I.J. Wireless and Microwave Technologies **2012, 1, 38-44**
Published Online February 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2012.01.06

Available online at http://www.mecs-press.net/ijwmt

Defense on Split-Network Attack in Wireless Sensor Network

[a]Du Chunlai , [a]hang Jianshun , [a]Ma Li

[a] *College of Information Engineering North China University of Technology Beijing, China*

Abstract

Wireless Sensor Network is an open self-organized network, which faces serious challenge. Whole network can be split up into many separate subnets which cannot communicate with each other because some vital sensor nodes are attacked. A defense scheme which based on frequency hopping and fast network integration was proposed to react against split-network attack. Frequency hopping makes the communication frequency of the network escape from attack frequency while fast network integration makes the separate subnets reintegrate into a whole network in new communication frequency. Simulation results show the proposed scheme significantly reduces the success rate of attack and increases the lifetime of network.

Index Terms: Wireless Sensor Network; split-network attack; frequency hopping; integration

© 2012 Published by MECS Publisher. Selection and/or peer review under responsibility of the Research Association of Modern Education and Computer Science

1. Introduction

When wireless sensor network (WSN) is deployed in a hostile environment, it is important to ensure network connectivity and security. Split-Network Attack (SNA) is to split the whole network into many separate subnets which cannot properly communicate with each other by attacking some vital nodes so that the collected data can not be uploaded to the monitoring center. SNA includes frequency interference attack, denial of service attack and sleep deprivation attack [1, 2]. Frequency interference attack interfere the vital node to receive the legitimate data at the same frequency. Denial of service attack make the vital node has no chance to receive the data from legitimate node. Sleep deprivation attack make vital nodes forward lots of data to exhaust their energy. Result of SNA is emergence of separate subnets. How to reduce the success rate of attack and how to fast reintegrate the separate subnets into a whole network are two questions. A defense scheme which based on frequency hopping and fast network integration was proposed to react against split-network attack. Frequency hopping makes the communication frequency of the network escape from attack frequency while fast network integration makes the separate subnets reintegrate into a whole network in new communication frequency. Simulation results show the proposed scheme significantly reduces the success rate of attack and increases the lifetime of network.

Corresponding author:
E-mail address: zhangjs0322@163.com

The sections were organized as follows. Section Ⅱ shows the related work. Section Ⅲ describes the defense scheme including frequency hopping escape and fast network integration. Section Ⅳ shows the simulations results. Section Ⅴ is the conclusion and future work.

2. Related work

David [3] proposed a framework to mitigate the threats of Sleep deprivation attack, which includes Strong Link-Layer Authentication, Anti-Replay Protection, Jamming Identification and Mitigation and Broadcast Attack Protection. David [4] proposed mechanisms to detect and mitigate the effect of Sleep deprivation attack. Rainer Falk [5] proposed a secure wake-up scheme that entities of holding secret wake-up token can wake up a sleeping sensor node. Matthew [6] proposed three algorithms of cluster dead selection to make it much more difficult for the attacker to become cluster head. These algorithms greatly reduce the impact of the sleep deprivation attack. David [7] proposed a mechanism, Clustered Adaptive Rate Limiting (CARL), based on lightweight intrusion detection techniques to defeat Sleep deprivation attack.

Frequency interference attack is a physical layer attack for WSN. The common strategy against physical layer interference attack is spread spectrum communication. But the low-power, low-cost sensor nodes are usually limited to simple radio transceiver, spread spectrum technology can not directly applied in sensor nodes [8-14]. Aristides[8] introduced several strategies against frequency interference attack, Regulated Transmitted Power, FHSS, DSSS, Hybrid FHSS/DSSS [9], Ultra Wide Band Technology, Antenna Polarization, Directional Transmission. In [8],Aristides emphasized and evaluated the advantages and disadvantages of each strategy, and discussed some open issues about jamming attack. Mario [10] proposed Uncoordinated Frequency Hopping (UFH), a new spread-spectrum anti-jamming technique that does not rely on secret keys. MULEPRO (MULtichannel Exfiltration PROtocol) has been presented in [11]. The protocol is designed to rapidly exfiltrate sensor data from an attacked region to areas of the network that are not under attack. Xu [12-14] researched on radio interference attack and countermeasures.

