An Energy Efficient and Trust-based Quality of Service Routing in Mobile Adhoc Networks

[1]G. Sripriya, [2] Dr. T. Santha

[1]Ph.D - Research Scholar, Department of Computer Science,
Dr. G. R. D. College of Science,
Coimbatore-14, Tamilnadu, India.
[2] Research Supervisor,
Dr.G.R.D. College of Science,
Coimbatore-14, Tamilnadu, India.

Email: [1]sripriya.gs8@gmail.com

Abstract - Mobile Ad-hoc Networks are widely used in all applications and are gaining attention towards reliable data delivery and efficient energy usage. Reliability of the data delivery is assured when the routing protocols are securely reliable and energy efficient. Limited resources being the main limitation of the wireless networks, there is a lack in providing security to the data and energy utilization. Trust aware routing can resolve the resource problems in MANETS. So, to overcome these limitations, an Energy Efficient and Trust-based Quality of Service Routing in Mobile Adhoc Networks is proposed. This protocol evaluates the trust score of the nodes based on the connectivity of the nodes and ACK sincerity, based on the comprehensive trust of the node's energy consumption required and communication cost for the communication between node is evaluated. This protocol efficiently identifies the malicious nodes based on the trust score it is the additional advantage of evaluating the trust score of nodes. The simulation results prove that the proposed protocol guarantees the reliable data delivery and aid to extend the life time of the network thereby improves the throughput of the network.

Keywords - QoS Routing, Trust based Scheme, Node Trust Evaluation, Algebraic Connectivity, Segment Routing

1. Introduction

The main objective of the Mobile Ad-hoc Network is to collect and analyze data information in the monitoring area in a cooperative manner and transmit it to the sink node [1], and Mobile Ad-hoc Network are often used for Large-scale wireless networks have the characteristics of dynamic topology and self-organization. However, Mobile Ad-hoc Network nodes are easily affected by many factors such as power, storage, bandwidth and energy [2]; Various factors such as interference and multipath effects may lead to temporary severe packet loss in data transmission [3-5]. Therefore, the research on Mobile Ad-hoc Network routing protocols needs to consider factors such as reliability and node energy consumption.

In 2004, Biswas et al. of the Massachusetts Institute of Technology (MIT) first proposed Opportunistic Routing [6]. Applying the broadcast characteristics of wireless channels to opportunistic routing can greatly improve the reliability and reliability of data transmission in wireless networks. Therefore, many researchers introduce opportunistic routing into sensor networks. Literature [7] reviews some important opportunistic routing protocols in recent years, and classifies these routing protocols at a deeper level according to different standards, and fully understands their analysed and compared. However, some early opportunistic protocols (such as ExOR [6] MORE [8]) did not consider the energy consumption problem, and the EEOR routing algorithm proposed by Mao et al [9]. used the adjustable transmission energy model and the non-adjustable transmission energy model to calculate the routing cost of sensor nodes. , and select the optimal candidate forwarding set, so that the total energy consumption when the data is forwarded to the sink node through these nodes is the smallest.The wireless nodes in the EEOR routing protocol forward data according to the energy priority. If the node with a high priority forwards the data, the node with a low priority will discard the monitored data packets, thereby reducing the possibility of wasting node energy. The segment routing method designed by AsOR minimizes the average energy consumption by selecting the optimal number of nodes in the segment [10]; however, AsOR optimizes energy consumption from a global perspective and belongs to a centralized routing algorithm. CBEEOR proposed by

Karyakarte, et al. [11], is an improved algorithm based on the adjustable transmission energy model in EEOR, and calculates the forwarding energy by allowing multiple nodes to forward packets at the same time. CBEEOR uses the back-off time mechanism to avoid the repeated transmission of data between nodes in the candidate forwarding set as much as possible, and the energy consumption is reduced compared with EEOR. Therefore, many researchers have started to study the trust degree of nodes [12-13] and the technology of identifying malicious nodes [14], and proposed various trust models [15]. It is applied to opportunistic routing to improve network security and data accuracy. In recent years, researchers have improved the trust management protocols and algorithms of ad-hoc networks, Internet of Things and other mobile wireless networks.

Su et al., [16] applied the trust model to opportunistic routing for the first time, and the calculation of trust value was based on the direct trust degree of direct interaction and the recommendation trust degree similar to trust; however, the parameter values used to calculate the direct trust degree mostly depend on expert experience. It will affect the objective evaluation of the trust model to a certain extent. Zhao et al., [17] further evaluates the trust degree of nodes by using the theoretical basis that wireless nodes obey the Beta distribution, but this method does not take into account that there may be non-malicious factors in failed interactions such as In [18], a new watchdog mechanism is used to detect the node information, and the link delivery rate of the node, the geographical information of the node and the trust of the node are calculated. The value is integrated into the routing measure. This mechanism not only causes more network overhead when optimizing the candidate set, but also does not take the recommendation information of other nodes as an important parameter for calculating the trust value of the node.

