Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2014, *8*, 67-71 67

Open Access

Research Based on the Trust Value of Wireless Sensor Network Security Evaluation Model

Wu Sijiu[1,*] and Zhang Haiyan[2]

[1]*Chengdu University of Information Technology, Chengdu, 610225, P.R. China;* [2]*Chengdu Aeronautic Vocational and Technical College, Chengdu, 611730, P.R. China*

Abstract: This article defines the importance of trust for the security. Based on the trust value theories and models for WSN, the trust value are calculated for the in-cluster node, the cluster node and the base-station. Then trust value is obtained for whole network. Finally, a Kadir plan for WSN security evaluation is constructed by using the security value and the trust value. It is used for network security evaluation. The simulation demonstrates the effectiveness of the proposed method.

Keywords: Kadir, security evaluation, trust value, WSN.

1. INTRODUCTION

Wireless sensor network (Wireless Sensor Networks, WSN) consists of sensor, data processing and sensor node with wireless communication capability. It can be widely used in fields such as health care, environment, family, and disaster rescue because of its wireless communication and monitoring ability. The applications include such as the U.S. patent 8600560 of method for controlling computer room air conditioning units (CRACs) in data centers [1]; the U.S. patent 8535223 of a system and method for wirelessly monitoring a patient [2]; the U.S. patent 8576063 of a system and method for tracking the position of a moving object [3] and the U.S. patent 8064387 of a wireless-linked remote ecological environment monitoring system [4]. As a result of wireless sensor network hardware resources limited, the solution for security issues has become a difficult problem. Therefore, WSN security issues have become a hot and difficult for the present study.

The effective WSN security evaluation method can promote the WSN viability and improve the system ability to deal with the various attacks of complex environment, but also can be tailored to the specific network threat analysis, and puts forward the effective security solution. The typical examples show a method for authenticating a message in a network provided in the recent US patent 8595504 [5], and a method for secure communications and communication networks with communication devices, using secure means like encryption system for securing communications in the recent US patent 8588411[6].

Currently, the research on security evaluation of WSN mainly focuses the attacks from its inside and outside [7]. This article constructed a security evaluation method by studying the internal attack of WSN and combining with trust value of WSN, so as to achieve the evaluation results.

2. SECURITY AND TRUST OF WIRELESS SENSOR NETWORKS

2.1. Security and Trust Relationship

Rasmusson & Jansson first proposed by hard security and software security. The hard security refers to authentication, access control and other methods to achieve the security of the system. Software security is trust and credibility to ensure the security of system [8]. It is obvious that trust is also a means of security. WSN security trust mechanism provided an effective method for the recognition of internal malicious node, "selfish" behavior.

2.2. Need for Trust

Trust is subjective expectations of the object behavior from the subject, that is, the belief to object. Generally speaking, It is an evaluation of the future behavior of the object evaluated by the subject according to its own experience and the previous behavior records of the object, In the wireless sensor network, it is difficult and expensive to detect for internal attack. At the same time, it may increase the energy consumption of 15% - 25%. If certain trust model established, the security service can be achieved by calculating the trust value of each node and excluding nodes with low trust value [9].

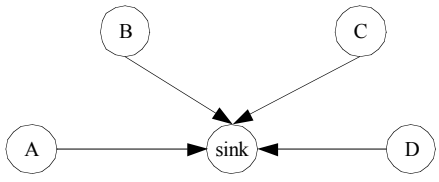

Fig. (1). WSN data fusion.

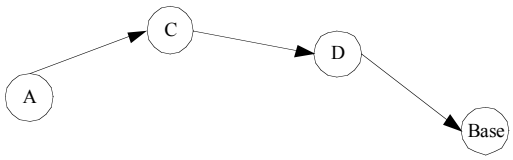

Fig. (2). WSN data forwarding.

1874-110X/14

The data fusion and the packet data forwarding are two key tasks in the hierarchical structure of WSN. The cluster node processes data collected by cluster-inside node. It is shown in Fig. (**1**) as data fusion. The data processed by backbone network, which is composed of various cluster nodes, is forwarded to the base station. This is shown in Fig. (**2**) as data forwarding. For these two types of services, the attacker generally achieves the purpose of attack by means of packet discard, routing trust drop and tampering with the data. By monitoring the packet, it implements security services with excluding the nodes with lower trust degree. It is very easy to identify the behavior of malicious nodes and reduce the trust degree of malicious nodes by the trust expression trust [10]. This shows the WSN security status can be effectively assessed while considering the trust value evaluation factor in the WSN security evaluation.

