The Topology of a Wireless Sensor Network Based on the Perception Needs of Internet of Things

https://doi.org/10.3991/ijoe.v14i02.8200

Yuanjun Wu
Anhui Finance & Trade Vocational College, Anhui, China
wuyuanjun2146@163.com

Abstract—In order to adapt to the multi network convergence of IoT, this paper summarizes the development status, existing problems and further research priorities of the Internet of Things (IoT) and wireless sensor networks (WSNs). Based on that, a generation method of the energy-saving and intrusion-tolerant self-organizing redundancy cellular architecture wireless sensor network (SORCA-W) topology is proposed to realize the interconnection of multiple sensor networks based on the improvement of the SORCA protocol of the wireless sensor topology. Through this generation method, the network can be firstly divided into hexagonal topology network structures according to the location of nodes, then the neighbor node table can be judged and modified by collection of other network nodes and the network name can be added, so that multiple WSNs can be connected for communication to complete the multi-network integration in the perception layer of IoT.

Keywords—Internet of Things; wireless sensor networks; perceptual requirements; topology

1 Introduction

The IoT, an integration of existing networks [1-2], is a ubiquitous network built on the Internet. It is growing along with the progress of various networks, especially the improvement on the process of the wireless sensor originals. WSNs are the most important part of the IoT [3] and an essential composition of the perception layer of the IoT. The functions of wireless sensor nodes become more diverse with the development of science and technology. Different perception nodes can perceive the information that people need and transfer it to the terminal applications timely and stably, which is a further expansion of the original network and a critical material foundation for the development of the IoT [4]. Security issues of WSNs will be more prominent under the growth of the IoT. The major problems and concerns are as follows: firstly, the existing security technologies fail to meet the requirement of multi-network integration of the IoT; secondly, how to avoid the impact of the newly-added nodes on other networks; thirdly, how to identify different network nodes and how to cooperate; fourthly, whether there are security risks during the message transmission and how to ensure the security of messages in reposting and how to repost messages of

different networks [5-6]. IoT is an expansion of the existing network and new problems, as mentioned above, will emerge in the process of network integration. These problems will directly affect the security and stability of the network. Only protocols that conform to the needs of IoT and guarantee the security and reliability of WSNs can tackle these problems. Hence how to design a new topology and routing protocol to solve the security problems of WSNs in the IoT is of great significance.

This paper briefly introduces the IoT and WSNs, summarizes the current research results, points out the existing problems, and puts forward new requirements for the IOT on WSNs. What's more, the network topology is improved upon previous researches, and an improved SORCA-W topology is proposed to serve the IoT based on the geographical location. Finally, the reliability and superiority of the improved protocol is verified after conducting the simulation experiments on relevant protocols.

2 State of the art

As the United States Department of Defense initiated the concept of "Smart Dust", the research on WSNs technology started, aiming to monitor actions of enemies without being detected. In 2001, "smart sensor network communication program" was proposed by the United States Army. The program unified the unmanned ammunition system, WSNs and the robotic system for future wars so as to increase the collection ability of a single sensor and thereby upgrade the survival ability of the future tactic system. In 2002, Intel released a "new computing development plan based on micro sensor networks" which mainly mentioned the t trends of micro sensor networks in the future, including their application in the field of medicine, environmental monitoring, forest fire fighting, sea plate and planetary exploration. In the same year, the European Union also put forward a three-year plan, EYES, which mainly engaged in the researches of the WSN framework, node cooperation means, the formulation of network protocols and safety standards. In 2003, the National Science Foundation established a research plan for WSNs, including the detection of toxic chemicals and the biological attack detection as well as the situation of sensor networks under different environments.

At present, there are three types of topology generation algorithms for WSNs, including the hierarchical topology generation method, the energy-saving topology generation method with power control, and the topology generation by redundantly enhancing the network life cycle [7]. The first one is the hierarchical structure. The nodes of WSNs are networked in a self-organizing way, the topology generation is very complex with various data transmission means. Therefore, the network structure can be simplified by clustering, which composes a local network by the nodes in a certain range through the algorithm of one node and then to elect a cluster head node. The selected cluster head node controls other nodes for data collection and forwarding, and non-cluster head nodes are often in a dormant state, waiting for notification of the cluster head node. With the good scalability of clustering topology algorithm, new nodes can be easily added to the existing networks. Most of the WSN topology is based on clustering algorithm now. The second one is the power control. Power can

be controlled by optimizing all levels of WSNs and the energy consumption of nodes can be reduced through controlling the transmitting power of nodes.

