Design of Trusted Security Routing in Wireless Sensor Networks Based on Quantum Ant Colony Algorithm

https://doi.org/10.3991/ijoe.v13i07.7273

Xiao-bin Shu, Cai-hong Liu, Chun-xia Jiao, Qin Wang
Luohe Vocational College of Food, Luohe, China

Hongfeng Yin (✉)
Beijing JiaoTong University Haibin College, Huanghua, China
csyinhongfeng@126.com

Abstract—To design an effective secure routing of trusted nodes in wireless sensor networks, quantum ant colony algorithm is applied to the design of large-scale wireless sensor network routing. The trustworthy network is used as the pheromone distribution strategy. Then, the pheromone is encoded by the quantum bit. The pheromone is updated by the quantum revolving door, and the energy consumption prediction is carried out to select the path. Finally, the trusted security routing algorithm of the wireless sensor network based on the global energy balance is realized. The quantum ant colony algorithm is superior to the traditional ant colony algorithm in algorithm convergence speed and global optimization. It can balance the energy consumption of the network node and can effectively resist the attacks such as Wormholes. It is very promising to apply the quantum ant colony algorithm to the routing algorithm of large scale wireless sensor networks.

Keywords—wireless sensor network, quantum ant colony algorithm, safe and reliable, routing algorithm

1 Introduction

Because many nodes in wireless sensor networks are distributed densely, messages often reach multi-hop relay nodes. Each node is a potential routing node, which has no fixed infrastructure and is more vulnerable to attacks. The nodes are assumed to be friendly nodes and lack the necessary trust mechanism, and are vulnerable to attacks such as fake nodes. As the wireless sensor network node and network characteristics and energy consumption constraints, leading to wireless sensor network security threats are different from traditional computer networks [1]. We believe that the design principles of WSN (wireless sensor networks) security routing algorithm are as follows: (1) to maintain the global energy load balance of the whole network; (2) to have certain fault tolerance and network self-healing function; (3) application is data centric, routing protocols will continue to be data-based, location-based; (4) it should have a credible security.

Considering the computing power and storage space of wireless sensor nodes are very small, we can design a credible routing algorithm of wireless sensor network based on trusted network, and construct a trusted secure routing algorithm based on quantum ant colony. The algorithm uses energy consumption prediction for path selection, which can effectively balance the global energy consumption of the sensor network. The node reliability is used as the pheromone allocation strategy, which can effectively resist the specific energy consumption attacks of the wireless sensor network, such as Wormholes, so as to improve the security of nodes and construct the trusted network environment.

2 Review

Wireless sensor network is a wireless self-organizing network composed of a large number of sensors with information sensing, data processing and wireless communication capabilities. Compared with the traditional network routing, each node of the wireless sensor network can be a routing node, and the node's energy, computing power and storage capacity are limited. As the wireless sensor network using the micro-battery cannot be replaced, it must be to reduce energy consumption as the primary goal. Because the energy consumption of data transmission is more, therefore, efficient routing algorithm is very important for energy saving [2]. Ant colony optimization (ACO) is especially suitable for wireless sensor networks with dynamic and self-organizing characteristics. Therefore, many researchers apply the basic ant colony algorithm to wireless sensor network routing. However, there are two problems in the application process. First, when the global optimal path is found, all the data will be transmitted along the optimal path, causing the sensor nodes to consume too much energy and cause node death. The second is to find the path will fall into local optimum [3]. The global optimization and fast convergence of quantum computation can solve this problem. Quantum ant colony algorithm is applied to large-scale wireless sensor network routing. Quantum bit coding is used to represent pheromone, and the pheromone is updated by the quantum revolving door, which can speed up the convergence speed and reduce the system complexity to reduce the node energy consumption.

As the wireless sensor network in a large number of nodes are densely distributed, often through multi hop relay messages can arrive at the destination node. Each node is the routing node potential. There is no fixed infrastructure and more vulnerable to attack. The nodes assumed a friendly node and lack the necessary trust mechanism, but also vulnerable to attacks such as fake nodes. Therefore, the wireless sensor network security is an important factor restricting its rapid development. Considering the computing power and storage space of wireless sensor nodes are very small, we can use the trusted network to design a trusted routing algorithm for wireless sensor networks and construct a trusted secure routing algorithm for wireless sensor networks based on quantum ant colony to solve the security problem of wireless sensor networks.

