Hindawi
Security and Communication Networks
Volume 2021, Article ID 9967829, 13 pages
https://doi.org/10.1155/2021/9967829

Research Article

Research on Manhattan Distance Based Trust Management in Vehicular Ad Hoc Network

Xiaodong Zhang,[1,2] **Ru Li**,[1,2] **Wenhan Hou**,[1,2] **and Jinshan Shi**[1,2]

[1] *Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Hohhot 010021, China*
[2] *College of Computer Science, Inner Mongolia University, Hohhot 010021, China*

Correspondence should be addressed to Ru Li; csliru@imu.edu.cn

Received 1 April 2021; Revised 31 May 2021; Accepted 23 June 2021; Published 6 July 2021

Academic Editor: Rongxing Lu

In recent years, Vehicular Ad Hoc Network (VANET) has developed significantly. Coordination between vehicles can enhance driving safety and improve traffic efficiency. Due to the high dynamic characteristic of VANET, security has become one of the challenging problems. Trust of the message is a key element of security in VANET. This paper proposes a Manhattan Distance Based Trust Management model (MDBTM) in VANET environment which solves the problem in existing trust management research that considers the distance between the sending vehicle and event location. In this model, the Manhattan distance and the number of building obstacles are calculated by considering the movement relationship between the sending vehicle and event location. The Dijkstra algorithm is used to predict the path with the maximum probability, when the vehicle is driving toward the event location. The message scores are then calculated based on the Manhattan distance and the number of building obstacles. Finally, the scores are fused to determine whether to trust the message. The experimental results show that the proposed method has better performance than similar methods in terms of correct decision probability under different proportions of malicious vehicles, different numbers of vehicles, and different reference ranges.

1. Introduction

With the development of wireless communication technology and the automotive industry, the Vehicular Ad Hoc Network (VANET) has made significant development, which enhances driving safety and traffic efficiency. Intelligent traffic management has been realized through the communication collaboration of Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrians (V2P), Vehicle to Cloud (V2C), and so on. The application scenarios in VANET mainly include safety application scenario and nonsafety application scenario [1]. These applications are based on the exchange of messages between entities. However, security is one of the main issues in VANET, and how to ensure the security of these messages has become an important issue in this filed. While mechanisms based on certificates [2, 3], signatures [4], and Public Key Infrastructure (PKI) [5] already exist to address the issue of message security, they can only solve the problem of transmitted message not being tampered maliciously and ensure that the message comes from an authorized vehicle; they cannot resolve the authenticity of the messages themselves (i.e., the trust of the message). For example, malicious vehicle can broadcast information that claims that the road is not congested, but that traffic accident or congestion has actually occurred. Such malicious behaviour may seriously jeopardize traffic safety or efficiency. The trust of message is therefore a key element of security [6]. How to effectively evaluate the trust of the messages sent by vehicles has become an important issue. In other words, trust management of the messages sent by vehicle is very important.

At present, many researches focus on trust management in the VANET environment, mainly including three types: entity-centric trust management [7–9], data-centric trust management [10–15], and combined trust management [16, 17].

Many researches [7, 10, 11, 13, 14] consider the distance between the sending vehicle and event location, suggesting that such distance can indirectly reflect trust of message. The farther away from the event, the lower trust value of message. However, in these researches, the calculation of the distance is not discussed in detail. As a matter of fact, the traditional Euclidean distance cannot reflect the actual distance when vehicles are on city roads. In addition, on city roads, there may be building obstacles from the sending vehicle to event location. The line of sight between the sending vehicle and event location is affected by the existence of building obstacles. Whether building obstacles exist or not, this can result in entirely different trust. However, the existing trust management model does not take into account the existence of building obstacles.

Manhattan distance is the city block distance, that is, from one point to another on the actual road. Manhattan distance can reflect the actual distance between the sending vehicle and event location. At the same time, on the path of the actual distance, the number of building obstacles can also be determined. Therefore, this paper proposes a Manhattan Distance Based Trust Management model (MDBTM) in VANET. In this model, the receiving vehicle first calculates the Manhattan distance and the number of building obstacles on Manhattan distance path, then calculates score based on the Manhattan distance and the number of building obstacles for each message about a certain event, and finally fuses all the scores to calculate its trust value to determine whether it trusts the received message.

The contributions of this paper mainly include the following:

(1) Considering that the vehicle is on the road and the Euclidean distance cannot reflect the actual driving distance of vehicle, a method of calculating the distance between the sending vehicle and event location using Manhattan distance is proposed.

(2) This paper proposes a trust management model that takes into account both the Manhattan distance and the number of building obstacles.

(3) The experimental results show that the proposed method has better performance than similar methods in terms of correct decision probability under different proportions of malicious vehicles, different numbers of vehicles, and different reference ranges.

The rest of the paper is organized as follows: Section 2 introduces current research on trust management in VANET and analyzes the existing problems. Section 3 introduces the system model and the problem formation. Section 4 introduces the MDBTM scheme. Section 5 verifies the effectiveness of the proposed scheme by experimental simulation. Section 6 summarizes full paper and proposes future work.

2. Related Works

At present, many researches focus on trust management in the VANET environment, mainly including three types: entity-centric trust management, data-centric trust management, and combined trust management.

In entity-centric trust management research, trust level of the entity mainly is studied and the trust value of message is judged indirectly. Minhas et al. [7] proposed a trust model that took into account the trustworthiness of the agents of other vehicles. This model considers location closeness, time closeness, experience-based trust, and role-based trust when aggregating messages. Marmol et al. [8] proposed an infrastructure-based trust and reputation model. This model considers recommendation value given by other vehicles and RSUs and trust value of vehicle at the last moment in calculating the trust value of message. Haddadou et al. [9] proposed a distributed trust management method which used the job market signaling model to motivate more cooperation among selfish nodes.

In data-centric trust management research, the focus is on the consistent judgment of received messages. Raya et al. [10] proposed a data-centric trust framework. The framework first calculates the trust levels of a report on the same event by default trustworthiness, event- or task-specific trustworthiness, dynamic trustworthiness factors, location, and time and then combines those trust levels to decide whether the reported event has occurred. Wu et al. [11] proposed an RSU-Aided scheme for data-centric trust establishment in VANETs. In this scheme, RSU calculates the observation factor of the received reports according to confidence (one of the factors that affect confidence is the distance from the sending vehicle to event location) and weight and then integrates the observation factor and feedback factor through the ant colony optimization algorithm to recalculate the trust level of each evidence. Gurung et al. [12] proposed an information-oriented trust model which considered three factors: content similarity, route similarity, and content conflict. Shaikh et al. [13] proposed a distributed intrusion-aware trust model for vehicular ad hoc networks that worked in three phases. The first phase calculates the confidence value of each message based on location closeness, time closeness, location verification, and time verification, and the second phase calculates trust value based on confidence of each message. A decision is taken in the third phase. Yang et al. [14] proposed a distributed trust management scheme based on the blockchain. First, the credibility of the message is calculated by the distance between the sending vehicle and event location, and the credibility of all messages is fused through Bayesian inference to generate a message rating. The message rating is aggregated to calculate trust value offset, and finally offset value is stored in the blockchain. Chen et al. [15] proposed a topology-based secure message transmission method, which modeled the actual transmission path of a message in network to determine the probability of the correct message decision.

In combined trust management research, the focus is on the trust level of the entity and the consistent judgment of received messages at the same time. Chen et al. [16] proposed a beacon-based trust management system which considered entity trust and data trust at the same time. This system constructs entity trust from beacon messages and calculates data trust by cross-checking the plausibility of event messages and beacon messages. Li et al. [17] proposed an attack-resistant trust management scheme that could detect and cope with malicious attacks and evaluate the trust of data and mobile nodes in VANET.

