IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 June 2023, accepted 30 June 2023, date of publication 4 July 2023, date of current version 11 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3292234

RESEARCH ARTICLE

Transmission Protocol of Emergency Messages in VANET Based on the Trust Level of Nodes

BING SU AND LING TONG
School of Computer and Artificial Intelligence, Changzhou University, Changzhou 213164, China
Corresponding author: Ling Tong (17416207@smail.cczu.edu.cn)

ABSTRACT Vehicle Ad Hoc Networks (VANETs) can help reduce traffic accidents and improve road safety by broadcasting Emergency Messages (EMs) between vehicles in advance so that the vehicle can take action to avoid accidents. However, its advantages are often compromised by factors such as high mobility, uneven nodes distribution, and signal attenuation, resulting in lower reliability and higher delay in the delivery of EMs. Besides, because of its open and mobility, VANETs are vulnerable to cyber security threats and are prone to multiple malicious attacks in the network. Malicious nodes can join the set of candidate forwarding nodes through collusion and identity forgery, which poses a serious challenge to EMs forwarding. In order to resolve the problems above, this paper proposes a geographic routing strategy to deliver EMs based on trusted nodes, focusing on measuring the reliability of link quality and node quality. The link quality between nodes is evaluated by measuring the actual transmission cost and the link signal-to-noise ratio to minimize the possible link interruption; at the same time, the node trust value is introduced to measure the credibility of the node and filter out the possible malicious nodes in the network. The research results show that the protocol is suitable for dense and sparse traffic conditions, can detect and identify malicious nodes, and has significant performance improvements in message delivery rate, end-to-end delay, and network throughput.

INDEX TERMS VANET, geographic routing, link quality, node trust, malicious node.

I. INTRODUCTION

Vehicle Ad Hoc Networks (VANETs) are one of the promising emerging technologies [1] in the intelligent transportation system (ITS). Safety apps can help reduce traffic accidents and alleviate road congestion by helping drivers predict accidents far beyond their vision in advance. The safety apps in VANETs include Emergency Messages (EMs) driven by events. When an incident is detected on the road, the vehicle will send EMs to inform nearby vehicles to avoid multiple vehicles accidents. The more vehicles receive emergency messages, the harm of traffic accidents will be reduced to a lower level. Due to the limited range of vehicle communication, the rapid movement of the vehicle caused dynamic changes in network topology, and EMs was forwarded to vehicles in the target region via multi-hop broadcasting methods [2]. Multi-hop broadcast in VANETs now faces significant challenges like instability, broadcast storms, and channel access due to data interference and fading of wireless channels. As a result, in the EMs transmission, how to improve the reliability of multi-hop transmission while minimizing delay is a critical problem that must be addressed right now.

In VANETs, nodes communicate with one another through dedicated short-range communication (DSRC). They can deliver messages with highs peed to enable real-time communication [3]. These communications are mainly divided into four main categories: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-roadside (V2R), and vehicle-to-passenger (V2P). Due to different road topologies, vehicles are ruled by traffic lights, intersections, and stop signs, and the distribution of nodes is uneven [4]. In addition, vehicles move fast, the status and number of vehicles on the road network are frequently updated, changes in network topology may lead the packet to be routed to a long path and the complex environment of wireless channels may lead to channel congestion, forcing the packet to be dropped; at the same time, the limited communication range of vehicles

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

makes the communication link established between nodes easy to be disconnected [5]. These problems further affect the reliability and timeliness of EMs forwarding. Instantly, multi-hop broadcast is the core technology to realize EMs transmission. The existing geographic protocols provide many valuable ideas, but they ignore the malicious nodes that may interfere with communication in the network. For example, a malicious node can conduct a black hole attack by receiving data packets but not forwarding them, resulting in the target vehicle being unable to receive messages and avoid them in a timely manner. In fact, due to the mobility and open of VANETs, attacks such as denial of service and black holes may occur in V2V communication [6]. However, the transmission of EMs is closely related to life security, it is one of the key challenges in VANETs to detect and identify malicious nodes so as to improve the security and efficiency of data transmission. When selecting a relay node, existing strategies often focus on mobility, link state, and other unilateral indicators, ignoring the forwarding quality and the credibility of the node itself. Therefore, it is necessary to consider real-time parameters from multiple perspectives to evaluate the comprehensive status of nodes [3]. In addition, DSRC security messages lack a Message feedback mechanism. If malicious behavior of the node occurs, the risk of transmission failure will increase.

At present, existing protocols do not consider external factors while ensuring the internal security of nodes and lack defense or detection mechanisms against external attacks. When messages are forwarded to problematic nodes, even messages forwarded over high-quality links may be lost due to malicious behavior by the nodes. To choose a more reliable relay forwarding node, we not only need to consider the quality of the node link to enhance the possibility of data packets passing through that link but also consider whether the selected node itself is trustworthy. Nodes with lower trust values have a higher risk of forwarding messages. Consider the above situations synthetically can help better routing in VANETs. To this end, we propose to consider the vehicles involved in routing as uncertain factors and propose the node trust level-based geographical routing solution (TBGR). The main contributions of this paper are as follows:

1.To reduce the impact of vehicle motion, we propose a position prediction mechanism that utilizes the predicted distance between the source and candidate vehicles to narrow the candidate area, screen out more stable vehicles to reduce the impact of link interruption.

2.We propose a relay forwarding node selection method based on node trust by utilizing the historical behavior of nodes. This method determines the trust level of nodes by calculating their packet forwarding rate and collecting neighbor recommendations. It uses dynamic weight coefficients to balance direct observation and neighbor evaluation, making our proposed protocol more flexible and increasing compatibility with the dynamic structure of the network. In addition, we improved the hidden terminal problem by utilizing a handshake mechanism based on Acknowledgement (ACK) message feedback.

3.We studied the impact of this method on changes in vehicle quantity, vehicle speed, and the number of malicious nodes added, and the results showed that this scheme is suitable for both sparse and dense traffic conditions.

The rest of this paper is organized as follows. Section II will give an overview of the literature. Section III and Section IV will introduce our proposed routing protocols. Section V describes simulation experiments and gives a comparison of the experimental results. Finally, Section VI summarizes the full text and discusses future work.

II. RELEVANT WORK

The existing routing protocols can be divided into four categories: topology-based, geography-based, probability-based, and delay-based [7]. Geographic routing does not need to establish and maintain routing tables, maintain topology maps or exchange link status information, making it more suitable for VANETs [8]. Greedy Perimeter Stateless Routing Protocol (GPSR) is a typical position-based routing protocol, which has two modes: greedy forwarding and peripheral forwarding. However, in real scenarios, due to the uneven distribution of nodes and highly dynamic topology, the next hop selected through greedy forwarding is usually located at the sender's communication boundary [9], which increases the probability of link disconnection and leads to packet loss, affecting the performance of GPSR protocol. Han et al. [9] proposed speed and location-aware dynamic routing (SPDR). SPDR dynamically narrows the range of routing decision area (RDA) based on the speed variance of candidate neighbors, and prioritizes the farthest vehicle in the reduced RDA as the optimal next hop, thus enhancing the reliable transmission of EMs. However, this route ignores the driving direction of vehicles, making it difficult to ensure the accuracy and timeliness of EMs transmission because it may be sent to vehicles in the opposite direction during packet forwarding. W-Geor [10] geographic routing is proposed for health monitoring applications in VANETs. It uses traffic awareness information such as traffic mobility, the distance between vehicles, speed difference, communication link expiration time, channel quality, and proximity factors to achieve the optimal next-hop node selection process. However, this routing focuses on mobility indicators of nodes unilaterally, it neglects the forwarding capability within nodes, and cannot fully ensure the reliability of EMs transmission. The location-based reliable emergency message routing scheme (REMR) [11] uses the future location information of neighbor nodes to exclude unstable neighbors from the candidate forwarding list, and at the same time uses the position, speed and movement of vehicles to minimize the link outage probability. REMR also provides a beacon control strategy to solve beacon congestion problems, improving message reliability. but the routing scheme does not take into account the changing channel condition and link state, lacking sufficient knowledge about network status.

Ullah et al. [12] based on the mobility measurement of nodes, considering the direction angle and path loss coefficient of each vehicle, introduced the stability index of the link to optimize the selection of the next hop node, and the proposed protocol is more suitable for dense networks. Haider et al. [13] suggested a novel idea for EMs transmission in Intermittently Connected Networks, combining V2V and V2I communication with the use of Roadside Units (RSUs). This method works well in both sparse and dense network situations. However, in practice, the expense of deploying and maintaining a large number of RSUs to enable network access is prohibitively expensive.

