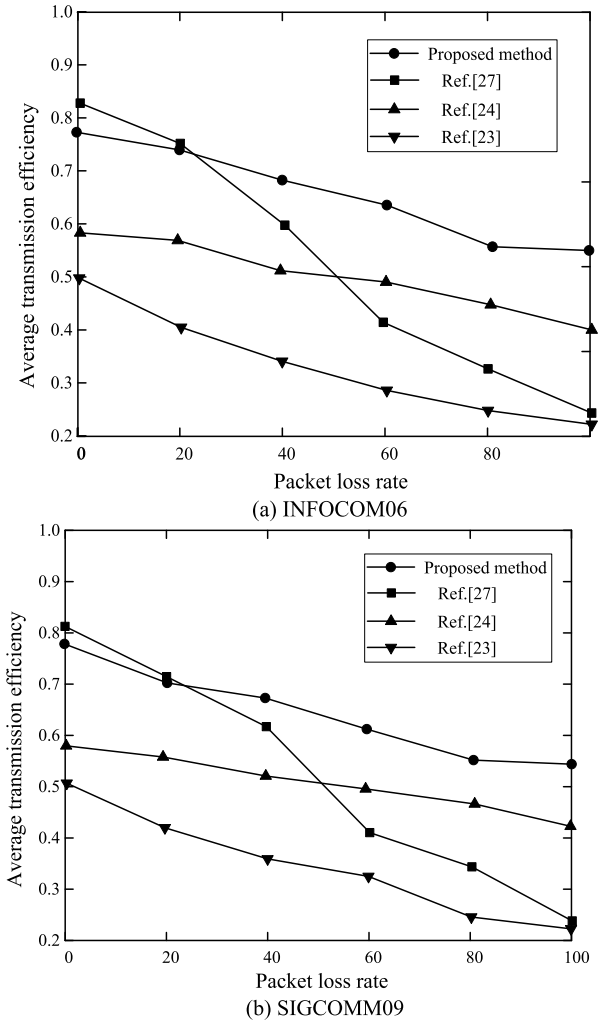

FIGURE 6. The relationship between packet loss rate and average transmission efficiency.

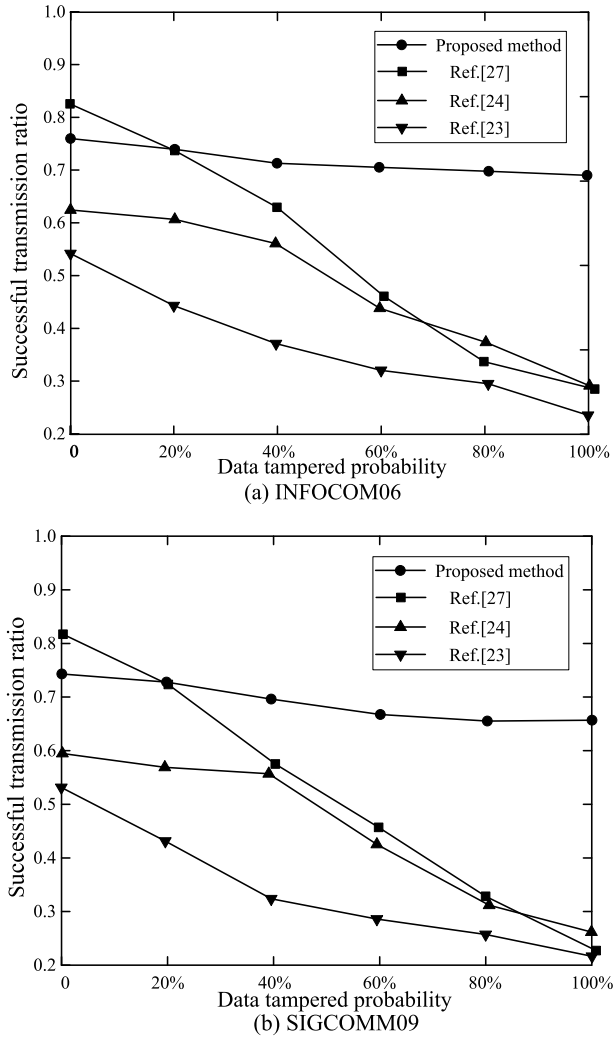

FIGURE 7. The relationship between data tampered probability and successful transmission ratio.

5) Successful transmission ratio: The ratio of correctly delivered messages to the total number of messages generated by system. This indicator describes the transmission success rate of an efficient data transmission mechanism.