Denial of service attack[15-17] can also cause paralysis of the vital nodes to form network segmentation.

3. Proposed scheme

Frequency interference attack, denial of service attack and sleep deprivation attack make the some attacked vital nodes lose their abilities of forwarding data, so the whole network can be split up into many separate subnets which cannot communicate with each other. The collected data from sensor node may not be transmitted to the monitoring center due to unconnected wireless signal between attacked vital nodes.

We propose a scheme of frequency hopping escape and fast integration in a new frequency against SNA. Frequency hopping escape includes active escape and passive escape. Active escape which reduces the probability of attackers' finding the communication bandwidth is an active self-protection. It actively adjusts the frequency according to the preset rule. Passive escape hops the frequency according to the affected degree when nodes suffered from malicious attack. The most important of frequency hopping is consistency which includes frequency selection and frequency hopping time. The proper frequency hopping time is more important to ensure consistency and network connectivity. The frequency selection ensures that it is difficult for attackers to capture the selected new frequency.

This scheme consists of evaluation of behavior, negotiation of frequency hopping, synchronization of frequency hopping and integration of network. The following discussion based on clustering topology includes sink node, cluster head node, management node and cluster member node. The management nodes are mainly used for the management of frequency selection and frequency hopping time.

3. 1 Evaluation of nodes' behavior

When nodes receive data packets, they execute the strategy of authenticating the source nodes' ID before forwarding packets. Legitimate packets will be forwarded to destination node. And illegitimate packets will be dropped. Each node analyses the number of illegitimate packets. In the certain period, when the number of

Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality. PHR201007121

illegal packets node has received exceeds the threshold, the followings will be done: a) if the attacked node is the cluster member node, it will send frequency hopping request to its management node; b) if the attacked node is cluster head node, it will send frequency hopping notification to its management node to consult frequency hopping.

Using the confidence interval in statistics to evaluate whether behavior of nodes are abnormal, we assume that each time slice has a counter C to count the number of illegal packet in this time slice. When the time slice ends, the counter C is stored and then cleared to recount. Assuming that the number of time-slice is n, sample values are C_1,C2,…C_n. The confidence interval is the (1):

$$\left[C - (1-\alpha)\frac{S}{\sqrt{2}}, C + (1-\alpha)\frac{S}{\sqrt{2}}\right] \qquad (1)$$

In (1): C denotes sample average, S denotes standard deviation, α denotes significance level. When the number of illegal packet exceeds the threshold, the node will send frequency request to its management node. According to the received request, management node decides whether to start frequency hopping. If cluster head is suffering from attack, it immediately starts hopping consultation. When received the hopping request from cluster member nodes, management node evaluates the risk level, according to ratio of the number of hopping request node in the certain time slice to the total number of the nodes, to determine whether frequency hopping start. If only fewer nodes request frequency hopping, frequency hopping will not be start. When the number of frequency hopping request from cluster member node exceeds the threshold, management nodes start frequency hopping consultation.

3. 2 Negotiation of frequency hopping

When frequency hopping consultation is started, management nodes will negotiate about next communication frequency and frequency hopping time. Consultations between the management nodes use the secret and not commonly used frequency. Thus, communication between the management nodes will not be interfered.

1) *Selection of communication frequency:* Next communication frequency use contribution mechanism described as below.

a) Each management node contributes a random number F_k and broadcast F_k to other management nodes.

b) Each management node receives these random numbers from other management nodes and then calculates the next communication channel F using (2):

$$F=\sum F_k \bmod 16 \qquad (2)$$

c) If the communication channel F is equal with current communication channel, go to a).