Aiming at the above problems, based on the research on the trust model, this paper proposes an energy-saving opportunistic routing protocol for Mobile Ad-hoc Networks that uses the connectivity between nodes to measure the trust degree of nodes. According to the forwarding sincerity, ACK sincerity and connectivity sincerity of the node, the concept of information entropy is used to calculate the trust degree of the node, and the node trust degree is innovatively used as the selection candidate forwarding set and the calculation of network energy. In order to ensure the reliability of the network, minimize the energy consumption of the network, and achieve the purpose of energy saving. This paper uses the NS2 simulation tool to simulate the PEEQOSR(Proposed Energy Efficient and trust-based Quality of Service Routing) algorithm, and analyses and compares it with the CBEEOR (Connectivity Based Energy Efficient Opportunistic Robust routing protocol) and EEOR (Energy-Efficient Opportunistic Routing) routing protocols. The experimental results show that the PEEQOSR algorithm ensures the trust of the entire network, improves the network end-to-end throughput, and prolongs the network life cycle, and the energy consumption of the network can be greatly reduced, so as to achieve energy saving.

Section 2 introduces the network model composed of Mobile Ad-hoc Networks; Section 3 introduces the calculation method of node connectivity; Section 4 describes the calculation method of node trust; Section 5 introduces the PEEQOSR algorithm in detail; Section 6 in this section, the experimental results of the routing algorithm are analysed in detail; at the end, the full text is summarized.

2. Network Model

The Mobile Ad-hoc Network is defined as an undirected simple finite graph G=(V,E), where V={v1,v2,...,vn} represents the vertex set of Mobile Ad-hoc Network nodes, E represents the link between nodes/ Edge set. An undirected graph indicates that all existing links in the network are bidirectional and can communicate with each other, that is, node vi can reach node vj and node vj can also reach vi.Suppose the parameter R is the communication range of wireless node u, and all nodes within the communication range are called neighbour nodes of node u, denoted as N(u). Link (u, vi) means that node u can directly transmit data packets to node vi within a predefined communication range, and vi $\in$ N(u); Et(u, v) and Er(u, v) represent the energy consumed by the wireless node to send and receive a data packet, respectively.

3. Connectivity of Nodes

Node connectivity indicates the possibility of communication and data transmission between nodes. The higher the possibility, the better the connectivity of the nodes, which further strengthens the connectivity of the network. In addition, the connectivity of the network and the degree of flow of traffic, for maintaining continuous communication between nodes plays an important role. Once a node fails to work properly, it will affect the communication of nodes. Therefore, the concept of algebraic connectivity [19] is introduced to calculate the connectivity properties of nodes. The connectivity property of a node u is quantified as the algebraic connectivity of a graph excluding node u and its associated edges, denoted as a(G). The algebraic connectivity a(G) of a graph G is a Laplace matrix the second smallest eigenvalue of L(G), and L(G) = D(G)-A(G). D(G) is the degree matrix of graph G, and A(G) is the adjacency matrix of graph G.

For graphs G1=(V, E1) and G2=(V, E2), as long as |E1|≤|E2|, a(G1)≤a(G2), it means that the connectivity of graph G2 is higher than that of graph G1. Therefore, the connectivity of node v2 is greater than that of node v1, and the ability of node v2 to maintain network connectivity is better than that of node v1. Therefore, the greater the value of a(G), the greater the connectivity of graph G. As shown in Figure 1, the algebraic connectivity of each node is a(Gv1)=2, a(Gv2)=1, a(Gv3)=2, a(Gv4)=2.

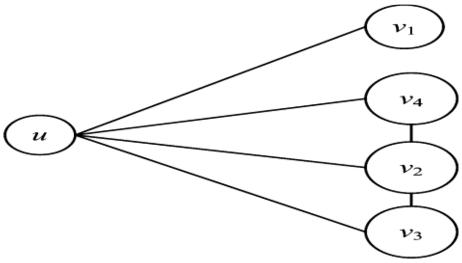

Fig 1: Network Model

4. Calculation of Node Trust

The node trust degree T is evaluated using forwarding sincerity, ACK sincerity and connectivity sincerity of the node. considering the various parameters in the trust degree evaluation on weight distribution and enhance the adaptability of each parameter, the concept of information entropy is introduced in this paper. The information entropy reflects the degree of influence of multiple evaluation indicators on the evaluation transaction [20]. Forwarding sincerity, ACK sincerity and connectivity sincerity are used to assign weights. The calculation of node trust is as follows:

$$T_{v_i} = W_{v_i}^{F} * F_{v_i} + W_{v_i}^{ACK} * ACK_{v_i} + W_{v_i}^{Con} * \mathrm{Con}_{v_i} \qquad (1)$$

Among them, F_{vi}, ACK_{vi} and Con_{vi} are the forwarding sincerity, ACK sincerity and connectivity sincerity of node i respectively; WFivi, WACKvi and WConvi are the adaptive weights of node i's forwarding sincerity, ACK sincerity and connectivity sincerity respectively.