At present, the WSN geared to IoT is still in the stage of research and exploration and has a series of challenges and needs in information security. The specific requirements are as follows: the first one is the authentication mechanism. It refers to the correct recognition of the true identities of the two sides of the communication. Considering the network security, authentication mechanism can effectively prevent the counterfeit attack and ensure the validity of information, so the authentication of the network layer and perception layer is very necessary. The public key infrastructure (PKI) can be used to realize the accurate judgment of the two sides of trust to accomplish the authentication of the communication parties in IOT. The second one is the password mechanism, which means the two sides of the communication can encrypt and decrypt the data by presetting the rules and keys. The original information cannot be obtained without the key so as to ensure the safety of data and prevent data from being eavesdropped or tampered. In IoT, it can be encrypted by means of end-to-end or node-to-node. Through the end-to-end means, the encrypted way and key are set in advance by the transmitting end and receiving end. This method can only be carried out in the application layer.

To sum up, concerning the characteristics of IoT, an integration of multiple WSNs can realize the data reposting by their mutual cooperation and an improvement in the utilization efficiency of the network. But a single expansion of WSNs scale will cause difficulties in management. Therefore, a new topology is designed here to increase the flexibility and utilization efficiency of the network by connecting multiple WSNs for communication. In regard to the new demands of energy saving and security in the WSN of the perception layer of the IoT, an improvement on the basis of SORCA protocol, the original wireless sensor topology protocol, is made and a generation method of SORCA-W, an energy-saving and intrusion-tolerant network topology, is provided here.

3 Methods

Currently, most of the researches on clustering algorithms in WSNs focus on two aspects: clustering methods and energy saving, while little attention has been paid to the future development trend of IoT. Therefore, in the premise of meeting the needs of specific network services (data security and network coverage), this paper proposes an improved topology algorithm, SORCA-W, to meet the needs of IoT in the future. By a collection of other added network nodes, the neighbor node table can be judged and modified and the network name can be added so that multiple WSNs can be connected for communication.

3.1 Calculation of cluster head number

In the clustering network, for the application requires a coverage of η, several cluster head nodes (assuming the number is k) are needed in each round for detection.

Here, the ratio of the total area covered by k cluster head nodes (repeated coverage is calculated once) to the aggregate monitoring area of ||A|| cannot be less than η. The maximum effective range covered by a single cluster head is $3\sqrt{3}r^2/2$. Thus, the probability of any point a(x, y) within A area not covered by the network cluster head $C_i(1\leq i\leq k)$ can be calculated as follows:

$$P_{a-n\text{cov}ered} = 1-(C_{i-\text{cov}er}/\parallel A\parallel) = 1-3\sqrt{3}r^2/2L^2 \tag{1}$$

Then, the probability $P_{a\text{-covered}}$ of any point a(x,y) in A area covered by at least one cluster head node is equal to the network seamless coverage rate (k refers to the number of cluster head nodes in the area):

$$P_{a-\text{cov}ered} = \eta = 1-P^k_{a-\text{cov}ered} = 1-(1-3\sqrt{3}r^2/2L^2)^k \tag{2}$$

The cluster head number k is:

$$k = [\frac{\ln(1-\eta)}{\ln(1-3\sqrt{3}r^2/2L^2)}] \tag{3}$$

3.2 Selection of cluster head

The cluster head selection is carried out by a distributed algorithm, and each node determines whether it will be a cluster head by computing the probability of competition. In order to realize a uniform energy consumption of nodes, the probability that the node i becomes the cluster head is:

$$P_{i-ch} = \max\left[\frac{k}{N}\times\frac{E_{i-current}}{E_{origin}}, \frac{k}{N}\times\frac{E_{\min}}{E_{origin}}\right] \tag{4}$$

In the above formula, k is determined by formula (3), and the role of k/N is to limit the number of initial cluster head. E_{origin} indicates the initial node energy, $E_{i\text{-current}}$ suggests the current actual node energy, and E_{min} refers to the minimum energy needed for competing the cluster head nodes. E_{min} value is defined as per specific applications and environments, and its existence ensures that the cluster head will not be frequently replaced. When the node energy is less than E_{min}, the node will not participate in the run for the cluster head. What's more, the energy consumption model of the proposed method is the same as the energy consumption model of LEACH. And the energy consumption of transmitting and receiving messages can be calculated by formula (5) and formula (6) respectively.

