Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 8302527, 11 pages
https://doi.org/10.1155/2021/8302527

Research Article

Security Guarantee for Vehicular Message Transmission Based on Dynamic Social Attributes

Lishui Chen[1], **Jing Wang**[1], **Xing Chen**[1] **and Yifu Zhang**[2]

[1]*The 54th Research Institute of CETC, Shijiazhuang, Hebei 050081, China*
[2]*Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Correspondence should be addressed to Lishui Chen; 78015159@qq.com

Received 26 August 2021; Revised 28 October 2021; Accepted 22 November 2021; Published 20 December 2021

Academic Editor: Hui Zhu

Copyright © 2021 Lishui Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Effective message forwarding between vehicles can reduce the occurrence of traffic accidents and improve the driving experience. Vehicle clustering can improve message utilization, but attackers in the network pose a serious threat to message forwarding. Based on vehicle clustering, we propose a message forwarding strategy for Vehicular Ad hoc Network. Specifically, the vehicles are clustered based on their directions and speeds. Besides, the friendship of vehicles is evaluated in terms of the interaction friendship and reference friendship. Based on the friendship of vehicles, the optimal vehicle can be selected as the cluster head. Thereafter, the double key technology is designed to encrypt vehicular messages such that the messages can be forwarded more safely and efficiently. The analysis results show that the proposed strategy can effectively improve the message delivery rate, reduce the message leakage rate, and improve the network performance.

1. Introduction

As an important basis of intelligent transport system (ITS), Vehicular Ad hoc Network (VANET) is committed to the realization of intelligent traffic management and intelligent dynamic information services [1, 2]. Through vehicle to vehicle (V2V) communication and vehicle to infrastructure (V2I) communication, VANETs can reduce traffic accidents, improve road use efficiency, and promote the realization of traffic intelligence and information construction [3–5].

VANETs can improve the performance of ITS through information interaction, and the behavior of vehicles is similar to that of mobile nodes [6], so VANETs belong to a kind of continuous ad hoc wireless mobile network. The topology of VANETs is usually unstable since it changes dynamically with the high-speed movement of vehicles. In addition, the communication between vehicles in VANETs is mainly based on wireless link, which provides an opportunity for malicious vehicles to launch attacks. Therefore, the dynamic network structure of VANETs leads to serious security and privacy threats to vehicles and drivers [7], which makes it urgent to design an effective secure communication strategy. To deal with the aforementioned issues, researchers usually design the security mechanism by using the authentication method based on public key infrastructure [8]. However, as a vehicle needs to store a large number of key pairs and their corresponding certificates that need to be transmitted with the message, the efficiency of those schemes in improving the network performance is low.

Given the high similarity of messages acquired or transmitted by vehicles in a certain range of VANETs, when a vehicle receives a useful message, the message also has reference value for its adjacent vehicles. In this case, if the vehicles independently repeat the security message transmission, it will not only cause the waste of communication resources but also be difficult to improve the communication efficiency. Although the message sharing method can solve the above problems to a certain extent, the effectiveness of the message in the communication process is not considered in the traditional broadcast method, which is prone to collision and loss of messages. As a result, the effectiveness of message sharing cannot be improved [9]. On the other hand, clustering technology is usually to group nodes in a network according to a certain relationship to enable

message transmission. Cluster communication can not only realize message sharing but also reduce the propagation of irrelevant and redundant messages, as well as reduce routing overhead and broadcast storm problems. Hence, message transmission efficiency and network performance can be improved [10]. Different clustering mechanisms have different optimization objectives and objects. Researchers have conducted in-depth research on cluster communication, and different clustering methods are introduced in detail in reference [11].

According to the characteristics of VANETs, the clustering methods of VANETs include static clustering based on the base station (BS) and dynamic clustering based on the vehicle [12]. Static clustering based on BS takes BS as cluster head, and the surrounding vehicles transmit messages to BS, and then, the BS transmits messages to other vehicles around [13]. The advantage of static clustering method is that it is easy to distinguish clusters. However, due to the long distance between two BSs and the fast change of network topology, static clustering usually leads to high message transmission delay, thus greatly reducing the accuracy and effective utilization of the message [14]. Hence, dynamic clustering based on V2V communication emerges. In this type of clustering, vehicles are screened and clustered according to certain rules, including location, speed, vehicle attribute relationship, and destination. Nevertheless, how to cluster vehicles reasonably with consideration of communication security and communication effectiveness remains an open issue.

Motivated by this, we propose a friendship assessment of security message forwarding (FASMF) strategy in VANETs. Firstly, considering the factors that affect the vehicle clustering performance and combining with the evaluation of friendship, the appropriate vehicle is selected as the cluster head. The cluster head is responsible for collecting the messages from its cluster members or other adjacent cluster heads and realizes the secure forwarding of messages by using double key message encryption within and between clusters. The effectiveness of the proposed scheme is finally validated by extensive simulations.

The reminder of the paper is organized as follows. Section 2 introduces the related works. Section 3 evaluates the vehicle friendship. Section 4 introduces the vehicle clustering scheme. Section 5 proposes a secure double key message forwarding strategy. In Section 6, simulation results are presented. Section 7 finally concludes the paper.

2. Related Work

In the literature, vehicular message transmission can be improved through vehicle clustering. In [15], the authors aimed to cluster a wide range of driving encounter scenarios based only on multivehicle GPS trajectories, where a generic unsupervised learning framework was proposed. In [16], a stochastic analysis of the impact of cluster instability on generic routing overhead was presented. In [17], the authors proposed to employ network representation learning to achieve accurate vehicle trajectory clustering, which could reduce the time and space resources. In [18], a power control scheme in an uplink clustering network was studied for a densely vehicular network with node clustering idea. In [19], an integrated network architecture for secure group communication was proposed by taking advantage of the software-defined network technology in fifth-generation mobile networks. However, those works only focused on the vehicle cluster based on wireless communication parameters, where social relationship between vehicles was not taken into account.

Recently, some works tried to improve the security performance of intracluster and intercluster message transmissions. In [20], the authors proposed a tool called as cryptographic mix-zone to enhance vehicle privacy, in which the safety messages of vehicles were encrypted using a group secret key. In [21], a ternary join exit tree was constructed to secure communication and efficient key updating for vehicles in a platoon. In [22], an efficient security risk analysis method was proposed through fitting for evaluating the risks of attacks in the context of AV and CAVs. In [23], an efficient privacy-preserving data aggregation and dynamic pricing service PADP in V2G IoT were proposed, by designing an identity-based sequential aggregate signed data based on factoring and a threshold homomorphic encryption. However, those schemes usually introduced large amount of extraoverheads, which may degrade the delay or energy efficiency performance of VANETs.

