# A New Security Routing Algorithm based on MST for Wireless Sensor Network

Zeng Meimei and Jiang Hua

Guilin University of Electronic Technology ,Guilin,Guangxi,China
zmmmmz123@163.com

**Abstract.** In order to solve the general problems of information overlap, low energy utilization rate and network transmission security in routing protocols of wireless sensor networks, a scheme of energy-efficient and security-high routing for wireless sensor networks (EEASHR) based on improved Kruskal algorithms is proposed in this paper. The proposed scheme takes the energy size required for transmission and the value of reliability between nodes and nodes as the edges value of graph, then uses improved Kruskal algorithm to generate the minimum spanning tree (MST) in sink node, in other words, the optimal route path. The simulation in NS2 shows that the proposed algorithm improves network energy efficiency, reduces the node packet loss rate and prolongs the life cycle of wireless sensor networks.

**Keywords.** Kruskal, wireless sensor networks ( WSNs ), reliability, energy efficiency

## 1 Introduction

With the development of Internet of Things, wireless sensor networks which are the ending net of Internet of Things meets more stringent requirements in security and energy consumption. It urges us to carry out more profound study on the development of wireless sensor networks.

Because of the resource constraints of sensor network nodes and the bad distributed environment, the tasks of improving the energy efficiency of sensor network nodes, and enhancing the network security are unusually formidable.

The following features should be included in a safe and efficient routing protocol. 1) Reduce the impact of the configuration error; 2) Reduce overall network energy consumption; 3) Ensure that only legitimate nodes participate in message transmission; 4) Prevent attackers from injecting spoofed routing information. All kinds of characteristics of wireless sensor networks make the routing protocols vulnerable for the attacks of spoofed routing information, such as selective forwarding, sinkhole, sybil attack, wormhole and so on[1-2]. Traditional security mechanisms based on the encryption system can’t resolve the internal attacks from the nodes which are easily captured in an open environment[3-4]. A lot of research work has been done to prolong the network life cycle and improve the network security transmission index[5-6].

According to the network topology, the routing protocols can be divided into flat and hierarchical routing protocols, and the relations between the nodes and the sink node are usually established in the form of multi-hop. The typical flat routing protocols include Flooding, Gossiping. Among them, there are the problems of information overlaps, abuses of resources, and poor expansibility in the Flooding[7] and Gossiping[8] protocol. Reference[9] shows an idea to send data by sending meta data to consult, but the reliability is poor. Besides the energy of nodes around the sink node is easy to run out. Nodes easily are captured. At present, the existing routing protocols are mainly focused on how to enhance the energy utilization of nodes or the credibility of network nodes[4][10].

## 2 System Model

### 2.1 Network Model

Assume that N sensor nodes are randomly distributed within a square area S, and will be no longer mobile after deployment. The unique sink node is deployed outside area S. It is the network that doesn't need human maintenance after the deployment. The network topology is relatively stable, and the mobility is small; All nodes are isomorphic with the same initial energy, data integration and unique identities (ID). These nodes do not require GPS equipment and do not need to know their specific location through methods of measurement; Wireless transmission power is controllable, namely nodes can adjust the size of the transmission power based on distance.

### 2.2 Wireless Energy Model [11]

Wireless energy model refers to the attenuation of the transmitted power decays exponentially with the transmission distance increases. For free space model, the transmit power was $d^2$ attenuation when the distance between the sending and receiving nodes is $d \prec d_0$, while multipath attenuation model the transmit power was $d^4$ attenuation under the same situation.

### 2.3 Wireless Transmission Energy Model [12]

Wireless transmission energy model as formula (1) and (2) shown, formula (1) indicates the energy loss of launching k bit data, and it is composed of the loss of launch circuit and the loss of power amplifier. $E_{elec}$ means the needed energy which communication module receives or sends per bit data. $\varepsilon_{fs}$ 、 $\varepsilon_{amp}$ respectively show the needed energy that launch amplifier transmits one bit data under two kind of channel models, $d_0$ is distance $d_0 = sqrt(\frac{\varepsilon_{fs}}{\varepsilon_{amp}})$. Formula (2) stands for the energy of receiving k bit data, which only depends on circuit loss. We assume the radio channel transmits information symmetrically, which means energy consumption from v to u equals that from u to v.

$$E_{T_x} = \begin{cases} k \times E_{elec} + k \times \varepsilon_{fs} d^2 & d \prec d_0 \\ k \times E_{elec} + k \times \varepsilon_{amp} d^4 & d \geq d_0 \end{cases} \qquad (1)$$

$$E_{R_x} = k \times E_{elec} \qquad (2)$$

### 2.4 The Method of Excluding Malicious Nodes

In order to void nodes with low confidence become members of transmission path nodes, excluding malicious nodes in networks. This paper improved Reliability evaluation mechanism proposed in paper [13]. As shown in formula (3), $V_{I_b}$ stands for information offered by Intrusion detection system, 1 indicates good node, 0 indicates malicious node; $V_{I_r}$ is an active observation value obtained by monitoring neighbor nodes actively; $V_{S_r}$ is an indirect observation value obtained by exchanging information with neighbor nodes; $f_1$ , $f_2$ , $f_3$ can be set different values in accordance with the specific requirements of the network, we assume $f_1 + f_2 + f_3 = 1$ and normalize them.