$$E_{tx}(h,d) = E_{tx-elec}(h)+E_{tx-amp}(h,d) = \begin{cases} hE_{elec}+h\varepsilon_{fs}d^2, d<d_0 \\ hE_{elec}+h\varepsilon_{mp}d^4, d\geq d_0 \end{cases} \tag{5}$$

$$E_{rx}(h) = E_{rx-elec}(h) = hE_{elec} \tag{6}$$

In the above two formulas, ε_{fs} stands for the energy consumption of the multiplex attenuation model, ε_{mp} represents the energy consumption in the free space model, h refers to the data bit of sending or receiving, E_{elec} means energy consumption of wireless transceiver, and d_0 is a constant. As a result, E_{min} can be obtained according to the following formula:

$$E_{\min} = hE_{elec}(N/K-1) + hE_{elec}(N/K) + hE_{elec} + h\varepsilon_{mp}d_{toBS}^4 \tag{7}$$

In formula (7), the energy consumed to aggregate the data is represented by E_{da}. When networking, all nodes run for the cluster head and each node calculates its own competitive probability and location information. Then the final cluster head is selected by the loop judgment. In order to better average node energy consumption, the location of nodes is also considered in the process of cluster head contest, so that the nodes near the grid center are more likely to become cluster heads.

The process of cluster head election is shown in Figure 1.

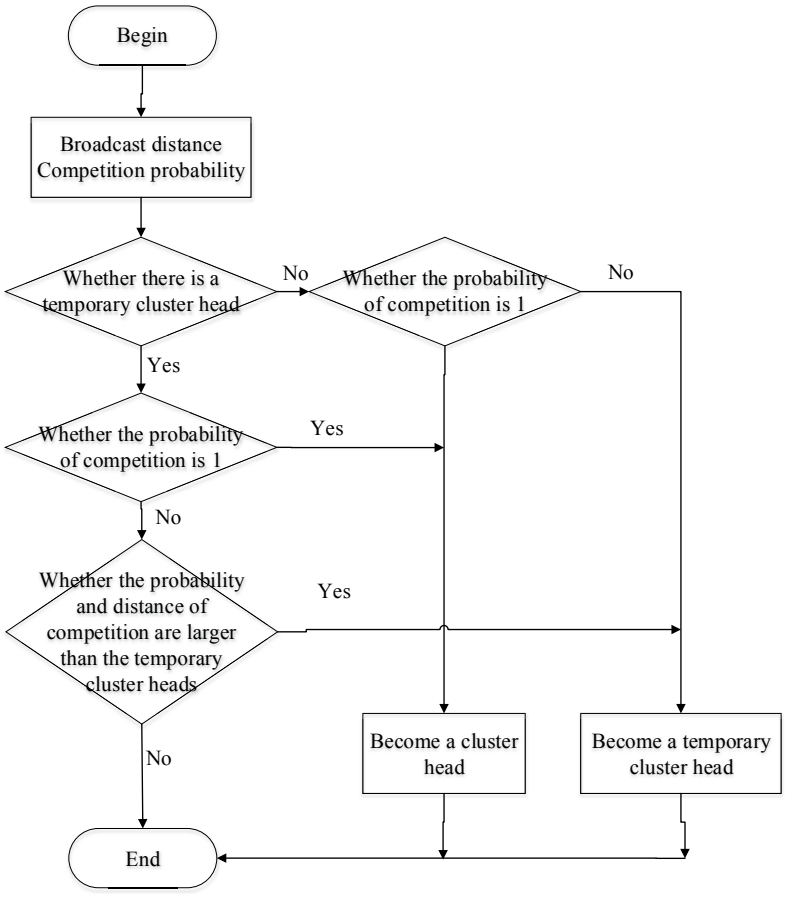

Fig. 1. Process map for cluster head election

At first, node i confirms its location through the GPS and calculates the corresponding $P_{i\text{-}ch}$. At the beginning of the cycle, node i firstly judges whether there is a temporary cluster head: if not, it will become a temporary cluster head; if yes, it will compare its competition probability with the temporary cluster head and broadcast the notification message of being the cluster head when the competitive probability $P_{i\text{-}ch}$ is 1. If $P_{i\text{-}ch}$ is larger than the competitive probability of the temporary cluster head, it will broadcast that it becomes a temporary cluster head [8]; if they are the same, the node in the grid center will be selected as the temporary cluster head; if it is less, no judgment will be made and the node will wait for the broadcast message of the selected cluster head. If the temporary cluster head has not received the broadcast information from other nodes in the grid, it means that it may become a cluster head or the only one in the grid. Then it will send broadcast messages to notify other nodes that it has become their cluster head.