2) *Selection of frequency hopping time:* to ensure synchronization of frequency hopping time, The process is described as below.

a) Management node i broadcast its hopping time T_i to other management nodes.

b) Each management node receives hopping time from other management nodes. Each management node calculates the true hopping time T according to the (3):

$$T=(\sum T_i - T_{min} - T_{max})/(n-2) \qquad (3)$$

In (3) T_{min} denotes minimum time, T_{max} denotes maximum time.

3. 3 Synchronization of frequency hopping

When the hopping time arrives, each cluster begins frequency adjustment. Because of unreliability of wireless, synchronization of frequency hopping must be taken into consideration.

Management nodes send frequency hopping notification to its cluster member node, and then cluster member nodes acknowledge the notification. Management nodes according to the received responses determine whether all nodes in the cluster have received notification. If there are some nodes don't acknowledge the notification, management nodes resend the hopping notification within the tolerance. When beyond tolerance, the management nodes deem that those nodes have become dead node due to physical damage or energy depletion . Management nodes will abandon those nodes, and those nodes wait for next round to join the network. When the cluster member nodes received hopping notification, they will forward notification to the neighbor nodes to make up for the unreliability of the link between management nodes and member nodes.

3. 4 Integration of network

There have two meanings about integration of network. One is maintaining the connection of whole network when it is attacked; the other one is integration of network after it was separated into subnets due to SNA.

For the former, WSN implement frequency hopping according to the evaluation of nodes' behavior. For the latter, there are two cases after frequency hopping shown as follows:

a) each node executes the frequency hopping according to the negotiated next frequency and start time, and then communicates with each other.

b) some nodes do not execute frequency hopping. If nodes have a good performance on section Ⅲ.C, the success rate of SNA is little. Taking into account wireless network congestion, time delay and packet loss, the member nodes may be not receives the frequency hopping notification all along. So after the frequency hopping network will form temporary separate subnets. The solution is described as follows.

a) The separated nodes first wait for a time slice to check whether there is arrival of delayed hopping notification. If there is arrival of notification, the node executes frequency hopping immediately;

b) If there no notification arrives all along, the node will select a frequency one by one from the communication channel pool in local to match the communication frequency. If the frequency is successful to be matched, the nodes communicate each other;

c) If the two solutions above are not feasible, the node will join the network as a new member of network.

4. Simulation and Analysis

4. 1 Simulation parameters

Experimental environment is Fedora12 and NS2.34. Main parameters of simulation scenarios: Topology of the network is in the range of 200 * 200 square regions. 20 nodes are laid randomly and kept still. IEEE802.11 protocol is used as MAC protocol. CBR is used to generate network traffic. There are three clusters in the scene shown in Fig. 1. The nodes, 4, 8 and 11, are the cluster head node. The nodes, 5, 6 and 9, are management node. The nodes, 0 and 1, are malicious node. The other nodes are the cluster member nodes.

4. 2 Simulation results and Analysis

1) Jitter Analysis: Network traffic is relatively small when WSN is not under attack, so the network has lower jitter. When sensor network is under attack, network traffic is sharply increased and the network has higher jitter. Fig. 2 shows jitter under attack, jitter after frequency hopping and routine jitter. In Fig. 2, abscissa denotes the number of packets and ordinate denotes jitter, "+" denotes jitter under attack, "×" denotes jitter after frequency hopping and "-" denotes routine jitter. Simulation shows the scheme effectively defends against SNA, and it makes the network rapid escaping from communication channel interference and reduces the success ratio of SNA.

2) Delay Analysis: In Fig. 3, ordinate denotes delay after frequency hopping and abscissa denotes time step. When network traffic increases, it must lead to channel competition and will have significant transmission delay. The delay after hopping is less than delay under attack.

3) Packet loss Analysis: Attacker launches SNA and then causes packet loss. The rate of packet loss under these attacks is larger than not under attack. By means of the defense scheme on SNA, the rate of packet loss is normal.