A. IMPACT OF PACKET LOSS PROFITS ATTACKS ON PERFORMANCE

The packet loss rate is the ratio of all nodes that perform packet loss profits attacks to all nodes in the network. The average transmission efficiency of proposed method when the packet loss rate changes is shown in Figure 6.

As can be seen from Fig. 6, no matter what datasets, when packet loss rate is less than 20%, the transmission efficiency of the method in reference [27] is higher than that of proposed method. Since when there is only a small number of malicious nodes, the performance of the method in reference [27] is not affected too much. After a sufficiently long simulation time, the method in reference [27] can successfully transmit most of messages. When packet loss rate increases, the average transmission efficiency of the methods in reference [27] and reference [23] decreases rapidly. The performance of proposed method and the method in reference [24] decreases slowly. Since both have designed corresponding attack defense strategies, they can prevent nodes from performing packet loss profit attacks.

B. IMPACT OF MESSAGE TAMPERING ATTACKS ON PERFORMANCE

Message tampering will have a certain effect on the rate of successful transmission. The experimental conclusion is shown in Figure 7.

It can be seen from Fig. 7 that when message tampering rate is lower than 20%, the successful transmission ratio of the method in reference [27] is higher than the proposed method. Since even in the presence of a small number of malicious nodes, the method in reference [27] can promote more selfish nodes to participate in message transmission. In addition, as the message tampering rate continues to

increase, the trend of successful transmission rate of messages in the proposed method tends to be flat, while the successful transmission rates of other algorithms decrease sharply. When message tampering rate is 20%, the successful message transmission rates of the proposed method, reference [27], reference [24] and [23] are 0.72, 0.72, 0.57 and 0.43 respectively. When message tampering rate is 80%, the performance indicators of the above four algorithms are 0.55, 0.31, 0.32 and 0.25 respectively. Since the proposed method can detect message tampering attacks and can ensure that the destination node receives correct messages, the other three methods lack this capability.

C. IMPACT OF SYBIL ATTACKS ON PERFORMANCE

References [27], reference [24] and the proposed methods are routing algorithms based on credit mechanisms, while reference [23] does not design any incentive mechanism. Thus, we compare the changes in the credit value of reference [27], reference [24] and the proposed method. With the change of Sybil attack rate, the changing trend of system's credit value is shown in Figure 8.

When Sybil attack rate is less than 16%, the performance of reference [27] and reference [24] is better than that of the proposed method. So reference [27] and reference [24] are routing algorithms based on social perception, which can greatly improve the transmission efficiency of messages. When the system has a small number of malicious nodes, its performance is not greatly affected. As the number of malicious nodes increases, the performance of the methods in reference [27] and reference [24] decreases sharply, while the performance of proposed method tends to be gentle. Since the fog nodes of proposed method can detect Sybil attacks by reporting information, it is guaranteed that malicious nodes cannot get rewards. When a malicious node cannot obtain a reward, in order to transmit locally generated messages, it must standardize its own behavior and legally participate in the message transmission process to obtain sufficient virtual currency to send local messages. However, the other two methods do not have a Sybil attack detection scheme. The virtual currency paid by the system will increase with the implementation of Sybil attacks.