3. Evaluation of Vehicle Friendship

The evaluation result of the vehicle-friendly relationship is the basis of the clustering strategy in this paper. The friendship of the vehicle in the network is evaluated by calculating the friendship of the vehicle. Specifically, the vehicle with high friendship is selected as the cluster head first, to ensure the reliability of message forwarding and improve the efficiency of message transmission. The direct interaction history behavior of both sides of the vehicle is selected to evaluate the interaction friendship, and the reference friendship provided by other neighboring vehicles is taken as the main factor to evaluate the vehicle friendship comprehensively.

3.1. Interactive Friendship. The vehicle has mobility and can be operated across geographical locations. If there is historical interaction between the vehicles that meet, the vehicle will obtain the vehicle interaction friendship according to the historical friendship calculated by the historical interaction experience and the interval of meeting again. If the interaction between vehicle v_i and v_j is more successful, the friendship of vehicle v_i to v_j is greater, which indicates that vehicle v_i has more sufficient evidence to forward the message to the vehicle v_j; on the contrary, if the number of successful interactions between vehicle v_i and v_j is not frequent enough, the friendship of vehicle v_i to vehicle v_j will be reduced. Therefore, taking the number of successful interactions between vehicles as a parameter can directly evaluate the historical friendship. If there are $\mathrm{Sum}_{i,j}$ historical interaction records between vehicle v_i and v_j in the historical interaction, the historical friendship $<\mathrm{His}, \mathrm{Fre}, \mathrm{Deg}>_{i,j}$ of vehicle

v_i to v_j can be expressed as:

$$<\text{His, Fre, Deg}>_{i,j} = \begin{cases} \dfrac{\text{Suc}_{i,j}}{\text{Sum}_{i,j}} \dfrac{1}{\sqrt{\text{Fai}_{i,j}}}, \text{Sum}_{i,j} \neq 0 \text{ and } \text{Sum}_{i,j} = \text{Suc}_{i,j} + \text{Fai}_{i,j}, \\ 0, \text{Sum}_{i,j} = 0 \text{ and } \text{Sum}_{i,j} = \text{Suc}_{i,j} + \text{Fai}_{i,j}, \end{cases} \tag{1}$$

where $\text{Suc}_{i,j}$ is the number of successful transactions and $\text{Fai}_{i,j}$ is the number of failed transactions. At the same time, if there is no interactive record, the historical friendship is 0.

In addition, the time interval of vehicles meeting again will inevitably affect the level of friendship between vehicles, and the time interval of vehicles meeting again is negatively correlated with the friendship of historical interaction. That is to say, the longer the interval, the lower the referential value of historical interaction, and the less its impact on current friendship; on the contrary, the shorter the interval, the higher the value of historical cross reference, should improve the impact on the current friendship. To solve the appealing problem, $\Delta t_{\max}$ is used to represent the effective time window size of historical behavior, δ is the decay rate factor, and its value is defined according to the specific application. Then, based on the historical friendship $<\text{His, Fre, Deg}>_{i,j}$, forgetting factor α is introduced, whose value is as follows:

$$\alpha = \begin{cases} \dfrac{e^{\Delta t_{\max}/\delta} - e^{(t-t')/\delta}}{e^{\Delta_{\max}/\delta} - 1}, t - t' < \Delta t_{\max}, \\ 0, \quad \text{else}, \end{cases} \tag{2}$$

where t is the current time and t' is the time of the last interaction.

In conclusion, according to the historical friendship $<\text{His, Fre, Deg}>_{i,j}$ and forgetting factor α, the interactive friendlship $<\text{Mul, Fre, Deg}>_{i,j}$ of vehicle v_i to v_j is shown in

$$<\text{Mul, Fre, Deg}>_{i,j} = \begin{cases} \dfrac{\sum_{t=t'}^{\Delta t_{\max}} \alpha \cdot <\text{His, Fre, Deg}>_{i,j}^{t}}{\Delta t_{\max}}, t - t' < \Delta t_{\max}, \\ 0, \quad \text{else}. \end{cases} \tag{3}$$

By introducing the forgetting factor, when the historical interaction occurs beyond the effective time length, the forgetting factor α is 0, which indicates that the past interaction has lost its value; as the past interaction time t' approaches the current time t, the value of α tends to 1, which indicates that the past interaction is valuable. Therefore, using the forgetting factor can reduce the impact on network security caused by the transformation of ordinary vehicles into malicious vehicles and improve network stability.

3.2. Reference Friendship. In the process of evaluating the friendship of vehicle v_i to v_j, not only the friendship formed by the historical interaction with vehicle v_i but also the evaluation factors of other vehicle v_k to v_j and the friendship evaluation of vehicle v_i to vehicle v_k should be considered, so as to obtain the recommended friendship $<\text{Rec, Fre, Deg}>_{i,j}$ of vehicle v_i to v_j. In order to make the recommendation reliable, the average friendship of all neighbor recommended vehicles v_k to v_i and v_j is calculated as the value of recommended friendship $<\text{Rec, Fre, Deg}>_{i,j}$ as shown in

$$<\text{Rec, Fre, Deg}>_{i,j} = \frac{1}{n}\left(\sum_{k=1}^{n} <\text{Mul, Fre, Deg}>_{i,k} \cdot <\text{Mul, Fre, Deg}>_{k,j}\right), \tag{4}$$

where n denotes the number of neighbor vehicles, $<\text{Mul, Fre, Deg}>_{i,k}$ denotes the interactive friendship of vehicle v_i to neighbor vehicle v_k, and $<\text{Mul, Fre, Deg}>_{k,j}$ denotes the friendship of vehicle v_j provided by v_k.

