A Quality of Service Routing Algorithm in Wireless Sensor Networks

https://doi.org/10.3991/ijoe.v13i07.7280

Xiaoqing Yang
Henan Technical College Of Construction, Henan, China
cfy8686@163.com

Abstract—An Quality of Service(QOS) secure routing algorithm based on ant colony optimization is put forward to solve a variety of security problems in wireless sensor networks. The algorithm combines the ant colony optimization algorithm with the credit evaluation mechanism, and introduces the node 's credit as the control factor to obtain better security performance. The algorithm first cuts the network topology according to the QOS requirements, kicks out the nodes that do not meet the QOS requirements, and then quickly converges the route to the optimal route according to the ant colony optimization method. Finally, the security analysis of the algorithm is carried out from various aspects of network layer attack. The experimental results show that the algorithm has very good performance in wireless sensor networks. As a result, it is concluded that it can be widely applied in wireless sensor networks.

Keywords—wireless sensor, ant colony algorithm, security algorithm

1 Introduction

With the development of computer and electronics industry, especially with the development of multimedia networks, people are no longer satisfied with the accessibility of information for wireless sensor networks, and they pay more and more attention to the research of quality of service (QOS) provided by wireless sensor networks [1]. Therefore, how to take effective measures to ensure the application of wireless sensor network service quality needs to become an important research area. However, due to the fact that people first design routing protocols, they often pay attention to the accessibility of data and ignore the security, which leads to a variety of security problems in wireless sensor networks [2,3].

The group intelligent ant colony algorithm has the advantages of self-organization, distributed computing and so on, and makes the algorithm solve the wireless sensor network routing problem which has a strong advantage [4]. In this paper, we propose a QOS secure routing algorithm based on ant colony optimization, which is designed to meet the problem of security consideration in wireless sensor networks. The algorithm combines the ant colony optimization algorithm with the credit evaluation mechanism, and introduces the node's credit as the control factor to obtain better security performance. The algorithm first cuts the network topology according to the QOS

requirements, kicks out the nodes that do not meet the QOS requirements, and then quickly converges the route to the optimal route according to the ant colony optimization method. Finally, the security analysis of the algorithm is carried out from various aspects of network layer attack.

2 Reviews

QOS routing task is to find a sufficient network resources to meet the QOS routing requirements [5]. Ant colony optimization algorithm is widely used to solve all kinds of NPC problems because of its global optimization and self-learning ability, and has achieved quite a lot of results [6]. In recent years, researchers at home and abroad have provided some strategies for QOS routing of antirex-based wireless sensor networks [7].

But these agreements in the design process focused on energy savings and data information accessibility, and did not pay attention to the security of network protocols. With the development of wireless sensor networks, network security is becoming more and more important, and even some applications are based on the security of network protocols as a prerequisite [8]. Because wireless sensor networks are deployed in an open physical environment, communication between nodes is susceptible to communication by other malicious nodes, resulting in a lot of security problems in the network itself [9]. For all these reasons, there are many types of attacks in the network, some of the localized areas of the attacked network are affected, and some networks are directly paralyzed. Therefore, the security protocol is an important aspect in the design of network protocols in wireless sensor networks.

In this paper, we propose a QOS secure routing algorithm based on ant colony algorithm. Based on the ant colony algorithm, this algorithm combines the ant colony algorithm with the credit evaluation mechanism, and introduces the credit of the node as the control factor to get the better security performance. In this algorithm, the ant colony algorithm uses the maximum and the minimum ant system, in order to give full play to the initial search function in the ant colony network and the late convergence of the network to the optimal route as soon as possible.

3 Methods

We introduce the credit evaluation mechanism, through the node of the existing neighbor nodes on the node's credit evaluation to determine the node's credit. In the ant colony algorithm, the reliability of the node is taken as the control factor, and the ant colony algorithm is converged, taking into account the factors such as delay jitter and link bandwidth, which converges to a routing link that satisfies QOS requirements.