4.1 Forward Sincerity

Forwarding sincerity represents the relationship between the number of successful data packets forwarded by the candidate node and the number of failed data packets forwarded. The calculation method is as follows:

$$F_{v_i} = \frac{FS_{v_i}}{FS_{v_i}+FF_{v_i}}, F_{v_i} \in [0,1] \quad (2)$$

Among them, F_{vi} represents the forwarding sincerity of node i, FS_{vi} represents the number of times that node i successfully forwards data packets, and FF_{vi} represents the number of times that node i fails to forward data packets.

4.2 ACK Sincerity

ACK sincerity indicates the sincerity of sending and receiving acknowledgment information between nodes, and records the number of times the acknowledgment information transmission succeeds and fails. This metric is very useful for calculating the probability of retransmitting packets, and it is calculated as follows:

$$ACK_{v_i} = \frac{SACK_{v_i}}{SACK_{v_i}+FACK_{v_i}}, ACK_{v_i} \in [0,1] \quad (3)$$

Among them, ACK_{vi} represents the ACK sincerity of node i, $SACK_{vi}$ represents the number of ACK packets that node i sends successfully, and $FACK_{vi}$ represents the number of ACK packets that node i fails to send.

4.3 Connectivity Sincerity

Connectivity sincerity is used to measure the degree of connectivity between nodes and is an indispensable parameter for measuring node trust. It is calculated as follows:

$$\mathrm{Con}_{v_i} = \frac{a\left(G_{v_i}\right)}{\sum_{i\in N(u)} a\left(G_{v_i}\right)}, \mathrm{Con}_{v_i} \in [0,1] \qquad (4)$$

Through the calculation of forwarding sincerity, ACK sincerity and connectivity sincerity, the information entropy of forwarding sincerity, ACK sincerity and connectivity sincerity are obtained, which are expressed as H(F$_{vi}$), H(ACK$_{vi}$) and H(Con$_{vi}$) respectively; The adaptive weights of, ACK sincerity and connectivity sincerity are expressed as W$^{F}_{vi,}$ W$^{ACK}_{vi}$ and W$^{Con}_{vi}$ respectively. The relevant calculation formulas are as follows:

$$H\left(F_{v_i}\right) = -F_{v_i} \log_2 F_{v_i} \qquad (5)$$

$$H\left(ACK_{v_i}\right) = -ACK_{v_i} \log_2 ACK_{v_i} \qquad (6)$$

$$H\left(\mathrm{Con}_{v_i}\right) = -\mathrm{Con}_{v_i}\, log_2\, Con_{v_i} \qquad (7)$$

$$W_{v_i}^{F} = \frac{H\left(F_{v_i}\right)}{H\left(F_{v_i}\right) + H\left(ACK_{v_i}\right) + H\left(\mathrm{Con}_{v_i}\right)} \qquad (8)$$

$$W_{v_i}^{ACK} = \frac{H\left(ACK_{v_i}\right)}{H\left(F_{v_i}\right) + H\left(ACK_{v_i}\right) + H\left(\mathrm{Con}_{v_i}\right)} \qquad (9)$$

$$W_{v_i}^{Con} = \frac{H\left(\mathrm{Con}_{v_i}\right)}{H\left(F_{v_i}\right) + H\left(ACK_{v_i}\right) + H\left(\mathrm{Con}_{v_i}\right)} \qquad (10)$$

To sum up, the node trust degree T$_{vi}$ is obtained through the organic integration of the three parameters of the node's forwarding sincerity F$_{vi}$, ACK sincerity ACK$_{vi}$ and connectivity sincerity Con$_{vi}$. A node with a higher trust degree is more likely to participate in reliable data transmission and communication. The greater the reliability, the further strengthens the cooperation between nodes, the stability of communication and the security of data, and reduces the problem of unreliable link transmission between internal nodes due to insufficient node trust.

5. Implementation of PEEQOSR Algorithm

The design of the PEEQOSR routing protocol includes the calculation of the expected cost and the description of the algorithm, so as to effectively select the candidate forwarding set and the next-hop relay node to reduce the energy consumption.