3.3 Generation of topology

After the nodes are arranged in the designated area, the orthohexagonally-leveled topology is organized via the broadcast information by themselves. The process is divided into three stages:

Initialization: each node gets its location information and the information of the neighbor nodes. Each node i prestores the temporary public symmetric key Ks and the key Ki of BSa before the broadcast. The coordinate of BSa is IDbs= (X, Y), and the network name is NAMEa. The node obtains its absolute position IDi= (Xi, Yi) through GPS, and then calculates the relative distance to base station to determine its own RC (the coordinate of grid center). Then via CSMA/CA protocol, Hello message (NAMEa, IDi, IDr, MAC (Ks (IDi)), Ei) is broadcasted with a radius of twofold side length of the hexagon. The IDr refers to the node's RC defined by the conversion with the base station coordinate, IDr= (Xr, Yr) IDr is the central coordinate of the RC and Ei stands for the energy of the node. After the Hello message is approved, the node stores the location information of the neighbor nodes.

Selection of the cluster head: by calculating the competition probability, the node with maximum probability is chosen as the cluster head. If all the probability values are the same, the node closest to IDr will be selected as the cluster head. When the competition is over, the non-cluster heads enter the dormant state and send information to the cluster head at intervals to query whether to be dormant or awakened.

Establishment of RC communication relationship: as shown in Figure 2, this stage is mainly responsible for the identification of different network nodes and the establishment of the communication relationship between the adjacent grids. Each active node i of RC broadcasts Request message (NAMEa, IDi, MAC (Ks (IDi)), Request) to neighbor nodes, and active node j receives the Request message and verifies the authenticity of the content. If it is the same network, the message will join the neighbor table by MAC authentication and if not, no conduct will be made when the node j is not a coordinated cluster head. While if the node j is the coordinated cluster head, it will be determined whether it is in the RC range of the cluster head by calculating the IDi: if it is, then the node sends messages (NAMEb, IDj, IDi, MAC (Kj) (IDj),

NAMEa) to BSb. When node i is confirmed by BSb to be not malicious, then the verification of coordinated cluster head proceeds; if it is not, then the first thing is to check whether the RC of IDi in local neighbor table can be reached or not: when it can be reached, no conduct will be done; if it cannot, IDi will be added in the neighbor table and it will be checked if there is NAMEa network in local RC. Then, the verification of coordinated cluster head will be conducted if the network exists, and the message (NAMEb, IDj, IDi, MAC (Kj (IDj)) NAMEa will be transmitted to BSb for the approval to proceed cluster head negotiation between clusters with the absence of NAMEa.

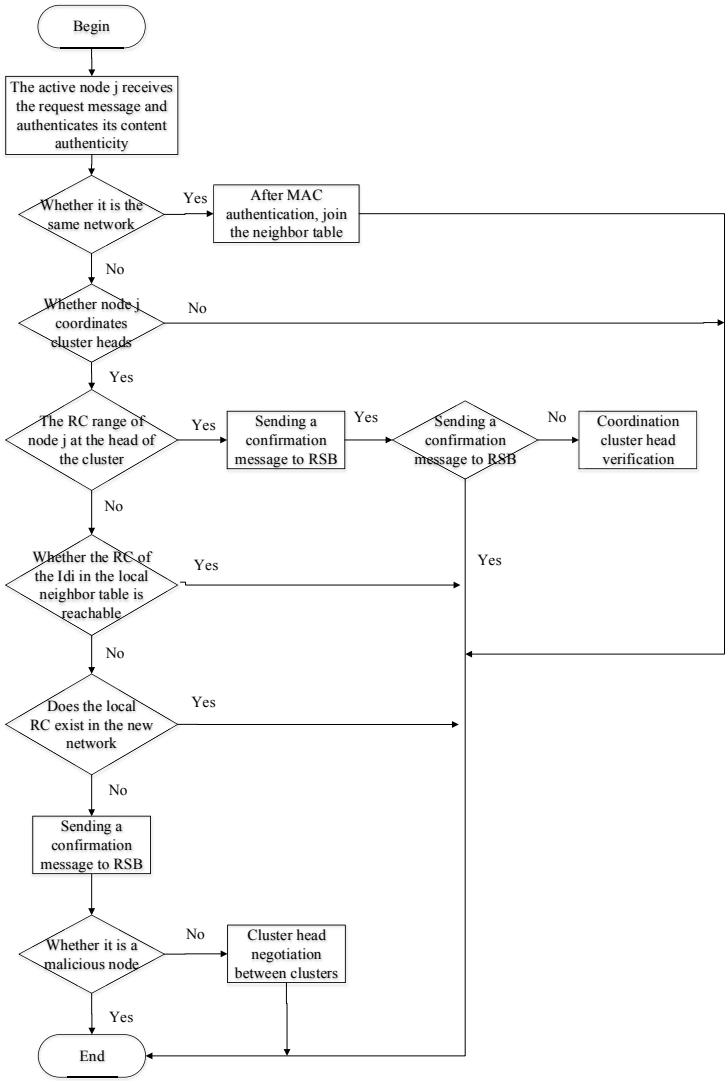

Fig. 2. Communication relationship establishment

Verification of the coordinated cluster: the coordinated cluster j sends the Answer message (NAMEa, IDi, NAMEb, IDj, Answer) to the cluster head node i and node i transmits the message (NAMEa, IDi, IDj, MAC (Ki (IDi)), NAMEb) to BSa for confirmation. If it is confirmed, then a confirmation message (NAMEb, IDj, NAMEb, IDi, Answered) will be sent to the cluster head node j, then the node j will be taken as the coordinated cluster head and be stored in the internal cluster head table.