As neighbor vehicle v_k may carry out malicious recommendation attacks, vehicle v_i does not fully trust the friendship $<\text{Mul, Fre, Deg}>_{k,j}$ provided by v_k. In order to prevent malicious attack from vehicle v_k, vehicle v_i introduces a penalty factor $\text{Pui}_{i,k}$. The size of $\text{Pui}_{i,k}$ is determined by the number of interaction failures during the historical interaction between v_i and v_k.

$$\text{Pui}_{i,k} = \arctan \frac{\text{Fai}_{i,k}}{\text{Sum}_{i,k}}. \tag{5}$$

We introduce a penalty factor when the number of unsuccessful communication between vehicles increases in a short period. That is, when the vehicle behaves as malicious behavior, the friendship value of the vehicle decreases rapidly, to achieve the purpose of the abrupt decline of friendly degree. At the same time, to prevent the collusion attack between neighbor vehicle v_k and v_j leading to the rapid increase of recommendation friendship, we also consider the adjustment factor $\text{Re g}_{i,k}$, which means that with the increase of the number of successful interactive communication between vehicles, its size is closer to 1, but the approaching speed will not increase suddenly. Therefore, the calculation of the adjustment factor $\text{Re g}_{i,k}$ is as follows:

$$\text{Re g}_{i,k} = 1 - \frac{\text{Suc}_{i,k}}{1 + \text{Suc}_{i,k}}. \tag{6}$$

In conclusion, according to the recommended friendship, penalty factor, and adjustment factor, the reference friendship $<\text{Con, Fre, Deg}>_{i,j}$ of vehicle v_i to v_j is calculated as follows:

$$<\text{Con, Fre, Deg}>_{i,j} = \text{Pui}_{i,k}^{-1} \cdot \text{Re g}_{i,k} \cdot <\text{Rec, Fre, Deg}>_{i,j}. \tag{7}$$

The introduction of penalty factor $\text{Pui}_{i,k}$ and adjustment factor $\text{Re g}_{i,k}$ in the calculation of reference friendship can not only effectively prevent the occurrence of malicious recommendation behavior of neighbor vehicle v_k but also reduce the influence of collusion attack between vehicles on the network, to prevent the rapid growth of reference friendship.

3.3. Friendship Integration. As mentioned above, measuring the friendship of vehicles from the above two aspects can improve the reliability of cluster heads, but the interaction between vehicles is different, so the influence of interaction friendship and reference friendship on friendship is also different. Therefore, it is necessary to allocate the weight dynamically.

Firstly, if the interaction between vehicle v_i and v_j is more frequent, the more information of vehicle v_i to v_j is, vehicle v_i has sufficient evidence to evaluate vehicle v_j; secondly, if there is less interaction between vehicle v_i and v_j, vehicle v_i has less information about vehicle v_j, so it needs to rely more on reference to evaluate the vehicle. Therefore, the dynamic weight distribution can be achieved more accurately by taking the interaction frequency factor between vehicles as the parameter. When vehicle v_i interacts with v_j at time t, according to the historical interaction records, the proportion of all interaction time between vehicle v_i and v_j before time t in the whole time can be calculated as follows:

$$\rho = \frac{1}{\mathrm{Sum}_{i,j}} \sum_{n=1}^{\mathrm{Sum}_{i,j}} \frac{t_w(n)}{t_w(n) + t_s(n)}, \tag{8}$$

where $t_w(n)$ is the duration of the nth interaction and $t_s(n)$ is the interval of the nth interaction.

The more interaction times between nodes, the greater the proportion of interaction time, indicating that the interaction between v_i and v_j is more frequent. Therefore, the interaction frequency factor between vehicles is defined as

$$\omega_1 = \frac{\mathrm{Sum}_{i,j}}{\mathrm{Sum}_i} \times e^{\rho - 1}, \tag{9}$$

where Sum_i denotes the total number of interactions of vehicle v_i before time t. Thus, the expression of friendship $<\mathrm{Fre}, \mathrm{Deg}>_{i,j}$ holds as follows

$$<\mathrm{Fre}, \mathrm{Deg}>_{i,j} = \omega_1 < \mathrm{Mul}, \mathrm{Fre}, \mathrm{Deg}>_{i,j} + \omega_2 < \mathrm{Con}, \mathrm{Fre}, \mathrm{Deg}>_{i,j}, \tag{10}$$

where ω_2 represents the weight of reference friendship and $\omega_2 = 1 - \omega_1$.

4. Vehicle Clustering

To improve the transmission performance of VANETs, this section proposes a clustering algorithm based on friendship, which mainly includes three processes: dynamic cluster generation, cluster head selection, and dynamic cluster maintenance.

4.1. Cluster Generation. Because the vehicles in the same direction have similar speeds and have a relatively stable communication environment for a certain period, therefore, to maintain the stability of the cluster to the maximum extent and minimize the maintenance cost, the driving direction and speed of the vehicle are used as the basis for vehicle clustering.

Firstly, the scene is established based on the two-dimensional coordinate axis. The position and speed of vehicle v_i and v_j at time t are, respectively, represented by (x_i, y_i), $S_i(t) \longleftarrow (S_{ix}(t), y_{iy}(t))$ and (x_j, y_j), $S_j(t) \longleftarrow (S_{jx}(t), y_{jy}(t))$, the relative direction $O_{ij}(t)$, and the relative distance $D_{ij}(t)$.

Direction is the primary considered factor in the proposed clustering algorithm. At t time, the relative direction between vehicle v_i and v_j is calculated as follows:

$$O_{i,j}(t) = \cos\vartheta = \frac{S_i(t)S_j(t)}{\left|S_i(t)\right\|S_j(t)\right|} = \frac{S_{ix}(t)S_{jx}(t) + S_{iy}(t)S_{jy}(t)}{\sqrt{S_{ix}^2(t) + S_{iy}^2(t)}\sqrt{S_{jx}^2(t) + S_{jy}^2(t)}}, \tag{11}$$

where ϑ is the driving angle between vehicle v_i and vehicle v_j. When the value of ϑ is between $[-4/\pi, 4/\pi]$, it means that the vehicles have the same driving direction and can generate clusters; otherwise, it indicates the opposite direction of travel and cannot generate clusters.

The V2V communication in VANETs adopts DSRC technology, and its communication range is limited. Therefore, distance is the reference content of VANET clustering algorithm. At t time, the relative distance between vehicle v_i and v_j is

$$D_{i,j}(t) = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}. \tag{12}$$

It is necessary for vehicle v_i and v_j to form a cluster when $D_{i,j}(t)$ is in the DSRC transmission range. If $D_{i,j}(t)$ is beyond its range, vehicle v_i and v_j cannot form a cluster.

4.2. Selection of Cluster Head. To sum up, vehicle clustering is carried out concerning vehicle driving direction and speed, and the structure diagram of vehicle clustering is shown in Figure 1.

Among them, ordinary vehicles can only participate in the interaction as service requester or service provider, and cluster head (with ordinary vehicle identity) is responsible for the maintenance and management of the blacklist of the cluster and the relay of intercluster communication.

As mentioned earlier, cluster heads play an important role in the communication process of VANETs [24]. To ensure the high reliability of the leader and reduce the computing cost of the vehicle, we adopt the method of combining the friendship evaluation with the roadside unit- (RSU-) assisted selection of cluster heads.