In general, broadcast protocols in VANETs obtain neighbor vehicle information within the communication range by sending periodic beacon messages. When the vehicle attempts to broadcast at the same time, this may lead to frequent channel contention and broadcast storms. In the sparse-density scenario, the vehicle will also face the risk of EMs transmission failure. Selvi et al. [14] introduced the adaptive scheduling partition broadcasting technology to dynamically adjust the beacon cycle to reduce the number of retransmission; at the same time, the lion optimization algorithm is used to evaluate the scheduling of each partition to forward EMs first. Although some biologically inspired intelligent routing protocols are effective in transmitting emergency data. However, their computational complexity and convergence speed may lead to increased delay. Based on this problem, Liu et al. [15] selected parked vehicles for forwarding, established a spider web transmission model based on parking lots, dynamically assigned node forwarding priority, and selected the path with the least delay to forward EMs. At present, the automatic application of the latest maps in the real world still faces many challenges, GPS-based vehicle positioning can lead to positioning errors. Afrashteh et al. [16] proposed to apply Radio Frequency Identification (RFID) technology to route segment broadcasting protocol to eliminate the accuracy problem based on GPS and improve the efficiency of EMs broadcasting by improving the positioning accuracy of vehicle. Abbas et al. [17] combine GPS measurement and map-matching technology to obtain the vehicle position. In addition, the scheme also considers mobility and social parameters of nodes and uses the fitness function to select the best forwarding node. Marques et al. [18] proposed a strategy to utilize the location, direction, speed, number of neighbors, and urban area characteristics of vehicles, so as to transmit emergency messages to all vehicles with the lowest network overhead in the shortest time. Tian et al. [19] proposed a location-based EMs transmission protocol, which makes messages broadcast only along the region of interest, and the message replay depends on the information in the received messages. This protocol can reduce broadcast conflict and avoid the unnecessary replay. Considering the impact of physical channels, Zhang et al. [20] proposed an adaptive urban security information transmission scheme based on link quality. By evaluating the connectivity probability between vehicles and assigning priority to candidate forwarders (CF) according to CF scores, they proposed an integrated physical channel connectivity calculation method.

In order to reduce the latency of data collecting, Chen et al. [21] presented a data caching strategy based on the temporal and spatial properties of data, taking into account the criteria for content retrieval effectiveness in the Internet of Vehicles. Emergency safety messages, traffic efficiency communications and commercial messages were split into three categories, and matching caching strategies were developed in accordance with their temporal and spatial properties. The open of the wireless unloading channel and the vehicle's rapid mobility will substantially affect the safety and stability of the unloading operation in the vehicle network. Ju et al. [22] presented a joint secure offloading and resource allocation (SORA) approach based on deep reinforcement learning to reduce system processing latency while ensuring the wireless offloading process, using physical layer security technology and spectrum-sharing architecture. To guarantee the effectiveness of each V2V link's communication, a penalty system for rate degradation has also been established.

VANETs heavily rely on node communication and lack defense against internal attacks, making it simple to disregard the security of vehicles approaching the source vehicle. According to the evaluation standards, trust-based models are divided into two categories: physical-centric and data-centric [3]. To identify malicious nodes, the entity-centric trust model focuses on assessing the reliability of vehicles. The data-centric trust model, on the other hand, concentrates on determining the reliability of the data transmitted by other tools. There are three methods to get data about the vehicle's level of trust: directly, indirectly (via recommendations), and in combination. Direct trust is obtained through the vehicle's ability assessment, whereas indirect trust is obtained through the evaluation of other vehicles. The sum of the two, which is achieved using various techniques, is the comprehensive trust value. In VANETs, vehicles are typically used to fulfill trust agglomeration. Venitta et al. [23] proposed a source routing based on trust perception similarity. Considering that some vehicles may maliciously discard packets, and in combination with the social characteristics of nodes, they adopted two methods of game theory broadcast strategy and direct confirmation in encounter strategy. This protocol can identify malicious nodes and overcome vulnerabilities of different types of attacks. VANET itself has a low-security factor and is prone to various types of attacks in the network. To ensure sufficient communication between network nodes, nodes must be able to reliably exchange information with their neighbors. Decisions based on incorrect or manipulated information can harm traffic safety, Fernandes et al. [24] proposed a decentralized reputation system based on alliance blockchain and smart contracts called BRS4VANETs. The system analyzes the reliability of data generated by vehicles

TABLE 1. Comparison of routing schemes.

Protocol	Metrics Used	Limitations
GPSR	Distance	Link rupture caused by uncertain node position and uneven distribution
REMR	Position Prediction	Hidden terminal problem is still unsolved
MM-GPSR	Partition of communication area	High delay in discontinuous network density
W-Geor	Node mobility,link expiration time,channel SNR and destination proximity information	Simply combine multiple routing metrics, ignoring routing reliability
SPDR	Velocity variance,collaborative forwarding	The application scenario is limited and channel congestion is not considered
MBM-EMD	Vehicle density, relative movement, channel quality	Ignore the security of nodes participating in routing
TCEMD	Incorporate entity-oriented trust values into data-oriented trust estimates	The application scenario is limited, and the motion state of vehicle nodes is not considered
RBO-EM	Cluster stability,link stability	Not applicable to sparse network

and can successfully detect suspicious and malicious vehicles. Liu et al. [25] proposed a new emergency message propagation model based on trust cascading for traffic interruption and congestion caused by possible malicious attacks in the network. They combined the entity-oriented trust value with the data-oriented trust evaluation. The model can better identify malicious nodes and resist various types of attacks, but it is only applicable to high-speed scenarios. Relatively speaking, It is more significant to improve the transmission of EMs on urban roads. Ullah et al. [26] built a reputation mechanism to deal with malicious nodes in the network through the social utility, historical behavior and contribution of each node, but this protocol is only applicable to high-speed scenarios. Rayeni et al. [27] used dynamic spatial partition density to spread emergency plans. They designed a scheduling method for each partition by calculating the size of each partition so that the routing protocol can adapt to traffic scenarios with different densities. In addition, Dynamic Partitioning Scheme (DPS) also uses the busy tone handset system to solve the terminal problems hidden in the transmission. In fact, the hidden terminal problem [28] faced by EMs transmission in VANETs is more serious than that in the traditional network. Due to the lack of the ACK message feedback mechanism, even if the message is lost in the transmission process, it is difficult for the sender to find it, let alone retransmit the message. Benrhaiem et al. [29] used zero correlation monopole orthogonal codes to solve the hidden terminal problem. The scheme uses periodic beacons to evaluate the reception quality of 802.11p wireless links in each cell; the information is then used to determine the optimal number of broadcast repetitions in each hop. Table 1 compares the standards used by some advanced routing protocols to determine candidate forwarding sets and summarizes the current research gaps.

III. SYSTEM ASSUMPTIONS AND ARCHITECTURE

A. SYSTEM ARCHITECTURE

As shown in Fig.1, The TBGR system architecture is mainly composed of four parts: Candidate forwarding node set screening, Node mobility evaluation, Link quality evaluation, and Node trust evaluation. Firstly, Candidate forwarding sets are filtered out by predicting the positions of source vehicles and neighbor vehicles. Secondly, The Node mobility

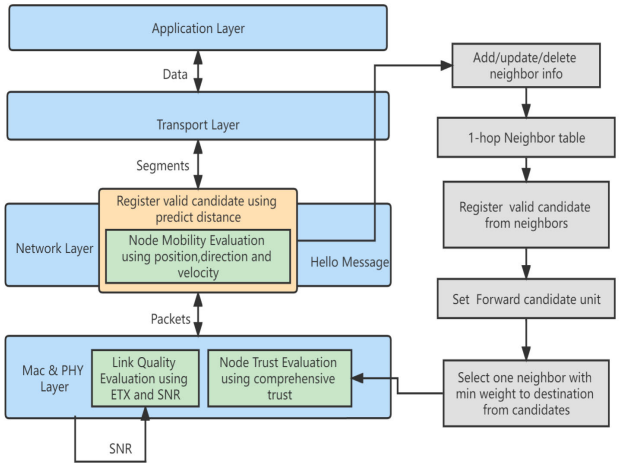


FIGURE 1. TBGR system architecture.

evaluation module updates the mobility information of neighbor nodes based on the periodically exchanged Hello message, and evaluates the mobility of candidate nodes relative to the destination using the distance, direction, and speed between source nodes, candidate nodes, and destination nodes. Link quality evaluation uses real transmission count (RTC) and link signal-to-noise ratio to evaluate the link quality between the current node and the candidate node. The Node trust evaluation module obtains the comprehensive trust value of the node by calculating the direct trust and indirect trust. TBGR calculates the weight value according to the routing metrics evaluated by the above modules and selects the candidate node with the lowest weight value for forwarding.

B. NETWORK MODEL AND ASSUMPTIONS

For geographic routing protocols, the following assumptions are made. First, vehicles at each node are equipped with GPS and other navigation systems, and nodes can use GPS and stored digital maps to determine their positions; Secondly, based on the assumption that the destination address is known, each node uses the location service to query the location service to obtain the location of the destination [4]. Third, node vehicles have the same communication radius. Within the range, nodes use periodically exchanged Hello messages to update the information of adjacent nodes.

TABLE 2. Notations used in the model.

