A Secure Routing Algorithm for Hierarchical Cluster-tree WSN Based on Energy Aware Mechanism

Qing YE\textsuperscript{1,*}, Qiong XUE\textsuperscript{2} and Deng-tao WU\textsuperscript{3}

\textsuperscript{1}Department of Information Security, Naval University of Engineering, Wuhan 430033, China
\textsuperscript{2}Unit 92390, PLA, Guangzhou 510000, China
\textsuperscript{3}Unit 92118, PLA, Zhoushan 316000, China

\*Corresponding author

Keywords: Energy aware, Key pre-distribution, Dynamic key management, Secure routing algorithm.

Abstract. Routing algorithm based on hierarchical cluster-tree topology is comparatively ordinary and easy to expand, yet it lacks consideration in best energy consuming structure in WSN network and the route security problems. This paper exploits energy aware mechanism to make sensible choices of relay node in communication rout, decreasing the hops of data transmitting, saving the energy and prolonging the life time of WSN. On basis of the algorithm, the security problem of net data leakage and missing caused by hostile intrusion is improved with cryptography and authentication. Simulation results show that the algorithm owns advantage over traditional ones based on hierarchical cluster tree topology on aspects of survivability, transmit hopss and network robustness.

Introduction

Routing protocol plays an important role in WSN protocol stack, transmit the data obtained by nodes in the network to the destination through best route, it is the foundation of data transmission and collection. The resources including energy, storage and computation of nodes in wireless sensor network are limited. Thus it’s necessary to design an efficient routing protocol.

Routing protocol should firstly consider the life limitation of sensor nodes and improve the energy consumption and indexes, which can prolong the life limitation and reduce the energy consumption [1]. To meet the design demands, general wireless sensor network aims to design routing algorithm with high multi-hop count, low cost and low energy consumption[2,3]. Routing algorithm based on hierarchical cluster tree structure is rather simple and easy to expand, instead of transmitting data from root node to other nodes through a high power transmitter with single hop, it transmits through cluster tree. However, the protocol lacks consideration in best structure of energy consumption and routing security problems, leaving the algorithm easy to hack in and data theft. This paper introduces energy aware mechanism in routing establishment and exploits cryptology and authentication to improve the security of routing.

Basic Information of Energy Aware Model

The energy aware routing protocol proposed by Shah et al. is to improve the data consumption of directed diffusion protocol [2,3]. The idea of which is to establish several routes between source node and target node, and assign every route with choosing probability according to wireless communication routes energy consumption and remaining energy states in every nodes. This protocol balances the communication of the whole network and energy consumption of nodes, hence prolonging the life period of network[4-7].

In this model, the establishment of communication route must take cost into consideration. When node \(N_i\) needs to send message to node \(N_j\), the communication cost is the initial cost of \(N_i\) plus the energy consumption of communication.
The nodes will give up routes with too much cost and chooses routes with low cost, which will be added into routing table. Every node will compute choosing probability for next hop node in routing table, the choosing rate is inversely proportional to energy consumption, as is shown in equation (1).

\[ P_{i,j} = \frac{1/C_{i,j}}{\sum_{k \in FT_i} 1/C_{k,j}} \]  

In which \( P_{i,j} \) is the probability of node \( N_i \) choosing node \( N_j \), \( C_{i,j} \) is the energy consumption of node \( N_i \) to node \( N_j \), \( FT_i \) is the routing table of node \( N_i \). Generally, node will take the choosing rate of next hop as weighting coefficient, compute every energy cost of itself to the next node according to the routing table and consider the reasonability of route comprehensively. This paper uses channel propagation model and radio communication energy model to analyze the communication energy consumption.

