IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE RELIABILITY SOCIETY SECTION

Received November 29, 2021, accepted December 13, 2021, date of publication December 24, 2021,
date of current version January 13, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3138370

A Wireless Mesh Opportunistic Network Routing Algorithm Based on Trust Relationships

YAN ZHAO[1,2] AND GAUTAM SRIVASTAVA[3,4], (Senior Member, IEEE)
[1]Department of Information and Intelligent Engineering, Ningbo City College of Vocational Technology, Ningbo 315199, China
[2]Department of Information Sciences & Engineering, Management & Science University, Shah Alam, Selangor 1340100, Malaysia
[3]Department of Mathematics and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada
[4]Research Centre for Interneural Computing, China Medical University, Taichung 40402, Taiwan

Corresponding author: Gautam Srivastava (srivastavag@brandonu.ca)

ABSTRACT To solve the problem of low message delivery rate and high network resource consumption when forwarding messages in opportunistic networks, an opportunistic routing algorithm based on trust relationships for wireless mesh networks is proposed. Firstly, the wireless mesh network is analyzed and the opportunistic routing model is constructed; By analyzing the security mechanism and security threat of communication entities, then measuring the trust degree of links and nodes, establishing the trust relationship between nodes, and defining and quantifying a new security measurement method based on the trust model; Finally, according to the security measurement method defined by the model, select the node with high trust value to participate in the message forwarding process. At the same time, give priority to the node with greater trust with the destination node as the relay node, and allocate the message copy according to the trust degree to make the message pass along the direction of increasing trust, to complete the design of opportunistic routing algorithm in wireless mesh networks. Experimental results show that the routing algorithm can effectively improve the message delivery rate, up to about 95%, and reduce the consumption of network resources.

INDEX TERMS Communication link, opportunistic routing, relay nodes, safety measurement, trust relationship, wireless mesh network.

I. INTRODUCTION

Wireless Mesh Networks (wireless Mesh network, referred to as "WMN," wireless Mesh network or wireless Mesh network) can not only form a self-organizing network and multi-hop network but also form a certain hierarchical structure and be compatible with other networks. It has become a kind of Internet access solution for community broadband in the metropolitan area network, It is different from any traditional wired or wireless network and has some unique advantages. Wireless Mesh network greatly improves the coverage of wireless systems and has the advantages of low cost, fast networking, self-organization, high bandwidth, good compatibility and scalability [1], [2]. As wireless Mesh structure can solve the "last 1 km" network access bottleneck problem, it has been written into the IEEE802.16 (WiMax) wireless broadband access network standard, which is now into the IEEE802.15 Mesh and is working on IEEE802.11 s Mesh in the standard. It is also incorporated into the IEEE802.15 Mesh and being developed IEEE802.11s Mesh standards. From the perspective of technical characteristics, the wireless Mesh network will become the ideal networking model for the future wireless metropolitan area network (WMAN) core network and is likely to challenge 3G technology and become one of the potential technologies to build B3G/4G [3], [4], as well as the only feasible technology to build commercial mobile Ad Hoc network so far. It is widely used in military communication and tactical command network. The research on wireless mesh networks can improve the continuous development of communication and other network technologies. Among them, the optimization of its routing and path is very helpful to improve the performance of the network [5]. Therefore, it is very important to study the opportunistic routing algorithm in wireless mesh networks.

At present, the attacks on network routing are becoming more and more common and have serious consequences, and the security of network routing has been widely concerned [6]. The routing problem in wireless Mesh networks

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

has become a research hot spot in recent years, and opportunistic routing is one of the important research directions [7]. Opportunistic routing is a Mobile Ad hoc network with the characteristics of a general delay-tolerant network, based on a ''store-carry-forward'' message transmission mechanism. When a node receives a message, it stores the message in the local cache and then carries the message until it encounters a suitable relay node for forwarding. The opportunistic routing makes full use of the broadcast characteristics of wireless communication and selects multiple potential forwarding nodes to improve the success rate of packet forwarding. Opportunistic routing is required to solve two main problems of the selection and sorting of the forwarding list.

As one of the key technologies of WMN, routing protocol is a hot research topic at home and abroad. Patil *et al.* [8] proposed a trust - and opportunity-based routing framework in wireless sensor networks using hybrid optimization algorithms, which operates in two key aspects: One is to select the security node, the other is to select the opportunity node from the selected security node, and based on the fitness parameters trust, distance, delay and connectivity, the proposed M-CSO is used to optimize the selection of opportunity node, but this technology has the problem of high packet loss rate. Ziaur *et al.* [9] proposed a fully opportunistic routing algorithm for underwater wireless sensor networks, and proposed an arbitrary broadcast, geographic and fully opportunistic routing algorithm called TORA for UWSN. The nodes in the network are located recursively by arrival time and range-based equations. The position coordinates and residual energy are then used as a matrix to select the best available transponder. All packets may or may not be acknowledged, depending on the state of the sender and receiver. Therefore, the number of confirmations for a particular packet can jump from 0 to 2. Extensive simulations were performed to evaluate the performance of the proposed scheme for high network traffic loads in very sparse and very dense network scenarios, but the technique has poor message delivery across the network. Chithaluru *et al.* [10] proposed an improved opportunistic routing based on adaptive sequencing in wireless sensor networks. After analyzing that the sleep state of nodes is an infeasible mechanism, cluster heads and node sets participating in routing are determined. However, this technology has the problem that the throughput decreases greatly when the load increases.