Negotiation of inter-cluster cluster heads of different networks: the coordinated cluster j sends Answer message (NAMEa, IDi, NAMEb, IDj, Answer) to the cluster head node i, and the node i submits a message to BSa for confirmation. If it is confirmed, a message (NAMEb, IDj, NAMEb, IDi, Answered) will be sent, and each party will join the neighbor RC table [9].

Join of new nodes: every node prestores Blundo polynomials as public keys before broadcasting, and when broadcastsing new nodes, the BS will broadcast message to update public keys. First of all, the new node determines its own RC and then sends a message (NAMEa, IDi, IDr, MAC (Ks (IDi)), Ei) [10,11]. If there is the cluster head of the network within the RC, the new node can join directly and enters the dormant state. When there is no network node in RC, the network can be seen as a new network, then the method is generated with the topology. Substitution of cluster heads: when the energy of the cluster head node is less than the preset threshold value, the node notifies the local nodes within the RC to run for the cluster head. After the campaign, the original cluster head node sends a message to notify the neighbor RC and the local coordinated cluster heads. If the node is a coordinated cluster head, the other cluster heads in the RC will be notified. When the number of the nodes within the network of cluster head node in the RC is less than the threshold value, it will give up being the coordinated cluster head. The first in the local cluster head node table is chosen as the coordinated cluster head, and the cluster head table will be sent to it. It also broadcasts the information of the change of the cluster head, and the coordinated cluster head conducts its verification [12-14].

4 Results

4.1 Feasibility experiment

It is assumed in the experimental scene that 3000 nodes are randomly generated and distributed in 632 RCs on a site of 800*800 square meters. The distribution of nodes is shown in Figure 3 with a node communication radius of 40 meters and a sensing radius of 20 meters. The initial energy of nodes is 100 joules and the base station coordinate is (400 400). The energy attenuation model is the same as that of LEACH protocol introduced in the third chapter.

The condition of energy consumption of WSNs without attacks or different network nodes is primarily taken into consideration. Here, the transmission radius of SORCA-W and SORCA is 20 meters and 40 meters respectively, as shown in Figure 4.