In short, current researches of trust management mainly focus on trust level of the entity and the consistency of the message content. At present, in the researches of distance considerations shown in Table 1, there is the problem of no detailed discussion on the method of calculating distance. In this paper, a method of calculating distance is proposed to solve the above problems. This method takes into account the vehicle in the city road environment and the situation where buildings block the line of sight, which makes up for the inadequacy of existing work.

3. System Model and Problem Formation

In this section, this paper first introduces the system model including network model, data propagation model, and attack model. Then it briefly describes the problem to be solved in this paper.

3.1. Network Model and Data Propagation Model. This system operates in the city road environment. Vehicles on the road have the function of communicating via VANET. Vehicles in the network can send messages on their own initiative, for either entertainment-related or security-related ones. This paper considers security-related messages. The content of a specific report is called event $e_i\,(i = 1, 2, \ldots, \text{Enum})$, where i is used to distinguish between event types, and Enum is the number of events. For example, "whether or not a traffic accident occurred at X location" is an event, with two situations occurring and not occurring for each event, expressed in terms of 1 and 0, respectively.

The vehicle receiving a message will decide whether to respond to the message, for example, by changing the driver path based on what is reported in the message. However, due to the existence of malicious vehicles, the vehicle will receive false messages and be required to manage the trust of message. The roads in the city are very complicated. There are many vehicles on the roads. Messages sent by vehicles away from the event location have no referential meaning and increase the amount of computation during trust management. Therefore, this paper considers a reference range R. The reference range R is a circular area centered on the event location and only the messages sent by vehicles within this range are considered when calculating the trust value of message. The specific network model diagram is shown in Figure 1.

When vehicles report safety-related messages, there is no need to consider which is the destination vehicle. Therefore, this paper considers the way of broadcasting to transmit the messages. In addition to the content of the event, the transmitted message also requires the transmission of vehicle identification and Global Positioning System (GPS) information. The information transmitted belongs to the vehicles' privacy data. In order to protect their private data, the data are encrypted during transmission, and other vehicles must be authorized to access them. The specific methods of privacy preserving are not the focus of this paper. Please refer to [18–21] for details. Because propagation speed of message is much faster than moving speed of vehicle, it ignores the time it takes to propagate messages from a vehicle to other vehicles. The process is considered to be a static network [22]. Therefore, when a vehicle receives a message, it can be assumed that the message is at the current moment. In other words, there is no need to consider how the delay in message propagation causes the state of the event to change.

3.2. Attack Model. Vehicles on the road include normal vehicles and malicious vehicles. Normal vehicles will send true message about an event. However, malicious vehicles will send false message about an event.

In the VANET environment, the malicious vehicles can generate three types of threats including attacks addressing secure communications, attacks addressing safety applications, and attacks addressing infotainment applications. Different types of threats target different services, including authenticity, confidentiality, privacy, availability, integrity, and nonrepudiation [23]. This paper mainly solves the problem that the malicious vehicle launches betrayal attack aiming at authenticity; i.e., vehicle deliberately sends false messages to affect the traffic safety.

The vehicle sending the message is called the source vehicle, and the vehicle receiving the message is called the destination vehicle. Due to the high dynamic characteristics of VANET, the source and destination vehicles may not be able to communicate directly, and relayed vehicles may be required for forwarding messages. Therefore, vehicles that affect the credibility of the destination vehicles' judgment include source vehicle and relay vehicle. In other words, malicious vehicles may exist in both source vehicles and relay vehicles. When the source vehicle is a malicious vehicle, a false message will be sent. When the relay vehicle is a malicious vehicle, it will tamper with the content of the received message before forwarding it, thus resulting in a false message. This paper mainly studies the effect of the distance on the trust value of message and assumes that the system has adopted the methods of certificate and signature to ensure the relay vehicle cannot tamper with the message. Therefore, this paper mainly studies the situation where the source vehicle is a malicious vehicle.

Table 1: Comparison of researches considering distance.

Approach	Trust metric	Architecture	Advantage	Disadvantage
Minhas et al. [7]	✓Time closeness ✓Location closeness (distance) ✓Experience ✓Role	Centralized	Easy to find malicious vehicles.	No discussion of the calculation method of distance.
Raya et al. [10]	✓Time ✓Distance ✓Node type ✓Event type	Distributed	Easy to find false messages.	No discussion of the calculation method of distance.
Wu et al. [11]	✓Distance ✓Number of sensors ✓Node type	Centralized	Easy to find false messages.	No discussion of the calculation method of distance.
Shaikh et al. [13]	✓Location closeness (distance) ✓Time closeness ✓Location verification ✓Time verification ✓Number of senders	Distributed	Easy to implement in VANETs.	No discussion of the calculation method of distance.
Yang et al. [14]	✓Distance	Distributed	Provide security trust management method using blockchain.	No discussion of the calculation method of distance.

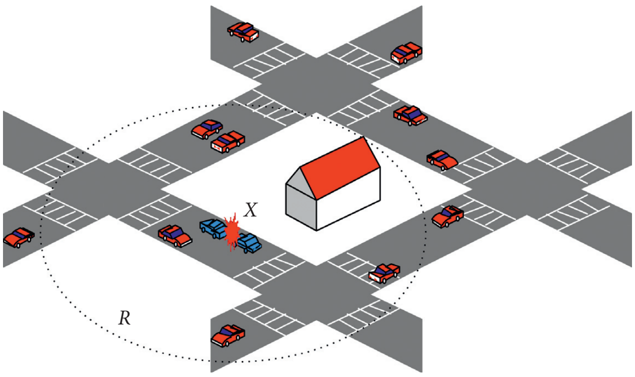


Figure 1: The diagram of network model.

3.3. Problem Formation. Vehicles on the road will send safety-related messages. When the destination vehicle receives the message m_0, it needs to determine whether it is trusted. Assume that the message is about a certain event $e\prime, e\prime \in e_i\, (i = 1, 2, \ldots, \text{Enum})$, where Enum represents the number of the event types. If a judgment is made immediately upon receipt of a message, the trust value of message cannot be judged because no message is referenced. Therefore, it requires a waiting time T and then uses the messages received in the time period T about event e' as a reference message set $M'\{m_1, m_2, \ldots, m_{\text{Num}}\}$ to determine whether the message is trusted. The Num is the number of messages received, which can be calculated in equation (1):

$$\text{Num} = \text{Fre} \times V\text{num} \times T, \tag{1}$$

where Fre represents the frequency at which messages are sent by the vehicle, Vnum represents the number of vehicles in the reference range R, and T represents the waiting time. However, if the vehicle sends messages very frequently, it may receive multiple messages about event e' from the same vehicle within the T time. Therefore, it is necessary to remove duplicate messages from the reference set M' and then use the rest of the messages as the final reference message set $M\{m_1, m_2, \ldots, m_N\}$, in which N is the number of messages from different vehicles within a reference range R about event e'.

If the report of event e' in the reference set M is consistent with that of the message m_0, the trust value of message can be directly judged. However, because of the existence of malicious vehicles, they can send false messages about certain events. When other vehicles receive messages about event e', they receive conflicting messages and cannot directly determine the trust value of message m_0.