To solve the above problems, a trust-based opportunistic routing algorithm for wireless mesh networks is proposed. By analyzing the wireless mesh network, the routing model is designed according to the characteristics of the network, the risk factors of security mechanism between communication entities are considered, and the trust degree of each node in the network is calculated, and a certain security measurement method is determined. This method is used to diffuse between nodes, enhance the trust relationship between nodes and enhance the routing effect. Compared with the existing methods, the time overhead in the routing process of this method is shorter and the throughput is larger.

II. ANALYSIS OF OPPORTUNISTIC ROUTING IN WIRELESS MESH NETWORKS

A. WIRELESS MESH NETWORK ANALYSIS

To realize the design of an opportunistic routing algorithm in wireless mesh networks, it is necessary to analyze the characteristics of the wireless network [11].

An air backbone network is a flexible and efficient Mesh network constructed by a large air backbone platform with a large load [12], long space capacity and stable connection through wideband data link in the form of wireless Mesh. User nodes (such as fighter jets) are connected to the air backbone network to realize information transmission and interaction. The air backbone node has mobility, so the air backbone Mesh network has mobility and is not completely stable compared with the access nodes of the ground backbone Mesh network. However, the characteristics of the large air backbone platform with poor tactical mobility and high node stability make the air backbone Mesh network have stronger stability than the aviation self-organizing network. The air backbone Mesh network can ensure that the network structure remains relatively stable within a certain period under the influence of external non-wars destruction factors, and the topology of each backbone access node remains unchanged. Therefore, its network topology can be illustrated in Fig. 1.

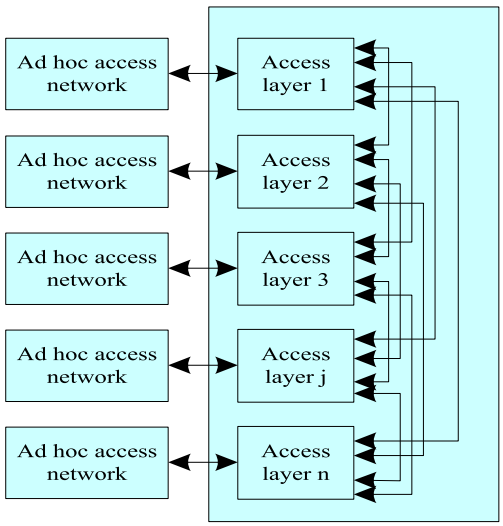

FIGURE 1. Schematic diagram of air backbone mesh network.

In the data transmission process of each node in the network topology diagram, it is assumed that only one node can be used as the source node to transmit data, only one node can be used as the destination node to receive data, and the other nodes are used as intermediate nodes to participate in data forwarding.

B. THE CONSTRUCTION OF OPPORTUNISTIC ROUTING MODEL

Based on the characteristics of opportunistic routing and node topology determined above [13], [14], to improve the quality of routing, this chapter designs the trust relationship model of opportunistic routing and determines the nodes in the network through this model.

Figure 1 is abstracted to obtain the node model of the air backbone Mesh network, which is transformed into a directed graph $G = (R, E, D)$, where the set R represents all nodes within the network coverage range, including network nodes $r_i = \{r_0, r_1, r_2, \cdots, r_n, r_{n+1}\}$. The set represents the communication link $e_{ij} \in E$ formed between any two nodes r_i, r_j; The set D represents the successful delivery rate between two nodes when data packets are transmitted in the link. The delivery rate of the link between any two nodes r_i and r_j is represented by $d_{i,j}$, where, $d_{i,j} \in D$, $d_{i,i} = 1$.

Assuming that in the process of sending data packets from the source node to the destination node, the delivery rate among nodes is constantly participating in data transmission and reception, and the coherence time of single-channel is much longer than the transmission time of data packets in the channel. It can be assumed that the links between the same node and different neighbours remain statistically independent. To realize the high efficiency of data transmission among forwarding nodes in the node cooperative transmission, suppress data re-transmission, and deal with the asymmetry of bidirectional link at the same time, and ensure that the reply sent by forwarding nodes after receiving packets can be received by sending nodes, a trusted response mechanism can be introduced to ensure that the response success rate is close to 100%.

1) THE CONSTRUCTION OF THE ROUTING MODEL

According to the determination of the trust relationship of opportunistic routing, to realize the research of this paper, it is necessary to process the data packets sent by the nodes and build the routing model on this basis.

Set $s, d \in R$ as any two nodes in the node-set R, which are used to send and receive packets respectively. Variable F: $R \times R \rightarrow V$ represents the forwarding priority of each node in the ordered forwarding node-set $V_{s,d}$ formed from the source node to the destination node. $V_{s,d}$ represents the forwarding list formed from the source node to the destination node, $V_{s,d} = \{(s = r_0, r_1, r_2, \cdots, r_n, r_{n+1} = d) : F_{r_i,d} \leq F_{r_{i+1},d}\}$. As the subscript increases in the node-set, the priority increases accordingly. Any node r_i can forward packets to the destination node. Only the node with the highest priority can forward packets. Among all forwarding nodes that receive the data packet, each node responds in turn according to the forwarding priority order.

Set p_{r_i,r_j} denote the probability, which is that a data packet sent by a node $r_i \in V_{s,d}$ to a destination node is received by a node r_i $(i < j)$ with a higher priority than the node r_i, but not received by a node r_k $(j < k)$ with a higher priority r_j. According to the statistical independence of the link transmission data packet, it can be obtained:

$$p_{r_i,r_j} = \begin{cases} d_{r_i,r_j} \prod_{k=j+1}^{n+1} \left(1 - d_{r_i,r_k}\right) & \forall i \leq j \\ 0 & \forall i > j \end{cases} \quad (1)$$

According to the above definition, the routing and node forwarding model can be shown in Fig. 2.