Notations	Description
$FCSV_n$	Forward candidate aggregate of vehicle n
Δt	Time elapsed since the last Hello message was received
(x_i,y_i)	Location coordinates of vehicle i
(v_x^i,v_y^i)	Velocity coordinates of vehicle i
$D_{v'_S,v'_N}$	The Euclidean distance between V_S and V_N at time t
N_{v_s}	Neighbours aggregate of vehicle s
θ	Direction angle of vehicle
φ_{v_S}	Velocity of vehicle s
RTC	Link actual transmission count
r	Retransmission threshold
P_{signal}	Average signal power
P_{noise}	Average noise power
ITV_i	Indirect trust value of node j relative to node i
DTV_i	Direct trust value of node i
NRV_{V_i}	Total neighbour recommended value of vehicle i
M(V_i,V_D)	Mobility of candidate vehicle i relative to destination D
LQ(V_n,V_i)	Link quality between V_n and V_i
Trust(v_i)	Comprehensive trust value of vehicle i

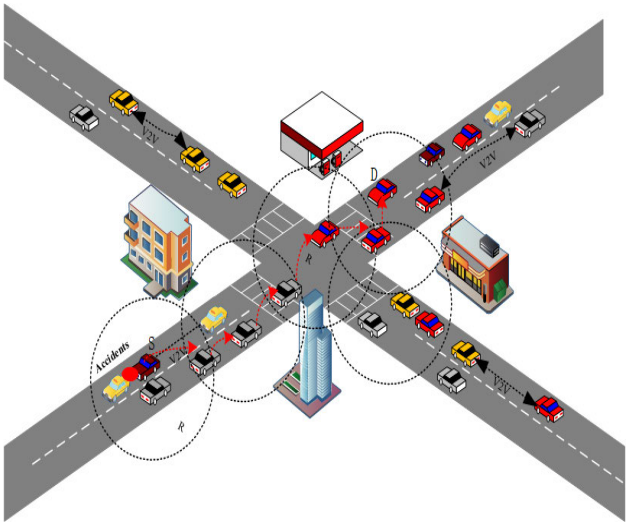


FIGURE 2. EMs propagation network model.

TABLE 3. HELLO message format.

Data Field	Size
Sender Ipv4Address	4 bytes
Sender position	16 bytes
Sender velocity	16 bytes
Sender trust	8 bytes

As shown in Fig.2, when the front vehicle sends a traffic accident, the accident vehicle will generate corresponding EMs, which will be transmitted to the adjacent vehicles within the communication range through V2V communication until the emergency message is transmitted to the target vehicles in the rear area to remind the following vehicles to avoid in time. It can be seen from the above assumptions that the vehicle can obtain its position and speed through the GPS positioning system and wheel speed sensor respectively. The EMs sent by the accident vehicle (AV) is forwarded to the vehicle in the target area in the form of a multi-hop. The transmission route of EMs is shown in the red dotted line in Fig.2. The symbols used in our model are summarized in Table 2.

TABLE 4. A neighbor entry format.

Data Field	Size
Neighbour Ipv4Address	4 bytes
Position	16 bytes
Velocity	16 bytes
Direct trust	8 bytes
SNR	8 bytes
Packet_{count}	4 bytes
Packet_{suc}	4 bytes
Lifetime	4 bytes

Table 3 shows the Hello message format used in TBGR, which consists of neighbor node information such as IP, location, speed, etc. The neighbor ID is used to judge the freshness of received Hello message information. To avoid collisions and mitigate the impact of possible packet collisions, Hello packets are generated periodically at predefined time intervals (+jitter), in which random jitter is added. Parameters such as speed, location, and neighbor address are extracted from the Hello message. The Hello packet interval should be brief to receive more precise and current node location information. Therefore, we set the lifetime of the neighbor list to 2 seconds and the interval between sending Hello packets to 1 second, so that the node can receive the latest traffic messages within the communication range promptly to update the neighbor table.

Nodes in the neighbor's table can be incorrectly erased due to the delay or loss of the Hello packet, and the next hop selection is erroneous. The neighbor table has a fixed life cycle, and the vehicle must maintain and update regularly. First, when receiving a new Hello message, the current sender compares the serial number of the neighbor node from the Hello packet with its serial number from the current neighbor database to ascertain the neighbor node's freshness. If the received serial number already exists, the current sender deletes the node's historical information and inserts a new node record to update the neighbor node's information. If the node doesn't be located in the existing neighbor table, it is the newly discovered neighbor node. The collected information from the Hello packet is then appended to the end of the neighbor table, and a new neighbor node is added. Additionally, the lifetime of each node in the neighbor database is fixed. The neighbor entries of the node are treated as expired and are immediately erased if no new Hello messages are received before the expiration date. The format of neighbor table entries is shown in Table 4.

IV. ROUTING STRATEGY

The routing protocol proposed in this paper uses V2V without RSUs, which is more suitable for road traffic information exchange and message delivery within an accident happening places. In urban life, vehicles move fast and topology changes frequently, thus it is very difficult to obtain the dynamic information of all vehicles on a specific path. Algorithm 1 describes our routing scheme. In our proposed scheme, senders at the neighbor nodes are forwarding messages, without obtaining all vehicle information on a certain road

Algorithm 1 Node Trust Based Geographic Routing Algorithm at Node V_n

V_n creates and updates the $N_T able$ when receives HELLO messages from neighbor vehicles.
V_n maintains $H_T able$ and $E_T able$ according to neighbor information.
for any message m that needs to be forwarded by V_n **do**
    Obtain the destination position of $V_n(m)$ using location-service.
    Obtain neighbor V_i' position at t_1 from $N_T able$ and predict neighbor V_i' position at t_2.
    if Predicted $EuclideanDistance(V_i', V_n) < R$ **then**
        $FCSV_n \longleftarrow V_i$.
    else
        Delete V_i from neighbor Candidate.
    end if
    if $!FCSV_n$ **then**
        for each node V_i in $FCSV_n$ **do**
            $Measure(V_i) \longleftarrow \mathrm{M}(V_i,V_D)+\mathrm{LQ}(V_n,V_i) + Trust(V_i)$.
            Calculate weight(V_i) using M, LQ and Trust.
            Next hop$\longleftarrow V_i$ with $weight_{min}$.
        end for
    else
        Forward message m at node V_n using Right-Hand rule and Left-Hand rule.
    end if
end for

section. We regard the current communication range of the sender as the forwarding area, dynamically narrow the area through the location prediction scheme, exclude the unstable nodes, and then take the effective neighbor nodes as the forwarding candidates of the sender (represented by $FCSV_n$). The current sender selects the next hop forwarding message based on the mobility, link quality, and trusted node of the candidate node. The workflow of TBGR is shown in Fig.3. This section will introduce our proposed routing scheme, including filtering of candidate forwarding sets, next hop node selection mechanism, and recovery mechanism.

A. IDENTIFY FORWARDING SETS OF CANDIDATE NODES

In EMs transmission, priority should be set for neighbor nodes to enable reliable nodes to forward messages first. Since VANETs have high mobility and the location of nodes is updated frequently, the selected relay nodes may have left the communication range of the current sender at the next moment, resulting in transmission interruption. Therefore, this paper proposes to filter stable nodes in the forwarding area by using the predicted location of nodes to narrow the range of candidate forwarding. The node whose predicted distance between the source vehicle and the neighbor vehicle is still less than the communication range of the sender is determined as a valid candidate node and enters the forwarding candidate set $FCSV_n$. As shown in Fig.4, the vehicle position changes at time point t_1 and t_2 respectively. We use the location prediction mechanism to calculate the position of the source vehicle and the neighbor vehicle: predicted position=current position + displacement [30]. The future position of a vehicle node i can be defined as:

$$\Delta t = t_2 - t_1$$

$$\begin{aligned} x_i' &= x_i + \Delta t \times v_x^i \\ y_i' &= y_i + \Delta t \times v_y^i \end{aligned} \tag{1}$$

The initial position (x_i, y_i) and speed (v_x^i, v_y^i) are obtained from received Hello messages.

The predicted relative distance between the source vehicle and the candidate vehicle can be calculated by:

$$D_{v_s', v_N'} = \sqrt{\left(x_s' - x_n'\right)^2 + \left(y_s' - y_n'\right)^2} \tag{2}$$

The condition for judging valid candidate [11] nodes can be defined as:

$$\mathrm{FCSV_n} = \left\{ V_n \mid D_{(v_S', v_n')} < R, \forall v_n \in N_{v_s} \right\} \tag{3}$$

R is the communication range of the vehicle. When the location distance between the source vehicle and the adjacent vehicle at the next time is still less than the communication range R, the neighbor node is selected into $FCSV_n$.

B. NEXT-HOP NODE SELECTION

1) NODE MOVEMENT EVALUATION

For emergency information related to life, it is essential to ensure high reliability and low delay of its transmission. In the forwarding process, in order to quickly send the message to the destination vehicle and reduce the delay, the closest node to the destination of the mobile process is usually selected [31]. This paper considers three parameters to measure the mobile process of nodes relative to the destination, and reflect the length of link life between nodes indirectly.