3 Methods

3.1 Quantum ant colony algorithm

Quantum-Inspired Evolutionary Algorithm (QEA) is a recently developed probability evolutionary algorithm based on some concepts and theories of quantum computation. It uses state-of-the-art computer simulation of quantum state representation and quantum rotation gate operation [4]. Compared with the classical evolutionary algorithm (EA), QEA has better population diversity and global optimization ability; the population size is smaller but does not affect the performance of the algorithm. Compared to traditional genetic algorithms in some problems to show better performance, and has been applied in a variety of optimization problems. Based on the theory of quantum computation and evolutionary computation, this paper proposes a quantum ant colony algorithm, in which each ant carries a set of qubits representing the current position information of the ants. First, the probability of selection is constructed based on pheromone intensity and visibility. And then the Q-gate is used to update the ant bit to complete the movement of the ant. The quantum non-gate is used to realize the variation of the position of the ant and increase the diversity of the position. At last, the strength and visibility of the ant colony pheromone are updated according to the position after the movement. The algorithm considers the two probabilities of the qubit as the current position information of ants. When the number of ants is the same, the search space can be doubled. It can solve the problem that ant colony algorithm is easy to fall into local optimum and slow to converge when solving the problem [5].

3.2 The reliability of wireless sensor networks

The main purpose of the attack on WSN is to make the network unable to collect data effectively. False routing information, selective forwarding, Sybil attacks can use data encryption algorithm makes the opponent unable to crack the transfer content, and bidirectional identity authentication system based on public key cryptography, verification of wireless sensor network node legitimacy and monitor the malicious node identity change behavior, so as to improve the security of routing protocols. However, due to the energy-limited and self-organizing network, WSNs cannot replicate the black hole security attacks of Sinkhole, especially Wormhole, which is the energy consumption of rogue nodes. The traditional computer network security technology cannot be copied. Some scholars have proposed the wireless sensor network of the trusted security routing algorithm, analysis shows that the use of collaborative trust can effectively resist Wormhole attack [6].

Trusted secure routing algorithm: The trustworthy security routing algorithm of WSN includes three aspects: definition of node reliability, prediction of energy consumption, and availability of available bandwidth.

1.In the wireless sensor network, $W\_Credibility(a,b)$ is used to represent the degree of reliability of the node b adjacent to the current node a, so as to decide

whether the node b should be chosen in the next hop. The representation is shown in equation (1).

$$W\_Credibility(a,b) = \frac{\alpha}{D} + \frac{\beta}{L} + \lambda E \tag{1}$$

Where, D represents the delay, L represents the packet loss rate, E represents the remaining energy of node b, α, β, λ selection makes the value of delay, packet loss and residual energy between 0~1.

2. In the formula (1), the calculation of the reliability needs to obtain the residual energy of the node b, and the usual method is to carry out the energy consumption prediction. Some scholars use the Markov chain M state simulation node M mode, they first calculate the sensor single-hop communication energy consumption E_{1-hop}: define the state transition probability between nodes P_{ij}, calculate the energy consumption of the node by the probability E_s, the energy consumption of the radio transmitting and receiving E_r, E_R, the antenna radiation energy $E_A = E_0 d^r$, CPU processing energy E_{CPU}. So, it can conclude that:

$$E_{1-hop} = E_0 d^r + E_r + E_R + E_{CPU} \tag{2}$$

And the total energy E_r consumed by the nodes in T time steps is:

$$E_T = \sum_{s=1}^{M} \left(\sum_{t=1}^{T} P_{is}^t \right) \times E_s \tag{3}$$

$$\Delta E = E_T / T \tag{4}$$

The energy consumption rate of each node in each time step is averaged with ΔE to represent the energy consumption of the nodes in the next T time steps, and the residual energy of the neighbor nodes is obtained [7].

3. Trusted nodes need to determine the availability of the current node is enough bandwidth. Because in the wireless sensor network, the sharing channel between the nodes, to determine the effective bandwidth capacity need to consider the transmission of this node and all neighbor nodes. Assuming that the total bandwidth of the channel is B, the current total load of the channel where the node i is located can be simulated by the sum $\sum Bself(j)$ of all the nodes in the transmission range.

Among them, node j is any node within the transmission range of node i. Therefore, the effective bandwidth of nod i is $Bavail(i) = B - \sum Bself(j)$.

Cooperative trust Wormhole attack: For large-scale wireless sensor network partition management method, Wormhole attack is mainly located between two multi-hop nodes, by adding a strong ability to send and receive attack points to achieve relay, so that the original multi-hop two nodes into a single hop. In order to achieve single hop, the remote node will usually increase the power until the energy is prematurely depleted.