The Manhattan distance and the number of building obstacles can indirectly reflect the trust value of message. The vehicles are driving on the road, so the actual road needs to be modeled first. The actual road is a road network composed of nodes and road sections. Therefore, this paper uses the graph in the data structure to model the actual road. In the graph, nodes are represented by the vertices, and the road segments between two nodes are represented by the edges of graph. The node is an intersection on a city road. Its basic attributes include the node identifier, node longitude, and node latitude. The road segment is a road between two nodes. Its basic attributes include the road identifier, starting node, end node, road length, whether it can go straight, whether it can turn right, or whether it can turn left. The attributes of the forward and reverse road segments are not necessarily the same between the two nodes, so the weighted directed graph $G = (V, E)$ is used to model the actual road. The weight value is a specific attribute value of the road segment. In this paper, the road identifier is selected as the weight to easily correspond to the road segment attributes.

Through the above method, the actual road can be modeled, and the Manhattan distance and the number of building obstacles can be calculated by combining with the vehicle's motion state. The research goal of this paper is to calculate the message score $S_i^{e'}(i = 0, 1, \ldots, N)$ by the Manhattan distance and the number of building obstacles between the vehicle sending message m_i about event e' and the event location. Then all the scores are fused to calculate the trust value of message m_0 about event e' denoted by $\text{Trust}(e' \longrightarrow m_0)$. If $\text{Trust}(e' \longrightarrow m_0) > 0$ then the message m_0 can be trusted; otherwise the message cannot be trusted. $\text{Trust}(e' \longrightarrow m_0)$ is formally defined by

$$\text{Trust}\left(e' \longrightarrow m_0\right) = \text{Fuse}\left(S_0^{e'}, S_1^{e'}, \ldots, S_N^{e'}\right). \tag{2}$$

4. Proposed MDBTM

The proposed MDBTM scheme is discussed in detail in this section. First, according to the event e' reported by the received message m_0, the reference message set $M\{m_1, m_2, \ldots, m_N\}$ is obtained, and the Manhattan distance and the number of building obstacles of vehicles that sent these messages including message m_0 and messages in M are calculated. Then scores of all these messages are calculated by the Manhattan distance and the number of building obstacles. Finally, all these scores are fused to calculate the trust value of event e' reported by the message m_0. That is, the trust value of message m_0.

4.1. The Calculation of Manhattan Distance. For a town street that is regularly laid out in the direction of south and north, east and west, the Manhattan distance is the distance from north to south plus the distance from east to west. However, the actual road is not the same. The attributes of the nodes are different, and the road cannot go straight, turn left, or turn right at any time. Therefore, it is necessary to calculate the Manhattan distance in combination with the actual road. In addition, the movement relationship between the sending vehicle and event location is different, which will lead to different Manhattan distance. Therefore, when calculating the Manhattan distance, it also needs to consider the movement relationship.

There are three types of movement relationship: driving away from the event location, not passing the event location, driving toward the event location.

Driving away from the event location: If the vehicle passes the event location based on the historical trajectory information of that vehicle, the movement relationship is driving away from the event location. The Manhattan distance can be obtained from the historical trajectory information of the vehicle. The historical trajectory information can be obtained from RSU and is also privacy data of vehicle. In order to protect it, the data are encrypted during transmission, and other vehicles must be authorized to access them from RSU.

Not passing the event location: If the vehicle does not pass through the event location based on the historical trajectory information of the vehicle and the vehicle's movement direction is far away from the event location, the movement relationship is not passing the event location. In this case, we believe that the vehicle will not pass the event location or the probability is small, so the Manhattan distance is infinite.

Driving toward the event location: If the vehicle does not pass the event location based on the historical trajectory information of the vehicle and the vehicle's movement direction is close to the event location, the movement relationship is driving toward the event location. In this case, the vehicle may or may not pass the event location. Therefore, it is necessary to predict whether the vehicle will pass the event location based on the GPS information of sending vehicle and the actual road.

The Manhattan mobility model is a model that simulates the movement of vehicles on city roads. In this model, when the vehicle reaches the intersection, it will go straight with a probability of 0.5 and turn left or right with a probability of 0.25 [24]. If the vehicle is not allowed to go straight, turn left, or turn right at the intersection, the corresponding selection probability will be divided equally to other options. For example, if an intersection is not allowed to turn left, then it will go straight with a probability of 0.625 and turn right with a probability of 0.375 when the vehicle arrives at the intersection. It can be seen that this model can describe the movement of vehicles at the intersection on city roads. Therefore, this paper uses this model and the actual road to predict the probability of the vehicle passing the event location. There may be multiple paths from the vehicle to event location. This paper selects the path of maximum probability to calculate the Manhattan distance.

In summary, the flow chart for calculating the Manhattan distance between the sending vehicle and event location is shown in Figure 2.

4.1.1. The Vehicle's Movement Direction. The vehicle's movement direction includes close to the event location and far away from the event location. The location of the vehicle can be obtained by the GPS information on it. Assume that the sending vehicle is located in $A(lng_1, lat_1)$ at the previous time t' and that vehicle is in $\text{B}(lng_2, lat_2)$ at the current time t and the event occurred in $\text{C}(lng_3, lat_3)$. So, the movement direction vector of the vehicle is $\overrightarrow{AB}(lng_2 - lng_1, lat_2 - lat_1)$, and the vector from its current position to event location is $\overrightarrow{BC}(lng_3 - lng_2, lat_3 - lat_2)$. Define the angle between vector $\overrightarrow{AB}$ and vector $\overrightarrow{BC}$ as θ. If $0^\circ \leq \theta < 90^\circ$, i.e., $\cos\theta > 0$, the vehicle's movement direction is close to the event location. If $90^\circ \leq \theta \leq 180^\circ$, i.e., $\cos\theta \leq 0$, the vehicle's movement direction is away from the event location. The $\cos\theta$ is calculated as

$$\cos\theta = \frac{\overrightarrow{AB} \cdot \overrightarrow{BC}}{|\overrightarrow{AB}| \cdot |\overrightarrow{BC}|} = \frac{(\ln g_2 - \ln g_1) \cdot (\ln g_3 - \ln g_2) + (lat_2 - lat_1) \cdot (lat_3 - lat_2)}{\sqrt{(\ln g_2 - \ln g_1)^2 + (lat_2 - lat_1)^2} \cdot \sqrt{(\ln g_3 - \ln g_2)^2 + (lat_3 - lat_2)^2}}. \tag{3}$$