When selecting a cluster head, not only the friendship is calculated according to the interaction behavior but also the relative mobility of vehicles should be considered. The main reason of considering the relative mobility of vehicles instead of the driving speed is that the vehicles in VANETs are all moving. The relative mobility RM_i of vehicle v_i can be

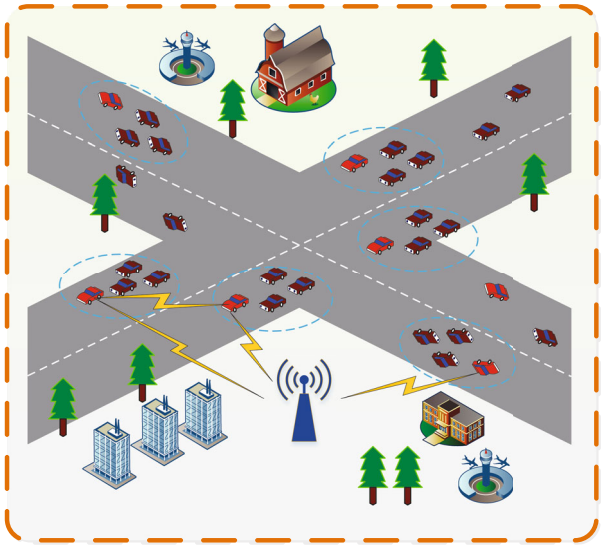

Figure 1: Vehicle cluster structure.

calculated in the following [25]:

$$\mathrm{RM}_i = 1 - \frac{1/n\sum_{j=1}^{n} V_{i,j}}{2V_{\max}}, \tag{13}$$

$$V_{i,j} = \frac{D_{i,j}}{T}, \tag{14}$$

where $V_{i,j}$ denotes the relative speed between v_i and v_j and T denotes the time length of a cluster remaining duration. According to the above expression, the value of RM_i is within the range [0,1]. The larger RM_i of a cluster head holds, the more stability the cluster is.

As mentioned above, vehicle-friendship conditions $<\mathrm{Fre}, \mathrm{Deg}>_{i,j}$ and RM_i are two factors for selecting cluster heads. However, compared with the size of RM_i, the friendly state $<\mathrm{Fre}, \mathrm{Deg}>_{i,j}$ of the vehicle has priority over RM_i. The reason is that the stability of the cluster can be maintained not only by selecting the larger RM_i but also by the subsequent cluster maintenance process. However, if the friendly vehicle is selected as V_{head}, the probability of a malicious vehicle as V_{head} will be increased accordingly, which will have an irreversible negative impact on network stability and security.

Therefore, the specific process of selecting V_{head} is as follows: firstly, the friendship of vehicle v_j is calculated and sent to RSU by cluster vehicle v_i according to the friendship assessment proposed in section 2-B; then, RSU selects the most friendly vehicle as cluster head V_{head}. If there are vehicles with the same friendship, V_{head} is selected according to the size of RM_i. Algorithm 1 describes how to select V_{head}. According to Algorithm 1, each vehicle can calculate and report its friendship to other vehicles independently; as a result, the friendship value comparison among all the vehicles needs computation complexity $O(n)$. Moreover, if there exist some vehicles with the same highest friendship evaluation, the cluster head is chosen by further comparing the relative mobility of those vehicles, the number of which (denoted by constant C) is far lower than n. In summary, the computation complexity of the cluster head selection holds as $O(nC)$.

4.3. Maintenance of Dynamic Cluster. Due to the rapid movement of vehicles in the network, the vehicles in the cluster will leave continuously or the vehicles outside the cluster will join at any time, which leads to the change of the network topology of the cluster. Therefore, to maintain the relative stability of the cluster topology as far as possible and reduce the impact of the change of the vehicle cluster structure on the network performance, this section aims to formulate the corresponding dynamic cluster maintenance strategy to ensure the stability of the whole network as far as possible.

Firstly, the departure of different types of vehicles in the cluster can be divided into the following two cases:

(1) If cluster head vehicle v_{head} wants to leave, the cluster will no longer exist

(2) If vehicle v_i is ready to leave the current cluster, v_i will first send the departure message to v_{head}, and then, vehicle v_i can leave after v_{head} confirms. At the same time, v_{head} sends the message of vehicle v_i leaving to the vehicles in the cluster to update the information in time. When v_i leaves the region of the original cluster and enters the region of other clusters, that is, v_i detects a new v'_{head} instead of the original v_{head}, v_i will join a new cluster as a cluster member or become a cluster head according to the cluster head selection process

Secondly, the addition of vehicles outside the cluster can also be divided into the following three cases:

(1) If vehicle v_j joins the network for the first time, it can use the supervision of neighbor vehicles and calculate the friendship according to Equation (10) as the friendship of v_j

(2) If the vehicle v_j moves from cluster C_1 to cluster C_2, in order to reduce the observation time, the behavior of v_j in cluster C_1, i.e., $v_{\mathrm{head}-1}$ is the friendship issued by v_j as the recommended friendship from $v_{\mathrm{head}-1}$ to $v_{\mathrm{head}-2}$, and the reference friendship of $v_{\mathrm{head}-2}$ to C_1 is calculated according to formula (7).

In addition, according to the direct interaction history of $v_{\mathrm{head}-2}$ and v_j, the interaction friendship of $v_{\mathrm{head}-2}$ to v_j is calculated by using formula (3). Furthermore, the friendship of v_j in cluster C_2 is calculated according to formula (10).

It is worth noting that in the above two cases, if the calculated friendship to vehicles outside the cluster is lower

1: Calculate $O_{i,j}(t) \longleftarrow$ Equation (11), $D_{i,j}(t) \longleftarrow$ Equation (12) to generate a cluster head
2: **if** failed **then**
3: return
4: else
5: vehicle v_i and $v_j ... v_n$ are in the cluster
6: calculate the friendship degree for all vehicles each other in the cluster by Equation (10) and sends them to RSU
7: **if** the friendship degree of v_i is the highest **then**
8: the vehicle v_i is selected as cluster head
9: **else**
10: calculate the mobility of v_i and v_j
11: **if** it still cannot select the cluster head **then**
12: return to the step 6
13: **else**
14: the mobility of v_i higher than v_j
15: the vehicle v_i is selected as cluster head
16: **end if**
17: **end if**
18: **end if**

Algorithm 1: Optimal power allocation algorithm.

than the average friendship in cluster C_2, then $v_{\text{head-2}}$ will not be added to the cluster.