According to the energy consumption rate and the available bandwidth, the node can judge the normal energy consumption rate and the available bandwidth, and take an untrustworthy attitude to the abnormal information sent by the attacking node. In the Wormhole attack, because of the energy consumption rate and the available bandwidth between two nodes, the threshold can be resisted by setting the threshold value.

4 Experiment

4.1 Experimental process

Routing algorithm: The specific algorithm of wireless sensor network routing based on quantum ant colony is described as follows.

1. Set the number of ants is n, the size of sensor network space is M_C, the convergence node is i, initialize the pheromone τij, the number of initial iterations $t = 0$, t_{MAX} is the set maximum iteration number, initial shortest path $S_{best} = \infty$. According to the number of ants and the size of the space to determine the size of the region, each ant will be placed in the search area.
2. Calculate the distance d_{ij} of the path S_{ij} to the convergence node i, the visibility function, the pheromone level and the transition probability.
3. The k-th ant chooses the path to the sink node i according to the size of the trustworthiness and records, and releases the pheromone at the same time. The shorter the path, the greater probability the path belongs to the optimal path.
4. Record the optimal solution S_{new} of this iterative process and compare the updated optimal solution S_{best}.
5. Apply the quantum gate rotation rule to update the pheromone on each path.
6. If $t = t + 1(t < t_{MAX})$, go to step 3. If the end condition is satisfied, that is, if the loop numbers $t \geq t_{MAX}$ the loop ends and the iteration is terminated.

7. Output optimal solution S_{best}.

Initialize the pheromone: There are n ants in the ant colony. Each ant carries m qubits. In wireless sensor networks, all possible methods from the source node to the destination node are defined as paths in the quantum ant colony algorithm. There are M_C paths to destination node i, denoted as path $S_{ij}(j=1,2,\cdots,M_C)$.

The population containing n individuals in the t-th generation of the ant colony is $\tau(t)=(\tau_1^t,\tau_2^t,\cdots,\tau_n^t)$, and the initial pheromone τ of the j-th individual is:

$$\tau_j^t=\begin{bmatrix}\tau_{\alpha 1}^t & \tau_{\alpha 2}^t & \cdots & \tau_{\alpha m}^t\\ \tau_{\beta 1}^t & \tau_{\beta 2}^t & \cdots & \tau_{\beta m}^t\end{bmatrix}=\begin{bmatrix}1/\sqrt{2} & 1/\sqrt{2} & \cdots & 1/\sqrt{2}\\ 1/\sqrt{2} & 1/\sqrt{2} & \cdots & 1/\sqrt{2}\end{bmatrix} \tag{5}$$

Among them, the initial iteration times $t=0$, m is the quantum bit number, α, β for the quantum bit of the two probability amplitude, the beginning of α_i, β_i are $1/\sqrt{2}$.

Selection of next hop node: When the ant at the node a chooses the next hop node, firstly, the energy consumption rate and the residual energy E of the neighbor nodes are calculated by the energy consumption prediction method. At the same time, calculate the distance d between nodes as delay D. Then, according to the formula (1), the credibility of the neighbor nodes W_Credibility(a,b) is obtained and compared with itself. If the credibility of W_Credibility(a,b) and its own difference is less than a certain threshold, then it is assumed that the neighbor node is a trusted node. Otherwise, the other neighbor nodes are recomputed until a trusted node is found.

Pheromone update: In QACA, after the n ant completes a search, the updating of each path pheromone is realized by using quantum revolving door. The specific algorithm is shown in formula (6).

$$\begin{bmatrix}\tau_{\alpha i}^{'}\\ \tau_{\beta i}^{'}\end{bmatrix}=\begin{bmatrix}\cos\theta_i & -\sin\theta_i\\ \sin\theta_i & \cos\theta_i\end{bmatrix}\begin{bmatrix}\tau_{\alpha i}\\ \tau_{\beta i}\end{bmatrix} \tag{6}$$

Among them, θ_i is the rotation angle of the i-th qubit, and the size of θ_i is related to the convergence rate of the algorithm.

