Journal of Software Engineering

ISSN 1819-4311

Academic Journals Inc.

www.academicjournals.com

Journal of Software Engineering 10 (1): 163-169, 2016
ISSN 1819-4311 / DOI: 10.3923/jse.2016.163.169

A Security Assessment Architecture of WSNs Based on Energy Detection

[1]Feng Shen and [2]KaiPeng
[1]College of Information and Network Engineering, Anhui Science and Technology University, Fengyang, China
[2]College of Engineering, Huaqiao University, Quanzhou, China

Corresponding Author: Feng Shen, College of Information and Network Engineering, Anhui Science and Technology University, China

ABSTRACT

As the core of Internet of Things (IoT), Wireless Sensor Networks (WSNs) have received widespread concerned and widely used for different scenes. However, WSNs usually consist of nodes with limited energy; moreover, it is not possible to supply additional energy. Furthermore, insecure network nodes will increase the overall energy consumption and thus, how to effectively and accurately evaluate whether the status of the node is security or not becomes much more paramount. In this study, we propose anew security assessment architecture of WSNs based on energy detection. Compared with the previous one, our method is energy-efficient. The main contributions are as follows. On the one hand, the energy information of nodes in our architecture is being transferred to the cluster-header and then the security assessment method is only performed by the cluster-header, therefore, it not only reduces the transmission cost and network delay but also reduces the calculation times of each node. On the other hand, we introduce the Euclidean distance method for the security assessment and then divide the state of nodes into two sections according to the normalized result, thus it reduces the cost of further determine. Furthermore, although, different sensors differ from the detailed energy parameters, we give the generic value of security section by extended analysis.

Key words: WSNs, energy detection, security assessment

INTRODUCTION

With the development of wireless communication and sensor technology, as the core of Internet of Things (IoT), Wireless Sensor Networks (WSNs) received widely concerned (Qian and Wang, 2013). In addition, due to the characters of self-configuration, quick deployment and strong concealment, the WSNs are widely used for a variety of everyday services, such as; temperature and humidity collecting system and intelligent transportation systems. However, the WSNs usually consist of nodes with limited energy; moreover, it is not possible to supply additional energy. Many researchers (Alrajeh *et al*., 2013; Cai *et al*., 2009; Cao *et al*., 2013; Chehri and Mouftah, 2010; Chipara *et al*., 2006; Dong *et al*., 2013; Pantazis *et al*., 2013) are engaged in the research on how to reduce the energy consumption as, the energy management directly impacts the network life-time while a few of them focus on whether the state of the node is security or not. Furthermore, insecure network nodes in WSNs will increase the overall energy consumption and thereby reducing the life of the network and thus, whether the status of the node is security or not becomes much more paramount.

In order to evaluate the status of nodes, we should firstly detect and obtain the energy information accurately. In general, the main energy detection method (Cheng *et al*., 2009) can be divided into two categories; the software detection method and the hardware one. The main idea of the software method is to calculate the remaining charge of a node by detecting changes in signal strength while the latter one is to calculate the energy consumption according to the supply voltage and current monitoring model. After that, we can evaluate the status of nodes based on the giving energy information. A trust evaluation method of sensors based on energy monitoring was proposed by Fan *et al*. (2013). Firstly, they establish an energy monitoring mechanism of wireless sensors. Secondly, they use the correlation coefficient method to calculate the data of energy monitoring and conclude the trust metric of sensors. All in all, this method indeed gets good results but the efficiency can be improved. Based on the previous one, in this study, we propose a new security assessment architecture of WSNs. In our architecture, the energy information of each node is only transmitted to the cluster-header instead of the base station in a certain interval and then the security assessment algorithm is executed by the cluster-header. The method mainly consists of two main aspects. For one thing, we use two vectors for the storage of the actual energy and the theoretical energy. For another, we introduce the Euclidean distance method for the security assessment. According to the calculation result by the introduction of normalized method, we divide the state of nodes into two sections; the security section and the insecurity one. In particular, although different sensors differ from the detailed energy parameters, we give the generic security range by extended analysis. Compared with the previous one (Fan *et al*., 2013), our architecture is energy-efficient. The main improvements are as follows. On the one hand, the energy information of nodes is only transferred to the cluster-header rather than to the base station, therefore, it reduces the transmission cost and network delay. On the other hand, the security assessment method is only performed on the cluster-header and this not only reduces the calculation times of each node but also reduces the energy consumption caused by the calculation.

We briefly introduce the node energy detection method in this section, which is the basic for our study.