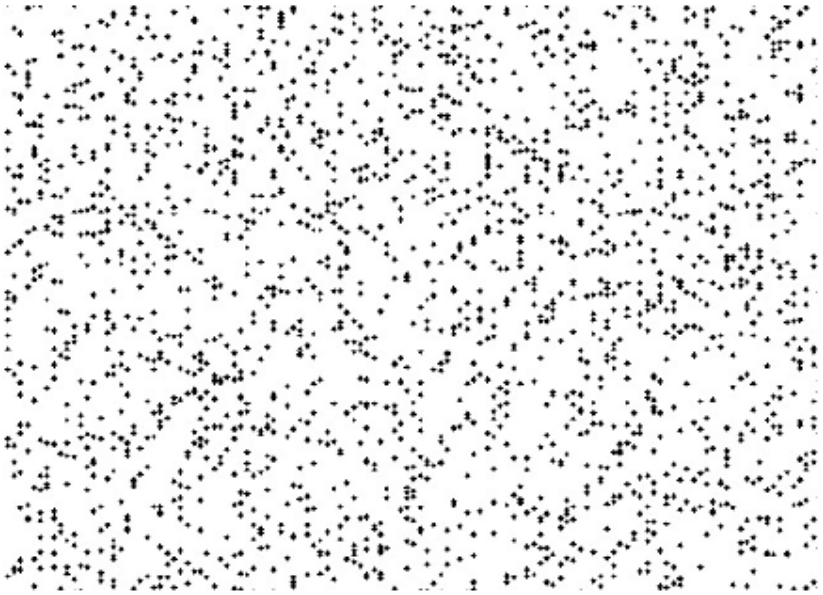

Fig. 3. Node distribution in simulation scene

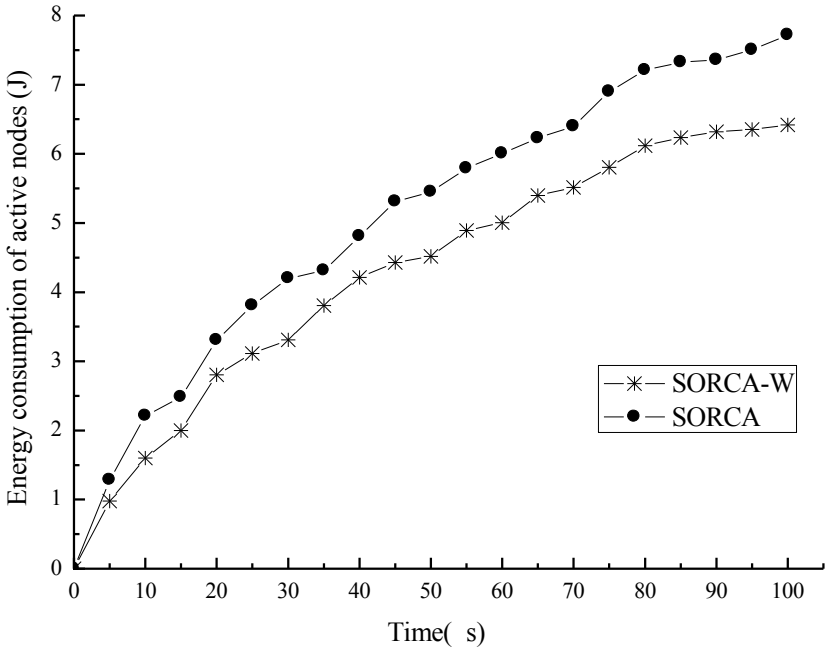

Fig. 4. Comparison of energy consumption in the case of no attack

According to the energy consumption model, it can be seen that when the distance between communication nodes is less than 0d, the energy loss of the sender is directly proportional to the square of the distance; otherwise, it is directly proportional to the biquadrate of the distance. It turns out that a reduction on the radius nodes can save a large amount of energy without affecting the normal communication of the nodes. In the first 20 seconds, because the topology generation needs to carry out massive collection, transmission and verification of data packets, the energy is consumed rapidly. As soon as the topology is formed, the cluster head nodes will remain awake, while other nodes enter dormancy, and the energy consumption is reduced.

4.2 Simulation experiment in multi-network state

The same network is mostly considered in the existing WSN topology methods . For the topology on the integration of different networks, only the sink node is proposed to make transformation when malicious nodes try to access, and the corresponding energy consumption of the network simulation is considered under the simulation condition with only one malicious node attack in which the malicious node sends 100 messages with a length of 1K per second. The energy consumption of nodes with different topology algorithms is collected respectively for comparison. The experiment results are shown in Figure 5.