Parameter 1: Distance

With signal fading, the longer the distance is, the shorter the link life and the higher the probability of link interruption

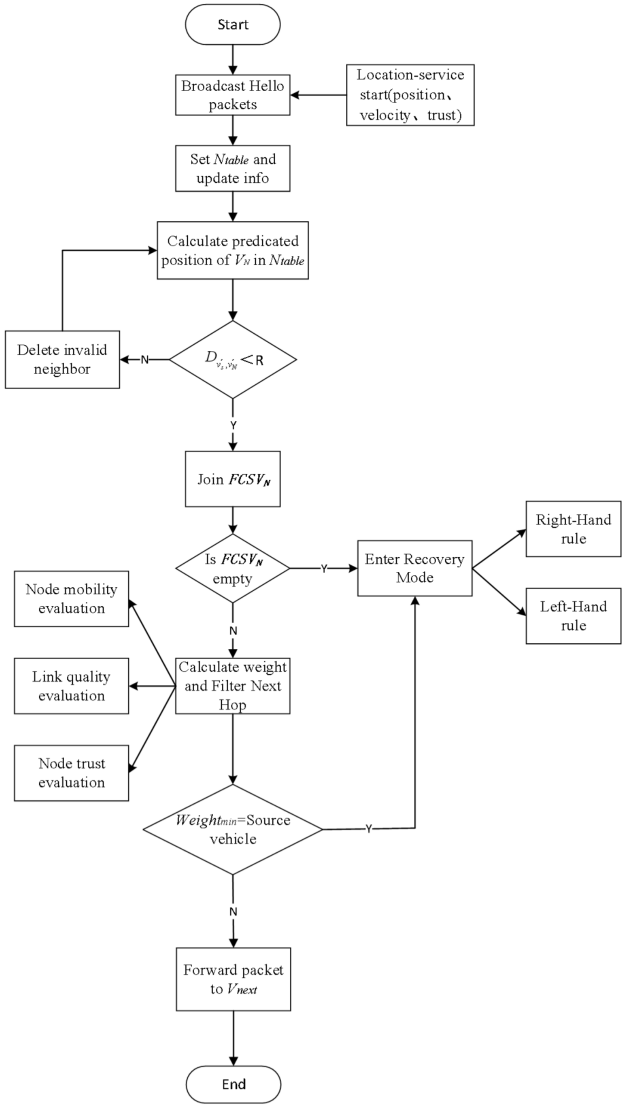


FIGURE 3. TBGR working flowchart.

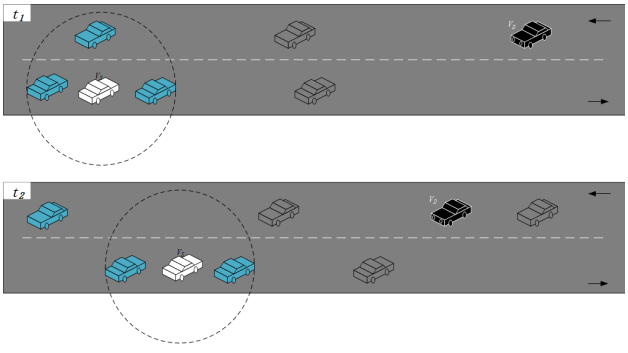


FIGURE 4. Schematic diagram of relative changes in vehicle position.

will be. In addition, unnecessary hops may be added during the transmission process, resulting in additional signal interference. In this paper, the location of candidate neighbor nodes and destination nodes is obtained through Hello messages and location service. The distance between candidate nodes and destination nodes is calculated by using

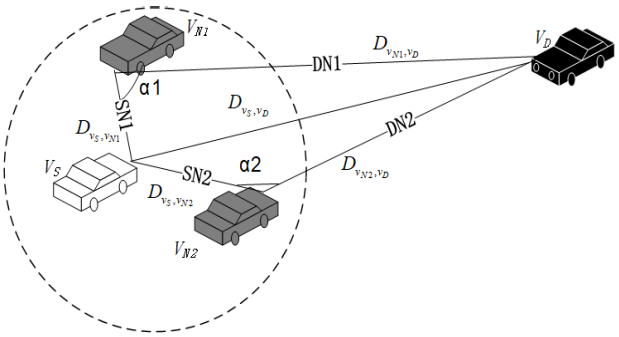


FIGURE 5. Diagram of relative vehicle angles.

Pythagoras theorem and the nodes that are closer to the destination are selected. We employ the Euclidean distance between cars, which indicates the true distance between two spots in a two-dimensional environment. In the actual world, physical obstructions such as large buildings and trees will exist between automobiles. We have not yet considered the impact of these impediments on message transmission. As a result, when measuring the distance between vehicles, we did not enter the three-dimensional angle of space, instead measuring only two-dimensional plane distance. In the simulation environment, assuming that all vehicles move on the same plane, we first choose a few candidate vehicles that are in a stable state based on their Euclidean distance from one another, it is calculated by the following equation:

$$D_{v_i,v_j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{4}$$

Parameter 2: Bearing

When the next hop vehicle is chosen in the opposite direction as the current sender, the message may stray from its intended destination, resulting in a routing loop. However, if it is solely determined by whether the direction of the vehicles at the node is consistent, it is also possible to run into an intersection situation, in which case vehicles may leave at the next intersection going in the same direction as the source vehicle, which will also cause the message to deviate from its intended course. To improve the reliability of the next hop, this study examines the motion progress of the candidate vehicle toward the destination by measuring the motion angle between the source vehicle, the candidate vehicle, and the destination vehicle. Measuring the angle of direction can help you determine the angle between the source vehicle, the neighbor vehicle, and the target vehicle and the neighbor with the smallest angle with the source and the target is closer to the destination. Fig.5 depicts line segments connecting the source and destination nodes for planning vehicles N1 and N2. We assume that vehicles N1 and N2 are valid candidate neighbors of the source vehicle S, $\alpha 1$ is the included Angle between line DN1 and SN1, and $\alpha 2$ is the included Angle between line DN2 and SN2. When $\alpha 1 > \alpha 2$, we can infer that vehicle N2 is traveling more quickly than vehicle N1, and thus vehicle N2 has a higher priority for forwarding than

vehicle N1. Bearing calculation [10] is shown in the following formula:

$$\theta = \frac{D^2_{v_S,v_N} + D^2_{v_S,v_D} - D^2_{v_N,v_D}}{2 * D_{v_S,v_D} * D_{v_S,v_D}} \tag{5}$$

Parameter 3: speed difference

It is crucial to ensure the timeliness of emergency messages transmission. Generally speaking, fast vehicles have higher priority than slow vehicles. If the distance between two vehicles is close, the speed difference is small, and the deviation in the moving direction is small, it can indicate that the two vehicles will travel together for a long time in a period, that is, the link established between them will be more stable, and the link life will be relatively long. The speed difference between the source vehicle and the candidate vehicle can be calculated by:

$$\Delta v = \left|\varphi_{v_S} - \varphi_{v_N}\right| \tag{6}$$

Therefore, the movement process of candidate vehicle i relative to the destination can be evaluated by weighting the calculation, as shown in the following equation:

$$M_{v_i,v_D} = W_D \times D_{v_s,v_D} + W_\alpha \times 1/\theta + W_V \times \Delta v \tag{7}$$

W_D,W_α,W_V represents the weight factors of distance, bearing and speed respectively. The importance of each parameter is determined according to the assignment, $W_D + W_\alpha + W_V = 1$.

In the node mobility evaluation module, vehicles are able to determine their exact locations through positioning technologies like GPS and wheel speed sensors. In actual applications, these systems struggle with issues like imprecise positioning, broken communications, and lack of privacy. With real GPS, positioning mistakes or faulty data transmitted to another vehicle may happen, which will limit the reliability of the relay vehicle selection and surely lower the routing performance in real circumstances. The geographical location of nodes is used to estimate the distance and direction between nodes in this article. As a result, when faults occur in the GPS service, the node location generates errors, and the distance and direction angle parameters determined based on the node position will be incorrect in the routing process, which will damage the accuracy of the routing choice. We included link quality and node trust parameters in our suggested model to lessen the interference of positioning errors. Node mobility modules contributed to a limited fraction of forwarding node selection, and neighbor node information was not the only factor in routing decisions.

2) LINK QUALITY ASSESSMENT

a: REAL TRANSMISSION COUNT VIA LINK

Wireless links may encounter link breakage during the transmission of messages under the influence of signal fading. In the past routing protocols that only consider the node mobility index, the links usually established are unstable, with a high probability of message transmission failure or retransmission. To select a more reliable next-hop node, this paper measures the link quality between the current node and the next-hop node based on the geographical location information of the node. The classical routing metric expected transmission count (ETX) measures the link asymmetry by considering the loss ratio dually [32], but ETX only considers the transmission rate of the link and does not measure the actual transmission cost, which may lead to underestimating or overestimating the loss. Therefore, we choose to measure the link's real transmission count, taking into account not only the link transmission rate and actual transmission cost but also the link retransmission limit r. The link transmission rate q represents the probability that data packets pass through the link successfully in two directions (probe packet transmission and ACK packet transmission). The transmission rates in these two directions are calculated using the probe packets sent periodically by the node. Because each node broadcasts Hello messages periodically, Hello messages can act as a detection packet. r indicates the maximum number of retransmissions allowed by the sending node before giving up forwarding messages, and an appropriate threshold should be set in advance. Because RTC does not account for the effects of network interference and flow loads, neighboring nodes may experience collisions or even packet loss. This article is based on the assumption of ignoring the effects of network interference and traffic loads.