Energy detection method: Generally speaking, the main energy detection method can be classified into two categories, the software detection method and the hardware one. The basic idea of the software method is as follows. The signal message in WSNs is send by the internal RF chip while the RF chip is also the maximum power consumption device of WSNs. In addition while the signal intensity of the transmitted RF chip is associated with its own power. Therefore, we can estimate the energy consumption and the remaining power of a node according to the change of signal strength. In general, a typical method was observed in (Choongill *et al*., 2003). We can use the following formula for the related calculation:

$$RSSI = 10^{\frac{G_{tf}}{10}} \frac{1.2567 \times 10^4 V_C^2}{(2^{2B})R} \{\frac{1}{N}\sum_{n=0}^{N-1} Y_{IorQ}^2[k,n]\} \quad (1)$$

where, G_{tf} represents the analog gain from the receiving antenna to the ADC, B is the resolution bits of ADC, R expresses the input impedance of ADC. The Vc is the reference voltage of ADC. $Y^2_{iorQ}[k, n]$ is the signal strength's N-th sampled value after AD conversion.

The other one is hardware detection method (Ai *et al*., 2007). The main idea is as follows. As the power of node is related with Emf and thus we can obtain the supply voltage through AD converter and then collect to the micro control unit. As shown in Fig. 1, we can see the core

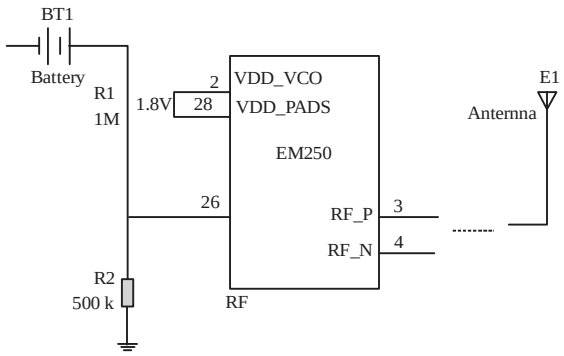

Fig. 1: Construction of hardware energy detection

construction of hardware energy detection. The RF transceiver chip is an integrated RF chip MCU, which contains voltage reference and the output voltage.

MATERIALS AND METHODS

Our method is based on the following theory, the energy of the node will get a significant change when the node affected by external attacks and thus we can evaluate whether the node is security according to the gap between the theoretical value and the actual value and thus, how to calculate the related energy is become very important. In this section, we firstly give the introduction of the node energy consumption calculation formula and then describe our node security assessment method.

Node energy consumption calculation formula: First of all, we discuss how to calculate the theoretical energy and then for the actual energy. We design a reasonable standard function. Let W_s (t) represent the theoretical value of the energy consumption of nodes when the node performs tasks at a certain time. More specifically, W_s (t) can be obtained by the power consumption parameters when a node performing a specific task, which is provided by the manufacturer.

In addition, we use differential method (Fan *et al*., 2013) for the calculation of the actual energy consumption, Let E(t) can be denoted as the remaining energy of node in a certain time.

Let $\Delta E(t_2\text{-}t_1)$ mean the energy consumption of the anytime such as, $[t_1\text{-}t_2]$, then $\triangle E(t_2\text{-}t_1)$ can be expressed as follows:

$$\Delta E(t_2 - t_1) = E(t_2) - E(t_1) \tag{2}$$

When the received information is a piece of remaining energy when the energy information length. In starting time of t_0, assume that receiving remaining energy information, the length of which is t_{packet}. By introducing differential calculation method, we get a time-variable node power function. Let W_n (t) represent the actual value of the energy consumption of nodes. The function can be expressed as follows:

$$W_n(t) = -[E(t)]', t \in [t_0, (t_0 + t_{packet})] \tag{3}$$

Energy assessment method: Once we get the value of theoretical energy and the value of actual energy, we can use the Euclidean distance method for the node security assessment. We determine whether the node is safe or not by comparing the theoretical and actual values. First of all, we show the basic definition of Euclidean distance.

Definition 1: The Euclidean distance (Deza and Deza, 2009).

The Euclidean distance between point p and point q is the length of the line segment connecting them. Euclidean distance can be seen as the similarity between the comparison object. The closer the distance is, the more similar they are. In this study, we mainly consider the distance of two-dimensional space.

In cartesian coordinates, we assume $p = (p_1, p_2,...p_n)$ and $q = (q_1, q_2,...q_n)$ point q, which are two points in Euclidean n-space, then the distance (d) from p-q, (or from q-p) is given by the Pythagorean equation:

$$d(p,q) = d(q,p) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + ... + (q_n - p_n)^2} = \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2} \quad (4)$$

Generally speaking, as the result calculated by Euclidean distance is a number greater than 1 in order to reflect the similarity between the comparison targets, it can be normalized to the range of (0, 1) by using the formula of:

$$\frac{1}{1+d(p,q)} \quad (5)$$

and thus let Sim (q, q) express the normalized result, then:

$$\text{Sim}\ (p,q) = \frac{1}{1+d(p,q)} \quad (6)$$

According to the formula W_s (t) and W_n (t) mentioned in the previous section, we can get the calculation formula of our assessment method:

$$d(E_n) = \sqrt{\left(W_n(t)_i - Ws(t)_i\right)^2} \quad (7)$$

$$\text{Sim}((W_n(t)_i), W_s(t)_i) = \frac{1}{1+d(E_n)_i} \quad (8)$$

RESULTS

In this section, we mainly introduce the working process of our security assessment architecture.