2.3. Trust Property

The trust properties have been introduced in relevant document literatures [11, 12]. The main properties are summarized as follows:

(1) The trust subjectivity: at the same time and in the same environment, it is possible that there is different trust subjectivity to the same entity from various entities.

(2) The trust dynamics: trust is not always constant. The assessment to credibility of an entity can be changed with one's experience and recommendation and so on.

(3) The trust asymmetry: trust of Node A and Node B can't be represented with each other.

(4) The division of the trust degree: Trust can be indicated by using a qualitative variable, and/or by using a value of 0-1. The trust degree can also be indicated a value of probability.

(5) The association with the trust context: trust is established under certain conditions, and trust is not established while the condition does not exist.

(6) The trust based on past experience: The trust assessment to object can be deal with experience under similar conditions for the entity.

(7) The trust extension by recommendation: It is to assist other assessment subjects to evaluate by the mechanism of transferring recommendation.

(8) The trust transitivity: There are certain conditions for trust transferring. And the trust transitivity is relative to recommendation sources.

3. CALCULATION TRUST VALUE OF WSN

3.1. Calculation Theory and Model

The trust value is an uncertainty estimate to whether or not to perform the action by the subject to the object [13]. The object of belief is indicated by the real number in [0,1]. The bigger real number Indicates the higher belief by the subject to the object, and otherwise. The trust value of cluster-inside node in WSN is obtained from the cluster-inside node [14]. The trust value of cluster node is related to not only the trust value of the cluster-inside node, but the trust value of other cluster node. While the trust value of base stations is related to the trust value of cluster. The trust value calculation model is shown in Fig. (**3**). In which Base represents base stations, CN cluster node, SN cluster-inside node.

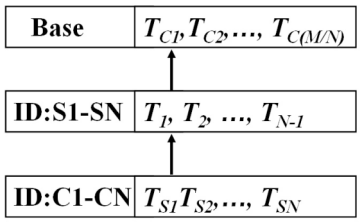

Fig. (3). The trust value calculation model of WSN.

Here, M represents total number of cluster nodes, N for number of nodes of each cluster and T for trust value. T_i means the trust value of an in-cluster node to the cluster node, T_{si}, the trust value of a cluster node to the cluster and T_{ci}, the trust value of base stations to one base stations.

3.2. Calculation for the Trust Value of in-cluster Node

In order to calculate for the trust value of in-cluster node, both telecommunication and its own energy consumption should be considered [15]. Communication capacity is reflected mainly by the historical actions of nodes and the neighbor node evaluation, and energy status mainly for completing data transmission by using its own energy of node, that is, whether less than the threshold value. For one moment, trust relation of the in-cluster nodes mainly consists of direct trust relation and indirect trust relation. The direct trust relation is a kind trust that node A trusts node B to complete the task, while the indirect trust relation refers to trust from node A to node C, which is obtained from trust path of other nodes such as node B [16]. As shown in Fig. (**4**). Having calculated for direct trust value ($T_{I,J}^{dir}$) and indirect trust value, ($T_{I,J}^{Indir}$), the trust value of a node is can be calculated. And the energy trust value can be calculated by comparing available energy with minimum energy. At the end, the trust value of the in-cluster node that is average of two trust value above is obtained.

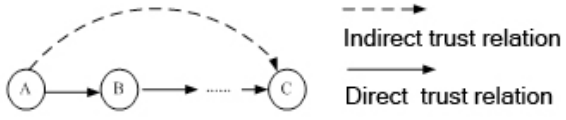

Fig. (4). Direct and indirect trust relation of WSN nodes.

The communication trust value ($T_{I,J}^{c}$) of Node I to Node J is the average of direct trust value and indirect trust value of its own.

$$T_{I,J}^{c} = \left(T_{I,J}^{dir} + T_{I,J}^{indir}\right) / 2 \quad (1)$$

If $T^{e}_{I,J}$ represents the energy trust value of Node I to Node J, E_j, the current energy of node J, then $T^{e}_{I,J}$ is as followed.

$$T^{e}_{I,J} = 1 / E_J / (e_c + e_s) \tag{2}$$

The trust value of Node I to Node J is the average of communication trust value and energy trust value.

$$T_{I,J} = \left(T^{c}_{I,J} + T^{e}_{I,J}\right) / 2 \tag{3}$$

3.3. Calculation for the Trust Value of Cluster Node

In addition to considering both aspects of communication and energy, the following aspects must be considered: number of cluster nodes trusted and the credibility of data fusion to calculate for the trust value of cluster node. The calculation to the communication trust value (T^{c}_{C}) and the energy trust value (T^{e}_{C}) of cluster node is same as that of in-cluster node.