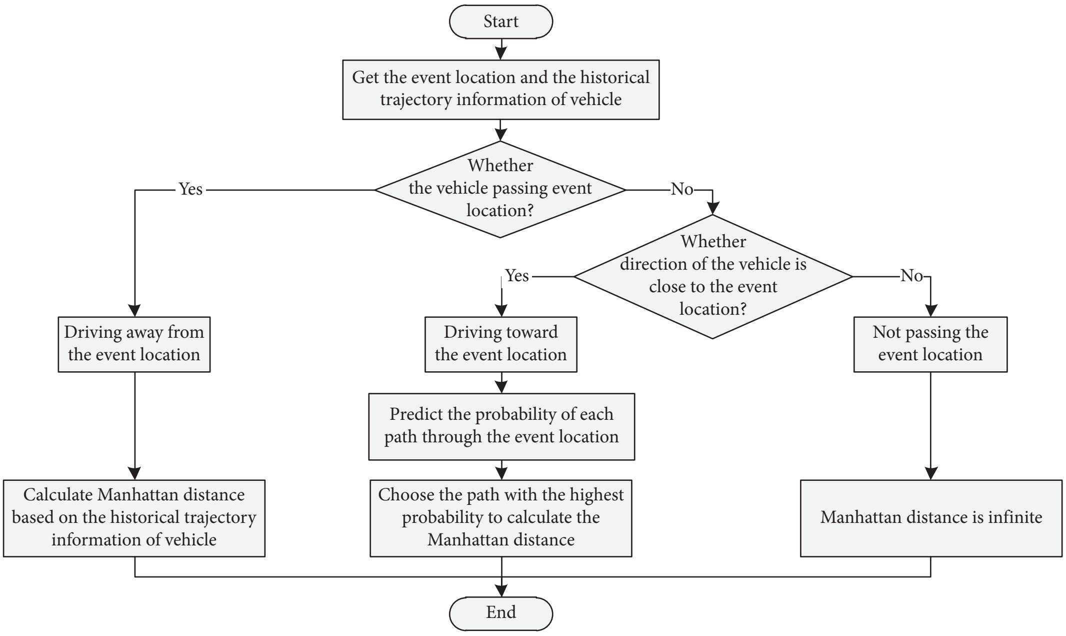

Start
Get the event location and the historical trajectory information of vehicle
Whether the vehicle passing event location?
Yes
No
Whether direction of the vehicle is close to the event location?
Yes
No
Driving away from the event location
Driving toward the event location
Not passing the event location
Predict the probability of each path through the event location
Calculate Manhattan distance based on the historical trajectory information of vehicle
Choose the path with the highest probability to calculate the Manhattan distance
Manhattan distance is infinite
End

Figure 2: Flow chart for calculating the Manhattan distance.

As shown in Figure 3, when a vehicle moves from position A to position B, the angle between movement direction vector of the vehicle and the vector from its current position to event location is less than 90°, so the vehicle's movement direction is close to the event location. When a vehicle moves from position A′ to position B′, the angle between movement direction vector of the vehicle and the vector from its current position to event location is greater than or equal to 90°, so the vehicle's movement direction is away from the event location.

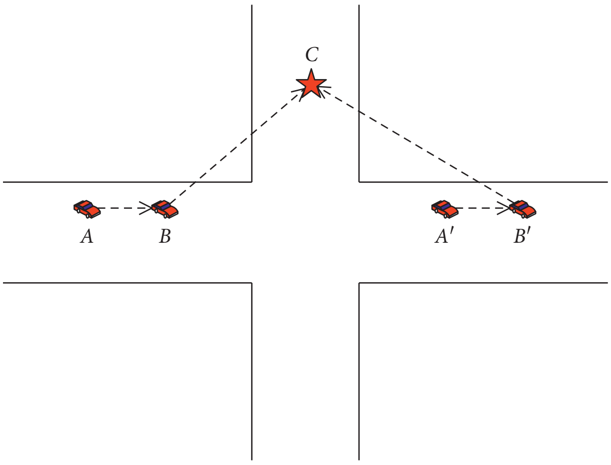


Figure 3: Diagram of the relationship between vehicle movement direction and event location.

4.1.2. The Prediction of the Path with Maximum Probability. There may be multiple paths for vehicle from the current location to event location. Based on the Manhattan mobility model and the actual road, this paper predicts the path with the maximum probability of the vehicle passing the event location.

Firstly, a weighted directed graph $G' = (V', E')$ based on the Manhattan mobility model and the actual road is established to record all the paths of sending vehicle from the current location to the event location and the transition probability at intersection. In weighted directed graph G', the vertex is the road segments in the actual road model, and the edge indicates the transition from one road segment to another road segment, and the transition direction is used as the direction of the edge. Whether the road segments can be transitioned (i.e., whether there is an edge between the two vertices) is determined by the three attributes of the road segment in the actual road model (whether it can go straight, whether it can turn right, or whether it can turn left). Combining these three attributes with the transition probability of vehicle at the intersection specified by the Manhattan mobility model, we can determine the transition probability of the vehicle at the intersection which is used as weight of the edge in graph G'. The sum of the probability of transition to other nodes is 1 in graph G', as shown in the following equation:

$$\sum_{j=1}^{n} W\left(\langle V_i, V_j\rangle\right) = 1, \tag{4}$$

where n is the number of nodes that the node V_i can transfer to other nodes, V_j is the other nodes to which the node V_i can transfer, and $W(\langle V_i, V_j\rangle)$ represents the weight of the edge $\langle V_i, V_j\rangle$.

According to the Manhattan mobility model combined with actual road, a weighted directed graph can be constructed as shown in Figure 4. Vertex A is the road segment where the sending vehicle is located, and Vertex M is the road segment where the event location is located. There are three paths from Vertex A to Vertex M, namely, ACEIM, AFGIM, and AFJLM.

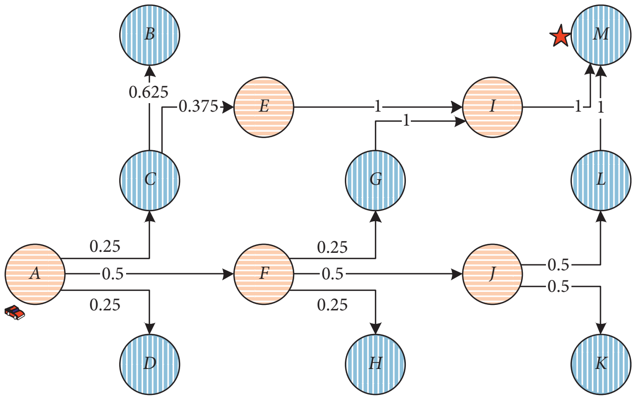


Figure 4: Weighted directed graph constructed.

The vehicle V_i that sends a message m_i may have Pnum paths to the event location. The j-th path path_i^j can be expressed as $\text{path}_i^j = \{V_j^1 V_j^2 \ldots V_j^{Vn_j}\}$ $(j = 1, 2, \ldots, P\text{num})$, where Vn_j represents the number of vertices contained in the j-th path. The probability $\Pr(\text{path}_i^j)$ that the vehicle moves on path path_i^j is defined as

$$\Pr\left(\text{path}_i^j\right) = \prod_{k=1}^{Vn_j-1} W\left(\langle V_j^k, V_j^{k+1}\rangle\right), \quad (5)$$

where Vn_j represents the number of vertices contained in the j-th path, and $W(\langle V_j^k, V_j^{k+1}\rangle)$ represents the weight of the edge $\langle V_j^k, V_j^{k+1}\rangle$.

Calculating the path with the maximum probability is equal to finding path by minimizing inverse probability. Therefore, the method for calculating the path with the maximum probability is given in the following equation

$$\max_{j=1,\ldots,Pnum}\left(\Pr\left(\text{path}_i^j\right)\right) = \max_{j=1,\ldots,Pnum}\left(\prod_{k=1}^{Vn_j-1} W\left(\langle V_j^k, V_j^{k+1}\rangle\right)\right) = \min_{j=1,\ldots,Pnum}\left(\frac{1}{\prod_{k=1}^{Vn_j-1} W\left(\langle V_j^k, V_j^{k+1}\rangle\right)}\right) = \min_{j=1,\ldots,Pnum}\left(\prod_{k=1}^{Vn_j-1} \frac{1}{W\left(\langle V_j^k, V_j^{k+1}\rangle\right)}\right). \quad (6)$$

The Dijkstra algorithm is used to calculate the shortest path from one vertex to the other vertices of the weighted graph. Since calculating the path with the maximum transition probability is equal to finding path by minimizing reciprocal of transition probability, the Dijkstra algorithm can be used to calculate the path with the maximum probability. The method of using the Dijkstra algorithm to obtain the shortest path is to add the weights of each path and select the path with the minimum result. However, when selecting the path with the maximum transition probability, we need to multiply the reciprocal of weight (i.e., the reciprocal of transition probability) and choose the path with the minimum result. Therefore, when using Dijkstra algorithm, it is necessary to change the addition of weights to multiplication. Algorithm 1 introduces the steps of calculating the path with the maximum probability in detail.