The RTC method works as follows: Each node needs to record the time t_0 of the first Hello message received from a neighbor node and calculate the number of messages received from a neighbor within the last w seconds. Then, compare the interval from t to t_0 at the current time with the size of window w using different calculation methods. The link transmission rate q [33] can be calculated as follows:

$$q = \begin{cases} count\,(t_0, t)\,, 0 < t - t_0 < 1 \\ \frac{count(t_0,t)}{(t-t_0)/\tau}, 1 \le t - t_0 < w \\ \frac{count(t-w,t)}{w/\tau}, t - t_0 \ge w \end{cases} \tag{8}$$

wherein, $count\,(t_0, t)$ is the number of Hello messages received during the period from t to t_0, τ is the broadcast interval of Hello messages and w are the window size. The last improved RTC calculation is based on two parameters: q and r, we get the following:

$$\begin{aligned} \mathrm{RTC} &= \sum_{k=1}^{r+1} k \cdot q^2 \left(1 - q^2\right)^{k-1} + (r+1) \cdot \left(1 - q^2\right)^{r+1} \\ &= \frac{1 - \left(1 - q^2\right)^{r+1}}{q^2} \end{aligned} \tag{9}$$

b: SIGNAL TO NOISE RATIO (SNR)

Signal to Noise Ratio (SNR) is defined as the ratio of the power of a meaningful signal to the power of the background noise. While a Hello message is receiving, SNR packet labels are extracted at the routing layer and stored in the neighbor table [10]. SNR calculation is shown in the

TABLE 5. Reply message format.

Data Field	Size
Sender IPV4Address	4 bytes
Packet received num	4 bytes

following equation:

$$\mathrm{SNR} = \frac{P_{\mathrm{signal}}}{P_{\mathrm{noise}}} \tag{10}$$

where P_{signal} is the average signal power and P_{noise} is the average noise power. Links with high SNR have higher priority than links with low SNR.

The link quality evaluation between nodes can be defined as:

$$\mathrm{LQ}_{\mathrm{v_n},\mathrm{v_i}} = \frac{\mathrm{RTC}}{\mathrm{SNR}} \tag{11}$$

3) NODE TRUST EVALUATION

At present, the criteria to measure the node's trust includes the node's activity, the success rate of forwarding packets, and the node's social attributes. These metrics directly reflect the node's behavior, but a node may become unreliable and insecure due to many factors. Therefore, this paper proposes to combine the direct and indirect factors that affect the node quality, and measure the node's comprehensive trust degree from two aspects: the node's success rate of forwarding packets and neighbor feedback. The success rate of forwarding data is the most intuitive and direct way to describe the forwarding capability of a node. As the number of packet forwarding failures increases, the probability of the node being judged as unreliable increases. Neighbor feedback is to obtain the evaluation value of neighbor nodes on candidate nodes, and then use the evaluation value as the neighbor recommendation factor to calculate the indirect trust value of nodes. The calculation process is mainly divided into the following two steps:

Step 1: Direct trust

When calculating the direct trust value, we use the periodic calculation of the success rate of forwarding packets to evaluate. In the forwarding process, we set a handshake mechanism based on the ACK message confirmation. When the receiver receives a message from the sender, it needs to return an ACK confirmation message to the sender to indicate that it has received the message. The Reply message contains two fields: the sending IP address and the number of packets, as shown in Table 5.

Assume that the total number of messages received by vehicle node i is N, and the number of messages successfully forwarded is expressed as suc; We calculate the direct trust value of the node using the following equation:

$$\mathrm{DTV_i} = \begin{cases} 0.5 \times \left(1 - \frac{0.1}{NV_i + 0.1}\right) & suc = 0 \\ \frac{suc}{NV_i} \times \left(1 - \frac{0.1}{NV_i + 0.1}\right) & suc \neq 0 \end{cases} \tag{12}$$

Step 2: Indirect trust

Indirect trust value is measured by collecting the neighbor evaluation value of candidate nodes, which is stored in Hello messages by the neighbor. Through the evaluation of neighbor nodes, it can be observed whether the historical behavior of the node is active. However, some malicious nodes may also be mixed in with neighbor nodes. Therefore, it is not advisable to directly use the neighbor recommendation value obtained from the Hello message as the indirect trust value of the candidate node. It is easy for malicious nodes to forge each other, Therefore, in this paper, the neighbor evaluation value obtained is used as a recommendation factor and combined with the direct trust value of candidate nodes for calculation.

When calculating the recommendation factor, we calculate the average value of the neighbor evaluation value of the candidate node extracted from Hello messages:

$$\alpha = \begin{cases} 0.5 & NV_i = 0 \\ \frac{NRVV_i}{Nnum} & NV_i \neq 0 \end{cases} \tag{13}$$

Among them, NV_i represents the number of neighbors of vehicle i, N_{num} represents the total number of neighbors providing evaluation values, and NRV_{V_i} represents the total evaluation value of neighbors of vehicle i.

According to the recommended factor α, the indirect trust value of vehicle node i can be calculated by:

$$\mathrm{ITV_i} = \alpha \times \frac{DTV_i}{ATV_{in} - DTV_i} \tag{14}$$

wherein, ATV_{in} is the sum of the direct trust values of candidate nodes of vehicle V_i.

Finally, based on the weighting of direct trust and indirect trust, the comprehensive trust value of the node is obtained, as shown in the following formula:

$$\mathrm{Trust_{v_i}} = \beta * DTV_i + (1 - \beta) * ITV_i \tag{15}$$

β refers to the ratio of the current node's routing time to the total routing time of all nodes in the neighbor list.

4) WEIGHT VALUE CALCULATION

In our scheme, the accident vehicle selects the most suitable node from the candidate forwarding set according to the weight value calculated by node mobility, link quality, and trust. The reliable and fast path to the destination depends on the comprehensive screening of multiple routing indicators. Therefore, the weight value of each node in the candidate forwarding set is calculated by entering the above-evaluated routing metrics into the weight function, and then the node with the lowest weight value is selected for forwarding. The weight function can be calculated by:

$$\mathrm{Fit_{v_N}} = W_\alpha \times M_{v_N,v_D} + W_\beta \times LQ_{v_S,v_N} + W_\gamma \times (1/Trust_{v_i}) \tag{16}$$

W_α,W_β,W_γ represents the weight factors of node mobility, link quality and trust respectively, $W_\alpha + W_\beta + W_\gamma$=1.

C. RECOVERY MECHANISM

In terms of average delay, the issue is that the communication link between nodes is unstable, which causes the average

delay to rise because of the high dynamic characteristics of VANETs. we improve the local maximum problem. when the sender encounters a local maximum problem and cannot find a better node to forward than itself, it will lead to the delay of EMs. The traditional geographic routing adopts a right-handed rule-based recovery model. However, the right-hand rule may lead to a long path to the destination, resulting in additional hops. In order to avoid routing redundancy and loops, this paper combines left-handed rules with right-handed rules. When the sender enters the recovery mode, it replicates the packets and forwards them using left-handed and right-handed rules [34] to minimize possible routing loops and redundancy. However, because the message is forwarded by copying the data packet, which will incur additional network overhead, in order to avoid the data packet being forwarded by two rules at the same time while forwarding, we have created a Neighborhood Extended Table (ET) consisting of two fields: neighbor IP and triple vector: (F, I, D). The F represents the forwarding type used for the message, with three modes: G (greedy forwarding), L (left-handed forwarding), and R (right-handed forwarding). The I represents the message identifier, and the D is the IP address of the destination. According to the message identification and the information used in the ET, messages that have been sent will not be forwarded.

V. PERFORMANCE EVALUATION

Simulation is an important factor in analyzing and verifying protocols. This paper compares the proposed protocol with the following:

GPSR: Consider the geographic information of the node and select the neighbor node closest to the location of the destination node for greedy forwarding.

MM-GPSR [35]: Select the next hop node based on the stability of neighbor node N and communication area Q, and use the predefined λ parameter to control the distance of the communication area. Only the nodes in the communication area can receive packets and the node with the highest stability is selected as the next hop.

GPSR and MM-GPSR are the classic benchmark solutions, When studying the routing indicators, the above two protocols concentrate on the node's movement. It is challenging to precisely determine the movement of ancillary vehicles according to the mobility state because of the high dynamics of vehicle nodes. At the above agreement, it is difficult to ensure the reliability and delay of EMs during the transmission process.

