Journal of Theoretical and Applied Information Technology
31 August 2012. Vol. 42 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A ROUTING ATTACK DETECTION METHOD FOR CLUSTER WIRELESS SENSOR NETWORKS

[1,2]SHEN ZIHAO, [1]LIU SHUFEN

[1] College of Computer Science and Technology, Jilin University, ChangChun 130012, China

[2]College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China

E-mail: szh@hpu.edu.cn

ABSTRACT

Wireless sensor networks have been widely used in many applications such as military monitoring, target tracking and surveillance. Security issue is need to more concern. Routing protocol is the core technology of the network layer in wireless sensor networks. Many attackers disrupt the network with routing attack, which will do serious damage to wireless sensor networks. Consider the scare energy and limitation computation capability of sensors, traditional security detection method is not fit for wireless sensor networks. In this paper, we focus on malicious attacks on routing and detection method in wireless sensor networks. We analyze most kinds of attacks and threats on routing, and then propose a routing attack detection method for cluster wireless sensor networks.

Keywords: *Wireless Sensor Networks (WSNs), Routing Attack, Detection Method, Cluster Networks*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of huge amounts of small wireless sensors that communicate with each other in an ad-hoc manner over wireless channels. Wireless sensors have many advantages such as: light weight, small size, low cost, low power, multi functional. Today, wireless sensor networks have been widely used in a variety of applications, such as industrial control[1], environmental monitoring[2], military monitoring[3], home automation[4], health monitoring[5, 6], intelligent agriculture[7], earthquake and weather forecast. In many applications of wireless sensor networks such as military target tracking and surveillance, secure is one of the important issues.

There are two goal of security in wireless sensor networks: one is to protect the transmitted data between all nodes in the network, another is to protect the network itself from being disrupted or altered. It is very important to provide authentic and accurate data to surrounding sensor nodes and to the sink. Routing protocol of the wireless sensor network is the core technology of the network layer, which is responsible for determining the optimal transmission path, providing a reliable and efficient transport for data packets from the source node to the destination node.

Routing protocol should be robustness against false data injected into the network by malicious entities. Secure routing protocol of the wireless sensor network has its own design constraint because of a limited amount of energy, short communication range, low bandwidth, and limited processing and storage in each node.

In this dissertation, we analyze the most typical attacks and threats to routing in wireless sensor networks, and then propose a routing attack detection method for cluster wireless sensor networks.

2. SECURITY THREAT TO ROUTING IN WIRELESS SENSOR NETWORKS

Protocol stack of a wireless sensor network consists of five standard protocol layers [8]: application layer, transport layer, network layer, data link layer, and physical layer. It is vulnerable to threats comparing with wired networks because wireless nodes broadcast their messages to the medium via the unreliable communication channels and unattended operation of wireless sensor networks. Wireless communication is particularly susceptible to eavesdropping and frequency jamming. An adversary can compromise a sensor node and alter the integrity of the data. It not only eavesdrops on messages and injects fake messages, but also wastes network resource. Security threat may occur at any layer in the protocol stack, but the

Journal of Theoretical and Applied Information Technology
31 August 2012. Vol. 42 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attacks toward routing protocols at network layer are more serious.

Routing protocol mainly includes two parts function: determining the optimal transmission path from source node to the destination node and correct transmitting the packets along the path.

Routing protocol of a wireless sensor networks has its own design features such as energy priority, data-center, local information based routing, data fusion at intermediate node, application related routing protocols etc.

Conceptually, the attacks on routing protocol of wireless sensor networks can be listed the following different categories as shown in Figure1: Sybil attack[9, 10], wormhole attack[11], sinkhole attack[12], selective forwarding attack[13], HELLO flood attack, acknowledgement spoofing attack, node replication attack, and local address spoofing attack[14].