2) TRUST MODEL AND SECURITY MEASUREMENT

Based on the historical interaction information between nodes and the recommendation information of trusted neighbour nodes, a trust evaluation model is established to analyze and judge the trusted status of nodes timely and accurately [15], [16]. Selfish nodes can be refused to participate in the process of message forwarding, and cooperative relations with low-trust nodes in the network are avoided to ensure safe and reliable communication between nodes.

The direct trust relationship between nodes is estimated and judged by periodically observing the interaction behaviour between nodes. At the same time, the indirect trust relationship between nodes is estimated and judged according to the recommendation information of trusted neighbour nodes, so the direct trust relationship and indirect trust relationship are considered comprehensively when judging the trust relationship.

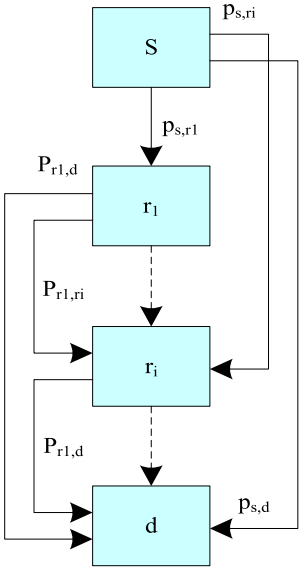

FIGURE 2. Routing and node forwarding model.

Communication link and routing node are two key network devices. Whether a node can safely forward packets to its neighbour depends on two aspects: on the one hand, the reliability of the link connected to; on the other hand, the reliability of neighbour nodes. Therefore, a trust relationship between neighbour nodes (trust pair) is proposed to establish secure information storage and forward a trusted path for communication between source and destination by packet. It assumes that links are secure and there are only two trust relationships between nodes, which are trusted or untrusted. Considering the simplicity of the trust theory, the trust model is improved and the concept of trust is used to describe the trust relationship between nodes more accurately.

Definition 1: The concept of Trust Degree (TD) includes the trust degree of communication links and the trust degree

of routing node. When $TD_t\left(e_{ij}\right)$ is set, it indicates the trust degree of the link e_{ij} connecting r_i to the neighbour node r_j.

Definition 2: Trust Relation (TR) set, $TR\{r_i \rightarrow\} r_j$ represents the trust relationship r_i with the neighbour node r_j. The main factor with affecting $TR\{r_i \rightarrow\} r_j$ is $TD_t\left(e_{ij}\right)$ and $TD_t\left(r_{ij}\right)$, so $TR\{r_i \rightarrow\} r_j$ at the time t can be formalized as:

$$TR\left\{r_i \rightarrow r_j\right\} = d_1 TD_t\left(e_{ij}\right) + d_2 TD_t\left(r_{ij}\right) \quad \left(d_1, d_2 \in [0,1], d_1 + d_2 = 1\right) \tag{2}$$

The weights d_1, d_2 unrelated to TD indicate the importance of a link TD and a node TD to the establishment of trust relationships between trust pairs. TD is unidirectional, and d_1 dynamically update with network security status changes: $TR_{t_1}\left\{r_i \rightarrow r_j\right\} \neq TR_{t_2}\left\{r_i \rightarrow r_j\right\}, t_1 \neq t_2$.

Definition 3: Security Metric (SM), For a link $e_{ij} \in E$, the security metric of its concavity is defined as $SM\left(e_{ij}\right)$ or $SM\left(r_i, r_j\right)$, indicating the degree of security from r_i forwarding data to r_j, SM is one-way. In this way, the security metric of the hop path G is:

$$\begin{aligned} SM(p) &= \min\left[SM\left(r_0, r_1\right), SM\left(r_1, r_2\right), \cdots, SM\left(r_{i-1}, r_i\right)\right] \\ &= \min\left[SM\left(e_{i-1,i}\right)\right], \quad 1 \leq i \leq h \end{aligned} \tag{3}$$

The higher the reliability of neighbour nodes and the communication links between them is, the more reliable the trust relationship between nodes will be and the higher the security of data transmission. The security path is to establish a trust relationship chain along the information transmission path. Therefore, the security metric of the link at the time can be set as:

$$SM\left(e_{ij}\right) = TR_t\left\{r_i \rightarrow r_j\right\} = d_1 TD_t\left(e_{ij}\right) + d_2 TD_t\left(r_{ij}\right) \quad \left(d_1, d_2 \in [0,1], d_1 + d_2 = 1\right) \tag{4}$$

Here, d_1, d_2 show that the security status of the link to the sensitive degree of links TD and nodes TD. It can be seen that SM is a dynamic variable updated with the changes of network security status and is suitable for route calculation. Security threats and security mechanisms taken by network devices when transmitting and forwarding data are two major factors related to link security measurement [17], so they should be taken into consideration when quantifying links TD and nodes TD.

Several security mechanisms work at the link layer in the OSI model that can give $TD\left(e_{ij}\right)$ with different increased trust values $IV\left(e_{ij}\right)$. Set the maximum trust degree of the link e_{ij} as $TD^{\max}\left(e_{ij}\right) = \sum_{x \geq 0} IV_{Label(x)}\left(e_{ij}\right)$ when implementing $x\ (x \geq 0)$ kinds of security mechanisms, for example, the $TD^{\max}\left(e_{ij}\right) = IV_C\left(e_{ij}\right) + IV_A\left(e_{ij}\right) + IV_T\left(e_{ij}\right)$ that applies C, A, and T security mechanisms. Of course, the link trust degree $TD^{\max}\left(e_{ij}\right) = 0$ without any security mechanism. And if $x'\left(x' \geq 0\right)$ kinds of link security mechanisms are dynamically increased or decreased, $TD^{\max}\left(e_{ij}\right)$ will also increase or decrease with the corresponding trust degree:

$$TD^{\max}\left(e_{ij}\right) = TD^{\max}\left(e_{ij}\right) \pm \sum_{x' \geq 0} IV_{Label(x')}\left(e_{ij}\right) \tag{5}$$