5.1 Calculation of Expected Cost

The expected cost of the source node forwarding the data packet to the sink node through the next-hop relay node includes the cost of transmitting the data and the communication book to maintain the trust degree between the nodes. The candidate forwarding set Fwd(u) of node u is the neighbour node set N(A part of u), that is, Fwd(u)⊆N(u). Since the energy of the node itself is used as the criterion for selecting the candidate forwarding set, the candidate forwarding set Fwd(u) of the node u is not selected according to the expected cost of the node. Therefore, its expected cost consists of three parts: First,the source node sends the expected cost of successfully receiving the data packet by at least one node in the candidate forwarding set, denoted as C$^{h}_{u}$(Fwd*); Second, the forwarding cost of a node in the candidate forwarding set forwarding the data packet to the sink node, denoted as C$^{f}_{u}$(Fwd*); and third the communication cost formed in order to maintain the stability of the network and the reliable transmission between nodes, denoted as C$^{ct}_{u}$(Fwd*). Therefore, the source node broadcasts the data packet and forwards the data to the sink node through the nodes in the candidate forwarding set. The expected cost C$_{u}$(wd*) is:

$$C_u(Fwd^*) = C_u^h(Fwd^*) + C_u^f(Fwd^*) + C_u^d(Fwd^*) \; (11)$$

The energy consumed when the data packet sent by node u is successfully received by at least one node v in the candidate forwarding set depends on the fixed energy and transmission probability of sending and receiving a data packet, so the expected cost of sending C^{hu}(Fwd*) is as follows:

$$C_u^h(Fwd^*) = \frac{w}{\rho} = \frac{E_t(u,v)+E_r(u,v)}{1-\prod_{i=1}^{|Fwd^*|} e_{uv_i}} \qquad (12)$$

Among them, e_{uvi} represents the probability that the data packet sent by the source node u is not successfully received by any node v in the candidate forwarding set.

The probability of node v1 successfully forwarding a packet is 1-euv1, and its expected cost is C_{v1}; the probability of node v2 successfully forwarding a packet is euv1 × (1-e_{uv2})), and its expected cost is C_{v2}. Theoretically, the nodes in Fwd*(u) allow only one node to forward data at the same time, thus avoiding the repeated transmission of data packets, so the calculation of the expected forwarding cost is as follows:

$$\beta = \left(1 - e_{uv_1}\right) * C_{v_1} + \sum_{i=2}^{|Fu\Sigma|} \left(\prod_{j=1}^{i-1} e_{uv_j}\right) * \left(1 - e_{uv_i}\right) * C_{v_i} \ (13)$$

According to the broadcast characteristics of opportunistic routing, all nodes in the candidate forwarding set have the possibility of receiving the broadcast data packets of the source node. If only one node in the candidate forwarding set can forward data at the same time, it is necessary to coordinate and communicate between the nodes. Cooperation; without this coordination, multiple nodes in the candidate forwarding set will forward the same data at the same time. In this case, the energy consumption generated by transmitting the same data packet to the sink node is calculated as follows:

$$\beta = \sum_{i=1}^{|Fwd^*|} \left(\prod_{j=1}^{i-1} e_{uv_j}\right) * \left(1 - e_{uv_i}\right) * C_{v_i} \qquad (14)$$

In order to maintain the normal operation of the Mobile Ad-hoc network and the orderly data forwarding process, this paper allows multiple nodes in the candidate forwarding set to forward the data packets. Therefore, the PEEQOSR routing algorithm uses the formula (14) to calculate the expected cost of forwarding data. Considering the probability of successful transmission between nodes, the expected cost of forwarding a packet is C^f_u(Fwd*):

$$C_u^f(Fwd^*) = \frac{\beta}{\rho} = \frac{|\sum_{i=1}^{|Fud^*|} \left(\prod_{j=1}^{i-1} e_{uv_j}\right)*\left(1-e_{uv_i}\right)*C_{v_i}}{1-\prod_{i=1}^{|Fw\ \ *|} e_{uv_i}} (15)$$

In the PEEQOSR routing protocol, although the connectivity between nodes is a necessary condition to measure the communication between nodes, and also to calculate the energy consumption required for node communication and cooperation, it is called the communication cost, namely C^{ct}_u (Fwd*). The communication cost between the two nodes is measured by the trust degree of the sending node and the receiving node respectively C^{ct}_u(Fwd*), calculated as:

$$C_u^a(Fwd^*) = \frac{E_t(u,v)}{T_u} + \frac{E_r(u,v)}{T_v} \qquad (16)$$

Among them, T_u and T_v represent the trust degree of the source node and the receiver node, respectively.

5.2 Algorithm Description

The specific steps of the trust-based energy-saving opportunistic routing algorithm are as follows:

Step 1: Randomly deploy sensor nodes to a target area of 100m × 100m, and select 5% to 20% of the nodes as the malicious node set, denoted as S.

Step 2: The sensor node determines the neighbour node N(u) according to its communication radius R.

Step 3: Calculate the algebraic connectivity of each node according to the distribution of sensor nodes.

Step 4: Make full use of formula (1) to comprehensively calculate the trust degree T of the node.

Step 5: Assume Cu=∞, Fwd=Ø, S≠Ø, and sort nodes in non-descending order according to expected cost.

Step 6: If the expected cost of the node is lower than the total expected cost, and the node does not belong to the malicious node set S, add the node to the candidate forwarding set, and calculate the expected cost according to formula (11); if the expected cost of the node is higher than The total expected cost, regardless of whether the node belongs to the malicious node set S, cannot add a node to the candidate forwarding set.