(3) If two adjacent vehicle clusters merge, it is similar to reclustering, and a new cluster head needs to be reselected

5. Secure Double Key Message Forwarding

Although the friendly degree management method can effectively solve the problem of network internal attack in the process of cluster head selection, it cannot prevent an external attack in the process of message sending. Therefore, we design a secure and effective message forwarding strategy based on vehicle clustering, which mainly includes communication key generation and cluster communication.

5.1. Communication Key Generation. For different communication objects, this section uses a dual key system composed of vehicle's own key and cluster key [26]. Bilinear pairing is mainly used to generate key, and bilinear pairing is a way to realize identity based encryption. It defines three multiplicative cyclic groups G_1, G_2, and G_T of order q; g_1 and g_2 are generators of G_1 and G_2, respectively, and defines a mapping relation $e : G_1 \times G_2 \longrightarrow G_T$ on these three groups. At the same time, it is assumed that he/she is completely credible, and the public parameters $\{g_1, g_2, G_1, G_2, G_T\}$ of the system are published.

As mentioned above, after the cluster head is generated, RSU will send the information in the cluster to him/her through the secure channel. Then, he/she selects a random number $s_i \in Z_n^*$ for v_i as its temporary private key and calculates the corresponding temporary public key $P_i = g_2^{s_i}$ in a short time. Finally, he/she generates the cluster key key_c of the cluster through the corresponding private key s_i of each vehicle in the cluster and constructs the polynomial as follows:

$$f_c(x) = \text{key}_c + (x - s_1)(x - s_2) \cdots (x - s_n), \tag{15}$$

where $i = 1, 2, \cdots, n$ and n is the number of vehicles in the cluster. He/she sends the polynomial $f_c(x)$ to the corresponding v_{head}, and then, v_{head} sends $f_c(x)$ to the vehicles in the cluster. At this time, each vehicle (including v_{head}) in the cluster can calculate the cluster key $f_c(x) = \text{key}_c$ by substituting the private key s_i.

However, considering that the cluster key will change with the change of cluster structure, and the same key is not suitable for long-term use, therefore, to protect the forward and backward security of the cluster, the double key should be transient and valid only when the cluster structure remains unchanged. Next, according to the cluster maintenance in section 3-C, the corresponding cluster key management scheme is developed.

When vehicle v_i leaves, he/she needs to update the cluster key of cluster C and delete its corresponding polynomial factor $(x - s_i)$ in polynomial $f_c(x)$ to protect the backward security of the cluster. Specifically, v_{head} sends the message that v_i leaves the cluster and the original $f_c(x)$ to him/her at the same time, and then, he/she regenerates $f_c'(x)$ according to section 4-A.

When vehicle v_j joins, to protect the forward security of cluster C, he/she also needs to update the cluster key of cluster C. Contrary to the case of vehicle v_i leaving cluster C, in this case, its corresponding polynomial factor $(x - s_j)$ needs to be added to the polynomial $f_c(x)$ so that v_j can participate in the communication of cluster C. Similarly, v_{head} sends the message that v_j joins the cluster with the original $f_c(x)$ to him/her at the same time, and then, he/she regenerates $f_c'($ $x)$ according to section 4-A. In the process of key update, to avoid excessive communication overhead caused by the

key update, as long as cluster C exists, that is, v_{head} does not leave C, he/she does not need to update the key for the original vehicle, just update the cluster key.

5.2. Message Forwarding. Cluster communication process is divided into intercluster communication and intracluster communication. When two cluster heads $v_{\text{head}-1}$ and $v_{\text{head}-2}$ confirm the communication, they will encrypt the messages to be sent with each other's public key, respectively. Take $v_{\text{head}-2}$ sending messages to $v_{\text{head}-1}$ as an example. $v_{\text{head}-2}$ encrypts the message M with $v_{\text{head}-1}$'s public key:

$$\left[E_{P_{\text{head}-1}}(\text{PID}_{\text{head}-2}||M)\right], \tag{16}$$

where $M = \{\text{Content}_M||\text{Distance}_M||\text{Time}_M\}$ and Content_M represent the content of the forwarded message, respectively, Distance_M and Time_M represent the time and place of message M, respectively, $P_{\text{head}-1}$ is the public key of $v_{\text{head}-1}$ and $\text{PID}_{\text{head}-2}$ is the pseudonym of $v_{\text{head}-2}$.

After receiving the encrypted message from $v_{\text{head}-2}$, cluster head $v_{\text{head}-1}$ decrypts the packet with its private key and uses the message:

$$\left[D_{s_{\text{head}-1}}\left(E_{P_{\text{head}-1}}(\text{PID}_{\text{head}-2}||M)\right)\right]. \tag{17}$$

Through intercluster communication, cluster head $v_{\text{head}-1}$ can obtain the specific content, time, and place of the message M from $v_{\text{head}-2}$. But at this time, only $v_{\text{head}-1}$ in cluster C_1 gets the message, so in order to make other vehicles in the cluster get the message, $v_{\text{head}-1}$ has the responsibility to forward the message to the members in the cluster. Firstly, $v_{\text{head}-1}$ encrypts the message through the cluster key Key_c of cluster C_1 and forwards it to the vehicles in the cluster:

$$\left[E_{\text{key}_c}(\text{PID}_{\text{head}-1}||M)\right]. \tag{18}$$

After receiving the message from $v_{\text{head}-1}$, the vehicles in cluster C_1 can use key_c to decrypt the ciphertext to obtain the message M:

$$\left[D_{s_{\text{head}-1}}\left(E_{\text{key}_c}(\text{PID}_{\text{head}-1}||M)\right)\right]. \tag{19}$$

It can be seen that by using clustering technology, only cluster head vehicles are required to participate in message forwarding to ensure that multiple vehicles can obtain messages at the same time, to reduce the communication resource consumption of independent communication between vehicles.

In addition, if $v_{\text{head}-1}$ obtains a malicious message from the malicious cluster head $v_{\text{head}-2}$ and forwards it to the member vehicles in the cluster, once the vehicles in the cluster, including $v_{\text{head}-1}$ and the member vehicles in the cluster, recognize that the message is false or malicious, they need to send the result to other vehicles immediately. If the malicious message is found in the vehicle $v_{\text{head}-1}$, the warning message is sent to the member vehicles in the cluster C_1 through the communication mode of the vehicles; if the vehicle that finds the malicious message is a cluster member vehicle, the cluster member vehicle forwards the warning message to the cluster head.