By modifying the strategy of the pheromone update of the slave, we make the pheromone update from the back to the ants to complete. The pheromone update is only on the optimal path in such a way that the pheromone is released in the optimal path in the current iteration or the pheromone is released on the currently optimal

path. In this way, the malicious nodes in the network cannot let the forward ant to the target node or the ant cannot return, so the path of the malicious node pheromone concentration is low, so as to effectively avoid the wormhole attack.

3.1 Establishment of credit model

In the wireless sensor network, the system may face a variety of threats, especially in the previous routing algorithm, and it often pay attention to the feasibility of the data, while ignoring the security of the network. By establishing a security model, the node with higher data forwarding capability in the network has higher credit value than other nodes. Since the system cannot successfully forward the data to the destination node, it causes the node to have no high credit. Thus, in the process of routing selection, the probability of other nodes to select the node is low, so as to improve the security of the system.

When the trust model is established, the trust model is validated by the success rate of the node forwarding to the target node and the retransmission rate of the node packet in the most recent period. In the most recent period, the node can successfully deliver the data to the next hop node of the target node. The higher the corresponding credit value, the higher the retransmission rate of the node, and the lower the credit value, the lower the node may be a malicious node.

1. Packet forwarding success rate

Forward success rate calculation formula is as follows:

$$\Pr = Ns / Na \tag{1}$$

Among them, Ns indicates that a packet is forwarded successfully over a fixed time interval, Na indicates that during this period, all nodes are transmitted to the data packets of this node.

2. Packet retransmission rate

The packet retransmission rate represents the proportion of packets that are retransmitted over the packets passing through the node. The formula is:

$$Pij = n / m \tag{2}$$

Where n is the number of packets forwarded from i to the target node j, and m represents the total number of retransmitted packets.

The direct trust value of the node is the trust value of the node itself, the credit value of a node itself is as follows:

$$Ti = \omega Tp + \xi Tr \tag{3}$$

In which, ω and ξ are two parameter factors, Ti is the node credit value, ω+ξ=1, Tp is the credit value obtained by forwarding the success rate, and Tr is the trust value obtained by retransmission. The definitions are as follows:

$$Tp = \frac{1 + \sum_{k=1}^{i} \beta^{Tc-tk} \Pr}{2 + \sum_{k=1}^{i} \beta^{Tc-tk} Pij} \tag{4}$$

$$Tr = \frac{1 + \sum_{k=1}^{i} \beta^{Tc-tk} n}{2 + \sum_{k=1}^{i} \beta^{Tc-tk} m} \tag{5}$$

In the above expression, β is the forgetting factor, Tc is the current time, and tk is expressed as the time of each sample.

The reliability of a node is determined by the trust of the node and other nodes, and the error will easily come out with the deception of the malicious nodes, so the trust value of node S to node D is S and all the common neighbor nodes of the node D.

3.2 Pheromone update

At the stage of the ant search, the ant is basically the same in each path, and the ants randomly choose a path to explore the path of the target node. After a period of time, the corresponding node on each path of the credit value is different, with high credit value of the node is easy to be selected as the next hop node, lower credit nodes or malicious nodes because of the lower trust value, the probability of being selected as the next hop node is relatively low.

The ant is responsible for the pheromone update. In this ant colony algorithm, the idea of the maximum and the minimum ant system is used to update the pheromone only on the optimal path so far or on the optimal path in this iteration. Because the malicious node has information such as high energy and bandwidth, it attracts the source node to send the information to the node for forwarding. If the node is not forwarded to the target node, the credit of the malicious node will be reduced. When the ant is updating the pheromone, the forward ants do not pass through this point and reach the target node, there is no backward node to update the pheromone of the node, resulting in a decrease in the degree of credit on the node. In this way, it creates a positive feedback process, makes it increasingly impossible for malicious nodes to accept data and forward data, and results in malicious nodes failing to affect the network.

3.3 Algorithm design

The algorithm uses the ant colony algorithm and introduces the node's credit value calculation model. The forward ant selects the next node according to the principle that the node with high credit value is selected.