Step 7: Execute Step6 in a loop until the neighbour nodes are traversed to obtain the candidate forwarding set. The node with the lowest expected cost is used as the next-hop relay node to forward the data packet.

First, according to Figure 2 and equations (1)-(10), the trust degree of each node in the candidate forwarding set can be calculated, that is, Tv1 =0.5, Tv2=0, Tv3=0.5, Tv4=0.5. Suppose Et(u,v)=0.7, Er(u,v)=0.3, and N(u)={v1,v2,v3,v4}, S={v2}. For simplicity, let ei represents euvi , and let ci represent the expected cost of node vi. Second, according to equation (11) to calculate Expected cost, the expected cost of adding node v1 to the candidate forwarding set, that is, Fwd(u)={v1}, is calculated as

(Et(u,v1)+Er(u,v1)+(1-e1)×c1)/
(1-e1)+Et(u,v1)/Tu+Er(u,v1)/Tv1=4.6;

although the expected cost of node v2 is 1 and will decrease, but v2∈S, it cannot join the candidate forwarding set; The expected cost of v3 is 1.5, so the node v3 will reduce the expected cost, that is, the expected cost of Fwd(u)={v1,v3} is calculated as (Et(u,v3)+Er(u,v3)+(1 -e1)×c1 +e1 ×(1-e2)×c2 +e1e2 (1-e3)×c3)/(1-e1 ×e2 ×e3)+Et(u,v3)/Tu+Er(u,v3)/Tv3 =4 .1;

The expected cost of node v4 is 5, and node v4 will increase the expected cost. If Fwd(u)={v1,v3,v4}, the expected cost is calculated as ((1-e1)×c1+e1(1-e2)×c2+e1e2 (1-e3)×c3 +e1e2e3(1-e4)×c4)/(1-e1 ×e2 ×e3 ×e4)+(Et(u,v4)+Er(u,v4))/(1-e1 ×e2 ×e3 ×e4)+Et(u,v4)/Tu+Er(u,v4)/Tv4 =4.45>4.1, so v4 cannot be added to the candidate forwarding set. Therefore, the candidate forwarding set is Fwd(u)={ v1, v3}, and the expected cost of forwarding the packet from the source node to the destination node is 4.1, node v3 is finally selected as the forwarding node to forward the packet to the destination node.

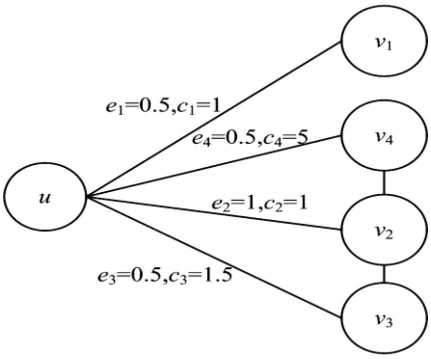

Fig 2: Evaluation of Expected Cost

6. Simulation Evaluation

6.1 Simulation Setup

The PEEQOSR algorithm proposed in this paper is tested by using the NS2 simulation tool. 50 to 200 sensor nodes are randomly deployed in an area of 100 m × 100 m, and 0-20% of all wireless nodes are randomly selected to reduce the network trust. The settings of the specific parameters in the experiment are listed in Table 1.

Table 1: Initial Parameters in Simulation

Parameter	Value
Simulator	NS 2.34
Routing Protocol	PEEQOSR, CBEEOR and EEOR
Scenario Size	100 x 100 m^2
Simulation Time	100 s
Number of Nodes	50
Malicious Nodes (%)	0, 5%, 10%, 15% and 20%
Pause Time	5s
Traffic Type	CBR/UDP

This paper will compare and analyze the performance of the four aspects of trust degree change trend, throughput, energy consumption, and life cycle, and compare it with the CBEEOR algorithm and the EEOR algorithm.

6.2 Analysis of Network Trust

In the evaluation of the network trust degree, when the percentage of malicious nodes is 0, 5%, 10%, 15% and 20% respectively, the changes of the network trust degree are shown in Figure 3. When there are no malicious nodes deployed in the network, the network trust is the highest, which can maximize the reliable transmission of data by nodes in the network. When the number of deployed malicious nodes is getting higher and higher, the network trust degree of the routing algorithm gradually decreases. Among them, the CBEEOR algorithm and the EEOR algorithm do not have a mechanism to directly judge and identify malicious nodes in the network, so their network trust degree will decrease greatly with the increase of the proportion of malicious nodes and the PEEQOSR routing algorithm proposed in this paper can identify potential malicious nodes in the candidate forwarding set. When the ratio is about 10%, the decreasing trend of network trust is slow and flat. Therefore, the performance of PEEQOSR algorithm in network trust is better than that of CBEEOR and EEOR, and it can effectively identify and eliminate malicious nodes in the candidate forwarding set, to ensure the reliability of the network and the reliable transmission of data as much as possible.