By using Algorithm 1, the path with the maximum transition probability denoted by $\text{path}_i^{\max} = \{V_{\max}^1 V_{\max}^2 \ldots V_{\max}^{Vn_{\max}}\}$ can be obtained. The Manhattan distance as expressed by $\text{man}Dis_i$ can be obtained from $\text{path}_i^{\max}$ and the actual road model. However, because the $\text{path}_i^{\max}$ is a prediction, and the vehicle may not move along the $\text{path}_i^{\max}$, the probability of $\text{path}_i^{\max}$ needs to be considered. The method of calculating the final Manhattan distance as expressed by $Man_i^{e'}$ is given in the following equation:

$$\text{Man}_i^{e'} = \frac{\text{man}Dis_i}{\Pr\left(\text{path}_i^{\max}\right)}, \quad (i = 1, 2, \ldots, N), \quad (7)$$

where $\Pr(\text{path}_i^{\max})$ represents the probability of the vehicle moving along the path $\text{path}_i^{\max}$.

4.2. The Calculation of the Number of Building Obstacles. Due to the existence of building obstacles, the line of sight of vehicle will be affected, which will affect the trust value of message. In a city road environment, building obstacles generally occur at intersection. Vehicle cannot obtain the conditions (traffic accident information) of another road segment to which the vehicle turns left or right from the current road segment. This paper takes the intersection where the vehicle turns left or right as the

```
INPUT:
The storage matrix $\mathrm{cost}[n][n]$ of the weighted directed graph $G'$ and the vertex set $V$, where $n$ represents the number of vertices in
  the graph.
OUTPUT:
    The path with the maximum probability ($\mathrm{path}[n]$)
(1)    Initialize the shortest path length array dist, let $\mathrm{dis}t[j] = \cos t[0][j]$, where $j = 0, 1 \ldots, n-1$;
(2)    Initialize the path array with the maximum probability, let $\mathrm{path}[j] = 0$, where $j = 0, 1 \ldots, n-1$;
(3)    Set $U = \{V_1\}$, vertex $V_1$ is the road segment where the vehicle sending message is located;
(4)    Select the vertex $k$ with the shortest path from the set $V - U$, ($k = \min\{\mathrm{dis}t[j]\}, j \in V - U$);
(5)    Add vertex $k$ to set U, let $U = U \cup \{k\}$;
(6)    For (each $j \in V - U$)
(7)      $IF(\mathrm{dis}t[j] > \mathrm{dis}t[k] \times 1/\cos t[k][j])$;
(8)        let $\mathrm{dis}t[j] = \mathrm{dis}t[k] \times 1/\cos t[k][j]$;
(9)        let $\mathrm{path}[j] = k$;
(10)     End If
(11)     End For
(12)   If $(V \neq U)$
(13)   Go to step 4;
(14)   End If
```

Algorithm 1: Calculating the path algorithm with the maximum probability.

turning point. The number of turning points between the sending vehicle and event location is that of building obstacles. In calculating the number of building obstacles as expressed by $Obs_i^{e'}$, three kinds of movement relationships between the sending vehicle and event location are also considered.

4.2.1. Driving away from the Event Location.

When the vehicle drives away from the event location, this means that the vehicle passes through the event location. Since there are no building obstacles when the vehicle passes through the event location, the number of building obstacles is set at 0 ($Obs_i^{e'} = 0$).

4.2.2. Not Passing the Event Location.

When the vehicle does not pass the event location, the Manhattan distance is infinite, and there is no path between the sending vehicle and event location, so the number of building obstacles is also infinite.

4.2.3. Driving toward the Event Location.

When the vehicle drives toward the event location, the number of building obstacles is the number of turning points with the maximum transition probability on the path $\mathrm{path}_i^{\max} = \{V_{\max}^1 V_{\max}^2 \cdots V_{\max}^{Vn_{\max}}\}$. For each edge $\langle V_{\max}^j, V_{\max}^{j+1}\rangle$ $(j = 1, 2, \ldots, Vn_{\max} - 1)$, if the vehicle turns left or right on the actual road, the number of building obstacles increases by 1 ($Obs_i^{e'} = Obs_i^{e'} + 1$). The final $Obs_i^{e'}$ is the number of building obstacles between the sending vehicle and event location.

4.3. The Calculation of Message Scores.

The score of the message can be calculated by the Manhattan distance and the number of building obstacles. However, the value of the Manhattan distance and the number of buildings obstacles are of different orders of magnitude. Therefore, before calculating the score, the value needs to be normalized first. The normalization method is given in the following equation:

$$\mathrm{Man}_i^{e'} = \frac{\mathrm{Man}_i^{e'} - \min\left(\mathrm{Man}^{e'}\right)}{\max\left(\mathrm{Man}^{e'}\right) - \min\left(\mathrm{Man}^{e'}\right)}, \tag{8}$$

$$Obs_i^{e'} = \frac{Obs_i^{e'} - \min\left(Obs^{e'}\right)}{\max\left(Obs^{e'}\right) - \min\left(Obs^{e'}\right)}, \tag{9}$$

where $\max(\mathrm{Man}^{e'})$ and $\min(\mathrm{Man}^{e'})$ are the maximum and minimum Manhattan distances between all sending vehicles about event e', respectively, and $\max(Obs^{e'})$ and $\min(Obs^{e'})$ are the maximum and minimum number of building obstacles between all sending vehicles about event $e\prime$, respectively.

After the value is normalized, the score $S_i^{e'}$ for the message m_i about event $e\prime$ can be calculated using the following equation:

$$S_i^{e'} = \alpha \cdot e^{-\rho \mathrm{Man}_i^{e'}} + \beta \cdot e^{-\sigma Obs_i^{e'}}, \tag{10}$$

where α, β, ρ, and σ are the four preset parameters. ρ and σ set the rate of exponential function change and control the influence of the Manhattan distance and the number of building obstacles on the message score. α and β control the influence ratio of the Manhattan distance and the number of building obstacles, where $\alpha + \beta = 1$. When $\mathrm{Man}_i^{e'}$ and $Obs_i^{e'}$ are infinite, let $S_i^{e'} = 0$.

4.4. The Fusion of Message Scores.

After obtaining the scores $S_0^{e'}, S_1^{e'}, \ldots, S_N^{e'}$ of all messages about event e', it is needed to fuse these scores together to finally determine the trust value of message. There are many methods of data fusion, including majority voting [25], weighted voting [26, 27], Bayesian inference [28], and Dempster-Shafer theory [29]. This paper mainly studies the influence of distance on the trust value of message and takes the score generated by distance as the weight of each message. Therefore, the weighted voting method is chosen for score fusion. The calculation method of the trust value of message m_0 about $e\prime$ is given in

$$\text{Trust}\left(e\prime \longrightarrow m_0\right) = \text{Fuse}\left(S_0^{e'}, S_1^{e'}, \ldots, S_N^{e'}\right) = \left\{ \sum_{i=1}^{N} d_i \cdot S_i^{e'}, \quad \text{if}\,(d_0 = 1), -\sum_{i=1}^{N} d_i \cdot S_i^{e'}, \quad \text{if}\,(d_0 = -1), \right. \tag{11}$$

where the value of d_i is +1 or −1. If the message m_i describes the occurrence of event e' as 1, then $d_i = 1$; otherwise $d_i = -1$. If $\text{Trust}\,(e' m_0)$ is greater than 0, the message m_0 is trusted; otherwise the message m_0 is not trusted.