On the other hand, communication link transmission may face various threats (such as MAC flooding attacks, ARP attacks, etc.), and there are many intrusion/misuse behaviour detection and response technologies to detect the attacks. In the fixed-length period Δt, if the λ link attacks are detected, $TD\left(e_{ij}\right)$ should decrease exponentially (it is easy to lose trust): $TD_t\left(e_{ij}\right) = TD_{t-\Delta t}\left(e_{ij}\right) - 2^{\lambda-1} DV\left(e_{ij}\right)(\lambda \geq 1)$, until $TD_t\left(e_{ij}\right) = 0$; On the contrary, if there is no link attack at the time Δt, $TD\left(e_{ij}\right)$ will have lost some trust linearly increased by a change value $CV\left(e_{ij}\right)$ (difficult to gain trust degree), and reset the attack times $\lambda = 0$ until $TD\left(e_{ij}\right)$ return to the maximum trust degree before e_{ij} is attacked.

r_j is not only a neighbour of r_i but also be a neighbour of other nodes $r_k \in R\left(k \neq i \neq j, e_{kj} \in E\right)$ in the network. Therefore, the quantification of trust degree $TD\left(r_{ij}\right)$ of routing nodes should include two parts: one is the direct trust degree $DTD\left(r_{ij}\right)$ of r_j obtained from r_i active observation; the other is the indirect trust $ITD\left(r_{ij}\right)$ r_j obtained r_i from other nodes r_k through routing information exchange, namely.

$$TD_t\left(r_{ij}\right) = w_1 DTD_t\left(r_{ij}\right) + w_2 ITD_t\left(r_{kj}\right) \quad \left(k \neq i \neq j, e_{ij}, e_{kj} \in E, w_1, w_2 \in [0,1], w_1 + w_2 = 1\right) \tag{6}$$

where, the weights w_1, w_2 show the proportion of DTD and ITD when quantifying $TD\left(r_{ij}\right)$. To prevent malicious slander by the enemy $w_1 > w_2$ is generally taken.

Direct trust measurement: The measurement of direct trust degree $DTD\left(r_{ij}\right)$ $r_i r_j$ is also based on the security threats faced by routing structures and the security mechanism of routing protocols. Authentication and confidentiality are the two main routing information security mechanisms, and both of them can provide information level (IL) or package level (PL) security services. D adopts different security mechanisms, which can bring the different added value $IV\left(r_{ij}\right)$ of trust degree to $DTD\left(r_{ij}\right)$. Set the maximum direct trust degree of a node r_j to node r_i with implementing $x\ (x \geq 0)$ kinds of security mechanisms as:

$$DTD^{\max}\left(r_{ij}\right) = \sum_{x \geq 0} IV_{Label(x)}\left(r_{ij}\right) \tag{7}$$

On the other hand, network routing attacks (including external attacks and internal attacks) are common and have serious consequences [18], [19]. Routing attacks can be detected and isolated using IDS. In the fixed-length period Δt, if the λ attacks to r_j are detected, $DTD\left(r_{ij}\right)$ should decrease exponentially: $DTD_t\left(r_{ij}\right) = DTD_{t-\Delta t}\left(r_{ij}\right) - 2^{\lambda-1} DV\left(r_{ij}\right)(\lambda \geq 1)$, until $DTD\left(r_{ij}\right) = 0$; If there is no routing attack in Δt, $DTD\left(r_{ij}\right)$ will have lost some trust degree linearly increased by a change value $CV\left(r_{ij}\right)$, and reset the number of attacks $\lambda = 0$ until $DTD\left(r_{ij}\right)$ return to the maximum trust degree: $DTD\left(r_{ij}\right) = DTD^{\max}\left(r_{ij}\right)$ before r_j is attacked.

The measurement of indirect trust degree: the indirect trust degree $ITD\left(r_{kj}\right)$ of r_i to r_j is measured by flooding the routing update information. At the time t, r_i gets the $TD_{t'}\left(r_{kj}\right)$

from r_k, then $ITD_t\left(r_{kj}\right)$ is updated:

$$ITD_t\left(r_{kj}\right) = \frac{\sum_{k=1,k\neq i\neq j}^{|R|}\left(TD_{t'}\left(r_{kj}\right) - TD_{t'}\left(r_{ij}\right)\right) \times TD_{t'}\left(r_{ik}\right)}{|R|}, \quad t' < t \tag{8}$$

where $|R|$ is the number of nodes in G. $ITD\left(r_{kj}\right)$ has the relationship with the trust degree $ITD\left(r_{kj}\right)$ of r_i to r_k. The higher $TD\left(r_{ik}\right)$ is, the greater the updated degree of $ITD\left(r_{kj}\right)$ is. It indicates that when $TD\left(r_{ij}\right)$ is quantified. The degree of acceptance that r_i adopts observations from other nodes depends on the degree of trust of r_i these nodes.

Through the above measurement of the trust degree of communication link and routing node, the trust relationship between routing nodes is established, and a quantitative trust model and the security metric $SM_t\left(e_{ij}\right)$ of link e_{ij} at a time t are obtained.

C. IMPLEMENTATION OF THE OPPORTUNISTIC ROUTING ALGORITHM IN WIRELESS MESH NETWORKS

The opportunistic routing of wireless mesh networks adopts the SRTR algorithm. Through the research of this algorithm, more nodes are deleted, and the trust degree of the remaining nodes is considered to realize the design of an opportunistic routing algorithm.