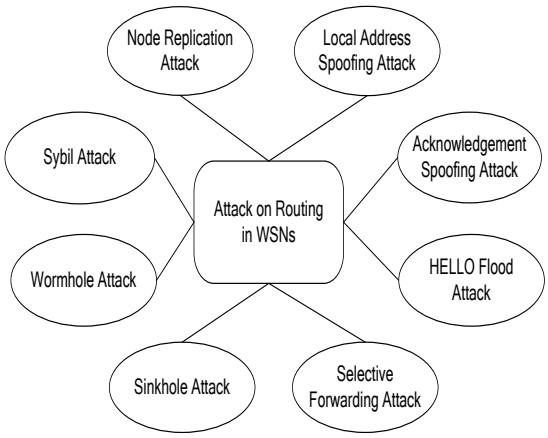

Fig. 1. Attack on Routing in WSNs

(1) Sybil attack

A Sybil attack has a pernicious influence on routing, voting, data aggregation, distributed data storage system and fair resource allocation. In a Sybil attack, an attacker takes on the identity of multiple nodes in its interaction with other sensors. It makes itself at different locations at the same time by announcing different locations, thus route multiple paths through itself.

(2) Wormhole attack

Wormhole is used to connect two distant part of the network with out-of –bound channel. In a wormhole attack, an attacker convince its neighbors itself is in the shortest path to the base station and choose it as the next hop. An attacker can replay packets through wormhole to convince two sensors in a different section of the network that they are neighbors. Wormhole attack can further bring convenience for sinkhole attack and selective forwarding attack.

(3) Sinkhole attack

The purpose of a sinkhole attack is to tempt most the network traffic possible to an attacker from a specific area to pass by the compromised node. It will lead to form an attacker-centered network sinkhole. In general, an attacker would promote itself as being along a high quality and low latency path to the base station so as to try to look more allure than other nodes with respect to the routing algorithm. The result is that the malicious node is elected to route the base station destined packets by most of its neighbor. Sinkhole attack can further bring convenience for other kind attacks such as selective forwarding attack.

(4) Selective forwarding attack

Wireless sensor network adopts a multi-hop routing. Selective forwarding attack means a malicious node determine whether it forwards the received packets or drops them. In order to mount selective forwarding, an attacker ensures itself in the data flow transmission path. In a selective forwarding attack, to achieve more beneficial, an attacker usually drops only some messages rather than all packets to avoid form a black hole, which can be easily detected by its neighboring nodes.

(5) HELLO flood attack

Some routing protocols of wireless sensor networks require each sensor node announce itself to its neighbors by broadcasting the HELLO message. Such message may trick the node receiving them into believing that the broadcasting sensor is within their broadcast range and is their neighbor. So, in a HELLO flood attack, an attacker with powerful transmission capabilities can use a powerful radio to broadcast HELLO message to other sensors even including far more away its normal radio range, then it can flood the whole network. The attacker can rebroadcast overhead message to all sensors to create one way route or wormhole to make these nodes send packets to oblivion.

(6) Acknowledgement spoofing attack

Most of routing algorithm using link layer direct or indirect acknowledgements. In an acknowledgement spoofing attack, an attacker send forged link layer acknowledgement for packets addressed to spoof its neighbor nodes believing that

Journal of Theoretical and Applied Information Technology
31 August 2012. Vol. 42 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the weak link is reliable, or that their dead neighbor node is alive. The result is an attacker lures its neighbor to transmit packet through the weak link and these data packets are lost with high probability.

(7) Node replication attack

Conceptually, a node replication attack means an attacker try to comprise an existing wireless sensor network and copy the node ID of an existing sensor. The attacker has the same legal information as the captured nodes, and then it may engage in destruction activities and severely disrupt the sensor network's performance. It may misroute or tamp with the data packets. So, certain area of the network will be manipulated by the attacker, even the network will be disconnected.

(8) Local address spoofing attack

The most direct attack method against routing protocol is to change the routing information. In a local address spoofing attack, an attacker may disguise itself as the local source or destination sensor to gain unauthorized information or to inject malicious information into the network. To do so, it manipulates the routing information by spoofing, altering, or replaying routing information. By these methods, an attacker may be able to create loops in routing, extend or shorten the path, increase latency, attract or repel the network traffic or generate false error message.