6. Simulation Results

In this section, the performance of the proposed strategy is validated through extensive simulations by NS2 software. To verify the effectiveness of the proposed FASMF algorithm, the proposed FASMF strategy is compared with NSTCM [20], SGC [19], and TJET [21] in terms of average message delivery rate, average message delay, and cluster stability. The simulation parameter settings are shown in Table 1.

6.1. Influence of Vehicle Number on Network Performance. With the increase of the number of vehicles in the cluster, the average delivery rate, average delay, and cluster stability of FASMF strategy and NSTCM, SGC, and TJET are shown in Figures 2, 3, and 4, respectively.

It can be seen from Figure 2 that with the increase in the number of vehicles, the message delivery rates of the FASMF strategy and the other three strategies are on the rise. Although NSTCM uses encryption to protect the security of message transmission in VANETs, it uses the method of region division to form a cluster of vehicles in the region; the vehicles in the cluster still exist independently without any social relationship, resulting in the low overall message delivery rate. In addition, the FASMF strategy, SGC, and TJET strategy proposed in this paper contain the cluster head and the corresponding security policy and forward the message to the member vehicles in the cluster through the cluster head, so it has a high message delivery rate. However, the message delivery rate of the FASMF strategy is higher than that of the SGC and TJET strategies. The reason is that SGC and TJET strategies lack corresponding security measures for messages in the process of message transmission, and SGC lacks a corresponding cluster head selection process. TJET only selects cluster heads according to the front and rear positions of vehicles, so the latter two cannot guarantee the reliability of cluster heads. After the cluster head fails, the message cannot be delivered in time.

Figure 3 shows that as the number of vehicles increases, the average message delay of the four strategies is on the rise. The delay of the NSTCM strategy is the lowest, mainly because the vehicles in its encrypted area can communicate directly and reduce the communication time. Compared with SGC and TJET strategies, the FASMF strategy has a lower average delay. The main reason is that although FASMF uses double key message encryption transmission to increase its delay, because it uses friendship to select cluster heads, the calculation process of the double key scheme adopted in this paper is smaller, while SGC and TJET strategies both use more complex key schemes; at the same time, TJET uses the tree to manage vehicles in a distributed way, which results in the highest delay.

Table 1: Simulation parameter setting.

Parameter	Parameter value
Network area (m^2)	3000×3500
Number of vehicles	50-450
Vehicle moving model	SUMO
Vehicle speed (km/h)	0-45
Vehicle communication protocol	802.11p
Vehicle communication mode	DSRC
Initial friendship	0
Simulation time (h)	6

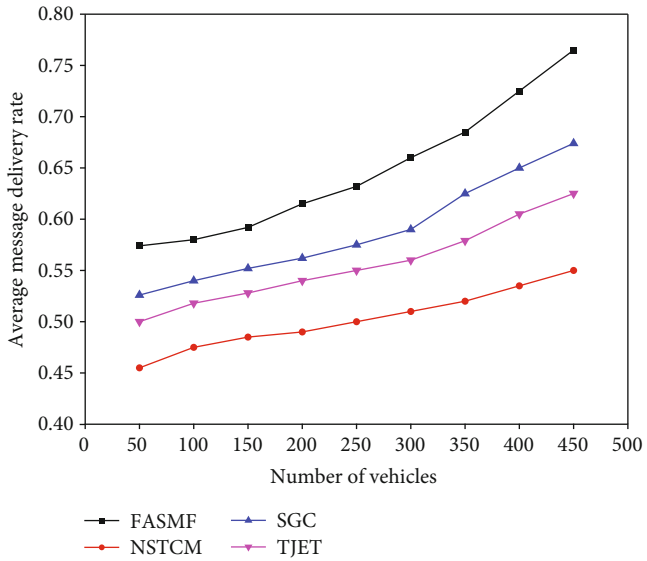

Figure 2: Influence of vehicle number on the average delivery rate of messages in each mechanism.

In Figure 4, with the increase of the number of vehicles in the network, the average lifetime of cluster heads of each strategy increases gradually, which indicates that the stability of clusters is positively correlated with the increase of the number of vehicles. However, the NSTCM strategy has no cluster head in the encrypted area and only uses the encryption algorithm to protect the security of the area. It cannot identify the attacker. Once the attacker enters the area and obtains the key, the security of the vehicle and communication in the area is threatened, so the network stability is the worst. In addition, the average survival time of cluster heads of the SGC strategy is longer than that of TJET. The main reason is that the vehicle tracking strategy is adopted in TJET, and the cluster head selection is determined only by the location of vehicles, so the stability of TJET is lower than SGC. Compared with the SGC strategy, the FASMF designed in this paper considers the factors of vehicle speed, direction, and so on in the process of cluster formation and uses the social friendship between vehicles to select the cluster head. If the friendship of new members is greater than the current cluster head, the FASMF will update the cluster head, so it has a better stability.

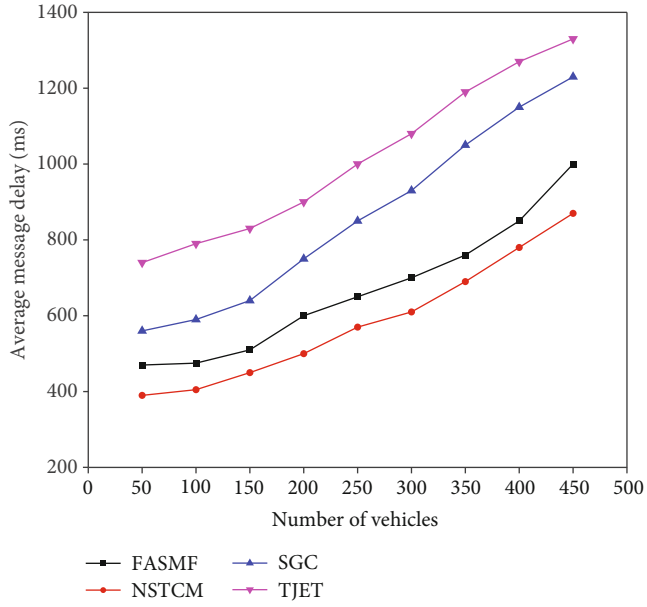

Figure 3: Influence of vehicle number on the average delay of messages in each mechanism.