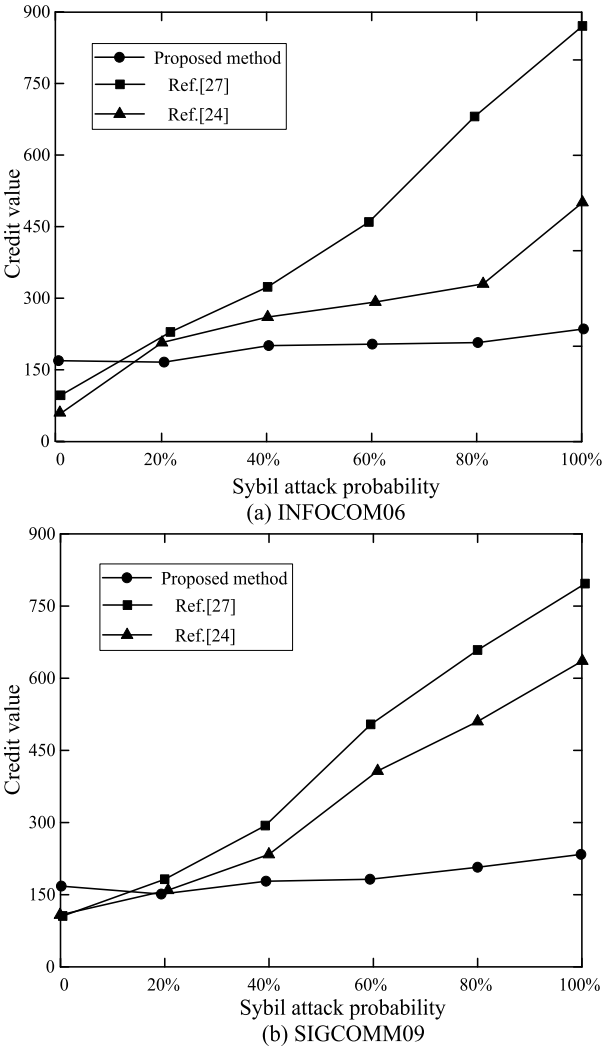

FIGURE 8. The trend of system credit value when Sybil attack rate changes.

D. IMPACT OF THE NUMBER OF FOG NODES ON PERFORMANCE

In the proposed method, messages are routed after fog nodes complete the key encryption. Therefore, the number and distribution of fog nodes have a significant impact on message transmission efficiency. At the same time, the proposed system uses a location prediction algorithm to intelligently determine the placement of fog nodes. In INFOCOM06 dataset, the effect of the number of fog nodes on message transmission efficiency is shown in Figure 9.

As can be seen from Figure 9, as the number of fog nodes increases, the transmission efficiency of messages also increases accordingly. Since the greater the number of fog nodes, the more opportunities for nodes to encrypt messages and keys, the shorter the time delay. Moreover, as the proportion of malicious nodes increases, the average transmission efficiency of proposed method will decrease, and the transmission delay will increase.

E. IMPACT OF THE NUMBER OF SELFISH NODES ON PERFORMANCE

The number of selfish nodes has different effects on the performance of our proposed method. In SIGCOMM09 dataset, when the number of selfish nodes is between 30% and 100%, the changes in the average transmission efficiency, average transmission delay and average transmission cost of each method are shown in Figure 10.

It can be seen from Figure 10. (a) that the proposed method is superior to the other three methods in terms of average transmission efficiency. Figures (b) and (c) show the average transmission delay and cost of the four methods. The delay of the algorithm in reference [23] is higher than that of the other three algorithms, because the algorithm cannot motivate

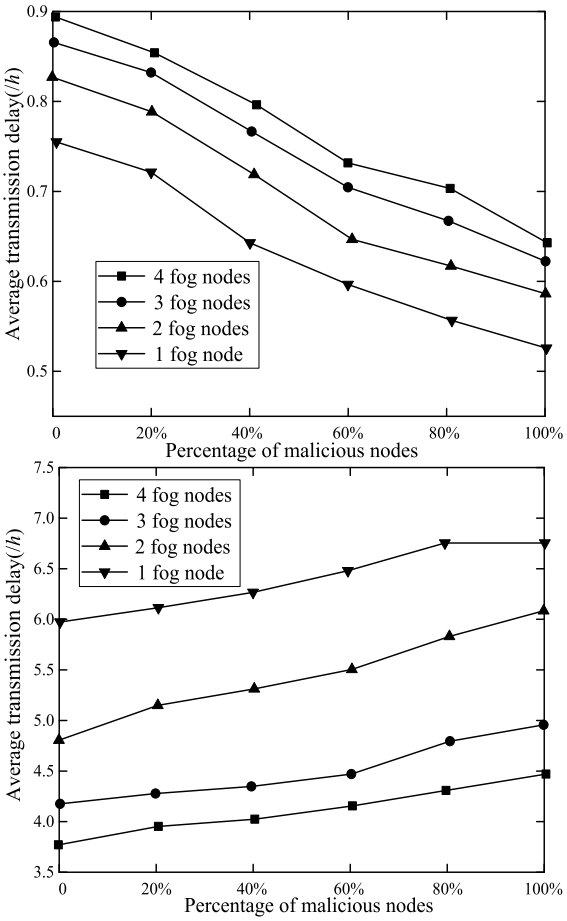

FIGURE 9. Performance trend of these algorithms when the number of fog nodes changes.

selfish nodes to transmit messages. The performance of proposed method is better than that of the other three methods. For example, when the ratio of selfish nodes is 50%, the average transmission delay and cost of the proposed method are 17% and 13% lower than those in reference [24]. Since the proposed system uses a game-based incentive mechanism to transfer between nodes, the virtual currency obtained and paid between nodes can reach the Nash equilibrium.