$$E = [ f_1 \left( E_{T_x} + E_{R_x} \right) + f_2 (1 - V_{I_r}) + f_3 (1 - V_{S_r}) ] \times V_{I_b} \qquad (3)$$

## 3 Algorithm Idea

Without considering the space difference, the proposed scheme abstracts nodes of the wireless sensor network into the vertices of the graph, and abstracts communication relation among network nodes into the edge of the graph between vertex and vertex. Thus, the wireless sensor network can be represented as graph G= (V, E), in addition, V represents the set of sensor network nodes and E represents communication relation among network nodes. The proposed scheme takes the energy required for transmission and the value of reliability between nodes and nodes as the edges of graph, using improved Kruskal algorithm to solve the problem existing in Flooding algorithm.

### 3.1 Kruskal Algorithm[14]

Kruskal algorithm is a classical algorithm to generate a minimum spanning tree. In this paper, the idea of minimum spanning tree is used to construct optimal routing paths in wireless sensor networks. The improved algorithm based on reference [13] as follows:

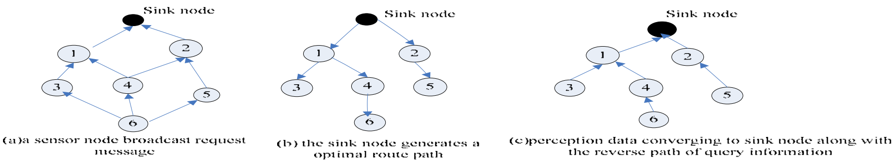
Assume that V is a set of vertices in the graph; E is the set of edges in the graph; RE is the set of edges of the optimal routing path. Optimal routing path can be achieved through the improved Kruskal algorithm.

1. Initialization: RV= {$v_0$, $v_1$,……, $v_{n-1}$},RV indicates a subgraph that includes n nodes but no edges.
2. If E={}, then output optimal path R, and the algorithm ended.
3. From the current position back to search (u,v) in sequential E (G) to get minimum weight edge (u,v). it should be noted that u and v are in different connected components. Namely (u,v) indicates the minimum weight edge. Move u and v into RE, merge them as one connected component and update E at the same time. If E{（u，v）=0}, then move edge (u,v).
4. Turn to the step 2.

### 3.2 Optimal Route Path

The algorithm consists of two parts: building the optimal route and steady operation stage. In each round, the algorithm real-time updates the optimal route path through setting a time stamp on the sink node.

1. The node in network to broadcast request packets which carry the node information (ID) of senders and the E value of sender node orderly marked by node.
2. At last, request packet information can converge on sink node along with the transmission of the request packets in network. Sink node can obtain the topology of the entire network , ID, and the E value.
3. The sink node uses improved Kruskal algorithm to generate an optimal route path.
4. The sink node sends out query information based on the optimal path, then perception data converge to sink node along with the reverse path of query information. The parent node uses data integration to process data to reduce the data traffic, as Fig. 1 and Fig. 2 shown.

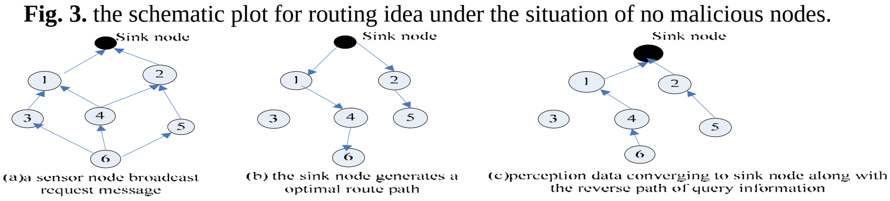


(a)a sensor node broadcast request message

(b) the sink node generates a optimal route path

(c)perception data converging to sink node along with the reverse path of query information

**Fig. 3.** the schematic plot for routing idea under the situation of no malicious nodes.



(a)a sensor node broadcast request message

(b) the sink node generates a optimal route path

(c)perception data converging to sink node along with the reverse path of query information

**Fig. 4.** the schematic plot for routing idea that No.3 is a malicious node.

## 4 simulation and analysis

The proposed method is simulated via C++ program based on NS2 simulation platform .The main parameters of the sensor network are as follows:100 nodes are evenly distributed in 50*50 geographical area which is named S .The sink node is outside the S .The energy of every node is initially $E_T$ =0.5J( $E_T$ is the total energy.).The optimal routing path is generated by Kruskal algorithm in sink node. In order to validate the performance of proposed algorithm, the experiment made a comparison with Flooding algorithm .The network lifecycles of different protocols in the same initial energy are shown in Fig. 3.We can see that the lifecycle of proposed algorithm is nearly 80 times than Flooding algorithm (lifecycle ended until the death of the last node). The packet loss rates along with different number of malicious nodes are shown in Fig. 5. To simplify the experiment, malicious nodes are set manually. From Fig. 6 we can see that the packet loss rate of the EEASHR is generally reduced by about 25% compared with Flooding in the same circumstances.