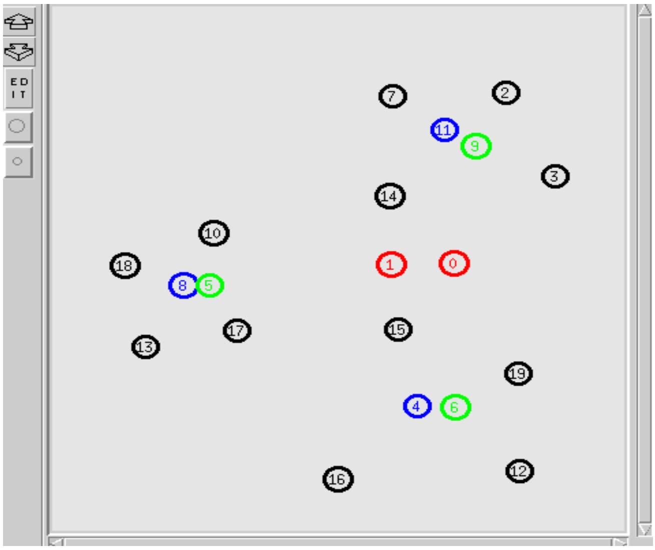

Figure 1 Topology of network

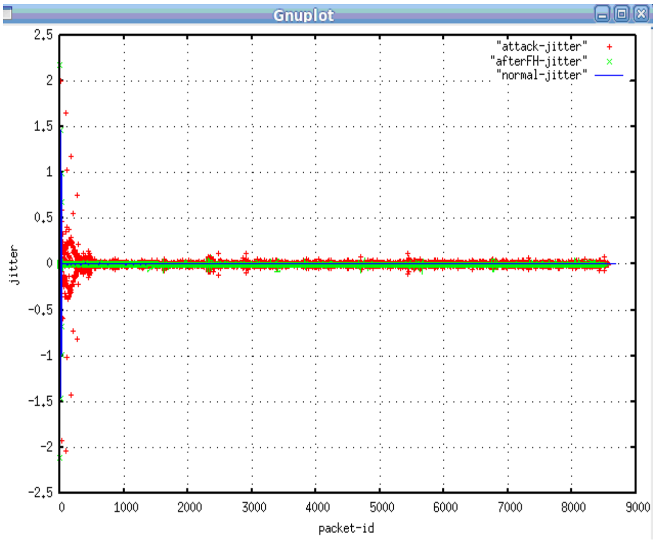

Figure 2 Jitter Comparison

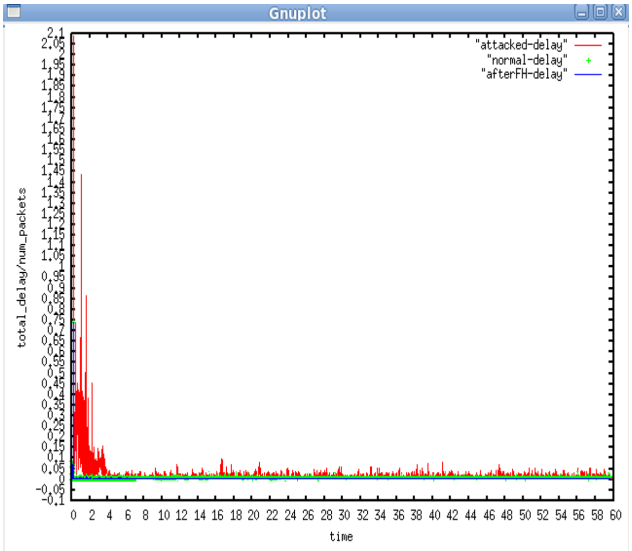

Figure 3 Transmission delay comparison

5. Conclusion

For split-network attack, we have proposed a defense scheme. This scheme consists of evaluation of behavior, negotiation of frequency hopping, synchronization of frequency hopping and integration of network. The simulation results show the scheme effectively resists SNA, and reduces network delay and jitter.

The future work will focus on improving the accuracy of evaluation of behavior and optimization of frequency synchronization algorithm.