(1) Channel propagation model

In the radio communication, the attenuation of electromagnetic wave is power function relation with communication distance. This paper determines transceiver power with Friis free space model and multi-route attenuation model. Assuming that distance threshold of sender and receiver is \( D_z \), the antennas have the same height, as is shown in equation (2).

\[ D_z = \frac{4\pi h^2 \sqrt{I}}{\lambda} \]  

In which, \( h \) is the height of antenna, \( I \) is the loss factor, \( \lambda \) is the wave length of the signal. Thus, when the distance of sender and receiver is \( d \), the receive power is shown in equation (3).

\[ P_r(d) = \begin{cases} \frac{PH_rH_t\lambda}{(4\pi d)^2} & \text{if } d < D_z \\ \frac{PH_rH_t h^4}{d^4} & \text{if } d \geq D_z \end{cases} \]  

In which \( P_t \) is the sending power, \( H_r \) is the gain of receiver, \( H_t \) is the gain of the sender. When the distance between sender and receiver is less than the threshold, the Friis free space model is adopted. When the distance is larger than threshold, the multi-route attenuation model is adopted.

(2) Radio communication energy model

In this model, both the transmitter and receiver of a single node consumes the energy, the energy consumption of former one is consisted of radio transmitting energy and amplifier energy. Since the later one is in charge of receiving the data, the energy of it equals the energy consumption of transmitter. When the distance is less than the distance threshold, the Friis free space model is adopted, and \( n \) equals 2. When distance is larger than the threshold, the multi-route attenuation model is adopted, \( n \) equals 4. Thus the energy consumption of transmitting 4 bit data is shown in equation (4).

\[ E_{\text{Tx}}(K,d) = \begin{cases} KE_{\text{elec}} + K\varepsilon_1 d^2 & \text{if } d < D_z \\ KE_{\text{elec}} + K\varepsilon_2 d^4 & \text{if } d \geq D_z \end{cases} \]  

In which \( E_{\text{elec}} \) is the energy consumption of transmitting unit data, \( \varepsilon_1,\varepsilon_2 \) are the different energy consumption index of amplifier in different model. When k bit data is received, the energy consumption of receiver is shown in equation (5).

\[ E_{\text{Rx}}(K) = KE_{\text{elec}} \]  

Since the efficient of node transmitting information to the route is determined by amplifier, the transmitting power of node is the radio power of amplifier, combining the channel propagation model, the receive power is shown in equation (6).
Through the consumption model above, once the initial data is set, the energy consumption and remaining data of a node can be calculated.

In the practical wireless sensor network, when a node needs to transmit information to target node and there is more than one route to choose, the source node will send routing request to relay node and ask the other nodes to inform the remaining energy states, then it chooses the best route according to the energy state and the energy consumption. Let the initial energy of \( n \) nodes is \( E_{\text{init}} \), the energy remaining is \( E_{m1}, E_{m2}, \ldots, E_{mn} \), the energy consumption of nodes communication is \( E_{c1}, E_{c2}, \ldots, E_{cn} \), then the source node will choose route according to the energy consumption, as is shown in equation (7). The route with smallest value of \( C_i \) is the best route.

\[
C_i = E_{\text{init}} - E_{mi} + E_{ci}, \quad i = 1, 2, \ldots, n
\]

\[ \text{(7)} \]

**A Routing Algorithm for Improved Cluster Tree Topology Based on Energy Aware**

Traditional cluster tree algorithm determines a routing path after the cluster network is established. Nodes out of the routing table is located through parents recursive query, and the procession usually passes several relay nodes and consuming much energy. This paper adopts the improved algorithm based on energy aware, aiming to make sensible choice of the relay nodes, reduces the hops of the transmission path and save the energy. In the subtree generated by nodes around cluster head, every node is in the hierarchy of tree as is shown in Figure 1.

![Figure 1. The hierarchy of cluster tree routing algorithm.](image)

The difference between traditional and improved algorithm lies in the procession of path establishment, every node will broadcast to nodes within one hop before transmit information to parent node, informing them the cluster ID (CID) and net ID (NID) of target node, and choose node close to it to transmit, the specific procedure is as below:

1. If the target node and node includes target node receive the information, it will return message to inform the source node that it is available to transmit route information, then the source node will compare the level of nodes returning message and choose the one with higher level as next transmitter.

2. If there is no response of target node or node includes target node, the source node will determine if there is node within one hop has same CID with target node, if there is, then it will choose best node according to energy aware model and transmit, if there isn’t, then it will transmit to it’s parent node through basic route. The parent node receives the message repeats the steps above until the target node is found, the node will transmit to next level and finally establish several transmit path and choose the best one according to the energy state of path.