Security assessment architecture: The whole security assessment architecture is shown in Fig. 2. The main process are shown as follows. Firstly, we monitor and obtain the remaining energy of each node and then get the actual energy consumption via differential treatment, as well as, the

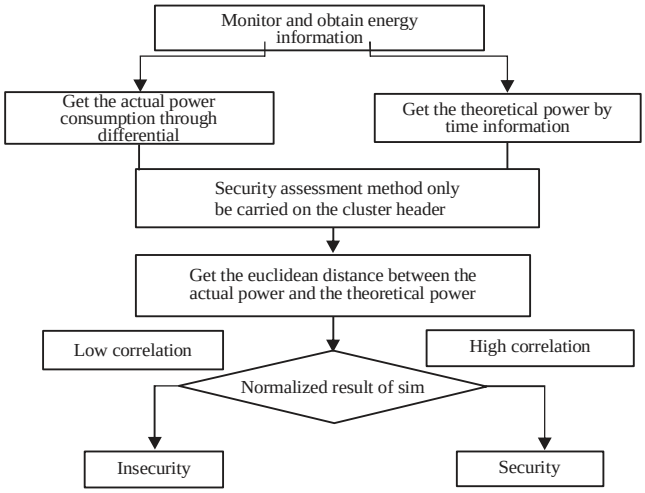

Fig. 2: Node security assessment architecture

theoretical energy by time information and then, each node sends the related energy information to the cluster-header as the algorithm only is carried by the cluster-header. Secondly, we design two vectors for the storage of the actual energy consumption and the theoretical one. Thirdly, we calculate the Euclidean distance between the two vectors and then obtain the normalized result by using the formula. Last but not the least; according to the range of the result, we got the state of the node. Especially, we will discuss how to choose the value for the Sim in the coming section.

DISCUSSION

In this section, we firstly introduce the comparison with the existing research and then discuss how to choose the section value for the Sim in the architecture.

To our best knowledge, from the perspective of security, the existing researches (Ma *et al*., 2008; Reddy, 2009; Agah *et al*., 2005) mainly focus on the Intrusion detection based on game theory. In this article (Ma *et al*., 2008), the security of WSNs is ensured by the intrusion detection system and the system is described as non-cooperative game theory framework. Especially, when opening intrusion detection system is determined by the cluster head in the frame. In addition, zero-sum game theory (Reddy, 2009) was use for solving the security problem in wireless sensors network. Non-cooperative game theory (Agah *et al*., 2005) was used to solve the security problem of wireless sensors. The author established a duo, the non-zero and non-cooperative game model and then obtain the Nash equilibrium strategy and WSN external attacks resistance strategy. All in all, these methods are mainly for the detection of certain attacks, such as Dos attack detection (Reddy, 2009). In addition, only detect attacks have occurred. Compared with these ones, the method in this study is universal as, it evaluate the node status based on the energy information and ignore the types of attack. Moreover, the proposed Markov chain forecasting method for predicting the malicious nodes in wireless sensor networks. However the method only predict the possible malicious nodes in the next round. Compared with this one, our method can evaluate the node status in real time.

Our method was inspired from the trust evaluation method (Fan *et al*., 2013). Compared with the previous one, our architecture can reduce the energy cost. The main improvement are as follows. On one hand, the energy information of nodes in our new architecture is only transferred

to the cluster-header rather than to the base station, therefore, it reduces the transmission cost and network delay. On the other hand, the security assessment method is only performed on the cluster-header and this not only reduces the calculation times of each node but also reduces the energy consumption caused by calculation. All in all, our node energy assessment architecture is effective and energy-saving.

Actually, for different types of sensor, the Sim may be different. Therefore, we will discuss on how to choose the general value for Sim. To make the problem in this issue much more generically, we simplify our discussion by using normalized method. We assume that the value of energy is between (0, 1) and we only discuss the two extreme situations, thus the node is at the border of security and insecurity:

- The best security situation. The actual energy of node got the same value of the theoretical energy. Thus, the Sim will get the value of 1(1/1+0=1)
- The worst one. In a certain time, we got the actual energy of node is 0, while the theoretical one is 1 and thus the Sim will be 0.5 (1/1+1=0.5)

According to the calculation result by the introduction of normalized method, we divide the state of nodes into two sections, the security section (0.5, 1) and the insecurity one (0, 0.5).