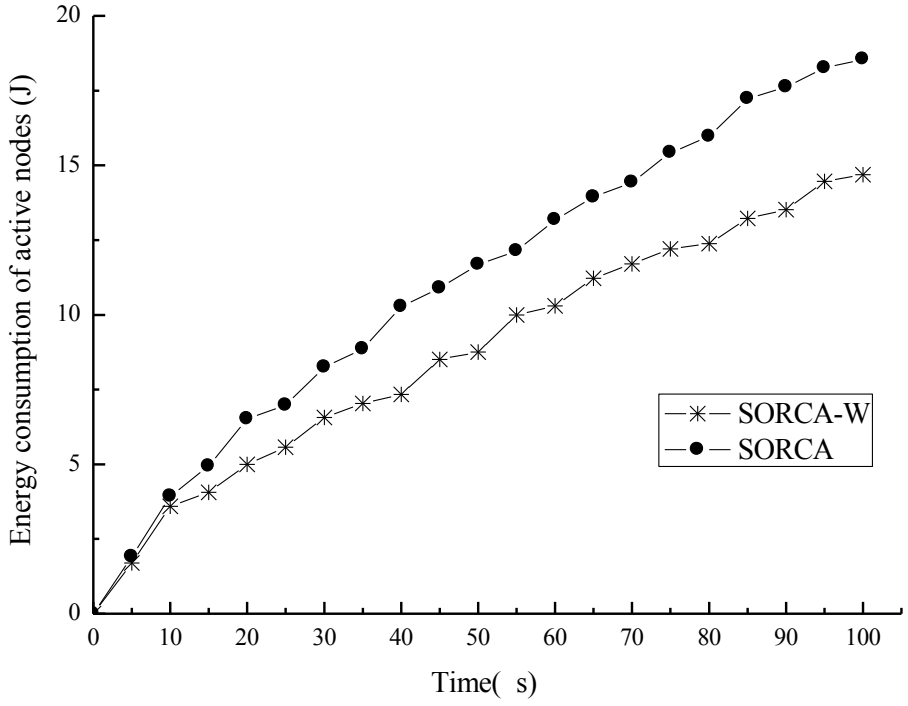

Fig. 5. Energy consumption of nodes with one attack

Compared with Figure 4, it can be known that when some malicious nodes enter the SORCA-W, a lot of energy is consumed in the first 20 seconds. The energy consumption, almost the same with that of SORCA, offsets the energy saved by reducing the emission radius. It turns out that SORCA-W has made no improvement in tackling node energy loss when there are malicious nodes. The reason is that SORCA-W will not directly take the added node as a malicious node as it receives the notification from different network nodes, instead, it will send a request message to the base station for confirmation, which will take a lot of energy and channels. What's more, it will consume lots of time in communication when the base station returns information to each cluster head node. Next, the performance of SORCA-W in multi-network integration is taken into account and the experiment scene is shown in Figure 3. The perceptive radius of the node is 20 meters, the communication radius 40 meters, and the initial energy of the node 100 joules. There are two different networks in the scope with two kinds of evenly distributed network nodes (1:1) and the base station coordinates are (200, 400) and (600, 400) respectively. The results of the experiment are shown in Figure 6.

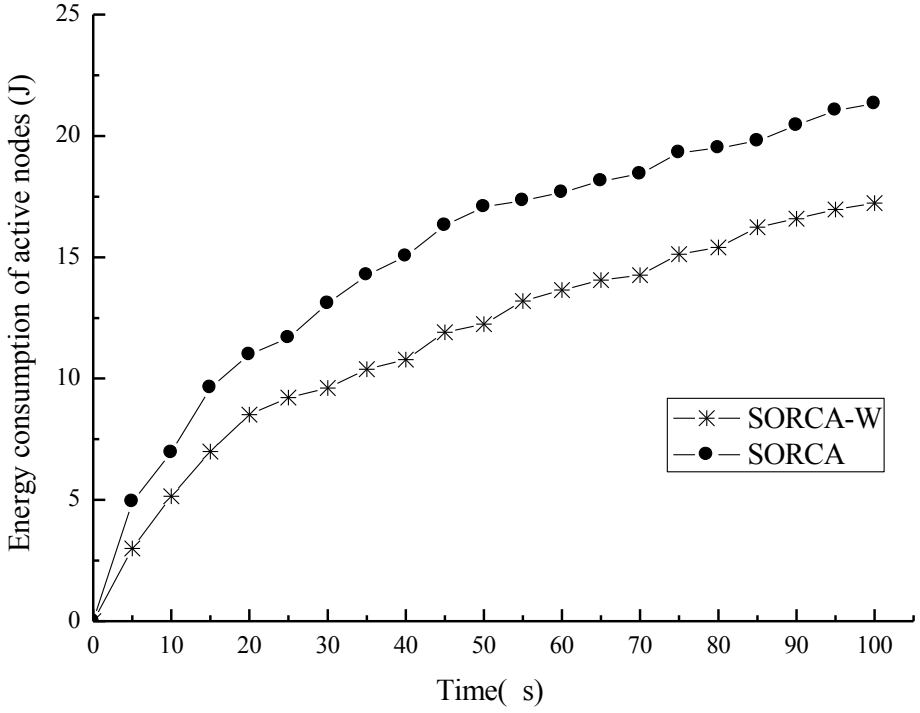

Fig. 6. Energy consumption of nodes with two parallel networks

Figure 6 shows that when the two networks are intersected, the energy consumption of SORCA-W is far below that of the protocol before improvement, and the slope of the first 20 seconds is also much less than that of the previous protocol, indicating that SORCA-W can cluster quickly. It is because that the improved protocol will firstly transmit messages to the base station which will reply with confirmation information after judgment when it receives the HELLO messages from different networks, and then after the network is confirmed to be legitimate, the node then treats the other network node as a legitimate node and can communicate with it normally. While for the protocol before improvement, it is impossible to judge the nodes of other networks. For the isolated nodes, the request message will be sent all the time, which will occupy a large number of channels, leaving no time for dormancy and consume energy dramatically. In the meanwhile, the conflict reduces along with the decrease in transmitting power of the protocol.

5 Conclusion

The IoT is a ubiquitous network built on the Internet. It integrates the existing networks organically and will be the main development trend of computer network in the future.

WSNs are applied widely in military, environmental monitoring, biomedical and other fields for its features and have great development prospects.

The security of the IoT has become a critical concern. The practical value of IoT can be only ensured under secure external and internal conditions. WSNs, being special in nature, face many threats different from the traditional Internet and AdHoc networks. And there are extensive challenges in solving the security problem of WSNs.