SRTR algorithm uses the limited copy message forwarding strategy, based on the interaction information between nodes and the recommendation information of the trusted neighbour to build the trust matrix. A local trust list is established according to the trust matrix, which is used to store trusted neighbour nodes, and then the forwarding decision is realized, and the number of message copies is divided according to the trust degree of the destination node to the relay node [20]. If the current node r_i has a message set M that needs to be forwarded, the specific steps of the algorithm are as follows:

1) In the current cycle, according to the trust matrix T, the node r_i stores the row vector $T_i = (T_{i1}, T_{i2}, \cdots, T_{in})$ in the trust matrix. The threshold of trust degree T_{th} is set according to the system environment, and the trust degree of the node r_i to other nodes is obtained by row vectors respectively. The nodes that meet the threshold conditions of trust degree are added to the local trust list of nodes $T_{list}\ (i)$. Similarly, the nodes that do not meet the threshold conditions are deleted from the local trust list.
2) For the message $m \in M$ carried by the node r_i, get the destination node r_d of the message m. When a node r_i encounters a node r_j, if $r_j = r_d$, the node r_j sends the message directly to the destination node. If the node $r_j \in T_{list}\ (i)$, go to step 3; otherwise, the node r_i continues to carry the message until it encounters the destination node or a node in the local trust list $T_{list}\ (i)$.
3) According to the trust vector of the node, calculate the social similarity $sim\ (r_i, r_d)$ and $sim\left(r_j, r_d\right)$ of the current node r_i, the encountered node r_j and the destination node respectively. If $sim\left(r_j, r_d\right) > sim\ (r_i, r_d)$, the node r_i is required to split the number of copies r_{c_j} of the message m, and forward the message m with the number of copies r_{c_j} to r_j, update the number of message copies $r_{c_i} \leftarrow r_{c_i} - r_{c_j}$ of the node r_i. And the partition calculation of the number of copies of the message is as follows:

$$r_{c_j} = \left\lceil \frac{sim\left(r_j, r_d\right)}{sim\ (r_i, r_d) + sim\left(r_j, r_d\right)} \cdot r_{c_i} \right\rceil \tag{9}$$

4) Otherwise, when $sim\left(r_j, r_d\right) \leq sim\ (r_i, r_d)$, the node r_i continues to carry messages until it encounters the destination node or node in the local trust list $T_{list}\ (i)$.

III. RESULTS

To verify that the trust relation-based opportunistic routing algorithm proposed in this paper, the application effect of actual opportunistic routing in wireless mesh networks is tested in the MATLAB simulation environment. The router of the routing node selected in this experiment is WNDR3800, which is used to construct the wireless mesh network. The router has five Gigabit ports, including LAN and WAN ports. The router complies with the IEEE 802.11n standard and is compatible with the 802.11/b standard. The maximum wireless transmission rate can reach 300mbit/s. The wireless transmission rate is fast. The coverage capacity of wireless signals uses 5GHz. The mobile node adopts random waypoint and CBR(Constant bit rate) as the transmission traffic model. The data sending rate is 6 packet/s, the data receiving rate is 3.4 packet/s, and the packet size is 50 bytes. The number of nodes is 30*150, the transmission range is 30m, and the data is randomly distributed in a space of 100*100m2. Each data can be randomly transmitted from one source node to another random target node, and the moving speed is between 0m/s and 20 m/s. After reaching the destination node, a pause time (0∼100 s) is passed before starting a new transmission process. The simulation verification times are 5000 times. The transmission structure of network nodes is shown in Figure 3:

At the same time, to further show the application performance of the method in this paper, the algorithm of literature [8] and the algorithm of literature [9] are taken as comparison algorithms to compare the indexes in the application of this algorithm and different comparison algorithms. The specific experimental results are as follows.

A. THE DELIVERY RATE OF MESSAGE

The message delivery rate is defined as the ratio of the number of messages successfully delivered to the destination node in the network to the total number of messages generated by the source node.

According to Fig. 4, with the increase of the ratio of selfish nodes, the delivery rates of the three routing algorithms all show a decreasing trend. Because there is no selfish node detection mechanism, the delivery rate of the algorithm in

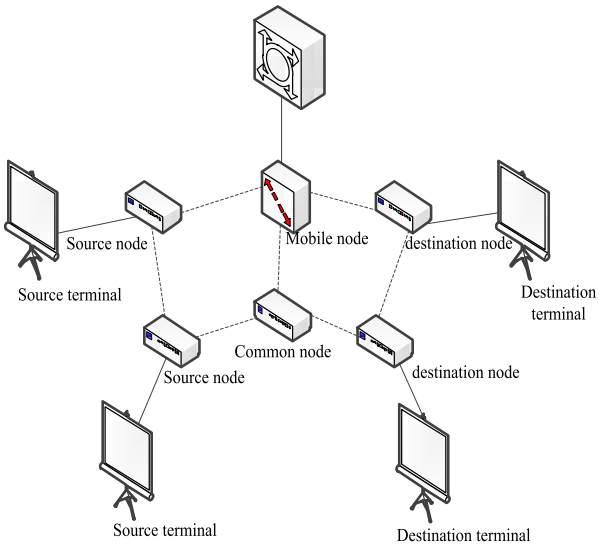

FIGURE 3. Network node transmission structure.

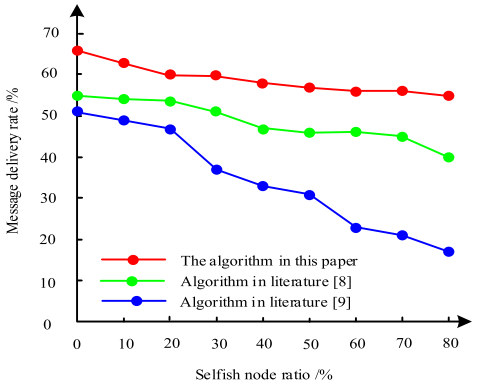

FIGURE 4. Message delivery rate and selfish node ratio.