The ant probability of selecting a next node j in an i node is calculated according to the following equation:

$$P_i(j)=\begin{cases}\dfrac{\tau_{ij}(t)^{\alpha}\times\eta_{ij}(t)^{\beta}}{\sum_{r\in n(i)}\tau_{ir}(t)^{\alpha}\times\eta_{ir}(t)^{\beta}}; & j\in n(i)\\ 0; & j\notin n(i)\end{cases} \tag{6}$$

The heuristic information is calculated using the following formula:

$$\eta_{ij}(t)=\begin{matrix}0;otherwise\\ Ti;bandwidth(eij)\geq B\min\end{matrix} \tag{7}$$

Where Ti is the credit of node i, bandwidth (eij) ≥ Bmin, which indicates that the estimated bandwidth of the link between node i and node j is greater than the minimum bandwidth required by the link. Obviously, this constraint controls local bandwidth information, which ensures that the bandwidth of the entire link selected by the ant is greater than the minimum bandwidth required.

The processing of the network link delay is processed by the backward slave. The formula for the pheromone update used in the poster is:

$$\tau ij=(1-k)\tau ij+\Delta\tau ij \tag{8}$$

Where Δτij in the above equation is the updated pheromone and the updated pheromone is:

$$\Delta\tau ij=1/C^{best} \tag{9}$$

3.4 Algorithm implementation steps

The flow chart of the algorithm is shown in Figure 1.

The algorithm is calculated as follows:

Network initialization. We initialize the credit value of each node, in the initial stage because each node has not been data forwarding and processing, firstly, all the node's credit value is set to a relatively low value.

Forward ant exploration stage. When the ant is in a node, according to the routing bandwidth constraints, the next hop node cannot meet the demand of the QOS node exclusion, so it selects a node from the remaining node as a forwarding node.

Calculate the credit value of each node of the next hop node, and select the next hop node according to the probability.

When the ants do not reach the target node before, according to the probability of the next hop node to select the next hop node.

After arriving at the target node, the forward ant becomes a backward ant, updates the pheromone on the current optimal path as well as the pheromone according to the formula in the above section.

Update the global pheromone.

The algorithm is terminated after a limited number of loops have been executed or after the route converges to a fixed route.