The security and robustness of the network topology and routing algorithm will directly affect the availability of the actual network. The attacks on the topology and routing protocols will have great impact on the service quality of the whole network and even result in paralysis.

This paper analyzes the security framework of the IoT and the intrusion-tolerant topology routing of WSNs. The SORCA topology is improved and the SORCA-W algorithm is put forward here. By collecting nodes from other networks, the neighbor node tables are judged and modified and network names are added, so that multiple WSNs can be connected for communication to realize the multi-network convergence in the perception layer of the IoT.

6 Acknowledgment

This work is supported by (1) 2016, the key project of natural science research in Anhui province (KJ2016A010); (2)2017, the natural science major project of Anhui Finance & Trade Vocational College's “connotation improvement and all action plan”.

7 References

[1] Zhou, J., Leppanen, T., Harjula, E., Ylianttila, M., Ojala, T., & Yu, C., et al. (2013). CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing.IEEE, International Conference on Computer Supported Cooperative Work in Design,651-657. https://doi.org/10.1109/CSCWD.2013.6581037

[2] Abidoye, A. P., & Obagbuwa, I. C. (2017). Models for integrating wireless sensor networks into the internet of things.Iet Wireless Sensor Systems,7.3: 65-72. https://doi.org/10.1049/iet-wss.2016.0049

[3] Zhong, D., Lv, H., Han, J., & Wei, Q. (2014). A practical application combining wireless sensor networks and internet of things: safety management system for tower crane groups.Sensors,14.8: 13794-814. https://doi.org/10.3390/s140813794

[4] Ma, J. (2016). Security issues of wireless sensor networks based on target tracking.International Journal of Online Engineering,12.10: 97.

[5] El-Emary, I. M. M., Husain, K. Q., & Alyoubi, B. A. (2012). Security issues of wireless sensor networks in various applications.International Journal of Academic Research,4.6: 317-328. https://doi.org/10.7813/2075-4124.2012/4-6/A.45

[6] Wu, H., & Gao, R. (2013). Delaunay network topology generation algorithm for wireless sensor networks.Sensor Letters,11.6: 1036-1041. https://doi.org/10.1166/sl.2013.2904

[7] Kabir, A. F. M. S., Shorif, M. A., Li, H., & Yu, Q. (2015). A study of secured wireless sensor networks with XBee and Arduino. International Conference on Systems and Informatics. 492-496.

[8] Aguirre E, Lopez-Iturri P, Azpilicueta L, Astrain JJ, Villadangos J, & Falcone F. (2015). Analysis of wireless sensor network topology and estimation of optimal network deployment by deterministic radio channel characterization. Sensors (Basel, Switzerland), 15.2:3766.

[9] Hao, X. C., Wang, M. Q., Hou, S., Gong, Q. Q., & Liu, B. (2015). Distributed topology control and channel allocation algorithm for energy efficiency in wireless sensor network: from a game perspective. Wireless Personal Communications An International Journal, 80.4:1557-1577. https://doi.org/10.1007/s11277-014-2100-9

[10] Gao, Teng, et al. (2016). An overview of performance trade-off mechanisms in routing protocol for green wireless sensor networks. Wireless Networks 22.1: 135-157. https://doi.org/10.1007/s11276-015-0960-x

[11] Kanwar, Neeraj, et al. (2017). Simultaneous allocation of distributed energy resource using improved particle swarm optimization." Applied Energy 185: 1684-1693. https://doi.org/10.1016/j.apenergy.2016.01.093

[12] Thakkar, A., & Kotecha, K. (2014). Cluster head election for energy and delay constraint applications of wireless sensor network. IEEE sensors Journal, 14.8: 2658-2664. https://doi.org/10.1109/JSEN.2014.2312549

[13] Jung, K., Lee, J. Y., & Jeong, H. Y. (2017). Improving adaptive cluster head selection of teen protocol using fuzzy logic for WMSN. Multimedia Tools and Applications, 76.17: 18175-18190. https://doi.org/10.1007/s11042-016-4190-8

[14] Jia, D., Zhu, H., Zou, S., & Hu, P. (2016). Dynamic cluster head selection method for wireless sensor network. IEEE Sensors Journal, 16.8: 2746-2754. https://doi.org/10.1109/JSEN.2015.2512322

8 Author

Yuanjun Wu is from Anhui Finance & Trade Vocational College, Anhui, China (wuyuanjun2146@163.com). His research interests lie at the application of the Internet of Things.

Article submitted 05 January 2018. Final acceptance 25 January 2018. Final version published as submitted by the author.