4.2 Experimental results

In this paper, through the Matlab programming, quantum ant colony algorithm and the traditional ant colony algorithm is simulated and analyzed respectively. In this paper, we choose 50 randomly distributed nodes and realize data fusion in each

transmission process. Here, it is assumed that each node transmits and receives 2000bit data of fixed size. In the range of 50 m × 50 m, the base station is located at (25, 100), and in the range of 100 m × 100 m, the base station is located at (50,200). The parameters of ant colony algorithm are set as α=0.9, ρ=0.95, m=30. The number of simulation experiments is 100. In the experiment, according to the network scale, the network scene area was scaled to keep the node density unchanged.

The network operating cycle is shown in Figure 1. The energy required to establish the routing comparison shown in Figure 2.

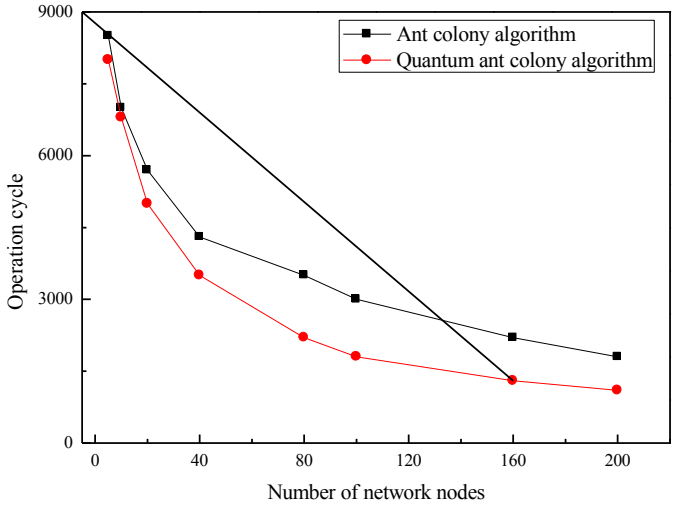

Fig. 1. Comparison of Network Operating Cycle

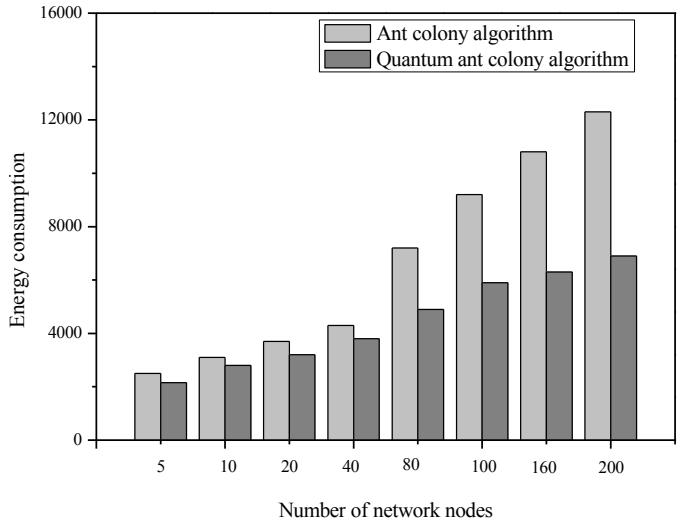

Fig. 2. Comparison of the energy required for route establishment

5 Discussion of the Experimental Results

In the quantum ant colony algorithm, the pheromone released by ants is not sprinkled on the whole path, but scattered in the current residence position of the ants, usually by a set of qubits probability bits to express the current position of the ant. Therefore, it can be used to represent the current pheromone directly, to update the pheromone with the quantum revolving door, and to realize the pheromone variation with the quantum non-gate, thus reducing the system design complexity.

In this paper, the reliability of neighboring nodes W_Credibility (a, b) is introduced. When ants select the next-hop node by node a, the credibility value of the neighbor node is calculated first, and then select the trusted node credibility and its difference is less than a certain threshold as the next hop node. In this case, the delay can be expressed as the distance between the nodes, and the greater the distance, the smaller the credibility. The residual energy of the node is related to the pheromone concentration of the current node. The greater the residual energy is, the less the ant is passed. The smaller the pheromone concentration is, the larger the credibility value is get. In this way, the global energy balance of the sensor network can be ensured. Such a routing mechanism takes into account delay, packet loss and residual energy and other factors. It cannot only establish trustful secure route, but also play the characteristics of quantum ant colony to improve the convergence speed of the sensor network routing algorithm, and avoid the premature convergence of the algorithm, to further balance the global energy consumption. Thus, it should be easy to avoid the premature consumption of energy consumption of a single node, and to improve the overall performance of wireless sensor networks.