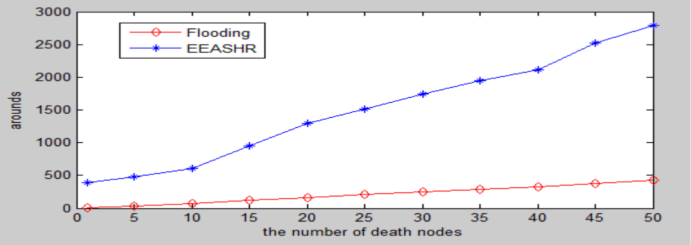


**Fig. 7.** network lifecycle of different protocol in the same initial energy

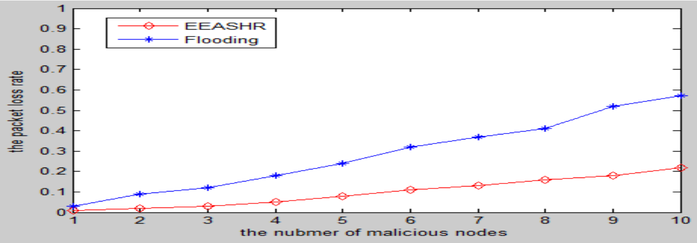


**Fig. 8.** network packet loss rate in different number of malicious nodes

## 5 Conclusions and Future Works

We have proposed EEASHR, an emerged efficient algorithm that uses the minimum spanning tree technique to provide data transport security in wireless sensor networks.

We have evaluated the cost, in terms of the network lifetime and the packet loss rate of the proposed Kruskal scheme and compared it with the Flooding protocol. The experiments showed that the proposed scheme can make full use of the node energy, and it also can significantly improve the WSN lifetime. At the same time, the proposed algorithm takes the reliability of nodes into consideration, thus it enhances network transition security by preventing malicious nodes from losing or interfering packets. In the future, we plan to study the hierarchical network topology which is suitable for large network nodes.

## References

1. Kifayat, K., Merabti,M., Shi, Q.: Security in Wireless Sensor Networks. In: STAROULAKIS, P., STAMP, M.: Handbook of Information and Communication Security. PP. 513-552. Springer. Berlin ( 2010)
2. Jaydip, S.: A Survey on Wireless Sensor Network Security. International Journal of Communication Networks and Information Security. 2, 55-78 (2009)
3. Boukerch, A., Xu, L., El-khatib, K.: Trust-based Security for Wireless Ad Hoc and Sensor Networks. Computer Communications. 30,2413- 2427 (2007)
4. Wu, Y.F., Zhou, X., Feng, R.J., Wan, J.W., Xu, X.F.: Secure Routing based on Node Trust Value in Wireless Sensor Networks. Chinese Journal of Scientific Instrument. 1,221-227 (2012)
5. Kan, B.Q., Cai, L.,Zhu, H.S., Xu, Y.J.: Accurate Energy Model for WSN Node and Its Optimal Design. Journal of Systems Engineering and Electronics. 19(3), 427-433 (2008)
6. Hu, X. D., Wei, Q.F., Tang, H.: Model and Simulation of Creditability-based Data Aggregation for the Internet of Things. Chinese Journal of Scientific Instrument. 31(11), 2636-2640 (2010)
7. Chang, D., Cho, K., Choi, N., Kwon, T., Choi, Y.,:A Probabilistic and Opportunistic Flooding Algorithm in Wireless Sensor Networks. Computer Communications. 35(4),500-506 (2012)
8. Tang, J.H., Dai, S.S., Li,J.H.: Gossip-based Scalable Directed Diffusion for Wireless Sensor Networks. International journal of communication systems.24(11), 1418-1430 (2011)
9. Joanna, K., Wendi, H., Hari, B.: Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks. Wireless Networks. 8,169-185 (2002)
10. Cui, Y.R, Cao, J,H., He, N., Zhu, F.: Energy-efficient Data Query Protocol for Wireless Sensor Network. Application Research of Computers.25(2), 216-217 (2008)
11. Rappaport, T.: Wireless Communications: Principles and Practice. Prentice Hall Inc, New Jersey (1996)
12. Heinzelman, W.R., Chandrakasan, A.B., Krishnan, H.: An Application Specific Protocol Architecture for Wireless Micro Sensor Networks. In: IEEE Trans on Wireless Communications, pp.660-670 (2002)
13. Zhang, J., Xu, L., Xu, D.W.: Secure Clustering Algorithm based on Trust Evaluation in Ad Hoc Network. Computer Application. 10(27),2426-2429 (2007)
14. Levin, M.S., Zamkovoy, A.: A Multicriteria Steiner Tree with the Cost of Steiner Vertices. Journal of Communications Technology and Electronics. 5(12), 1527-1542 (2011)