A. SIMULATION SCENARIO AND PARAMETER SETTINGS

We used ns-3.26 and traffic simulation software Sumo-1.13.0 to simulate all protocols. ns-3 encourages the development of sufficiently realistic simulation models to allow ns-3 to be used as a real-time network simulator. In sumo, we draw maps, then simulate road operations with different numbers of vehicles, and finally output files for testing in ns-3. Then, we input the vehicle random motion track file limited by the road network generated by sumo into ns-3. At the beginning of each simulation, the vehicles are randomly distributed in the road network and move randomly according to the Car flooding model. The road network area is 1100m × 1100m, there are 9 intersections in total, each road section is set with two-way lanes, and all vehicles have the same physical configuration. Each node pair (source to destination) adopts a constant bit rate (CBR) for data traffic, generating a fixed size of 512 bytes of data packets. This article randomly selects 5 pairs of source destination node pairs. The simulation parameters are shown in Table 6.

TABLE 6. Simulation parameter.

Parameter	Value	Unit
EM Packet Size	512	bytes
Hello Interval	1	s
Transmission Range	250	m
Simulation Time	200	s
Simulation Run	30	-
Channel Data Rate	3	Mbps
MAC Protocol	IEEE 802.11p	-
Data Type	CBR	-
MM-GPSR λ Factor	0.3	-
Transport Protocol	UDP	-
N_{Table} Entry Lifetime	2	s
Propagation Model	Two-ray Ground	
Number of Vehicles	110-300	
Speed of Vehicles	15-25	m/s
Protocol compared	GPSR, MM-GPSR	

B. ANALYSIS OF EXPERIMENTAL DATA

1) SCENARIO 1: ABSENCE OF MALICIOUS NODES

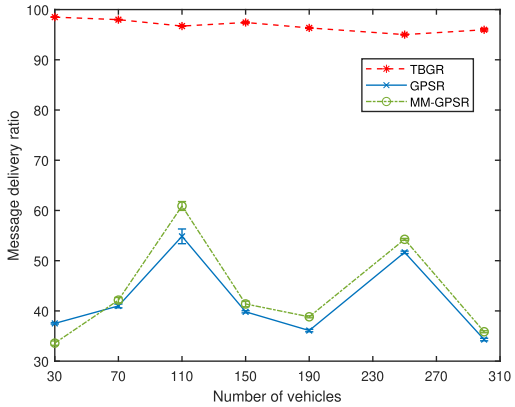
We conducted 30 independent experiments under the same configuration by changing the vehicle speed and density, and then comprehensively considered the average of the 30 simulation results. To simulate sparse and dense networks, we used 110 to 300 vehicles and set the speed range to low speed (15m/s), medium speed (20m/s), and high speed (25m/s). In order to measure the reliability and timeliness of emergency message forwarding, we simulated the following four performance indicators:

Message Delivery Rate (MDR): The ratio of the number of messages successfully sent to the destination to the total number, reflecting the reliability of the route. It can be calculated by:

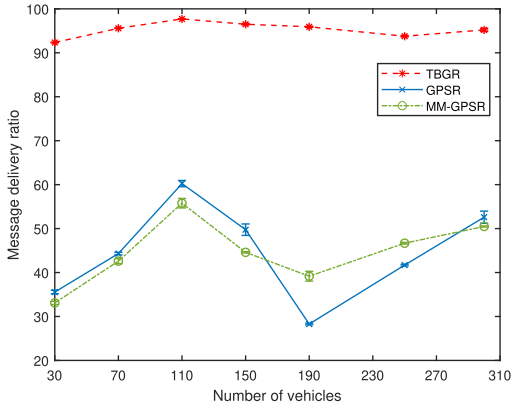
$$\mathrm{MDR} = \left(\frac{\sum M_{RD}}{\sum M_{TS}}\right) \times 100 \tag{17}$$

where $\sum M_{RD}$ indicates the total number of messages received by the destination, $\sum M_{TS}$ indicates the total number of messages sent by the source node.

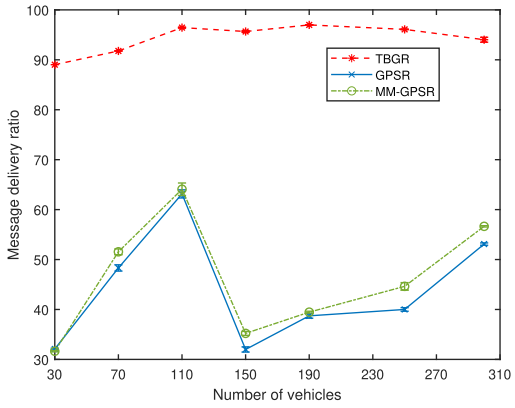
Fig.6(a-c) shows the MDR changes derived from varying vehicle density at three speeds to simulate different scenarios. In all scenarios, TBGR provides the highest MDR, reaching 95%; when compared to GPSR and MM-GPSR, it is increased by 36% and 28%, respectively. TBGR uses position prediction to choose a more stable vehicle node. When measuring link quality, TBGR considers channel state and selects links with a high signal-to-noise ratio for



(a) Low Speed



(b) Middle Speed



(c) High Speed

FIGURE 6. Effect of vehicle density and speed variation on average delivery rate.

forwarding, effectively alleviating channel congestion and reducing packet loss. MM-GPSR provides between 33% and 62%. GPSR provides a minimum MDR between 38% and 54%. The introduction of more messages in the network will increase the probability of buffer overflow or packet collision. Due to an increase in the number of forwarding failures caused by collisions, the MDR of GPSR and MM-GPSR decreased. TBGR adopts an ACK confirmation mechanism, which allows the sender to retransmit messages when message forwarding fails. When the number of vehicles increases, TBGR can always maintain a stable level.

Average latency (AD): The average end-to-end propagation delay for a message successfully received by a destination, including queuing delay, transmission delay, and retransmission wait time. it can be calculated by:

$$\mathrm{AD} = \frac{\sum_{i=1}^{Num} D_i}{Num} \tag{18}$$

where D_i is the delay for each packet received successfully.

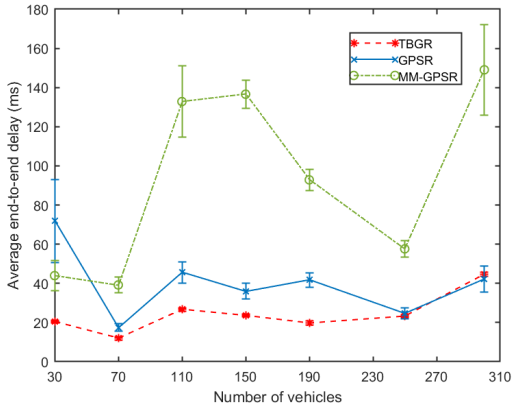
The end-to-end delay varies with the number and speed of vehicles, as shown in Fig.7(a-c). The delay variation of GPSR is within 100ms, and the right-hand rule in GPSR can lead to path redundancy (caused by incorrect next-hop selection), increasing end-to-end delay. We observed that the ADD of MM-GPSR increased linearly between 30 and 150 vehicle nodes, reaching a maximum of 150ms. MM-GPSR utilizes the positions of nodes and destinations to divide the plane into two parts, using the minimum angle to select the next hop, which may lead to erroneous judgments and path redundancy, thereby increasing end-to-end latency. The delay of TBGR is between 18ms and 55ms. When selecting the next hop, the link quality between nodes was measured, and a link with good channel status was selected to minimize frequent link interruption. However, due to the RTC index not taking into account node load and interference in routing decisions, delays increase as the density of vehicles in the network increases. Overall, TBGR can still maintain a stable low level, with end-to-end latency increasing by 40% and 60% compared to GPSR and MM-GPSR, respectively.

Throughput: The number of effective messages successfully transmitted from AV to destination per unit time in the network:

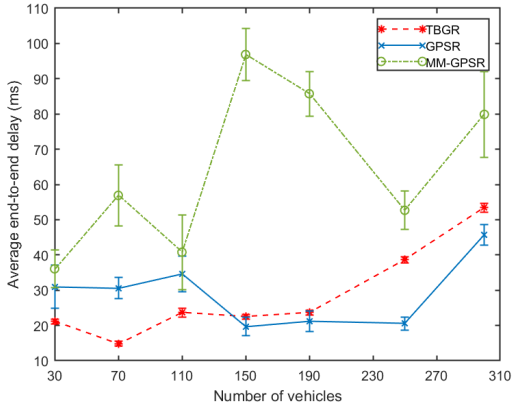
$$\text{Throughput} = \frac{\sum M_{RD}}{\sum M_{Ti}} \tag{19}$$

where, $\sum M_{RD}$ refers to the number of messages that the destination successfully received, $\sum M_{Ti}$ refers to all the messages from the source node number. It measures both the transmission cost and the throughput achieved in the network.