Figure 2 is the practical procedure of route establishment of cluster tree network. When nodes from different cluster build the communication route, source node broadcast to nodes within one hop to determine if there are other available nodes, where CID of source node and target node is 1 and 2.
Bidirectional Authentication Based on Key Pre-distribution and Dynamic Management

To ensure the security of nodes in the routing algorithm, methods of key pre-distribution, dynamic update and bidirectional authentication can be used to identify and transmit the legal message [8-10]. In the early stage of route establishment, all the nodes share same master key $K$ and one-way hash chain $OHC$. $OHC$ is a calculation and storage saving light hash function that applies for wireless sensor network. The value of $OHC$ is included in request message and is able to forbid attacker from forging $REQ$ message. The root node will generate a new master key encrypted with $K$ and broadcast to all the nodes and transmitted among them to inform them to change master key, which realize the update of master key. The specific procedure includes following three steps:

Step 1: network establishing period: when the root node propose a network establishment, all the available nodes in the network will receive a route message to inform them to establish communication with neighbors. The broadcast message format is as below:

\[
\text{Root} \rightarrow *: \text{REQ} \| \text{Root} \| OHC
\]

Where $REQ$ is the message type, $ROOT$ is identification of root node, $OHC$ is the serial number generated by one-way hash function.

$OHC$ serial is a serial of number $S_0, S_1, \ldots, S_n$, $S_i=F(S_{i+1})$ ($0<i<n$) generated by one-way function $F$. when the first network establishment begins, nodes can verify whether $OHC$ value comes from real root node through calculating $S_0=F(S_1)$. Generally, root node uses $S_i$ to conduct identity verification in $i$ establishment.

Step 2: key updating period: when a network establishment finishes, messages of updating key is transmitted to all the nodes and transmitted among them. The broadcast format is as below:

\[
\text{Root} \rightarrow *: \text{REQ} \| \text{Root} \| OHC \| E_K[K' \| \text{Root} \| OHC]
\]
Where $K'$ is the updated master key, through $OHC$ and $Root$ label obtained by decryption one can verify that the message is transmitted by root node. However, flaw exists in the broadcast procedure, if the key updating message cannot be received by a legal node, then the node won’t change the master key, hence not able to pass the authentication and become a failed node. To prevent nodes exiting network in this flaw, we present a solution: set a space that can store two key information of $K_a$ and $K_b$, when next key $K_c$ is updating, the earlier one $K_a$ is updated, and so forth.

Step 3: when communicating, nodes need bidirectional authentication to verify the legality of identity, as is shown in Figure 4, in this procedure, every node uses updated key but store the latest key used in network establishment.

![Figure 4. Bidirectional authentication of nodes.](image)

(I) Message from A to B is encrypted with master key, the information includes identity of A and B, data and a one-time random number $N_1$, which proves that A needs to communicate with B.

(II) B decrypts the message with master key shared with A and obtain the information, then it sent it’s identity and $F(N_1)$ to A to inform that message is received successfully.

When A receive that message, it decrypts the message with master key $K$ and know that B is legal and has received transmitted message successfully, then A will stop transmitting to save energy. But if the situation of node cannot update master key in time should occur, then B cannot get valid information and data through decryption, and the transmission is ceased. To prevent this situation, when B cannot decrypt the message in step (I), B will send a key update request message, then A will use the last key to encrypt the latest key and transmit it to B for it’s update, as is shown in Figure 5.

![Figure 5. Authentication when B failed to update the key.](image)

When B receive message from A, it can obtainnew key information with ordinary master key $K$, then it will transmit the message of identity and $F(N_2)$ after encryption with new key to inform the update is finished. Then A transmits the message encrypted with new key $K'$ to finish the core data information transmission.