Actually, the status of nodes can be divided into work, sleep, standby and etc., the value of energy consumption will be different under each state. Therefore, we should calculate the Sim for different sensors according to the Eq. 7.

CONCLUSION

Wireless Sensor Networks (WSNs) have received widely concerned. However, WSNs usually consist of nodes with limited energy and also insecure network nodes will increase the overall energy consumption and thus, how to effectively and accurately evaluate the status of nodes is become much more important. In this study, we propose a new security assessment architecture of WSNs. Compared with the previous one, we make two improvements. On one hand, the energy information of nodes is being transferred to the cluster-header rather than to the base station; therefore, it reduces the transmission cost and network delay. On the other hand, the security assessment algorithm is only performed by the cluster-header and this reduces the calculation times of each node, so as to reduce the energy consumption of each node caused by calculation. Although, different sensors differ from the detailed energy parameters, we give the generic security range by extended analysis. In our future, we will engage in the energy-saving of a particular application of WSNs.

ACKNOWLEDGMENTS

This study is supported by HuaQiao University Phase III fund to start research projects for attracting talent of in 2014 (No. 14BS316), Quanzhou Science and Technology Project No. 2015Z115, the Cloud Computing Platform for Internet of Things-Fujian Scientific Research Platform for Innovation (No. 2013H2002), National 863 High-tech Project of China under Grant No. 2011AA01A102, Funds for Creative Research Groups of China (60821001) and State Key Lab of Networking and Switching Technology. The PhD Programs Foundation of Ministry of Education (20110005130001).

REFERENCES

Agah, A., K. Basu and S.K. Das, 2005. Preventing DoS attack in sensor networks: A game theoretic approach. Proceedings of the IEEE International Conference on Communications, Volume 5, May 16-20, 2005, Seoul Korea, pp: 3218-3222.

Ai, C.L., F.D. Zhang and R.P. Liu, 2007. Research on energy monitoring method for wireless sensing network. Process Automation Instr., 28: 5-7.

Alrajeh, N.A., S. Khan, J. Lloret and Loo, 2013. Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks. Int. J. Distributed Sensor Networks. 10.1155/2013/374796

Cai, H.B., X.M. Ju and Q.Y. Cao, 2009. Energy prediction and reliable clustering routing protocol for multilevel energy heterogeneous wireless sensor networks. Chinese J. Comp., 32: 2393-2402.

Cao, L.J., X.B. Wen and J.H. Hu, 2013. Energy performance of OOFSK and FSK for wireless sensor networks. Sci. China Inform. Sci., 43: 1065-1078.

Chehri, A. and H. Mouftah, 2010. Energy-aware multi-hop transmission for sensor networks based on adaptive modulation. Proceedings of IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications. October 11-13, 2010, Niagara Falls, Canada, pp: 203-207.

Cheng, X.L., Z.D. Deng and Z.R. Dong, 2009. A model of energy consumption based on characteristic analysis of wireless communication and computation. J. Comp. Res. Dev., 46: 1985-1993.

Chipara, O., Z. He, G. Xing, Q. Chen and X. Wang *et al*., 2006. Real-time power-aware routing in sensor networks. Proceedings of the 14th IEEE International Workshop on Quality of Service, June 19-21, 2006, New Haven, CT., USA., pp: 83-92.

Choongill, Y., L. Hyoungsoo and K. Dongseung, 2003. RSSI Measurements. IEEE C802, 16d-03/92.

Deza, M.M. and E. Deza, 2009. Encyclopedia of Distances. Springer Berlin Heidelberg, USA., Pages: 583.

Dong, R.S., Z.X. Ma, Y.C. Guo and T.L. Gu, 2013. A markov game theory-based energy balance Routing Algorithm. Chin. J. Comp., 36: 1500-1508.

Fan, C.Q., S.G. Wang, Q.B. Sun, H.M. Wang, G.W. Zhang and F.C. Yang, 2013. A trust evaluation method of sensors based on energy monitoring. Acta Electr. Sin., 41: 646-651.

Ma, Y., H. Cao and J. Ma, 2008. The intrusion detection method based on game theory in wireless sensor network. Proceedings of the 1st IEEE International Conference on Ubi-Media Computing, July 31-August 1, 2008, Lanzhou, China, pp: 326-331.

Pantazis, N.A., S.A. Nikolidakis and D.D. Vergados, 2013. Energy-efficient routing protocols in wireless sensor networks: A survey. IEEE Commun. Surv. Tutorials, 15: 551-591.

Qian, Z.H. and Y.J. Wang, 2013. Internet of things-oriented wireless sensor networks review. J. Electron. Inform. Technol., 35: 215-227.

Reddy, Y.B., 2009. A game theory approach to detect malicious nodes in wireless sensor networks. Proceedings of the 3rd International Conference on Sensor Technologies and Applications, June 18-23, 2009, Athens, Glyfada, pp: 462-468.