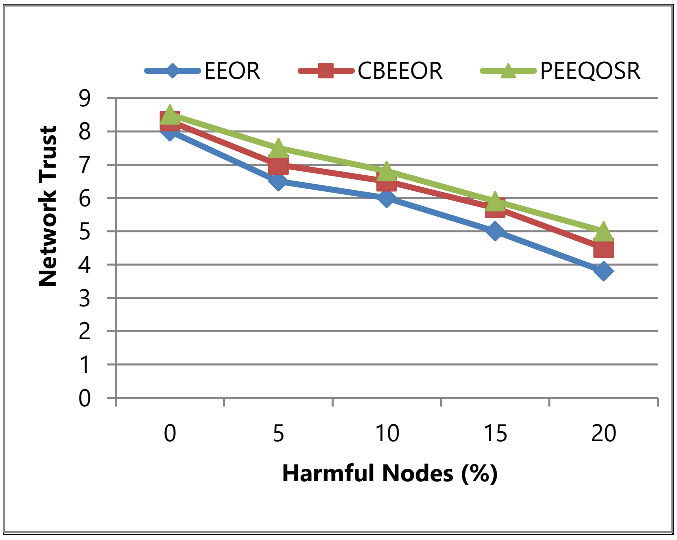

Fig 3: NetworkTrust

6.3 Energy Consumption Evaluation

This paper will verify the performance of PEEQOSR, CBEEOR and EEOR routing algorithms in terms of energy consumption by calculating the expected cost. When the number of network nodes is constant and the percentage of malicious nodes is different, the network energy consumption of PEEQOSR, CBEEOR and EEOR routing algorithms is shown in Figure 4. When the number of network sensor nodes is constant, as the percentage of malicious nodes increases, the network energy consumption of the PEEQOSR algorithm shows an upward trend, but the increase is very small, indicating that the number of malicious nodes in the network will increase with the monitoring mechanism. On the contrary, the energy consumption of the CBEEOR and EEOR algorithms both increase significantly with the increase of malicious nodes, but the energy consumption of the CBEEOR algorithm is not as much as that of the EEOR algorithm. , because the CBEEOR algorithm uses the connectivity attribute of nodes to measure the connectivity of the network. In conclusion, the method of calculating the expected cost proposed in this paper can greatly reduce the energy cost of the network and help to prolong the life cycle of the network.

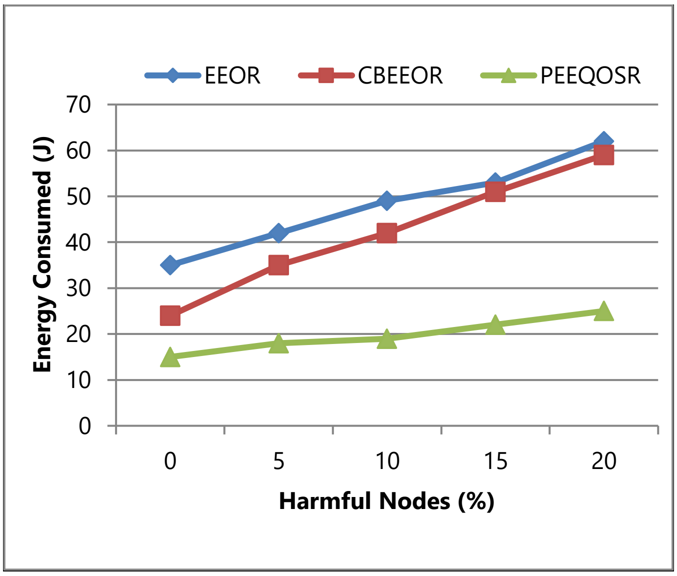

Fig 4: Network energy consumption

6.4 Network Throughput Analysis

When the number of network nodes is constant, with the increase of the percentage of malicious nodes, the change trend of the throughput of PEEQOSR, CBEEOR and EEOR routing algorithms is shown in Figure 5. It can be seen from Figure 3 that the increase in the proportion of malicious nodes in the network leads to a gradual decrease in the network trust of the three routing algorithms, which has a huge impact on the reliable transmission Figure 5 that the throughputs of the PEEQOSR, CBEEOR and EEOR routing algorithms all show a downward trend due to the influence of malicious nodes in the network, but the throughput of the PEEQOSR algorithm is always higher than that of the CBEEOR and EEOR algorithms. The two routing algorithms, CBEEOR and EEOR, do not have a mechanism to detect malicious nodes in the network, which leads to damage to the connectivity of the network by malicious nodes, and the throughput of the network shows a trend of significant decline. The PEEQOSR algorithm proposed in this paper the set detection mechanism can be used to effectively identify malicious nodes in the network, eliminate malicious nodes from the candidate forwarding set, select sensor nodes that meet the trust conditions, increase the reliability of data transmission in the network, and further improve End-to-end throughput of the network.