If the transmission between A and B needs multi-hop, then the relay node will write the path information into data format. Let relay node is C, then the transmission procedure is as follows.

$$A \rightarrow C : E_k \left[ ID_A \parallel ID_C \parallel Data \parallel ID_B \parallel N_1 \right]$$

$$C \rightarrow B : E_k \left[ ID_A \parallel ID_C \parallel Data \parallel ID_B \parallel N_2 \right]$$

Through analysis above, we can conclude that route protocol considering the distance energy cost reduce the communication, which prolongs the life period of WSN effectively. When the root node broadcast to establish a net, the application of one-way hash chain $OHC$ enable the other nodes to verify the authenticity of root node, and bidirectional authentication and encryption make the transmission more stable. When a net establishment is finished, nodes update the key to prevent key leakage through node hijack. And when key updating message is intervened, nodes can finish that through authentication with last key, which provide security insurance for the network.

**Simulation and Analysis**

We apply Matlab to conduct simulation on algorithm proposed above to verify the security and
efficiency. In the experiment, 100 sensor nodes are set randomly in a rectangular region of 150m*150m, root nodes in the centre among these nodes, assuming that it cannot be destroyed and has continual energy supply. Aggregation gateway is outside the region and responsible for collecting information of root node and cluster head nodes. Detailed parameters are shown in Table 1.

<table>
<thead>
<tr>
<th>Experiment parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region range</td>
<td>150m×150m</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100</td>
</tr>
<tr>
<td>Location of root node</td>
<td>(75,75)</td>
</tr>
<tr>
<td>Initial energy of node</td>
<td>1J</td>
</tr>
<tr>
<td>Size of transmitting data</td>
<td>4kb</td>
</tr>
<tr>
<td>$\varepsilon_1$</td>
<td>10pJ/bit/m²</td>
</tr>
<tr>
<td>$\varepsilon_2$</td>
<td>0.0013pJ/bit/m²</td>
</tr>
<tr>
<td>$E_{elec}$</td>
<td>50nJ/bit</td>
</tr>
<tr>
<td>$D_Z$</td>
<td>50m</td>
</tr>
</tbody>
</table>

Comparison and Analysis of Survivability

Experiment conducts networking communication based on 1 minute, and 100 times of communication is simulated, the sensor nodes are distributed randomly in the region of 150m*150m, as is shown in Figure 6. In the Experiment we analyze the survivability through comparing the nodes surviving state of traditional algorithm and this algorithm. In one communication, every node need to communicated with root node or cluster node for one time, when the energy of a node is 0, the node exit the network and no longer transmit or route, nodes have communication relationship with it establish communication with nearest node and update the topology. The result is shown in Figure 7. It can be learned that traditional algorithm starts to lose efficacy after 35 networking communication and the speed is rather rapid, it breaks down after 60 times of communication. And the improved algorithm is better than the traditional ones withumber of 55 and 85, which shows that the improved algorithm has stronger survivability and more energy saving.

Comparison and Analysis of Communication Hops

After the network establishment, the communication hops of all the nodes is collected and analyzed, the comparison is shown in Figure 8 which shows that hops of improved algorithm is about 4 while that of traditional algorithm is about 6, proving that improved algorithm has an advantage of efficiency over traditional one.
Comparison and Analysis of Robustness

Assuming that there are noises in the outer network environment. To simulate that, noise source is set in a random region of 20m×20m in every 5 networking communication to interrupt the key update. Compare the number of working nodes in different algorithm, as is shown in Figure 9. It can be seen that improves has a conspicuous advantage of anti-interference over traditional algorithm. Because traditional routing protocol doesn’t take key negotiation into consideration, nodes cannot update key after interferences, thus cannot pass the authentication, and the network will fail after several communications. On the contrary, improved algorithm solves that problem and keeps a stable communication. Thus, improved algorithm has better anti-interference ability and stability.

Conclusion

Considering the shortage of hierarchical cluster-tree routing algorithm in energy consumption and security, the method of energy aware is adopted to improve the transmission. The relay nodes are investigated and the best choice is made. Under the authentication of dynamic key management mechanism, root node needs to prove itself when the network establishment begins to prevent forged root nodes routing information. And the communication between nodes uses bidirectional authentication to protect the core data and defend the security. The simulation shows that the improved algorithm has an advantage of survivability, communication traffic and robustness over traditional ones.
References