The number of credible nodes in the cluster can be obtained from integrated trust value of the cluster node. Because the table of each node stored the trust values of the other nodes, the trust value of cluster node to In-cluster Node I is:

$$T_{s(i)} = \sum_{j=1}^{N-1} T_{j,i} / N - 2 \tag{4}$$

in which $i = (1,2,...N-1)$ and $T_{i,i} = 0$

The number of trusted nodes in cluster $NumB$ can be obtained by statistical method, then the proportion $NumB/N$ of trusted nodes calculated.

We consider only whether the result is credible after data fusion of cluster nodes. When result after data fusion of cluster node is the same as most part of the data transmitted in the cluster, data fusion plays a role and is credible. The trust value of data fusion T^{r}_{CI} is expressed as:

$$T^{r}_{CI} = S_I - D_I / S_I + D_I \tag{5}$$

In which, S_I represents consistent quantity of data, D_I represents inconsistent quantity of data. From the formula, it is can be seen that trust value of fusion declines rapidly as the inconsistent quantity is bigger.

The trust value of cluster node can be obtained based all above.

$$T_{C(I,J)} = \begin{cases} T^{n}_{C(J)} + T^{c}_{C(I,J)} + T^{e}_{C(I,J)} + T^{r}_{C(J)} & T^{e}_{C(I,J)} \neq 0 \\ 0 & T^{e}_{C(I,J)} = 0 \end{cases} \tag{6}$$

Here, $T^{n}_{C(J)}$ represents the proportion of trusted nodes.

3.4. Calculation for the Trust Value of Base Stations

The trust value of in-cluster node transmitted from cluster node ($T_{C(I)}$) is stored in base stations, each trust value of cluster can be calculated and stored by using trust table of cluster. The base stations updates the trust values of cluster nodes periodically, sends different command for cluster management according to the different trust values. The trust value of cluster node can be calculated by using average method. $T_{C(I)}$ represents the trust values of cluster node, then:

$$T_{C(I)} = \sum_{j=1}^{A-1} T_{C(I,J)} / (A-1) \tag{7}$$

Here, A means the number of clusters.

4. A SECURITY EVALUATION MODEL OF WSN BASED ON THE TRUST VALUE

4.1. Construction of Evaluation Model

A security evaluation model of WSN based on AHP is put forward in reference [1]. Have combined security value with Here and trust value, we recognize and analyze WSN security with Kadir plan in this article.

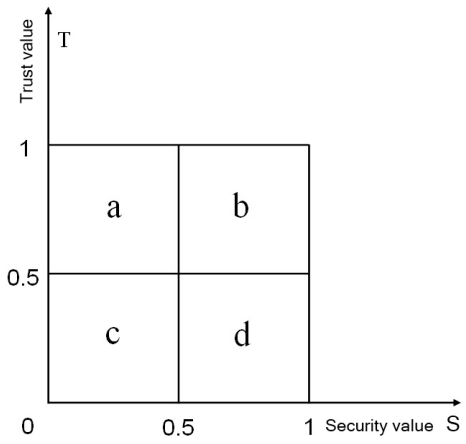

Fig. (5). Kadir plan of WSN security analysis.

As shown in Fig. (**5**), the final results of WSN evaluation can be divided into four areas (a, b, c, d). The less the security value is, the higher security there is. Area a indicates that WSN is secure with high security and trust value. Area d indicates that WSN is not secure with less relative security and trust value. Area b indicates that WSN is not secure because of its external attacks with high trust value and less security. Area c indicates that WSN is not secure because of its internal attacks with less trust value and high security. The diagram of security evaluation of WSN is shown in Fig. (**6**).