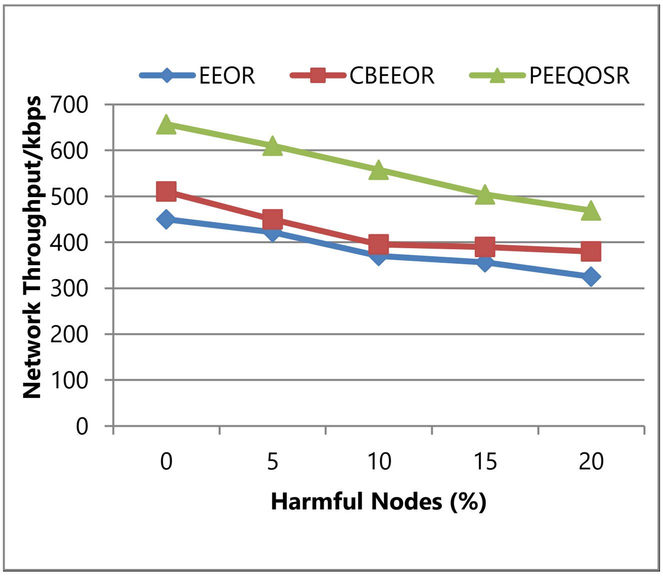

Fig 5: Network Throughput

6.5 Network Lifecycle Analysis

When the percentage of malicious nodes in the network remains unchanged, with the gradual increase of the number of nodes, the basic situation of the network life cycle change is shown in Figure 6. Based on the evaluation process of energy consumption, it can be seen that the method of calculating the expected cost in this paper is compared with other methods. The two routing algorithms can reduce the energy overhead of the network to a certain extent, and can effectively help the nodes in the network to fully utilize the energy, thereby prolonging the life cycle of the network It can be seen from Figure 6 that the network life cycle of PEEQOSR will be prolonged with the increase of the number of nodes in the network. Obviously, the CBEEOR algorithm utilizes the connectivity properties of nodes to reduce the possibility of nodes being attacked and destroyed. On the other hand, it effectively improves the performance of normal nodes in the network. The cycle is significantly longer than the life cycle of the EEOR algorithm. According to the above analysis results, the calculation method to improve the network energy consumption not only increases the number of times the node is used multiple times, but also reduces the possibility of premature death or failure of the node, thereby improving the life of the entire network cycle.

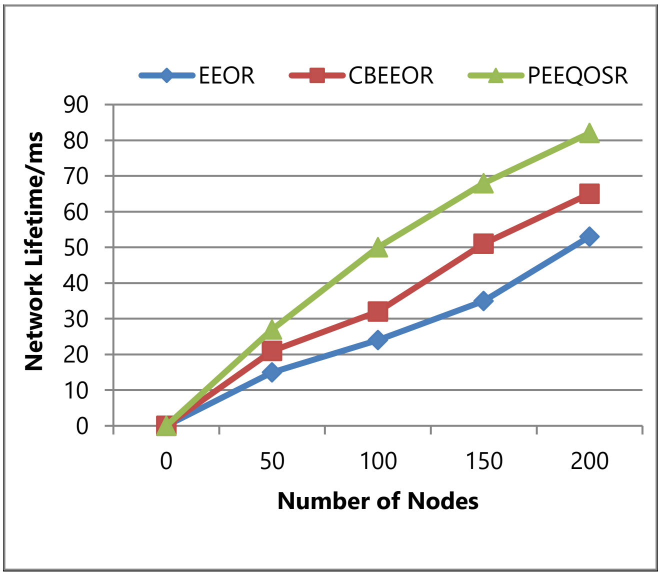

Fig 6: Network Lifecycle

6.6 Time and Space Complexity Analysis

The biggest difference between the PEEQOSR algorithm and the CBEEOR and EEOR algorithms is that the criteria for selecting nodes in the candidate forwarding set are different. Both the CBEEOR and EEOR algorithms take the expected cost of the node as the selection criterion when selecting the candidate forwarding set, so the time complexity of both is O(n^2), and the space complexity is O(1). The PEEQOSR algorithm not only uses the expected cost of the node as the criterion for selecting the candidate forwarding set, but also considers the node's expected trust degree. Although the PEEQOSR algorithm sets up a mechanism to detect malicious nodes, it is only a judgment of the node's trust degree, and does not increase the time complexity of the algorithm, so the time complexity of the PEEQOSR algorithm is also O(n^2) and the space complexity is O(1). From the above analysis, although the space complexity and time complexity of the PEEQOSR algorithm and the CBEEOR and EEOR algorithms are the same, the performance of the PEEQOSR algorithm is better than the other two routing algorithms in terms of reliable transmission of network data with minimum expected cost, less energy consumed and prolonging the life cycle of the network.