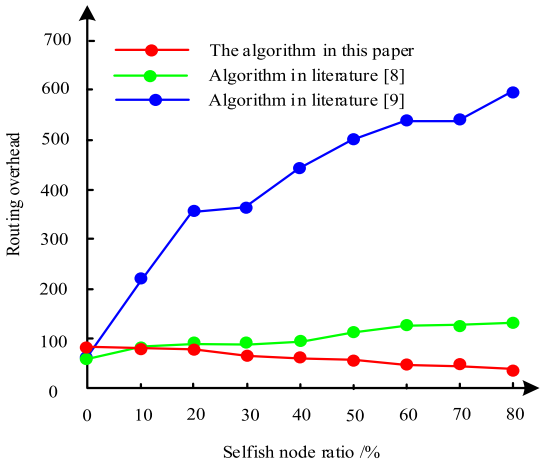

FIGURE 5. Test results of routing overhead.

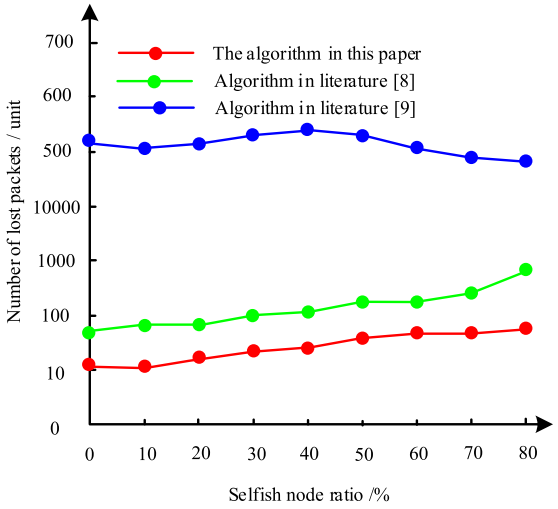

FIGURE 6. Packet loss test results.

the literature decreases faster than that of the algorithm in this paper. This is because the algorithm in this paper can ensure that nodes with a higher level of trust participate in the process of message forwarding, and relay nodes are selected according to social relationships. Therefore, the application performance of the proposed algorithm is generally superior to the two comparison algorithms.

B. THE ROUTING COST

The routing cost is the ratio of the total number of message copies in the network to the number of messages that are successfully transmitted to the destination node. The routing costs of the proposed algorithm and the two competitive algorithms under the different ratios of selfish nodes are shown in Fig. 5.

According to the analysis of Fig. 5, as more normal nodes in the network become selfish nodes, the propagation cost of the algorithm in literature [8] is on the rise. and the routing cost of this algorithm is the largest. When the ratio of selfish nodes is less than 40%, more copies of the message are discarded with the increase in the number of selfish nodes, and therefore the routing cost of the algorithm in literature [9] shows an upward trend, the algorithm chooses relay nodes according to the social relationship. When the ratio of selfish nodes exceeds 40%, the number of selected relay nodes reduces gradually, so that the ratio of the discarded message decreases. The transmission cost shows a decreasing trend, therefore, the performance of the algorithm in reference [9] is better than that in reference [8]. The routing cost of the algorithm in this paper shows a downward trend because the algorithm can detect selfish nodes.

C. THE NUMBER OF LOST PACKETS

The total number of messages discarded by selfish nodes in the network is called the number of lost packets. Fig. 6 shows the number of lost packets between the algorithm in this paper and the two competitive algorithms under different selfish node ratios.

As can be seen from the analysis of Fig. 6, compared with the literature algorithm, the algorithm in this paper has a smaller number of lost packets, because the literature algorithm does not consider the trust degree of nodes in the process of data transmission. In the actual operation process, the algorithm in this paper selects the next-hop transmission node based on the trust degree of the node, so the algorithm

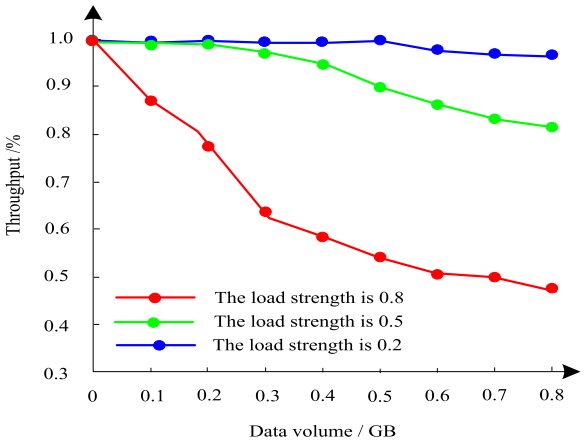

FIGURE 7. Throughput under different load conditions.

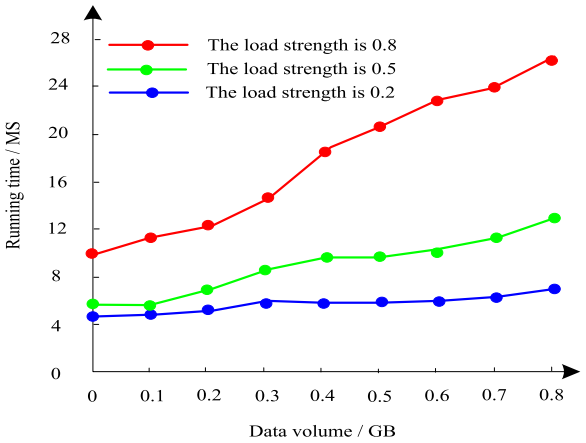

FIGURE 8. Routing overhead under different load conditions.

in this paper has less packet loss compared with the two algorithms. Compared with the algorithm in literature [8], the algorithm in literature [9] selects the next-hop nodes based on the social relationship, so the performance of this algorithm is better than that of the algorithm in literature [8].