Acknowledgment

The authors would like to thank the reviewers, whose comments helped to improve this paper. This work was supported by “Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality”. And its number is PHR201007121.

References

[1] Giruka, V. C., Singhal, M., Royalty, J. and Varanasi, S. (2008), Security in wireless sensor networks. Wireless Communications and Mobile Computing, 8: 1–24. doi: 10.1002/wcm.42

[2] Kashif Kifayat, Madjid Merabti, Qi Shi and David Llewellyn-Jones, Security in Wireless Sensor Networks. Handbook of Information and Communication Security, 2010, Part E, 513-552, DOI:10.1007/978-3-642-04117-4_26

[3] Raymond,D.R. Marchany,R.C.Brownfield, M.I.Midkiff,S.F, ”Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols”,*Vehicular Technology, IEEE Transactions on* On page(s): 367 – 380, Volume: 58 Issue: 1, Jan. 2009

[4] David Richard Raymond,”Denial-of-Sleep Vulnerabilities and Defenses in Wireless Sensor Network MAC Protocols”, Dissertation, Virginia Polytechnic Institute and State University, 2008

[5] Rainer Falk, Hans-Joachim Hof, "Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks," securware, pp.191-196, 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009

[6] MatthewPirretti,SencunZhu, N.Vijaykrishnan,Patrick McDaniel, Mahmut Kandemir and Richard Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense "in International Journal of Distributed Sensor Networks, Volume 2, Issue 3 September 2006, pages 267 - 287

[7] David R. Raymond and Scott F. Midkiff, "Clustered Adaptive Rate Limiting: Defeating Denial-of-Sleep Attacks in Wireless Sensor Networks" in Military Communications Conference 2007, MILCOM, IEEE, pages -1-7.

[8] Aristides Mpitziopoulos et al.."A Survey on Jamming Attacks and Countermeasures in WSNs", IEEE COMMUNICATIONS SURVEYS&TUTORIALS, VOL. 11, NO. 4, FOURTH QUARTER 2009

[9] Mpitziopoulos,A.and Gavalas, D.(2009),An effective defensive node against jamming attacks in sensor networks. Security and Communication Networks,2:145–163.doi: 10.1002/sec.81

[10] M.Strasser,C. Popper, and S. Capkun, "Efficient Uncoordinated FHSS Anti-jamming Communication," Proceedings of the tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 207-218, 2009.

[11] Ghada Alnifie, Robert Simon,"A multi-channel defense against jamming attacks in wireless sensor networks", Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks, October 22-22, 2007, Chania, Crete Island, Greece

[12] W. Xu, W. Trappe and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference", in Proc. 6th international conference on Information processing in sensor networks, New York, NY, USA, pages.499-508, 2007.

[13] W. Xu, K. Ma, W. Trappe, Y. Zhang, "Jamming sensor networks: attack and defense strategies", IEEE Network Magazine,vol. 20, pages. 41-47,2006.

[14] WENYUAN XU, WADE TRAPPE and YANYONG ZHANG, "Defending wireless sensor networks from radio interference through channel adaptation" in ACM Transactions on Sensor Network, Vol. 4, No. 4, Article 18, Publication date: August 2008

[15] Khusvinder Gill and Shuang-Hua Yang, "A Scheme for Preventing Denial of Service Attacks on Wireless Sensor Networks" in Industrial Electronics, 2009. IECON '09. 35th Annual Conference of IEEE, Identifier: 10.1109/IECON.2009.5415233, pages: 2603 - 2609

[16] Pelechrinis,K; Iliofotou,M; Krishnamurthy,V., in Communications Surveys & Tutorials of IEEE, Issue: 99, Identifier: 10.1109/SURV.2011.041110.00022, pages:1-13

[17] Raymond, D.R.; Midkiff, S.F.; Pervasive Computing, IEEE, Vol: 7 , Issue: 1, Identifier: 10.1109/MPRV.2008.6, pages: 74 - 81