4.2. Example Analysis

Appling the trust value security evaluation model, we assume security value of the wireless sensor network (WSN) is

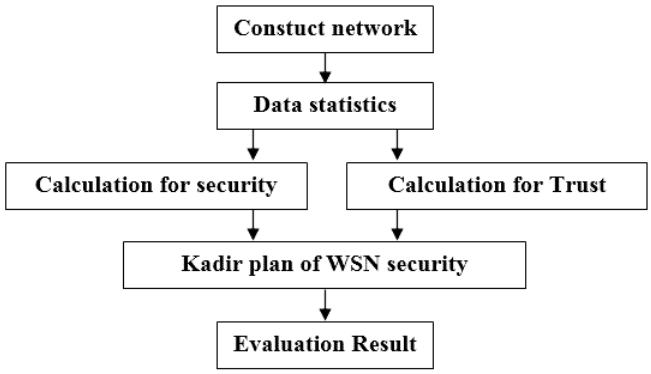

Fig. (6). Diagram of security evaluation of WSN.

S, deploy a certain amount of nodes with internal abnormal behaviors in the WSN, and calculate for the trust value T_{WSN} for the entire WSN by statistics, then we analyze WSN security by using security value. We deploy malicious nodes to test in a scene where there are 100 sensing nodes. Malicious node numbers are following: 5, 10, 20, 40.

4.2.1. Calculation for the Trust Value

Assign initial trust value of 0.5 for each node, after a period of time, we calculate the data preserved in the base stations by statistics. At first, according the trust value preserved in the base stations of cluster of node, we calculate the trust value of base stations T_{base} by means of average of security for base stations. Then we calculate the trust value T_{WSN} of entire WSN by means of average of trust value T_{base} for each base stations. The trust values of WSN T_{WSN} are obtained under different internal attacks. As shown in Fig. (**7**).

4.2.2. The Regional Division and Security Analysis

Assign initial trust value of 0.5 for each node, the same as initial security value. According to the different security requirements, different classification values (trust and security value) can be assigned to WSN. We change the trust value to narrow believable area if the internal attacks are more important, While the security trust value narrow secure area if the external attacks more attentional. As shown in Fig. (**5**).

In the Kadir Plan, the intersection Q can be found at which the security value S and trust value T_{WSN} of WSN intersect, then the area Q located is security evaluation result of the whole WSN. We can not only get WSN security status, but identify for security reasons by studying the area Q located.

Area A: This is a secure area as the trust value and the security value are given. It shows that the WSN evaluated is in complete secure status.

Area B: shows the area is not in secure status as classification values (trust value and the value of security) are given. It shows that the evaluated WSN is in secure status with lower security requirements. And the result of network attacked is caused from the external.

Area C: There are lower security requirements in the area and this area is not very secure. It shows that the evaluated WSN is in a relatively poor security status. And the result of network attacked is caused from the internal.

Area D: It is not very secure in the area. It shows that the evaluated WSN is in a very unsecure status. There may be more than one kind of attacks.

Assume that security value S of WSN is greater than 0.5, the trust value of WSN T_{WSN} can be calculated with the (Fig. **7**). As a result, when the number of malicious nodes is less than 30, the WSN security status in Area A; while the number is greater than 30, the status in the Area C.

Assume that security value S of WSN is less than 0.5, the trust value of WSN T_{WSN} can be calculated with the (Fig. **7**).

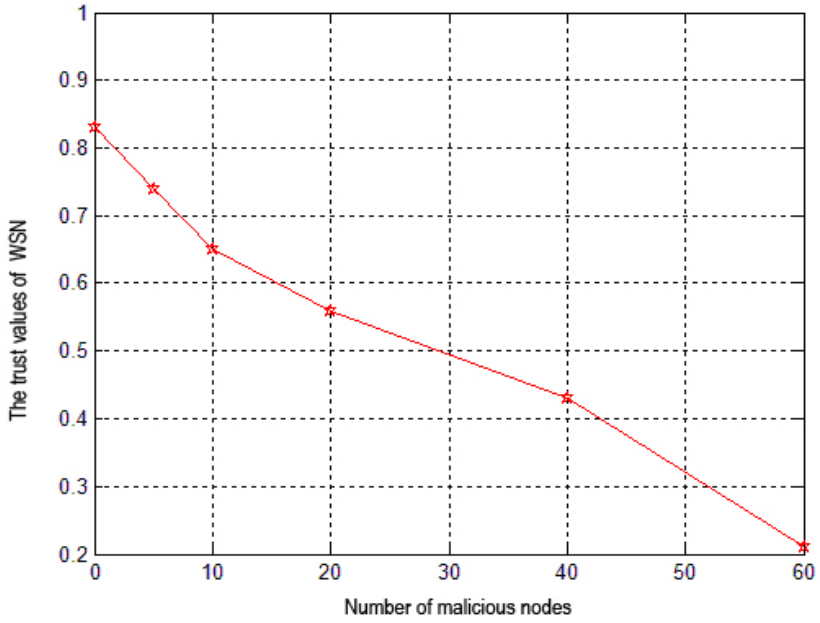

Fig. (7). The change of trust value.