D. THE PERFORMANCE TEST UNDER DIFFERENT LOAD CONDITIONS

1) THE THROUGHPUT TEST

The throughput of the algorithm in this paper is tested under different load conditions, and the result is shown in Fig.7.

Fig. 7 shows the relationship between the throughput of the proposed algorithm and the amount of data under different load conditions. It can be obtained from the analysis that, as the number of data increases, the throughput of the algorithm starts decreasing by 1%. When the load rate is 0.2, the throughput of the algorithm in this paper starts to decline when the amount of transmitted data is 0.5GB. This is because when the network load is low and the amount of transmitted data is small, the node cache capacity has little influence on the data transmission, so the throughput of the algorithm in this paper can remain relatively high. With the increase of load intensity, the effect of node cache capacity on the performance of throughput becomes very significant. When the load rate is 0.8 and the amount of transmitted data is low, the throughput of the proposed algorithm starts to decline, but the decline is slow. This is because the algorithm in this paper takes the transmission performance of links and nodes into consideration in the path selection so that the link can maintain relatively high transmission efficiency and relatively high throughput in the case of heavy load and large data business transmission [21]–[23].

2) THE PERFORMANCE TEST OF COST

The cost performance of the algorithm in this paper is tested under different load conditions, and the result is shown in Fig. 8.

In the analysis of Fig. 8, the algorithm in this paper selects the comprehensive optimal link to transmit information of different types of services and different amounts of data. The algorithm in this paper carries out quantitative data transmission, and the running time can be used to compare the cost performance of different routing protocols during the whole data transmission process. The running time is used to represent the total time of the opportunistic routing protocol from the detection packet to the packet, which carries data that is fully received.

As can be seen from Fig. 8, when L = 0.2, the amount of data is less than 0.5, when L = 0.5, the amount of data is less than 0.3 when L = 0.8, and the amount of data is less than 0.3, so the fluctuation of running time of the algorithm in this paper is not significant. This is because under the above conditions, nodes have little restriction on packet transmission and there is no congestion in the network. Therefore, the algorithm in this paper costs more resources to obtain more state information. At the same time, the running time of the algorithm in this paper is less than 30ms under different loads and different amounts of data, which indicates that the algorithm has faster operation efficiency.

IV. CONCLUSION

To improve the performance of network opportunistic routing, a trust-based opportunistic routing algorithm for wireless mesh networks is proposed. The algorithm comprehensively considers the direct trust and indirect trust and establishes the trust matrix between nodes according to the overall trust. Especially when obtaining recommendation information, the neighbour nodes are evaluated by establishing a trust similarity relationship, and the trust similarity is used as a constraint to avoid the possibility of false recommendation information of selfish nodes. Establish a local trust list of nodes to ensure that nodes with high trust levels participate in the secure forwarding process of messages. On the premise of ensuring the reliability of the relay node, making the message pass along the direction of increasing social similarity can avoid the occurrence of selfish behaviour between nodes, ensure the best path for the message to reach the destination node, improve the message delivery rate of the whole network, reduce the message forwarding delay in the network, and

make the message copy transmit efficiently and reliably. The experimental results show that:

(1) The highest delivery rate of messages using this method is about 95%, and the decline speed is slow;
(2) When using this method for network routing, the delay of message forwarding can be reduced.
(3) This method can reduce the overhead of network routing, and has certain feasibility.

Although this method has achieved some results at this stage and has a good effect in improving opportunistic routing in wireless mesh networks, there are still many disadvantages in the research. In the future, the energy consumption of opportunistic routing in wireless mesh networks and the key nodes affecting its selection of the best path will be studied to improve the effectiveness of this research method.

REFERENCES

[1] Q. Liu, L. Cheng, A. L. Jia, and C. Liu, "Deep reinforcement learning for communication flow control in wireless mesh networks," *IEEE Netw.*, vol. 35, no. 2, pp. 112–119, Mar. 2021.

[2] S. Wang, X. Liu, S. Liu, K. Muhammad, A. A. Heidari, J. D. Ser, and V. H. C. de Albuquerque, "Human short-long term cognitive memory mechanism for visual monitoring in IoT-assisted smart cities," *IEEE Internet Things J.*, early access, May 5, 2021, doi: 10.1109/JIOT.2021.3077600.

[3] M. Gheisari, J. Alzubi, X. Zhang, U. Kose, and J. A. M. Saucedo, "A new algorithm for optimization of quality of service in peer to peer wireless mesh networks," *Wireless Netw.*, vol. 26, no. 7, pp. 4965–4973, Oct. 2020.

[4] L. Derdouri, C. Pham, E. M. E. A. Zouaoui, and N. Zeghib, "Performance analysis of self-organised multicast group in multi-radio multi-channel wireless mesh networks," *IET Commun.*, vol. 14, no. 4, pp. 693–702, Mar. 2020.

[5] Y. Chai and X. J. Zeng, "Delay- and interference-aware routing for wireless mesh network," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4119–4130, Sep. 2020, pp. 1–12.

[6] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low power networks on Internet of Things," *J. Supercomput.*, vol. 77, no. 5, pp. 4778–4812, May 2021.

[7] Z. Chunyue, H. Tian, Y. Dong, and B. Zhong, "An energy-saving routing algorithm for opportunity networks based on asynchronous sleeping mode," *Comput. Electr. Eng.*, vol. 92, Jun. 2021, Art. no. 107088.