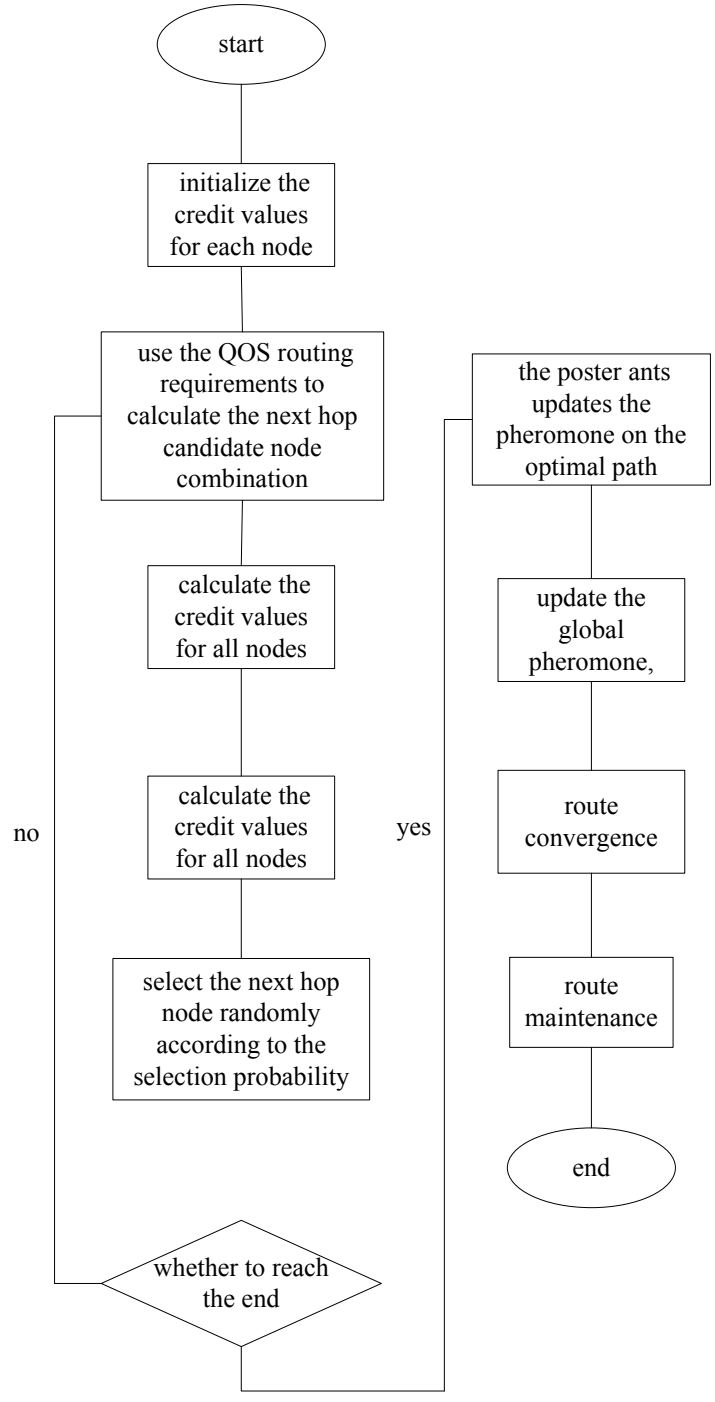

Fig. 1. Algorithm flowchart

4 Results

4.1 Simulation and analysis of algorithm performance

In this paper, we use OMNET ++ 3.2 to simulate the algorithm and the simulation network have 100 nodes. The lifecycle of a network is the lifecycle of a network from deployment to failure to provide the user with perceptual information. In this experiment, the lifecycle is exhausted by half of the energy deployed from the network to the network. The coverage of the network is defined as 100 × 100 units, the energy consumption of energy transmission is 0.002 transmission distance, the initial energy value of the node is 5. At last, the performance of the algorithm is illustrated by comparing with the SPEED protocol.

The following figure shows the graph of the life cycle of the wireless sensor network as the number of malicious nodes in the network changes, and Figure 2 is a malicious node in the communication distance which is five times of the normal node measured under the circumstances:

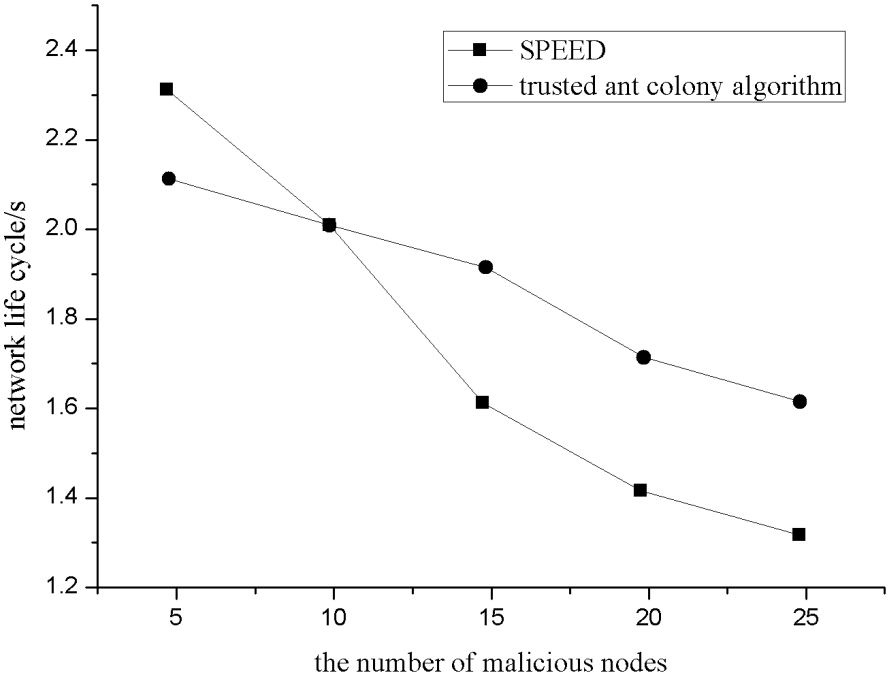

Fig. 2. The network lifecycle changes the number of malicious nodes along the network