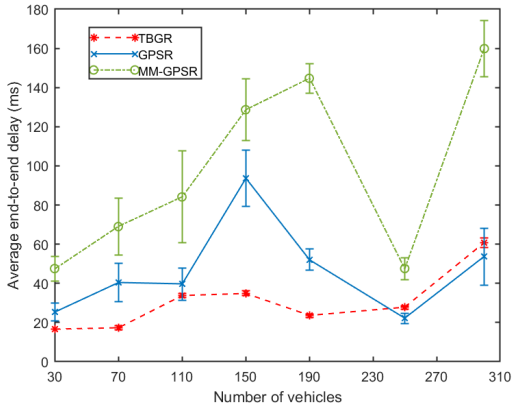
Fig.8(a-c) shows the network throughput of the three protocols at different speeds and densities. The performance of our proposed protocol outperforms the remaining two simulated protocols and remains stable at different vehicle densities. As the network density increases, the connectivity between vehicles rises the likelihood of redundant packets being transmitted and packed decreases, at the same time, the communication load capacity will increase, and there will be more and more data packets reaching the destination in a given amount of time. Therefore, the throughput of each scheme is slightly better than before. Due to the rise in vehicle speed, the throughput of the two protocols, MM-GPSR and GPSR has dropped. The TBGR has a tighter, steadier path. it can effectively establish a stable and robust routing using the mobility metrics of the nodes and the link



(a) Low Speed

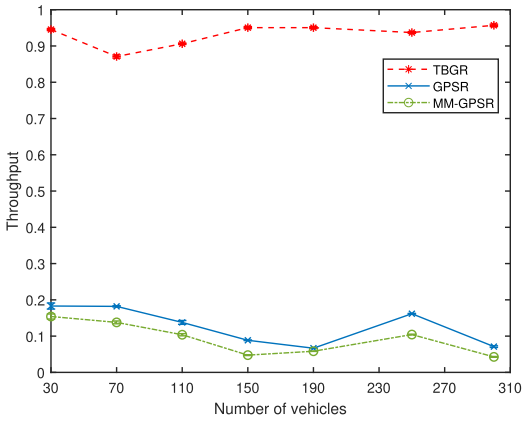


(b) Middle Speed

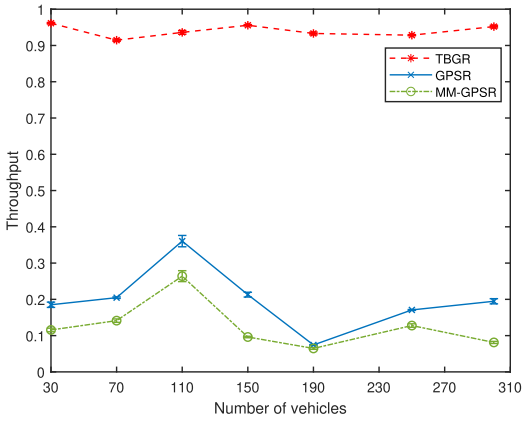


(c) High Speed

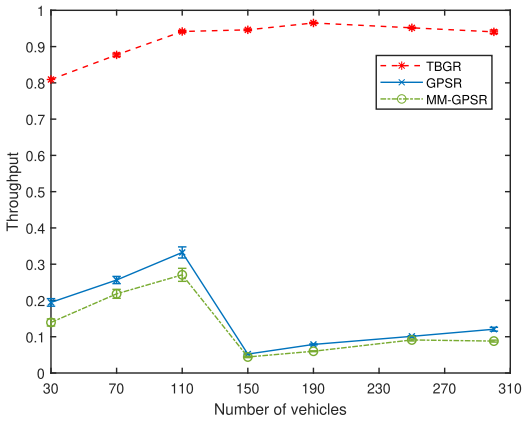
FIGURE 7. Effect of vehicle density and speed variation on average end-to-end delay.



(a) Low Speed



(b) Middle Speed



(c) High Speed

FIGURE 8. Effect of vehicle density and speed variation on throughput.

quality, which enables the network throughput to remain stable and makes it better suited for the prompt delivery of EMs.

2) SCENARIO 2: PRESENCE OF MALICIOUS NODES

Assuming that there are malicious nodes in network environment, we adopt the black hole attack to simulate the malicious behavior of nodes. When the malicious nodes receive messages, they directly discard them, forming a black hole mode in which messages only enter and cannot come out [36], to imitate the malicious behavior of nodes. The number of malicious nodes ranges from 10 to 40.

Black hole attack: After gaining control of the network data packet through the deception of the routing protocol, it is discarded directly when the malicious node receives the message, forming the black hole mode in which messages cannot be entered or exited to imitate malicious behavior, which can realize the malicious attack in VANETs.

Our simulation was measured using the following performance metrics:

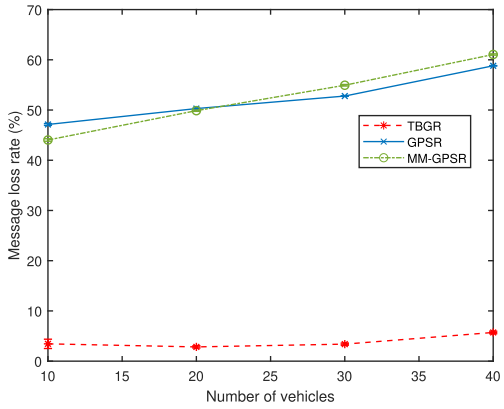


FIGURE 9. Effect of malicious node number change on message loss rate.

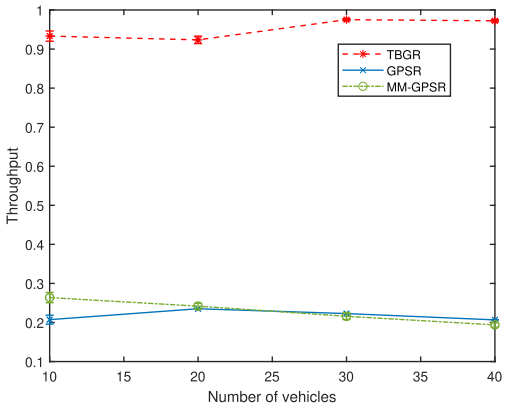


FIGURE 10. Effect of malicious node number change on network throughput.

Message Loss Rate (MLR): The ratio of the total number of lost messages to the total number of messages sent to the destination:

$$\mathrm{MLR} = \frac{\sum M_{loss}}{\sum M_{TS}} \times 100 \tag{20}$$

where $\sum M_{loss}$ is missing the total number of messages, Fig.9 shows the changes in packet loss rates of all simulated protocols encountered by malicious nodes in the network. The packet loss rates of MM-GPSR and GPSR are between 45% and 60%, showing an upward trend. Due to the lack of message confirmation feedback mechanisms in MM-GPSR and GPSR, it is impossible to know whether the sent message was successfully sent to the relay node, so even if the message is lost, it will not be retransmitted. When the number of malicious nodes in the network increases, MM-GPSR and GPSR do not take into account the reliability of the selected nodes themselves, making it difficult to determine whether the selected nodes are trustworthy, resulting in severe packet loss. TBGR sets up an ACK confirmation mechanism during the message propagation process, and measures the trust level of nodes, effectively identifying malicious nodes and avoiding the selection of malicious nodes for forwarding to a certain extent. As shown in Fig.9, TBGR always maintains the lowest packet loss rate, which is 40% higher than GPSR and MM-GPSR.

Throughput: The number of effective messages successfully transmitted from AV to destination per unit time in the network, as shown in (19).

As shown in Fig.10, as the number of malicious nodes increases, the throughput of all protocols in the network gradually decreases. Among the three protocols, GPSR and MM-GPSR are unable to make judgments and respond to malicious node packet loss behavior. Among them, GPSR heavily relies on neighborhood information and has the lowest throughput performance. TBGR can effectively select the appropriate next hop node for forwarding based on node trust, maintaining the highest throughput performance throughout the entire process. Compared to MM-GPSR and GPSR, it improves by 60% and 70%, respectively, surpassing the benchmark scheme. This is mainly because TBGR establishes a robust and reliable link, improves communication efficiency, and reduces latency.

VI. CONCLUSION

We propose a geographic routing strategy based on trusted nodes to accommodate the change in VANETs to achieve the reliable and fast transmission of emergency messages. The strategy is used to transmit emergency messages in flow and dense traffic conditions. Under normal circumstances, by predicting the location of nodes, we screen out more stable nodes in the forwarding area in advance, to ensure low latency and high reliability. Then measure the life cycle of links between nodes according to the mobility of nodes to select more stable links. At the same time, we introduce the improved link quality index. By calculating the actual transmission cost of the link between nodes, we set a limit on the number of link retransmissions to select the link with better quality. In addition, due to the insecurity of the vehicle network, malicious nodes may exist in the network. When messages are forwarded to unreliable nodes, message forwarding failure is very likely to occur. Therefore, the strategy described in the paper utilizes the forwarding ability and historical behavior of nodes to calculate the trust of nodes, so that they can also identify and avoid selecting problematic nodes to forward messages when malicious nodes exist. The algorithm is successfully simulated in flow and dense scenes of ns-3. Experiments show that the protocol outperforms the existing protocols GPSR and MM-GPSR in packet loss rate, end-to-end delay, and network throughput. Because RTC does not take into account the impact of interference and traffic in the network, neighboring nodes may have collisions and even packet loss. In subsequent work, we consider using physical interference models to dynamically reduce the impact of interference. In addition, this paper only implements the black hole attack type. We believe that the monitoring system can be used to further optimize the research scheme. Each vehicle can monitor the correct packet forwarding rate of its next hop and send its observation results of the next hop to its neighbors through push-based notifications. At the same time, in simulating the malicious behavior of nodes, we will attempt to adopt various

attacks for simulation to adapt to more complex scenarios in VANETs.