When event e' actually occurs, $\sum_{i=1}^{N} d_i \cdot R_i^{e'} > 0$. At this time, if the vehicle sending the message m_0 is a normal vehicle and sends a correct message, then $d_0 = 1$, and $\text{Trust}\,(e' \longrightarrow m_0) = \sum_{i=1}^{N} d_i \cdot R_i^{e'} > 0$, so the conclusion is that the message m_0 is trusted; otherwise, if the vehicle sending the message m_0 is a malicious vehicle and sends a false message, then $d_0 = 1$, and $\text{Trust}\,(ee' \quad m_0) = -\sum_{i=1}^{N} d_i \cdot R_i^{e'} < 0$, so the conclusion is that the message m_0 is not trusted. When event e' does not occur, $\sum_{i=1}^{N} d_i \cdot R_i^{e'} < 0$. At this time, the vehicle sending the message m_0 is a normal vehicle and sends a correct message, then $d_0 = -1$, and $\text{Trust}\,(e' \longrightarrow m_0) = -\sum_{i=1}^{N} d_i \cdot R_i^{e'} > 0$; the conclusion is that the message m_0 is trusted; otherwise, if the vehicle sending message m_0 is a malicious vehicle and sends a false message, then $d_0 = 1$, and $\text{Trust}\,(e' \longrightarrow m_0) = \sum_{i=1}^{N} d_i \cdot R_i^{e'} < 0$; the conclusion is that the message m_0 is not trusted. It can be seen that equation (11) can correctly determine whether message m_0 is trusted.

5. Simulation and Discussion

This section mainly performs experimental simulations to verify the effectiveness of the proposed MDBTM scheme. The tools used in the experimental simulations include the traffic flow simulation tool VanetMobiSim [30] (version 1.1) and the network simulation tool OPNET [31] (version 14.5).

5.1. The Experimental Setup

5.1.1. The Experimental Environment. The method proposed in this paper is based on the city road environment. First, it is necessary to use the VanetMobiSim tool to model city roads. This experiment uses the VanetMobiSim tool to generate a city road simulation area of 3200 m * 3200 m. There are 25 intersections, 40 road segments. Each road segment is 800 meters. The movement trajectories of the vehicles are generated by VanetMobiSim through the simulation area and then imported into the OPNET simulation environment for mobile nodes. The movement trajectories generated by VanetMobiSim cannot be used directly in OPNET and need to be converted to the format used by OPNET.

In the OPNET simulation environment, vehicles communicate with neighboring vehicles using a logarithmic normal connection model [32]. Through C–V2X technology [33], the communication range of the vehicle can reach 450 meters. Based on the 450-metre range of communications, it can be seen that at least 72 vehicles are required to communicate with each other via multihop. Therefore, the number of vehicles selected in this experiment is more than 72.

In the course of the experiment, the randomly selected road segment from the scene is chosen as the event location, and vehicles on the road periodically send messages about the event. Normal vehicles send the correct messages, while malicious ones send false messages.

5.1.2. The Experimental Parameters. The parameters used in the experiment are shown in Table 2.

5.1.3. The Performance Metric. For trust management, it is important to correctly judge the authenticity of a message. Therefore, in order to verify the performance of the method proposed in this paper, the correct decision probability of a message expressed by $P\text{succ}$ is used as the performance metric, and its definition is given in

$$P\text{succ} = \frac{\text{Num}_{\text{succ}}}{\text{Num}_{\text{total}}} \times 100\%, \tag{12}$$

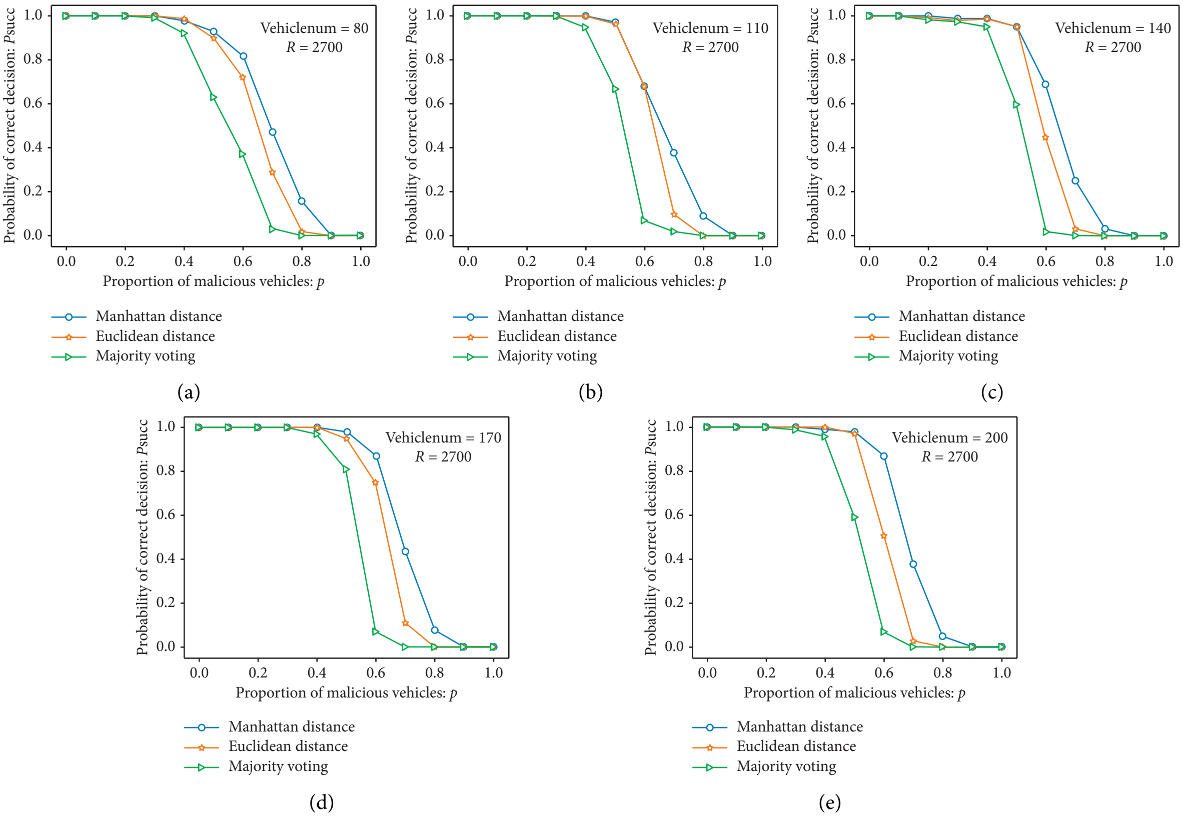
where Num_{succ} represents the number of successful decisions, and $\text{Num}_{\text{total}}$ represents the total number of decisions.

5.2. The Experimental Analysis. When analyzing the influence of the proportion of malicious vehicles and the influence of the reference range R, this paper compares the proposed MDBTM method (labeled with Manhattan Distance) with the method based on Euclidean distance (labeled with Euclidean Distance) and the majority voting [25] method (labeled with Majority Voting). The method based on Euclidean distance uses the formula $R_i^{e'} = b + e^{-\gamma \cdot d}$ proposed by Yang et al. [14] to calculate the message scores and uses the method of (11) to fuse message scores. During the experiment, the value of b is 0, the value of γ is 1, and the d is the Manhattan distance between the sending vehicle and event location. Moreover, the data in this experiment are averaged after multiple experiments.

5.2.1. The Influence of the Proportion of Malicious Vehicles. As shown in Figure 5, the abscissa represents the proportion of malicious vehicles from 0.0 to 1.0, and the ordinate represents the correct decision probability. Figures 5(a)–5(e)

Table 2: Simulation parameters.