In summary, the experiment mainly focuses on two factors that affect system performance, selfish nodes and malicious nodes. When malicious nodes exist, multiple types of attacks are considered, including Sybil attacks, packet loss profit attacks and message tampering attacks. It can be seen that the performance of our proposed method is more stable and better than the other three methods. Since the proposed method comprehensively considers attack defense strategies and data transmission mechanisms, this not only protects vehicle privacy information from malicious nodes, but also improves message transmission efficiency. When selfish nodes exist, the proposed method outperforms the other three methods. The reason is that the proposed method is a routing algorithm based on incentive mechanism, it can stimulate selfish nodes to transmit messages and achieve reliable transmission.

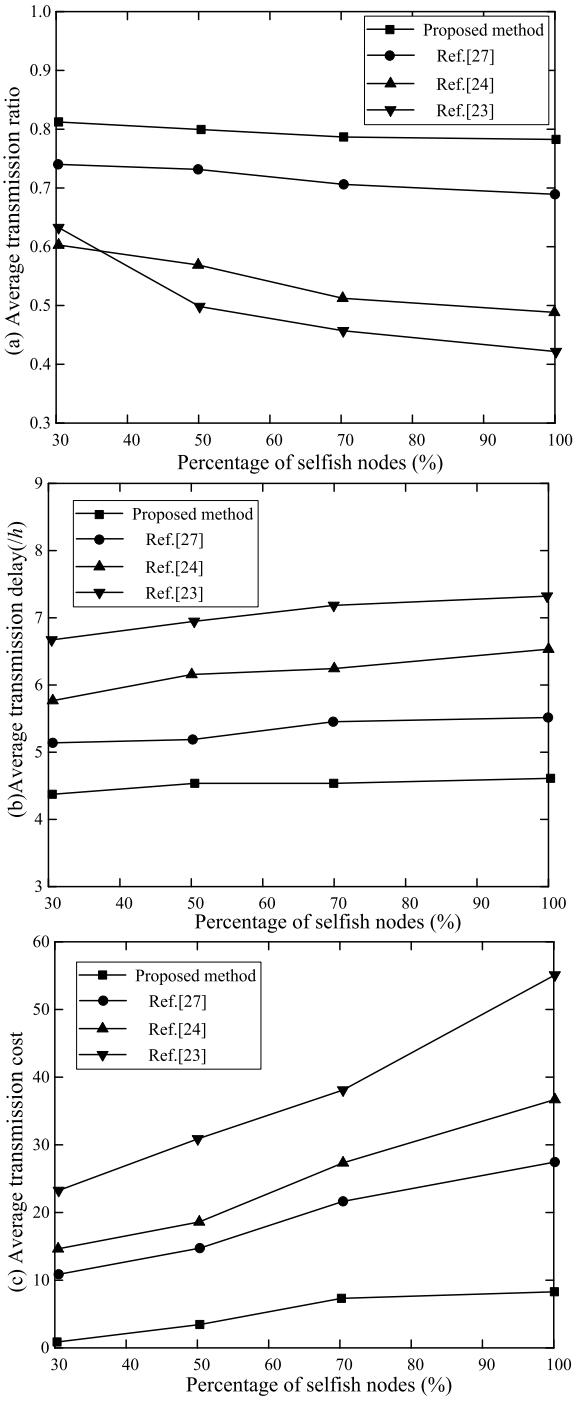

FIGURE 10. The effect of the number of selfish nodes on the performance of algorithms.

Therefore, the proposed method has strong competitiveness in simultaneously resisting attacks and improving message transmission efficiency.

VII. CONCLUSON

With the development of smart cities and intelligent transportation management systems, IoV has become an emerging

research hotspot. However, the highly dynamic, large-scale and heterogeneous features in IoV pose huge challenges for achieving efficient and secure data transmission. Therefore, this paper proposes an efficient data transmission mechanism for IoV using privacy protection in fog computing environment, which provides users with a safe and comfortable driving environment and convenient and efficient travel plans. Among them, PTAA mechanism is adopted to protect the privacy of perceived data and resist external attacks, and offload the computing load of terminal equipment to fog computing environment, which improves system robustness and reduces system latency. Moreover, the game model is used to design selfish node incentive mechanism to play the role of selfish nodes in data transmission and reduce time delay. The experimental results in ONE simulation software show that the proposed transmission mechanism has a strong competitiveness in defending against attacks and improving the efficiency of message transmission, and better guarantees users' privacy. It realizes efficient and secure data transmission in IoV.