It can be seen from Figure 1 that the proposed algorithm is superior to the ant colony algorithm. This is mainly because the proposed algorithm has a better path, no frequent reconstruction path, and fully considered the low energy node, try to balance the energy consumption of the network node, and reduce the probability of partial failure. In order to verify the low power consumption of the proposed algorithm, we make 100 statistics on the energy consumption of the network when the number of nodes is 5, 10, 20, 40, 80, 100, 160, and 200, respectively. When the entire path is established, all the nodes consume the sum of the energy. This is the average energy consumption after 100 simulations. As can be seen from Figure 2, with the increase of network size, this algorithm in the energy loss is less than the ant colony algorithm. Especially when the number of nodes is relatively large, the energy saving effect is more obvious.

6 Conclusion

On the basis of the original ant colony algorithm, the quantum ant colony algorithm is a new quantum evolutionary algorithm, which is combined with quantum computation. On the basis of preserving the self-organization of ant colony algorithm, it has better characteristics of global optimization and fast convergence. Therefore, it is more suitable for large-scale self-organizing network routing design.

The quantum ant colony algorithm is introduced into the routing design of large scale wireless sensor network. It can balance the node energy consumption during the routing process, and avoid the separation of the network due to the premature death of some key nodes. At the same time, considering the security characteristics of sensor networks, and the characteristics of wireless sensor network limited node energy and self-organizing network, it will lead to that wireless sensor network security is threatened, different from the traditional computer networks.

Aiming at the lack of trust mechanism between nodes of wireless sensor networks, and part of the attack is the consumption of node energy. We adopt the idea of trusted network, and consider the trustworthiness of the nodes when the route is established, so as to design a trusted secure routing algorithm based on quantum ant colony. The simulation results show that the proposed algorithm can converge quickly and avoid the premature convergence of wireless sensor network routing algorithms based on quantum ant colony algorithm. And the greater the network size is, the more the effects of the establishment of energy-saving routing are. In addition, resisting Wormhole attack, this kind of wireless sensor network's unique energy black hole attack will help to provide a secure network environment for wireless sensor network, and have certain application prospects.

7 References

[1] Daniel-Ioan, C. (2016). Wireless sensor network security enhancement using directional antennas: state of the art and research challenges. Sensors, 16(4): 488-502. https://doi.org/10.3390/s16040488

[2] Catarinucci, L., Colella, R., Fiore, G. D., Mainetti, L., Mighali, V., & Patrono, L., et al. (2014). A cross-layer approach to minimize the energy consumption in wireless sensor networks. International Journal of Distributed Sensor Networks, 3: 444-447. https://doi.org/10.1155/2014/268284

[3] Long, C. (2014). An improved leach multi-hop routing protocol based on intelligent ant colony algorithm for wireless sensor networks. Journal of Information & Computational Science, 11(8): 2747-2757. https://doi.org/10.12733/jics20103577

[4] Ghosh, B., Chakravarty, D., & Akram, M. W. (2014). Optimisation of digital circuits using quantum ant colony algorithm. Faseb Journal, 11(1): 17-21. https://doi.org/10.7158/e13-029.2014.11.1

[5] Xiao-Hu, H.E. (2016). Application research on quantum ant colony algorithm in grain logistics distribution path optimization. Electronic Design Engineering.

[6] Menaria, V.K., Soni, D., Nagaraju, A., & Jain, S.C. (2014). Secure and energy efficient routing algorithm for wireless sensor networks. International Conference on Contemporary Computing and Informatics (Vol.166, pp.118-123). IEEE. https://doi.org/10.1109/ic3i.2014.7019716

[7] Faghih-Roohi, S., Xie, M., & Ng, K. M. (2014). Accident risk assessment in marine transportation via markov modelling and markov chain monte carlo simulation. Ocean Engineering, 91:363-370. https://doi.org/10.1016/j.oceaneng.2014.09.029

8 Authors

Xiao-bin Shu is with the Department of Computer Science, Luohe Vocational College of Food, Luohe 462300, China.

Cai-hong Liu is with the Department of Computer Science, Luohe Vocational College of Food, Luohe 462300, China.

Chun-xia Jiao is with the Department of Computer Science, Luohe Vocational College of Food, Luohe 462300, China.

Qin Wang is with the Department of Computer Science, Luohe Vocational College of Food, Luohe 462300, China.

Hongfeng Yin (corresponding author) is with the Department of Computer Science, Beijing JiaoTong University Haibin College, Huanghua, 061199, China (csyinhongfeng@126.com).

Article submitted 11 June 2017. Published as resubmitted by the authors 15 July 2017.