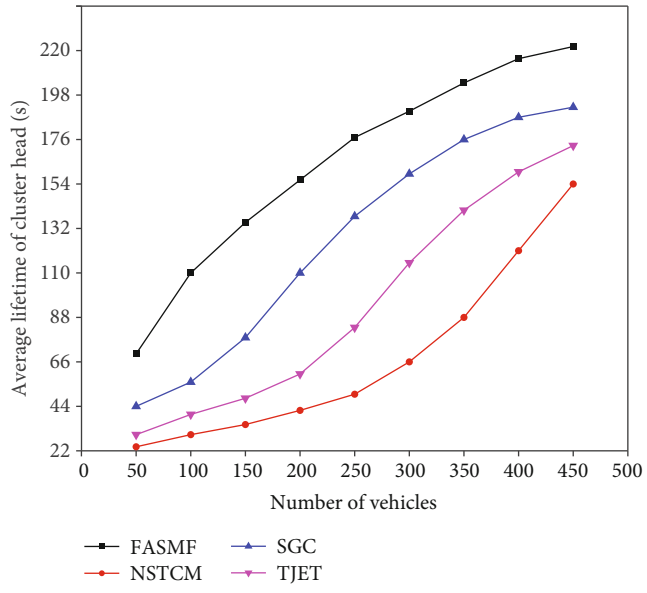

Figure 4: Influence of the number of vehicles on the average survival time of cluster heads.

6.2. Influence of Vehicle Speed on Network Performance. In VANETs, the speed of vehicles not only affects the formation of vehicle clusters but also the fast mobility of vehicles affects the stability of vehicle clusters. The analysis of vehicle speed on the average delivery rate, message average delay, and network stability of the proposed FASMF strategy and NSTCM, SGC, and TJET strategies are shown in Figures 5, 6, and 7, respectively.

As shown in Figure 6, the average message delivery rate of the FASMF strategy, NSTCM strategy, SGC strategy, and TJET strategy decreases with the increase of vehicle speed. This is because the faster the vehicle speed is, the frequent

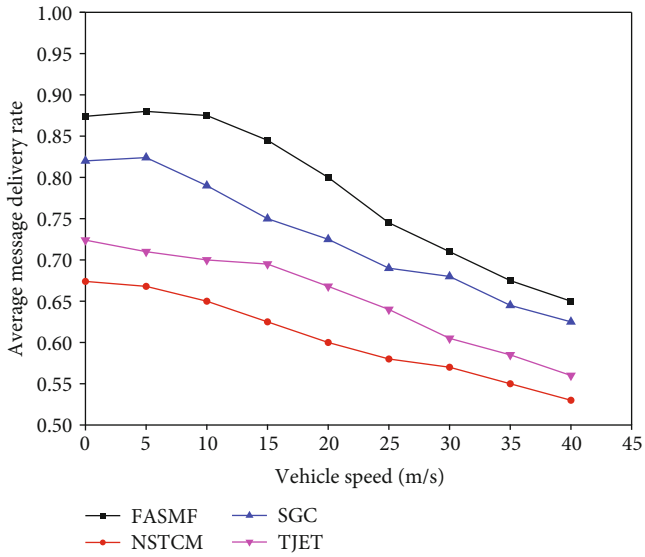

Figure 5: Influence of driving speed on average message delivery rate of each mechanism.

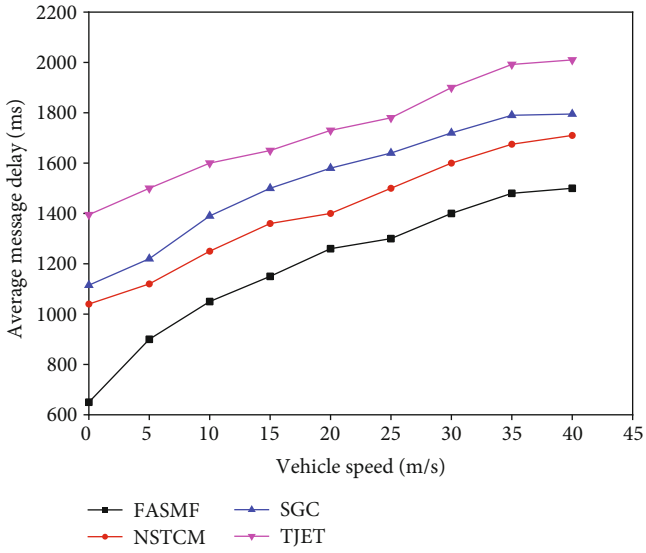

Figure 6: Influence of driving speed on average message delay of each mechanism.

interruption of communication links between vehicles increases the difficulty of message forwarding, and the average message delivery rate of the four schemes decreases. However, the FASMF strategy proposed in this paper involves reasonable cluster head selection, clustering, and cluster maintenance scheme, so compared with the other three strategies, the message delivery rate is higher.

As shown in Figure 7, with the increase of vehicle speed, the average message delay of FASMF, NSTCM, SGC, and TJET strategies increases in this paper. This is because the faster the driving speed is, the faster the relative relationship between vehicles will change, the easier the cluster head will be replaced by other vehicles, and more time will be consumed in cluster maintenance. In

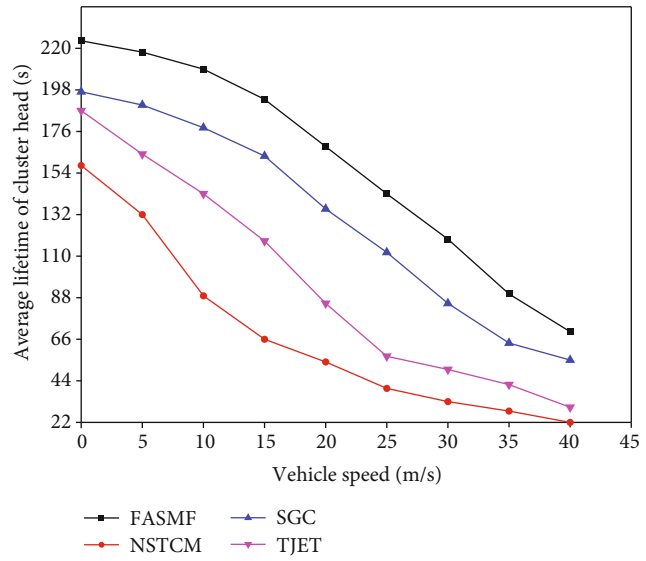

Figure 7: Influence of driving speed on average survival time of cluster heads.

addition, the higher the vehicle speed, the lower the stability of the cluster, and the frequent interruption of the communication link will also lead to the increase of the average message delay. However, because of the physical factors such as relative location factors and relative speed, the FASMF strategy introduced in this paper has stronger cluster stability than the other three strategies, so the time delay is the lowest. NSTCM uses the method of regional encryption, so when the vehicle speed increases, it will generate more time only in the cross-region, so its delay is lower than the SGC and TJET strategies.