At present, the research on energy management for IoV is still in its infancy, many problems have not been fully studied and solved, such as dynamic energy transmission mechanisms. The increasing use of electric vehicles and long-term charging has led users to seek other more convenient charging solutions, which makes the emergence of dynamic energy transfer strategies. In order to ensure the efficiency of energy transmission, how to design a reasonable and efficient energy transmission strategy is worthy of further study. In addition, how to achieve seamless switching of vehicle charging between different charging makeups is also an important research direction in the future.

REFERENCES

[1] K. Liu, X. Xu, M. Chen, B. Liu, L. Wu, and V. C. S. Lee, "A hierarchical architecture for the future Internet of vehicles," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 41–47, Jul. 2019.

[2] M. K. Priyan and G. U. Devi, "A survey on Internet of vehicles: Applications, technologies, challenges and opportunities," *Int. J. Adv. Intell. Paradigms*, vol. 12, nos. 1–2, pp. 98–119, 2019.

[3] A. Thakur and R. Malekian, "Fog computing for detecting vehicular congestion, an Internet of vehicles based approach: A review," *IEEE Intell. Transp. Syst. Mag.*, vol. 11, no. 2, pp. 8–16, 2019.

[4] H. Gao, W. Huang, and X. Yang, "Applying probabilistic model checking to path planning in an intelligent transportation system using mobility trajectories and their statistical data," *Intell. Automat. Soft Comput.*, vol. 25, no. 3, pp. 547–559, 2019.

[5] X. Wang, Z. Ning, X. Hu, L. Wang, L. Guo, B. Hu, and X. Wu, "Future communications and energy management in the Internet of vehicles: Toward intelligent energy-harvesting," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 87–93, Dec. 2019.

[6] H. Gao, W. Huang, Y. Duan, X. Yang, and Q. Zou, "Research on cost-driven services composition in an uncertain environment," *J. Internet Technol.*, vol. 20, no. 3, pp. 755–769, 2019.

[7] H. Gao, Y. Duan, L. Shao, and X. Sun, "Transformation-based processing of typed resources for multimedia sources in the IoT environment," *Wireless Netw.*, vol. 2019, Nov. 2019, doi: 10.1007/s11276-019-02200-6.

[8] Y. Zhang, R. Wang, M. S. Hossain, M. F. Alhamid, and M. Guizani, "Heterogeneous information network-based content caching in the Internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 10216–10226, Oct. 2019.

[9] N. Soni, R. Malekian, D. Andriukaitis, and D. Navikas, "Internet of vehicles based approach for road safety applications using sensor technologies," *Wireless Pers. Commun.*, vol. 105, no. 4, pp. 1257–1284, Apr. 2019.

[10] C. Wu, X. Chen, T. Yoshinaga, Y. Ji, and Y. Zhang, "Integrating licensed and unlicensed spectrum in the Internet of vehicles with mobile edge computing," *IEEE Netw.*, vol. 33, no. 4, pp. 48–53, Jul. 2019.

[11] H. Gao, Y. Xu, Y. Yin, W. Zhang, R. Li, and X. Wang, "Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services," *IEEE Internet Things J.*, early access, Dec. 2, 2019, doi: 10.1109/JIOT.2019.2956827.

[12] M. Cui, D. Han, and J. Wang, "An efficient and safe road condition monitoring authentication scheme based on fog computing," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9076–9084, Oct. 2019.

[13] Y. Liu, J. Wu, J. Li, W. Yang, H. Chen, and G. Li, "ISRF: Interest semantic reasoning based fog firewall for information-centric Internet of vehicles," *IET Intell. Transp. Syst.*, vol. 13, no. 6, pp. 975–982, Jun. 2019.

[14] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[15] H. Lu, Q. Liu, D. Tian, Y. Li, H. Kim, and S. Serikawa, "The cognitive Internet of vehicles for autonomous driving," *IEEE Netw.*, vol. 33, no. 3, pp. 65–73, May 2019.

[16] X. Ma, H. Gao, H. Xu, and M. Bian, "An IoT-based task scheduling optimization scheme considering the deadline and cost-aware scientific workflow for cloud computing," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 249, Dec. 2019, doi: 10.1186/s13638-019-1557-3.