7. Conclusion

According to the evaluation model of node trust degree and the energy consumption of nodes in the network, this paper innovatively proposes an energy-saving opportunity routing algorithm based on trust degree. The node trust degree is used to calculate the communication cost of the node and as the evaluation criterion for selecting the candidate forwarding set, and the next hop relay node is selected for the purpose of reducing energy consumption; in addition, the malicious node monitoring mechanism is used to ensure the network trust degree at the same time. The influence of malicious nodes on network performance is reduced, the end-to-end throughput of the network is further improved, the life cycle of the network is prolonged, and the possibility of wireless nodes not working or failing is reduced. When there is no real-time update, the trust degree of the node cannot fully reflect the real situation of the current network. Therefore, in the future research, the dynamic real-time change of the trust degree of the node will be considered to reduce the impact on the network performance.

References

[1] Popescu, D., Stoican, F., Stamatescu, G., Chenaru, O., &Ichim, L. (2019). A survey of collaborative UAV–WSN systems for efficient monitoring. Sensors, 19(21), 4690.

[2] Bhushan, B., & Sahoo, G. (2019). Routing protocols in wireless sensor networks. In Computational intelligence in sensor networks (pp. 215-248). Springer, Berlin, Heidelberg.

[3] Verma, L. P., Sharma, V. K., Kumar, M., &Mahanti, A. (2022). An adaptive multi-path data transfer approach for MP-TCP. Wireless Networks, 1-28.

[4] Guo, J., Liu, J., Liu, M., Zhang, T., Yang, T., & Cui, J. H. (2021, November). Analysis of the Factors Affecting the Communication Between AUV and Acoustic Modem: From the Perspective of Experiments. In The 15th International Conference on Underwater Networks & Systems (pp. 1-5).

[5] Tilwari, V., Maheswar, R., Jayarajan, P., Sundararajan, T. V. P., Hindia, M. H. D., Dimyati, K., ... &Amiri, I. S. (2020). MCLMR: A multicriteria based multipath routing in the mobile ad hoc networks. Wireless Personal Communications, 112(4), 2461-2483.

[6] Biswass,Morrisr,ExOR:Opportunisticmultihoprouting forwirelessnetworks [J]. ACM Sigcomm ComputerCommunicationReview, 2005, 35(4): 133 G 144.

[7] Zhang, Y., Zhang, Z., Chen, L., & Wang, X. (2021). Reinforcement learning-based opportunistic routing protocol for underwater acoustic sensor networks. IEEE Transactions on Vehicular Technology, 70(3), 2756-2770.

[8] Le, Y. (2021). Back-Pressure Based Throughput Enhancement Algorithms for Cognitive Radio Networks (Doctoral dissertation, The George Washington University).

[9] Xufei Mao, Shaojie Tang, Xiahua Xu, Xiang-Yang Li, Huadong Ma, Energy Efficient Opportunistic Routing in Wireless Sensor Networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2011.

[10] Zhou, C., Qu, W., Lu, Z., & Liu, Y. (2019). Energy Consumption Model of WSN Based on Manifold Learning Algorithm. International Journal for Engineering Modelling, 32(2-4 Regular Issue), 17-31.

[11] Karyakarte, M. S., Tavildar, A. S., & Khanna, R. (2015). Connectivity Based Energy Efficient Opportunistic Robust Routing for Mobile Wireless Sensor Networks. Wireless Personal Communications, 84(1), 729-744.

[12] Gao, H., Liu, C., Yin, Y., Xu, Y., & Li, Y. (2021). A hybrid approach to trust node assessment and management for vanets cooperative data communication: Historical interaction perspective. IEEE Transactions on Intelligent Transportation Systems.

[13] Alsarhan, A., Al-Ghuwairi, A. R., Alshdaifat, E., &Idhaim, H. (2022). A Novel Scheme for Malicious Nodes Detection in Cloud Markets Based on Fuzzy Logic Technique. International Journal of Interactive Mobile Technologies, 16(3).

[14] Rathee, G., Ahmad, F., Kerrache, C. A., & Azad, M. A. (2019). A Trust framework to detect malicious nodes in cognitive radio networks. Electronics, 8(11), 1299.

[15] Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., &Fotohi, R. (2020). Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The journal of supercomputing, 76(9), 7081-7106.

[16] Su, B., Du, C., & Huan, J. (2020). Trusted opportunistic routing based on node trust model. IEEE Access, 8, 163077-163090.

[17] Zhao, J., Huang, J., &Xiong, N. (2019). An effective exponential-based trust and reputation evaluation system in wireless sensor networks. IEEE Access, 7, 33859-33869.

[18] VandayBaseri, M., &Kuchaki Rafsanjani, M. (2022). DSNAODV: Detecting Selfish Nodes based on Ad hoc On-demand Distance Vector routing protocol. Journal of Mahani Mathematical Research, 57-68.

[19] Zhang, Y., Li, S., & Weng, J. (2020). Distributed estimation of algebraic connectivity. IEEE Transactions on Cybernetics.

[20] Wang, L. (2022). Application of a Fuzzy Information Analysis and Evaluation Method in the Development of Regional Rural e-Commerce. Advances in Multimedia.