Parameters	Values
Traffic flow model	IDM_LC model
The number of vehicles	80, 110, 140, 170, 200
The speed	10–60 km/h
Simulation time	1800 s
Safety distance	100 m
The proportion of malicious vehicles	0.0–1.0
Communication range	450 m
α	0.5
β	0.5
ρ	2
σ	5



(a)

(b)

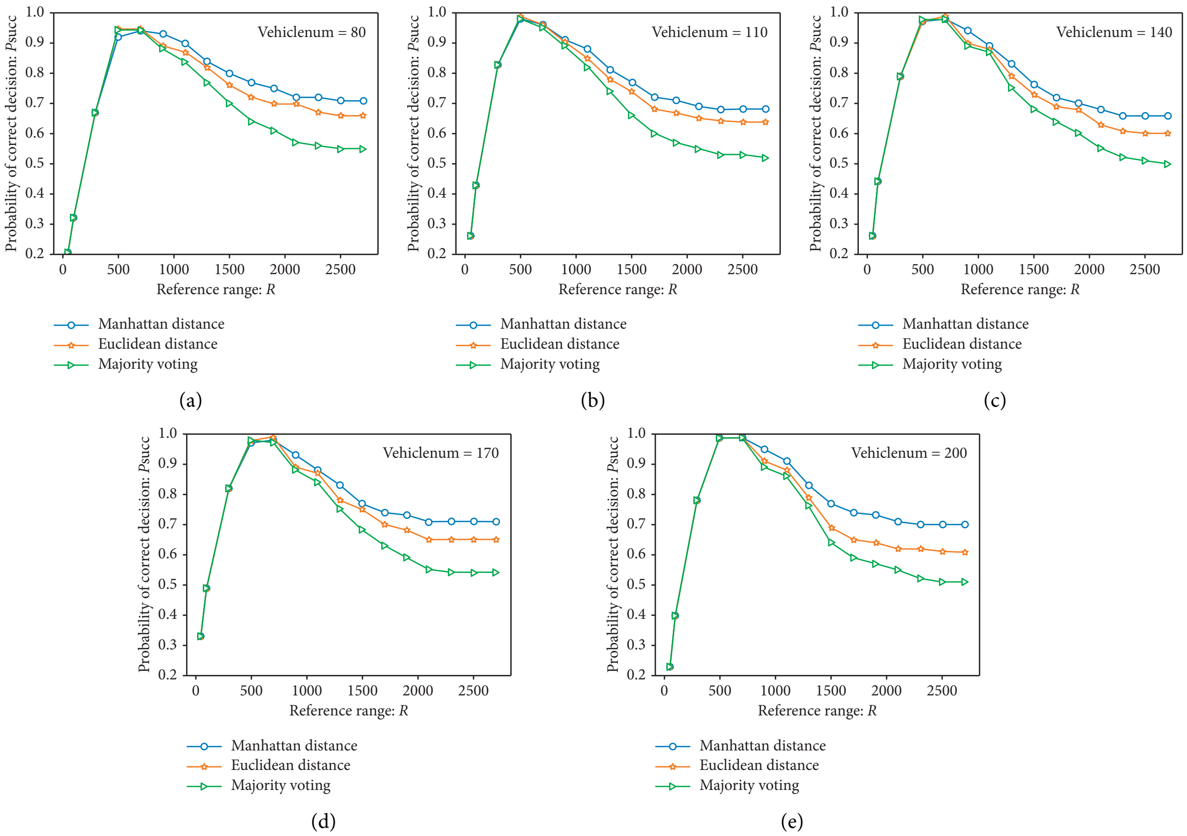
(c)

(d)

(e)

Figure 5: The comparison of correct decision probability under different proportions of malicious vehicles. (a) 80 vehicles. (b) 110 vehicles. (c) 140 vehicles. (d) 170 vehicles. (e) 200 vehicles.

represent the influence of the proportion of different malicious vehicles on the correct decision probability where the number of vehicles is, respectively, 80, 110, 140, 170, and 200, and the reference range R is 2700 meters. It can be seen from Figure 5 that when the proportion of malicious vehicles is less than 0.3, the correct decision probability for each method is close to 1 in the scene of different vehicle numbers. As the number of malicious vehicles increases, the correct decision probability for each method begins to decline when the proportion of malicious vehicles is greater than 0.4. However, the correct decision probability of the method proposed in this paper is higher than the other two methods. And for the other two methods, when the proportion of malicious vehicles is 0.8, the correct decision probability is close to 0. But the MDBTM method starts to approach 0 when the proportion of malicious vehicles is 0.9. It can be seen that the MDBTM method shows a better correct decision probability than the other two methods under different proportions of malicious vehicles and different numbers of vehicles. This shows that considering the Manhattan distance that the vehicle moves along the actual road and the obstruction of the line of sight by building



(a)

(b)

(c)

(d)

(e)

FIGURE 6: The comparison of correct decision probability under different reference ranges. (a) 80 vehicles. (b) 110 vehicles. (c) 140 vehicles. (d) 170 vehicles. (e) 200 vehicles.

obstacles can improve the robustness of the system against malicious vehicle attacks.

5.2.2. The Influence of the Reference Range R. Figure 6 shows the influence of different reference ranges on the correct decision probability. The abscissa represents the size of the reference range R (from 50 meters to 2500 meters), and the ordinate represents the correct decision probability (this probability is the average value under different proportions of malicious vehicles). Figures 6(a)–6(e), respectively, represent the influence of different reference ranges on the correct decision probability in the scenarios where the number of vehicles is 80, 110, 140, 170, and 200. It can be seen from Figure 6 that no matter the method proposed in this paper or the method based on Euclidean distance and majority voting, the correct decision probability is very low when the reference range R is too small in the scene of different vehicle numbers. This is because there are fewer messages for reference. As the reference range R increases, the number of reference messages increases, and the correct decision probability gradually rises. However, when the reference range R is too large, the number of malicious vehicles within the reference range R also increases which results in a decrease in the correct decision probability.

It can be seen from Figure 6 that there is a threshold. Whether it is greater than or less than the threshold, the correct decision probability is less than that of this threshold. When the number of vehicles is 80, 110, 140, 170, and 200, the threshold is 700 meters, which is close to the actual road length of 800 meters. This is because the number of building obstacles on the same road segment is 0, and vehicles are relatively close to the event location, thus leading to a higher correct decision probability. This is consistent with the theory of this paper. The design of this paper takes into account the Manhattan distance and the number of building obstacles at the intersection. On the same road segment, no building obstacles are blocking the line of sight, and the event location is relatively close to vehicles, so the correct decision probability is also high. As you can see, too large or too small reference range R will affect the correct decision probability. When the reference range R is close to the length of the actual road segment, the correct decision probability is higher.

It can also be seen from Figure 6 that with the same number of vehicles when the reference range R is less than the threshold 700 meters, the correct decision probability for each method is basically the same. This is because when the reference range R is small, the message available for reference is relatively small and the distance has little influence on the correct decision probability. When the reference range R is greater than the threshold 700 meters, because this paper considers the Manhattan distance and the number of building obstacles at the intersection, the method proposed in this paper has better performance than other methods in terms of the correct decision probability.