[17] X. Wang, X. Wei, and L. Wang, "A deep learning based energy-efficient computational offloading method in Internet of Vehicles," *China Commun.*, vol. 16, no. 3, pp. 81–91, Mar. 2019.

[18] S. Yaqoob, A. Ullah, M. Akbar, M. Imran, and M. Shoaib, "Congestion avoidance through fog computing in Internet of vehicles," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 10, pp. 3863–3877, Oct. 2019.

[19] Z. Ning, P. Dong, X. Wang, L. Guo, J. J. P. C. Rodrigues, X. Kong, J. Huang, and R. Y. K. Kwok, "Deep reinforcement learning for intelligent Internet of vehicles: An energy-efficient computational offloading scheme," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 4, pp. 1060–1072, Dec. 2019.

[20] Z. Ning, J. Huang, X. Wang, J. J. P. C. Rodrigues, and L. Guo, "Mobile edge computing-enabled Internet of vehicles: Toward energy-efficient scheduling," *IEEE Netw.*, vol. 33, no. 5, pp. 198–205, Sep. 2019.

[21] X. Wang and B. Yang, "An improved signature model of multivariate polynomial public key cryptosystem against key recovery attack," *Math. Biosci. Eng.*, vol. 16, no. 6, pp. 7734–7750, 2019.

[22] P. S. Xie, T. X. Fu, and H. J. Fan, "An algorithm of the privacy security protection based on location service in the Internet of vehicles," *Int. J. Netw. Secur.*, vol. 21, no. 4, pp. 556–565, 2019.

[23] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[24] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H.-N. Dai, Y. Wu, and W. Wang, "SCTSC: A semicentralized traffic signal control mode with attribute-based blockchain in IoVs," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1373–1385, Dec. 2019.

[25] M. T. Abbas, A. Muhammad, and W.-C. Song, "SD-IoV: SDN enabled routing for Internet of vehicles in road-aware approach," *J. Ambient Intell. Hum. Comput.*, vol. 11, no. 3, pp. 1265–1280, Mar. 2020.

[26] K. Xiong, S. Leng, J. Hu, X. Chen, and K. Yang, "Smart network slicing for vehicular fog-RANs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3075–3085, Apr. 2019.

[27] M. T. Abbas, A. Muhammad, and W.-C. Song, "Road-aware estimation model for path duration in Internet of vehicles (IoV)," *Wireless Pers. Commun.*, vol. 109, no. 2, pp. 715–738, Nov. 2019.

[28] Y. Dai, D. Xu, S. Maharjan, G. Qiao, and Y. Zhang, "Artificial intelligence empowered edge computing and caching for Internet of vehicles," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 12–18, Jun. 2019.

[29] Y. F. Zhou and N. Chen, "The LAP under facility disruptions during early post-earthquake rescue using PSO-GA hybrid algorithm," *Fresenius Environ. Bull.*, vol. 28, no. 12, pp. 9906–9914, 2019.

[30] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating reputation management schemes of Internet of vehicles based on evolutionary game theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5971–5980, Jun. 2019.

[31] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[32] J. Jian, Y. Guo, L. Jiang, Y. An, and J. Su, "A multi-objective optimization model for green supply chain considering environmental benefits," *Sustainability*, vol. 11, no. 21, p. 5911, 5911.

[33] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[34] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," *IEEE Netw.*, vol. 33, no. 5, pp. 27–33, Sep. 2019.

[35] W. Zhong, K. Xie, and Y. Liu, "Admm empowered distributed computational intelligence for Internet of energy," *IEEE Comput. Intell. Mag.*, vol. 14, no. 4, pp. 42–51, May 2019.

[36] M. Katsomallos, K. Tzompanaki, and D. Kotzinos, "Privacy, space and time: A survey on privacy-preserving continuous data publishing," *J. Spatial Inf. Sci.*, 2019, vol. 2019, no. 19, pp. 57–103.

WENJUAN ZHANG graduated from Yanshan University, in 2009, and received the master's degree in computer science. She is currently working as a Lecturer with Zhoukou Normal University. Her research interests include information security, the Internet of Things, and the Internet of Vehicles.

GANG LI born in Urumqi, Xinjiang, China, in 1974. He received the master's degree in computer science. He is currently working as an Associate Professor with the Xinjiang Vocational and Technical College of Communications. He has published many academic articles in these relevant fields. His main research interests include the Internet of Things and cloud computing.