As can be seen from the above figure, when the malicious nodes in the network are at a low level, because the improved ant colony algorithm based on the trust model needs to calculate the trust value of the network node as well as the indirect trust value of a node requires the node's common neighbor node to be confirmed, so that the

performance of the network node is less and the SPEED protocol is almost the same. However, with the increase of malicious nodes in the network, because SPEED will continue to send data to the malicious nodes, resulting in the node's energy quickly consumed, as well as after establishing the trust model, the ant colony algorithm based on the trust model will not send the data to the malicious nodes, thus effectively reducing the influence of the malicious nodes and prolonging the network lifetime. As the number of network nodes increases, the number of nodes affected by the network changes, as shown in Figure 3:

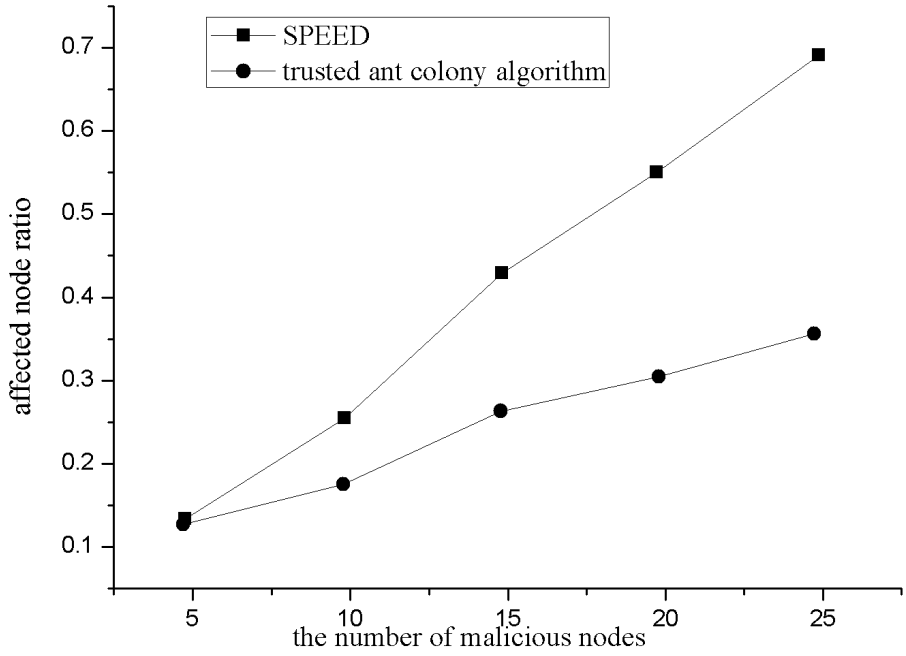

Fig. 3. The change of affected nodes with the number of malicious nodes

The figure shows that the ratio of nodes affected by the network changes as the number of malicious nodes changes. As a result of the information model, the malicious node is no longer used as a forwarding node, the network will converge to the best route, and this will affect the malicious node is controlled in a certain degree. With the increase of the number of malicious nodes, the nodes in the communication node of the SPEED protocol will be affected by the malicious nodes, which lead to the increase of the number of nodes affected by the malicious nodes.

4.2 Algorithm security analysis

Direct malicious behavior refers to the behavior of malicious nodes directly intervening in the network, usually including discarding data bits, changing the data content, changing the packet address, frequently sending the forged number and so on.

Since the credibility is used as a control factor in the system, any direct malicious behavior of the point will result in a decrease in its own trust value. In the DOS attack model, the malicious node will send the request information continuously. Since the node is not authenticated, all the non-authentication request messages will be discarded by the neighbor node.