[8] P. A. Patil, R. S. Deshpande, and P. B. Mane, "Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm," in *Wireless Pers. Commun.*, vol. 115, no. 2, pp. 4–7, 2018.

[9] Z. Rahman, F. Hashim, M. F. A. Rasid, and M. Othman, "Totally opportunistic routing algorithm (TORA) for underwater wireless sensor network," *PLoS ONE*, vol. 13, no. 6, Jun. 2018, Art. no. e0197087.

[10] P. Chithaluru, R. Tiwari, and K. Kumar, "Arior: Adaptive ranking based improved opportunistic routing in wireless sensor networks," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 2–3, 2021.

[11] M. Salehi and A. Boukerche, "Secure opportunistic routing protocols: Methods, models, and classification," *Wireless Netw.*, vol. 25, no. 2, pp. 559–571, Feb. 2019.

[12] Y. L. Su, H. Feng, H. Hu, W. Wang, T. Duan, Y. S. Wang, J. H. Si, X. P. Xie, H. N. Yang, and X. N. Huang, "Simultaneous polarization separation and switching for 100-Gbps DP-QPSK signals in backbone networks," *Chin. Phys. B*, vol. 28, no. 2, pp. 295–301, 2019.

[13] K. P. Mhatre and U. P. Khot, "Energy efficient opportunistic routing with sleep scheduling in wireless sensor networks," *Wireless Pers. Commun.*, vol. 112, no. 2, pp. 1243–1263, May 2020.

[14] X. Zhong, L. Li, S. Zhang, and R. Lu, "ECOR: An energy aware coded opportunistic routing for cognitive radio social Internet of Things," *Wireless Pers. Commun.*, vol. 110, no. 1, pp. 1–20, Jan. 2020.

[15] M. O. Kabaou and H. Hamouda, "Implementation and evaluation of opportunistic routing protocols for wireless and new generation communication networks," *Wireless Pers. Commun.*, vol. 112, no. 2, pp. 1165–1183, May 2020.

[16] D.-G. Akestoridis and E. Papapetrou, "A framework for the evaluation of routing protocols in opportunistic networks," *Comput. Commun.*, vol. 145, pp. 14–28, Sep. 2019.

[17] L. Liu, W. Chen, T. Li, and Y. Liu, "Pseudo-random encryption for security data transmission in wireless sensor networks," *Sensors*, vol. 19, no. 11, p. 2452, May 2019.

[18] M. Vigenesh and G. T. Arasu, "Flow-based mitigation for manet routing attacks detection using time-variant snapshot," *Int. J. Comput. Inf. Technol.*, vol. 11, no. 2, pp. 149–159, 2019.

[19] A. Raoof, A. Matrawy, and C.-H. Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1582–1606, 2nd Quart., 2019.

[20] T. M. Navamani, "Trust based secure reliable route discovery in wireless mesh networks," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 7, pp. 1–4, 2019.

[21] R. H. Jhaveri, S. V. Ramani, G. Srivastava, T. R. Gadekallu, and V. Aggarwal, "Fault-resilience for bandwidth management in industrial software-defined networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3129–3139, Oct. 2021.

[22] S. Liu, S. Wang, X. Liu, A. H. Gandomi, M. Daneshmand, K. Muhammad, and V. H. C. De Albuquerque, "Human memory update strategy: A multilayer template update mechanism for remote visual monitoring," *IEEE Trans. Multimedia*, vol. 23, pp. 2188–2198, 2021.

[23] A. Belhadi, Y. Djenouri, G. Srivastava, A. Jolfaei, and J. C.-W. Lin, "Privacy reinforcement learning for faults detection in the smart grid," *Ad Hoc Netw.*, vol. 119, Aug. 2021, Art. no. 102541.

YAN ZHAO was born in Huaide, China, in 1980. He received the bachelor's degree in engineering from Northeast Dianli University, China, in 2003, and the master's degree in engineering from Qiqihar University, China, in 2012. He is currently pursuing the Ph.D. degree with the University of Management Science, Malaysia.

From 2003 to 2019, he was acted as an Assistant Lecturer, a Lecturer, and an Associate Professor with Qiqihar University. Since 2019, he has been studying as an Associate Professor with the Ningbo City Vocational and Technical College. He published nearly ten papers on research direction of wireless communication network.

Dr. Zhao won the first prize of 2013 Qiqihar 13th Social Science Outstanding Achievement Award.

GAUTAM SRIVASTAVA (Senior Member, IEEE) received the B.Sc. degree from Briar Cliff University, USA, in 2004, and the M.Sc. and Ph.D. degrees from the University of Victoria, Victoria, BC, Canada, in 2006 and 2011, respectively.

He taught for three years with the Department of Computer Science, University of Victoria, where he was regarded as one of the top undergraduate professors in the Computer Science Course Instruction at the University. Since 2014, he has been holding a tenure-track position at Brandon University, Brandon, MB, Canada, where he is currently active in various professional and scholarly activities. He was promoted to the rank as an Associate Professor, in January 2018. He is active in research in the field of data mining and big data. In his eight year academic career, he has published a total of 43 papers in high-impact conferences and high-status journals (SCI, SCIE) and has also delivered invited guest lectures on big data, cloud computing, the Internet of Things, and cryptography at many Taiwanese and Czech universities.

Dr. Srivastava is also an Editor of several international scientific research journals. He currently has active research projects with other academics in Taiwan, Singapore, Canada, Czech Republic, Poland, and USA. He received Best Oral Presenter Award in FSDM 2017 which was held at the National Dong Hwa University (NDHU), Shoufeng, Hualien County, Taiwan, in November 2017.