3. A ROUTING ATTACK DETECTION METHOD FOR CLUSTER WIRELESS SENSOR NETWORKS

In wireless sensor network, most routing protocols are designed to ensure the operational functionality and usability but neglect security. This result is that they are vulnerable to a large number of attacks. Network monitoring can detect any misbehavior of the network communications. Usually, when an adversary compromises the network this misbehavior occurs in the network. In wireless sensor network, nodes can be grouped into clusters with cluster heads (CHs) in the clustering hierarchy distribution. These CHs are responsible for forwarding the information from all nodes in the WSN to the base station. There are two types of clustering hierarchy: static clustering and dynamic clustering. During the whole network lifecycle, static clustering select special nodes with special abilities take on CHs, while dynamic clustering select regular sensors that change from time to time work as CHs. In fact, any attacks on the CHs will affect all the sensors in its cluster. So, it is necessary to protect these CHs and detect any attacks that may occur.

In this paper, we propose a method to detect routing attacks that can be used during wireless sensor networks communications. This method has a perfect effect on the clustered wireless sensor networks.

In this method, a sensor node forwards the message including its previous activities to its CHS, and then the CHS sends the special message to the base station. These activities contain the ID of the CH that is responsible for forwarding the previous message from that sensor and the serial number of the message. The base station uses a kind of "activities table" to store all activities in the network. When the base station receives new information, it will compare the new information with the activity table item that it has regarding the activity. If the base station can find the information or find mismatching information, it will assume that there is a problem in the sensor or its previous CH and put the information into a kind of "Suspected Nodes Table". To attain the goal of an efficient reaction to the problem for the base station, it does not take measure until the mismatching or missing information occurs in the "Suspected Nodes Table" more than once. Then, the base station can conclude the node is compromised or there is an intruder and save the node information in the Attacker Table.

This method works as follows (see Figure 2):

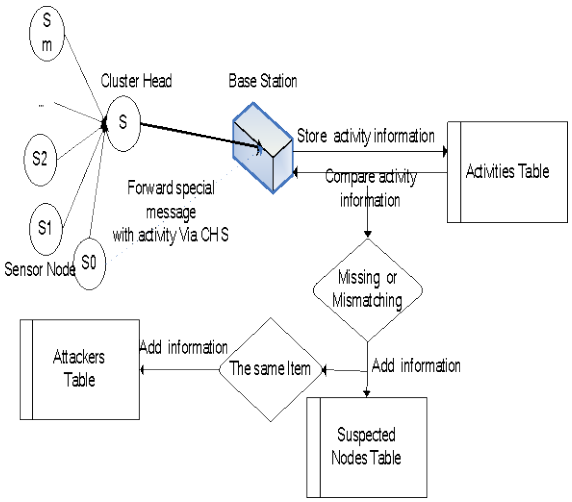

Fig. 2. Routing Attack Detection Method for Cluster Wireless Sensor Networks

(1) Forward the activity information. Sensor node S0 forwards the special message to the base station via the cluster head sensor S. The message

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

includes its previous activity which contains its ID and the ID of its CH and the serial number.

(2) Store the activity and detect the information. First, the base station stores the activity information in the "Activities Table", and then compares it with the table item information that it has regarding the activity. If there are missing or mismatching information, the problem may occur in sensor itself or its previous CH. The base station put it to the "Suspected Nodes Table".

(3) Identify the attack. If the base station finds repeat information mismatching related to the same CH or the same sensor in the "Suspected Nodes Table", it can identify the attack. The sensor node is compromised or is an intruder.

(4) Announce the intrusion information. The base station stores the attacker information in the "Attackers Table" and broadcasts a warning signal to all sensors to neglect future communication with the sensor S0 and terminate or update all the keys that are shared with that sensor.

This method uses communication information with additional activity information to detect any misbehavior in the routing path. Because of there are few additional data overhead, it will not induce more energy consumption. The efficiency of its function has a relation with the proportion of the number of sensors and the CHs. If the CHs is an intruder or it has been compromised, it will forward more messages to the base station in the next round when it has higher number of sensors in its group. This will help the base station to make a quick decision regarding this attack, but will lead to more damage to the network in the specific cycle because the CH connect more sensors. Basing on that, the base station needs to choose a reasonable percentage of CHs and the sensors, which is to be changed during the network lifecycle.