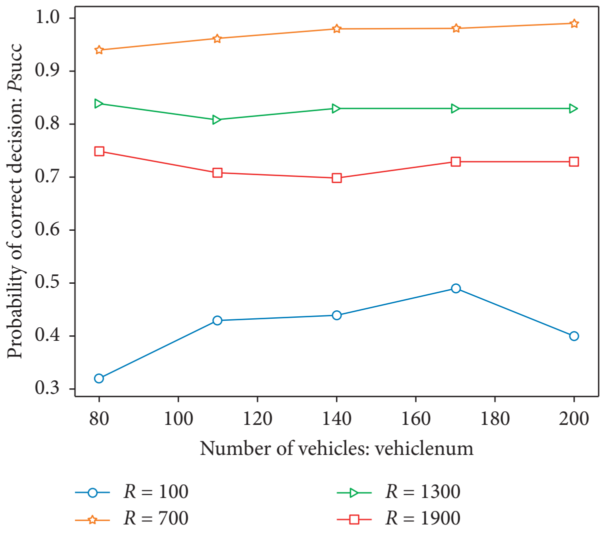


Figure 7: The comparison of correct decision probability under different number of vehicles.

5.2.3. The Influence of the Number of Vehicles in the Network. Figure 7 shows the influence of the number of vehicles (i.e., vehicle density) on the correct decision probability. The abscissa represents the different numbers of vehicles (80, 110, 140, 170, and 200), and the ordinate represents the correct decision probability (this probability is the average value under different proportions of malicious vehicles). As can be seen from Figure 7, when the reference range R is 100 meters, the correct decision probability varies greatly in the scene of different vehicle numbers because of too few messages available for reference. When the reference range R is 700 meters, 1300 meters, and 1900 meters, the correct decision probability varies very little. It can be seen that the number of vehicles in the network will not affect the correct decision probability of the proposed method when the reference range R is appropriate.

6. Conclusions

In this paper, a MDBTM model for calculating the distance in VANET is proposed, which solves the problem of no detailed discussion about the way of calculating the distance. In this model, the Manhattan distance and the number of building obstacles are calculated by considering the movement relationship between the sending vehicle and event location. The experimental results show that the method proposed in this paper shows better performance in terms of the correct decision probability than similar methods in the case of different proportions of malicious vehicles, different numbers of vehicles, and different reference ranges. It is also found that the correct decision probability is higher when the reference range R is set close to the length of the actual road segment, and the number of different vehicles in the network will not affect the correct decision probability.

In future work, we will consider the combination of this method and blockchain technology to store the score information in the blockchain, which can ensure the data's security (nontampering, traceability) and further improve the security of trust management in the VANET environment.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was supported by the National Natural Science Foundation of China under Grant 61862046; the Inner Mongolia Autonomous Region Science and Technology Achievements Transformation Project under Grant CGZH2018124; the Graduate Research Innovation Foundation Project of Inner Mongolia University under Grant 10000–15010109; and the Science and Technology Program of Inner Mongolia Autonomous Region under Grant 2019GG376.

References

[1] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): current state, challenges, potentials and way forward," in *Proceedings of the 2014 20th Conference on Automation and Computing*, pp. 176–181, Cranfield, UK, September 2014.

[2] K. P. Laberteaux, J. J. Haas, and Y. C. Hu, "Security certicate revocation list distribution for VANET," in *Proceedings of the Fifth International Workshop on Vehicular Ad Hoc Networks*, pp. 88-89, San Francisco, CA, USA, September 2008.

[3] S. Dietzel, R. V. D. Heijden, H. Decke et al., "A flexible, subjective logic-based framework for misbehavior detection in V2V networks," in *Proceedings of the 15th International Symposium on A World of Wireless, Mobile and Multimedia Networks*, pp. 1–6, WoWMoM), Sydney, Australia, June 2014.

[4] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proceedings of 2007 Mobile Networking for Vehicular Environments*, pp. 103–108, Anchorage, AK, USA, May 2007.

[5] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks," *IEEE Wireless Communications Security and Privacy in Emerging Wireless Networks*, vol. 17, no. 5, pp. 22–28, 2010.

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

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

[8] F. G. Mármol and G. M. Perez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks,"

Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934–941, 2012.

[9] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, “A job market signaling scheme for incentive and trust management in vehicular ad hoc networks,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3657–3674, 2015.

[10] M. Raya, P. Papadimitratos, V. D. Gligor et al., “On data-centric trust establishment in ephemeral ad hoc networks,” in *Proceedings of the IEEE INFOCOM 2008-the 27th Conference on Computer Communications*, pp. 1238–1246, Phoenix, AZ, USA, April 2008.

[11] A. Wu, J. Ma, and S. Zhang, “RATE: a RSU-aided scheme for data-centric trust establishment in VANETs,” in *Proceedings of the 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–6, WiCom), Wuhan, China, September 2011.

[12] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, “Information-oriented trustworthiness evaluation in vehicular adhoc networks,” *Network and System Security, Lecture Notes in Computer Science*, vol. 7873, pp. 94–108.

[13] R. A. Shaikh and A. S. Alzahrani, “Intrusion-aware trust model for vehicular ad hoc networks,” *Security and Communication Networks*, vol. 7, no. 11, pp. 1652–1669, 2013.

[14] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchain-based decentralized trust management in vehicular networks,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[15] J. Chen, G. Mao, C. Li, and D. Zhang, “A topological approach to secure message dissemination in vehicular networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 1, pp. 135–148, 2020.

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

[17] W. Li and H. Song, “ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[18] C. Lai, R. Lu, D. Zheng, and X. Shen, “Security and privacy challenges in 5G-enabled vehicular networks,” *IEEE Network*, vol. 34, no. 2, pp. 37–45, 2020.

[19] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, “Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7940–7954, 2020.

[20] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, “Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[21] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, “PA. CRT.: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[22] J. Chen and G. Mao, “On the security of warning message dissemination in vehicular Ad hoc networks,” *Journal of Communications and Information Networks*, vol. 2, no. 2, pp. 46–58, 2017.

[23] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, “Trust management for vehicular networks: an adversary-oriented overview,” *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[24] F. Bai F, N. Sadagopan, and A. Helmy, “IMPORTANT: a framework to systematically analyze the impact of mobility on performance of routing protocols for adhoc networks,” in *Proceedings of the IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 825–835, IEEE Cat. No.03CH37428), San Francisco, CA, USA, April 2003.

[25] B. Ostermaier, F. Dotzer, and M. Strassberger, “Enhancing the security of local danger warnings in VANETs-a simulative analysis of voting schemes,” in *Proceedings of the Second International Conference. on Availability, Reliability and Security*, pp. 422–431, ARES’07), Vienna, Austria, April 2007.

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

[27] Y. Zhu, *Multisensor Decision and Estimation Fusion*, Kluwer Academic Publishers, Amsterdam, Netherlands, 2002.

[28] J. P. Huelsenbeck and F. Ronquist, “MRBAYES: Bayesian inference of phylogenetic trees,” *Bioinformatics*, vol. 17, no. 8, pp. 754-755, 2001.

[29] J. Dezert, P. Wang, and A. Tchamova, “On the validity of dempster-shafer theory,” in *Proceedings of the International Conference on Information Fusion*, pp. 655–660, Singapore, July 2012.

[30] H. Jérme, M. Fiore, F. Filali, and C. Bonnet, “Vehicular mobility simulation with VanetMobiSim,” *Simulation*, vol. 87, no. 4, pp. 275–300, 2011.

[31] M. Chen, *OPNET Network Simulation*, Tsinghua University Press, Beijing, China, 2004.

[32] G. Mao, *Connectivity of Communication Networks*, Springer International Publishing AG, New York, NY, USA, 2017.

[33] Y. Li, *5G and Internet of Vehicles: Internet of Vehicles Technology and Intelligent Connected Vehicles Based on Mobile Communication*, Publishing House of Electronics Industry, Beijing, China, 2019.