As shown in Figure 7, the average lifetime of cluster heads of FASMF, NSTCM, SGC, and TJET strategies shows an overall downward trend. The reason is that the topology of VANETs is greatly affected by vehicle speed. The increase of speed leads to frequent changes in the network topology of clusters, which makes it difficult to maintain the relative stability of clusters. The NSTCM strategy uses area encryption, and the vehicles in the area can communicate. Therefore, network stability is most affected by the increase of speed, and the increase of vehicle speed reduces the duration of vehicles in the region. In addition, the average time of cluster heads of SGC and TJET strategies is lower than the FASMF strategy proposed in this paper. This is because the FASMF strategy designed in this paper not only takes into account the mobility of vehicles but also takes into account the friendship of vehicles, so the cluster heads still have strong stability.

7. Conclusion

To enhance the security of VANET message forwarding process and improve the efficiency of message forwarding, we propose a VANET message forwarding mechanism with the dynamic evaluation of friendship by combining friendship evaluation and double key method. The vehicles on

the road are divided into several clusters by clustering technology, and then, the vehicles in the cluster select the cluster head as the vehicle of intercluster communication according to the result of friendship evaluation and forward the message using message encryption. The results show that vehicle mobility as a factor of vehicle clustering can effectively improve the message delivery rate and reduce the message leakage rate, and the proposed strategy can effectively enhance the stability of the cluster topology.

Data Availability

The experiment data used to support the findings of this study are currently under embargo while the research findings are commercialized. Requests for data, 12 months after publication of this article, will be considered by the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the anonymous reviewers for their thorough and constructive comments that have helped improve the quality of the paper.

References

[1] J. Xiong, R. Bi, Y. Tian, X. Liu, and D. Wu, "Towards lightweight, privacy-preserving cooperative object classification for connected autonomous vehicles," *IEEE Internet of Things Journal*, 2021.

[2] D. Wu, R. Bao, Z. Li, H. Wang, H. Zhang, and R. Wang, "Edge-cloud collaboration enabled video service enhancement: a hybrid human-artificial intelligence scheme," *IEEE Transactions on Multimedia*, vol. 23, pp. 2208–2221, 2021.

[3] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. Park, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15824–15838, 2021.

[4] B. Zhao, X. Liu, W.-N. Chen, W. Liang, X. Zhang, and R. H. Deng, "Price: privacy and reliability-aware real-time incentive system for crowdsensing," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17584–17595, 2021.

[5] H. Zhu, F. Wang, R. Lu, F. Liu, G. Fu, and H. Li, "Efficient and privacy-preserving proximity detection schemes for social applications," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2947–2957, 2018.

[6] J. Li, J. Ma, Y. Miao, F. Yang, X. Liu, and K.-K. R. Choo, "Secure semantic-aware search over dynamic spatial data in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 8912–8925, 2021.

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

[8] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[9] X. Li, H. Zhang, Y. Miao et al., "Can bus messages abnormal detection using improved SVDD in internet of vehicle," *IEEE Internet of Things Journal*, 2021.

[10] D. Wu, B. Yang, H. Wang, C. Wang, and R. Wang, "Privacy-preserving multimedia big data aggregation in large-scale wireless sensor networks," *Acm Transactions on Multimedia Computing Communications & Applications*, vol. 12, no. 4s, pp. 1–19, 2016.

[11] J. Yu and P. Chong, "A survey of clustering schemes for mobile ad hoc networks," *IEEE Communications Surveys Tutorials*, vol. 7, no. 1, pp. 32–48, 2005.

[12] T. Maniak, R. Iqbal, and F. Doctor, "Hierarchical spatial-temporal state machine for vehicle instrument cluster manufacturing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4131–4140, 2021.

[13] M. Yang, B. Ai, R. He et al., "Measurements and cluster-based modeling of vehicle-to-vehicle channels with large vehicle obstructions," *IEEE Transactions on Wireless Communications*, vol. 19, no. 9, pp. 5860–5874, 2020.

[14] Z. Li, Y. Jiang, Y. Gao, L. Sang, and D. Yang, "On buffer-constrained throughput of a wireless-powered communication system," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 283–297, 2019.

[15] W. Wang, A. Ramesh, J. Zhu, J. Li, and D. Zhao, "Clustering of driving encounter scenarios using connected vehicle trajectories," *IEEE Transactions on Intelligent Vehicles*, vol. 5, no. 3, pp. 485–496, 2020.

[16] K. Abboud and W. Zhuang, "Impact of microscopic vehicle mobility on cluster-based routing overhead in <roman>VANETs</roman>," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5493–5502, 2015.

[17] W. Wang, F. Xia, H. Nie et al., "Vehicle trajectory clustering based on dynamic representation learning of internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3567–3576, 2021.

[18] Z. Liu, Y.-A. Xie, Y. Yuan, K. Ma, K. Y. Chan, and X. Guan, "Robust power control for clustering-based vehicle-to-vehicle communication," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2557–2568, 2020.

[19] C. Lai, H. Zhou, N. Cheng, and X. S. Shen, "Secure group communications in vehicular networks: a software-defined network-enabled architecture and solution," *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 40–49, 2017.

[20] L. Zhang, "Otibaagka: a new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2998–3010, 2017.

[21] C. Xu, R. Lu, H. Wang, L. Zhu, and C. Huang, "TJET: ternary join-exit-tree based dynamic key management for vehicle platooning," *IEEE Access*, vol. 5, pp. 26973–26989, 2017.

[22] J. Cui and B. Zhang, "Vera: a simplified security risk analysis method for autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 10494–10505, 2020.

[23] L. Chen, J. Zhou, Y. Chen, Z. Cao, X. Dong, and K.-K. R. Choo, "PADP: efficient privacy-preserving data aggregation and dynamic pricing for vehicle-to-grid networks," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7863–7873, 2021.

[24] Y. Tian, Z. Zhang, J. Xiong, L. Chen, J. Ma, and C. Peng, "Achieving graph clustering privacy preservation based on structure entropy in social IoT," *IEEE Internet of Things Journal*, 2021.

[25] Z. Cui, J. Sun, X. U. Songyan, and X. Jiang, "A secure clustering algorithm of ad hoc network for colony UAVs," *Journal of Shandong University(Natural Science)*, vol. 53, no. 7, pp. 54–62, 2018.

[26] X. Liu, R. H. Deng, K.-K. R. Choo, and Y. Yang, "Privacy-preserving outsourced clinical decision support system in the cloud," *IEEE Transactions on Services Computing*, vol. 14, no. 1, pp. 222–234, 2021.