4. CONCLUSION

In this paper, we study the routing security issue of wireless sensor networks. We analyze most of malicious attacks and threats to routing in wireless sensor networks. These attacks can disrupt or alter the routing, which lead to the transmitted data is lose or sensors energy is exhausted. Then, a routing attack detection method for cluster wireless sensor networks is proposed and the method is detailed elaborated. In the future, our work will focus on new security routing algorithm.

REFRENCES:

[1] Fei Hui, Xiang-mo Zhao, Xin Shi, Jiang-yang Zhang, "A multi-interface WSNs based hazardous materials transportation monitoring system", International Journal of Digital Content Technology and its Applications, Advanced Institute of Convergence Information Technology, vol. 6, no. 5, pp. 255-263, 2012.

[2] Victor-M. Sempere-PayaSalvador Santonja-Climent, "Integrated sensor and management system for urban waste water networks and prevention of critical situations", Computers, Environment and Urban Systems, Elsevier Ltd, vol. 36, no. 1, pp. 65-80, 2012.

[3] John Heidemann, Milica StojanovicMichele Zorzi, "Underwater sensor networks: Applications, advances and challenges", Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Royal Society of London, vol. 370, no. 1958, pp. 158-175, 2012.

[4] Sudipta Bhattacharjee, Pramit Roy, Soumalya Ghosh, Sudip Misra, Mohammad S. Obaidat, "Wireless sensor network-based fire detection, alarming, monitoring and prevention system for Bord-and-Pillar coal mines", Journal of Systems and Software, Elsevier Inc., vol. 85, no. 3, pp. 571-581, 2012.

[5] M. J. Chae, H. S. Yoo, J. Y. Kim, M. Y. Cho, "Development of a wireless sensor network system for suspension bridge health monitoring", Automation in Construction, Elsevier, vol. 21, no. 1, pp. 237-252, 2012.

[6] Hyun Jae Baek, Gih Sung Chung, Ko Keun Kwang Suk Park, "A smart health monitoring chair for nonintrusive measurement of biological signals", IEEE Transactions on Information Technology in Biomedicine, Institute of Electrical and Electronics Engineers Inc, vol. 16, no. 1, pp. 150-158, 2012.

[7] Serge Zhuiykov, "Solid-state sensors monitoring parameters of water quality for the next generation of wireless sensor networks", Sensors and Actuators, B: Chemical, Elsevier, vol. 161, no. 1, pp. 1-20, 2012.

[8] Huixian Li, Liaojun PangYumin Wang, "Secure communication protocol based on trust management", Advances in Information Sciences and Service Sciences, Advanced Institute of Convergence Information Technology, vol. 3, no. 11, pp. 248 ~ 255, 2011.

[9] Xiaojiang DuHsiao-Hwa Chen, "Security in wireless sensor networks", IEEE Wireless

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Communications, Institute of Electrical and Electronics Engineers Inc., vol. 15, no. 4, pp. 60-66, 2008.

[10] Shan-Shan Chen, Geng YangSheng-Shou Chen, "LEACH protocol based security mechanism for Sybil attack detection", Tongxin Xuebao/Journal on Communications, Editorial Board of Journal on Communications, vol. 32, no. 8, pp. 143-149, 2011.

[11] Eliana StavrouAndreas Pitsillides, "A survey on secure multipath routing protocols in WSNs", Computer Networks, Elsevier, vol. 54, no. 13, pp. 2215-2238, 2010.

[12] Chao Wang, Guang-Yue HuHuan-Guo Zhang, "Lightweight security architecture design for wireless sensor network", Tongxin Xuebao/Journal on Communications, Editorial Board of Journal on Communications, vol. 33, no. 2, pp. 30-35, 2012.

[13] P. S. Ramesh, F. Emily Manoz PriyaB. Santhi, "Review on security protocols in Wireless Sensor Networks", Journal of Theoretical and Applied Information Technology, Little Lion Scientific, vol. 38, no. 1, pp. 79-82, 2012.

[14] Shen Zihao, Liu Shufen, "Security Threats And Security Policy In Wireless Sensor Networks", AISS: Advances in Information Sciences and Service Sciences, Vol. 4, No. 10, pp. 166 ~ 173, 2012

.