Sinkholes attack is a more serious attack, which can hinder the base station to obtain a complete and effective information. In general, this attack is the use of the node itself claims that their own electricity sufficient, efficient and reliable, so that other nodes with this node can form a forwarding path. In this protocol, the ant colony algorithm includes forward ants and backward ants, as the ant through the node did not reach the end point, the backward ants are less, and the higher packet loss rate caused by lower credit, so that the convergence of the route to avoid convergence to the route up, so, it effectively avoids the hole attack.

In the Hello flood attack model, a malicious node continually sends a connection request to all neighboring nodes that it can access, thereby consuming the node's resources. The easiest way to prevent Hello attacks is to have valid measures for both parties to communicate. In this protocol, we use the mutual authentication mechanism. Therefore, after receiving the Hello message sent by the malicious node, the regular node sends the authentication request message repeatedly. If there is no authentication reply, the node directly adds the malicious node to the tabu list.

5 Conclusions

The concept of credit is introduced, and the security of the algorithm is improved by using the trust model. Then, the simulation environment and simulation results of the algorithm are discussed, and the simulation results are analyzed. The major part is that an ant colony-based security algorithm that can reduce the influence of malicious nodes by the credit value is proposed, but the influence of nodes still existed, and the algorithm could not resist the witch attack. Therefore, in the next step, the algorithm can be combined with network authentication. The nodes in the network establish a trusted connection through authentication, and the information communication is only carried out on the trusted connection, which focuses on the key distribution of the network and lightweight network authentication energy consumption issues.

6 References

[1] Cheng L, Niu J, Cao J, et al. (2014). QoS Aware Geographic Opportunistic Routing in Wireless Sensor Networks. IEEE Transactions on Parallel & Distributed Systems, 25(7): 1864-1875. https://doi.org/10.1109/TPDS.2013.240

[2] Jing, H.C. (2014).Coverage holes recovery algorithm based on nodes balance distance of underwater wireless sensor network. International Journal on Smart Sensing and Intelligent Systems, 7(4):1890-1907.

[3] Kumar, J., Tripathi, S., & Tiwari, R. K. (2016). A survey on routing protocols for wireless sensor networks using swarm intelligence. International Journal of Internet Technology and Secured Transactions, 6(2): 79-102. https://doi.org/10.1504/IJITST.2016.078574
[4] Mokdad L, Ben-Othman J, Yahya B, et al. (2014). Performance evaluation tools for QoS MAC protocol for wireless sensor networks. Ad Hoc Networks, 12(1): 86-99. https://doi.org/10.1016/j.adhoc.2012.01.004
[5] Wang, Y., Chen, B., Zhang, D., & Xiong, L. (2016, July). Link weights-based ANT colony routing algorithm for wireless sensor networks. In Control Science and Systems Engineering (ICCSSE), 2016 2nd International Conference on (pp. 29-32). IEEE. https://doi.org/10.1109/ccsse.2016.7784346
[6] Lee S K, Koh J G, Jung C R. (2014). An Energy-Efficient QoS-aware Routing Algorithm for Wireless Multimedia Sensor Networks. International Journal of Multimedia & Ubiquitous Engineering, 9(2): 245-252. https://doi.org/10.14257/ijmue.2014.9.2.24
[7] Eiza, M. H., Owens, T., & Ni, Q. (2016). Secure and robust multi-constrained QoS aware routing algorithm for VANETs. IEEE Transactions on Dependable and Secure Computing, 13(1): 32-45. https://doi.org/10.1109/TDSC.2014.2382602
[8] Shao X, Wang C X, Rao Y. (2015). Network Coding Aware QoS Routing for Wireless Sensor Network. 10: 24-32.
[9] Younis M, Akkaya K, Youssef M. (2015). Handling QoS Traffic in Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications, 28(7): 1105-1115.

7 Author

Xiaoqing Yang is with Henan Technical College Of Construction, Henan, China (cfy8686@163.com).

Article submitted 12 June 2017. Published as resubmitted by the author 15 July 2017.