REFERENCES

[1] J. Wu, M. Fang, H. Li, and X. Li, "RSU-assisted traffic-aware routing based on reinforcement learning for urban VANETs," *IEEE Access*, vol. 8, pp. 5733–5748, 2020.
[2] S. Li and C. Huang, "A multihop broadcast mechanism for emergency messages dissemination in VANETs," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, Jul. 2018, pp. 932–937.
[3] S. Shokrollahi and M. Dehghan, "TGRV: A trust-based geographic routing protocol for VANETs," *Ad Hoc Netw.*, vol. 140, Mar. 2023, Art. no. 103062.
[4] O. Alzamzami and I. Mahgoub, "Geographic routing enhancement for urban VANETs using link dynamic behavior: A cross layer approach," *Veh. Commun.*, vol. 31, Oct. 2021, Art. no. 100354.
[5] K. N. Qureshi, F. Bashir, and A. H. Abdullah, "Distance and signal quality aware next hop selection routing protocol for vehicular ad hoc networks," *Neural Comput. Appl.*, vol. 32, no. 7, pp. 2351–2364, Apr. 2020.
[6] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior detection for position falsification attacks in VANETs using machine learning," *IEEE Access*, vol. 10, pp. 1893–1904, 2022.
[7] G. D. Singh, M. Prateek, S. Kumar, M. Verma, D. Singh, and H. Lee, "Hybrid genetic firefly algorithm-based routing protocol for VANETs," *IEEE Access*, vol. 10, pp. 9142–9151, 2022.
[8] O. Alzamzami and I. Mahgoub, "Link utility aware geographic routing for urban VANETs using two-hop neighbor information," *Ad Hoc Netw.*, vol. 106, Sep. 2020, Art. no. 102213.
[9] R. Han, J. Shi, Q. Guan, F. Banoori, and W. Shen, "Speed and position aware dynamic routing for emergency message dissemination in VANETs," *IEEE Access*, vol. 10, pp. 1376–1385, 2022.
[10] P. Singh, R. S. Raw, S. A. Khan, M. A. Mohammed, A. A. Aly, and D. Le, "W-GeoR: Weighted geographical routing for VANETs health monitoring applications in urban traffic networks," *IEEE Access*, vol. 10, pp. 38850–38869, 2022.
[11] G. Abbas, S. Ullah, M. Waqas, Z. H. Abbas, and M. Bilal, "A position-based reliable emergency message routing scheme for road safety in VANETs," *Comput. Netw.*, vol. 213, Aug. 2022, Art. no. 109097.
[12] S. Ullah, G. Abbas, M. Waqas, Z. H. Abbas, S. Tu, and I. A. Hameed, "EEMDS: An effective emergency message dissemination scheme for urban VANETs," *Sensors*, vol. 21, no. 5, p. 1599, Feb. 2021.
[13] S. Ullah, G. Abbas, M. Waqas, Z. H. Abbas, and A. U. Khan, "RSU assisted reliable relay selection for emergency message routing in intermittently connected VANETs," *Wireless Netw.*, vol. 29, no. 3, pp. 1311–1332, Apr. 2023.
[14] M. Selvi and B. Ramakrishnan, "Lion optimization algorithm (LOA)-based reliable emergency message broadcasting system in VANET," *Soft Comput.*, vol. 24, no. 14, pp. 10415–10432, Jul. 2020.
[15] H. Liu, T. Qiu, X. Zhou, C. Chen, and N. Chen, "Parking-area-assisted spider-web routing protocol for emergency data in urban VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 971–982, Jan. 2020.
[16] M. Afrashteh and S. Babaie, "A route segmented broadcast protocol based on RFID for emergency message dissemination in vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16017–16026, Dec. 2020.
[17] S. Ullah, G. Abbas, M. Waqas, Z. H. Abbas, and Z. Halim, "Multi-hop emergency message dissemination through optimal cooperative forwarder in grid-based 5G-VANETs," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 4, pp. 4461–4476, Apr. 2023.
[18] M. Marques, C. Senna, and S. Sargento, "Evaluation of strategies for emergency message dissemination in VANETs," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.
[19] D. Tian, C. Liu, X. Duan, Z. Sheng, Q. Ni, M. Chen, and V. C. M. Leung, "A distributed position-based protocol for emergency messages broadcasting in vehicular ad hoc networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1218–1227, Apr. 2018.
[20] X. Zhang, Q. Miao, and Y. Li, "An adaptive link quality-based safety message dissemination scheme for urban VANETs," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2104–2107, Oct. 2018.
[21] C. Chen, J. Jiang, R. Fu, L. Chen, C. Li, and S. Wan, "An intelligent caching strategy considering time-space characteristics in vehicular named data networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 19655–19667, Oct. 2022.
[22] Y. Ju, Y. Chen, Z. Cao, L. Liu, Q. Pei, M. Xiao, K. Ota, M. Dong, and V. C. M. Leung, "Joint secure offloading and resource allocation for vehicular edge computing network: A multi-agent deep reinforcement learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 5555–5569, May 2023.
[23] R. V. Raj and K. Balasubramanian, "Retracted article: Trust aware similarity-based source routing to ensure effective communication using game-theoretic approach in VANETs," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 6, pp. 6781–6791, Jun. 2021.
[24] C. P. Fernandes, C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham, "A blockchain-based reputation system for trusted VANET nodes," *Ad Hoc Netw.*, vol. 140, Mar. 2023, Art. no. 103071.
[25] Z. Liu, J. Weng, J. Ma, J. Guo, B. Feng, Z. Jiang, and K. Wei, "TCEMD: A trust cascading-based emergency message dissemination model in VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4028–4048, May 2020.
[26] N. Ullah, X. Kong, Z. Ning, A. Tolba, M. Alrashoud, and F. Xia, "Emergency warning messages dissemination in vehicular social networks: A trust based scheme," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100199.
[27] M. S. Rayeni, A. Hafid, and P. K. Sahu, "Dynamic spatial partition density-based emergency message dissemination in VANETs," *Veh. Commun.*, vol. 2, no. 4, pp. 208–222, Oct. 2015.
[28] M. U. Ghazi, M. A. K. Khattak, B. Shabir, A. W. Malik, and M. S. Ramzan, "Emergency message dissemination in vehicular networks: A review," *IEEE Access*, vol. 8, pp. 38606–38621, 2020.
[29] W. Benrhaiem, A. Hafid, and P. K. Sahu, "Reliable emergency message dissemination scheme for urban vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1154–1166, Mar. 2020.
[30] I. Cherifi and Z. M. Maaza, "Link failure tolerant GPSR protocol," *Int. J. Networked Distrib. Comput.*, vol. 9, pp. 94–104, Jul. 2021.
[31] S. Din, K. N. Qureshi, M. S. Afsar, J. J. P. C. Rodrigues, A. Ahmad, and G. S. Choi, "Beaconless traffic-aware geographical routing protocol for intelligent transportation system," *IEEE Access*, vol. 8, pp. 187671–187686, 2020.
[32] A. Ghaffari, "Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 4, pp. 1593–1603, Apr. 2020.
[33] A. Silva, N. Reza, and A. Oliveira, "Improvement and performance evaluation of GPSR-based routing techniques for vehicular ad hoc networks," *IEEE Access*, vol. 7, pp. 21722–21733, 2019.
[34] J. Wang, Y. Liu, Y. He, W. Dong, and M. Li, "QoF: Towards comprehensive path quality measurement in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 4, pp. 1003–1013, Apr. 2014.
[35] X. Yang, M. Li, Z. Qian, and T. Di, "Improvement of GPSR protocol in vehicular ad hoc network," *IEEE Access*, vol. 6, pp. 39515–39524, 2018.
[36] K. N. Tripathi and S. C. Sharma, "A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS)," *Int. J. Syst. Assurance Eng. Manage.*, vol. 11, no. 2, pp. 426–440, Apr. 2020.

BING SU received the B.S. and Ph.D. degrees from the Nanjing University of Aeronautics and Astronautics (NUAA), China. He is currently an Associate Professor with the Department of Computer Science, School of Information and Mathematics, Changzhou University. His current research interests include network security, wireless sensor networks, the Internet of Things, routing protocols, and cloud computing.

LING TONG was born in October 1998. She is currently pursuing the master's degree with the Computer Science Department, Changzhou University. Her current research interests include network security and vehicle ad hoc networks.