As a result, when the number of malicious nodes is less than 30, the WSN security status in Area B; while the number is greater than 30, the status in the Area D.

5. CURRENT & FUTURE DEVELOPMENTS

A Kadir plan is constructed by the trust value in this article. The internal network attacks can be identified effectively, and the WSN security evaluation carried out with the trust value. The above example proves that internal attack can be identified effectively by the method. It is not the final purpose to evaluate network security. After analyzing the unsecure factors, it is the next target to put forward the effective solution.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] G. Smith, R. Pandey, R. Pfeifer, "Apparatus and method for controlling computer room air conditioning units (CRACs) in data centers " U. S. Patent, 8,600,560, December 3, 2013.

[2] S. Corroy, K. Klabunde, H. Baldus, "Wireless patient monitoring using streaming of medical data with body-coupled communication" U. S. Patent, 8,535,223, September 17, 2013.

[3] J.H. Jo, M.S. Kim, K.S. Kim, J.H. Park, "System and method for tracking position of moving object" U. S. Patent, 8,576,063, November 5, 2013.

[4] J.A. Jiang, E.C. Yang, C.L. Tseng, "Wireless-linked remote ecological environment monitoring system" U.S. Patent, 8,064,387, November 22, 2011.

[5] S.I. Huang and S.P. Shieh, "Light weight authentication and secret retrieval" U. S. Patent, 8,595,504, November 26, 2013.

[6] M. Maas and O.G. Morchon, "Method for secure communication in a network, a communication device, a network and a computer program therefor " U. S. Patent, 8,588,411, November 19, 2013.

[7] F. Rui, C. Xiaofei, Z. Lei, AHP-based wireless sensor network security evaluation model, "*iTAP 2011 International Conference*", Wuhan, 2011, pp. 311-317.

[8] L. Rasmusson and S. Janssen. Simulated Social Control for Secure Internet Commerce. In Catherine Meadows, editor, Proceedings of the 1996 New Security Paradigms Workshop. ACM, 1996.

[9] Dong Hui-hui,Guo Ya-jun, Peng Yun. Grouping and Hierarchical Trust Model in Wireless Sensor Networks. *Computer Engineering*, Vol. 36, No 16, pp. 121-123, 2010.

[10] Q. Yi, Z. Zhaoshu, L. Dan. WSNS routing security assessment model Based on improved BP neural network. *Computer Security*, Vol. 6, No 4, pp. 11-13, 2008.

[11] H. Ming, D. Qiang, Y. Li-miao. Model for evaluating reliability of wireless sensor networks. *Journal of PLA University of Science and Technolog*, Vol. 11, No 4, pp.392-396, 2010.

[12] Y. Bin-yu, L. Fang-yuan, D. Min-jian, Z. Ji-liu, L. Wei. Trust model based on risk eavaluation in wireless sensor networks. *Journal of Central South University*, Vol. 42, No 6, pp.1657-1662, 2011.

[13] H. G, C. D, L. W. A Novel Sensor Node Selection Method Based on Trust for Wireless Sensor Networks, Proceedings of 2007 IEEE WiCom. Shanghai, China: IEEE Press, 2007,p. 1-4.

[14] M. Shouming, W. Ruchuan, and Y. Ning. Secure Data Aggregation Algorithm Based on Reputations Set Pair Analysis in Wireless Sensor Networks. *Journal of Computer Research and Development*, Vol. 48, No 9, pp. 1652-1658, 2011.

[15] W. Liangmin, Wireless sensor network survivability research of theory and technology. Beijing: *The People Post and Telecommunications* Press, 2011.

[16] Z. Yong-zhao, R. Jing-yi, W. Liang-min. Security Evaluation Model of WSN Based on Routing Attack Effect. *Computer Science*, Vol. 37, No 7, pp. 70-73, 2010.

Received: September 22, 2014 Revised: November 30, 2014 Accepted: December 02, 2014