Security Issues in Wireless Sensor Networks

Dr. Khawla Hussein, Entesar Barges, Nadra Jameel

Computer Science-College of Pure Education-Univ. Basrah

khawlahussen@yahoo.com,

entesar.barges@yahoo.com

***Abstract* —A wireless sensor network (WSN) is a network formed by a large-number of sensor nodes, where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solutions, WSNs feature easier deploy met and better flexibility of device. With the rapid technological development of sensors, WSNs will become the key technology for IoT. Starting with a brief overview of WSN, and discusses the current state of the security attacks in WSNs. various types of attacks are discussed and future direction in WSNs security is also included.**

Keywords: Wireless Sensor Networks (WSNs), Attacks, Security, and Threats.

I. Introduction

The wireless networks contain hundred or thousand tiny and low cost , low power and self-organize sensor nodes perform the functions in network. The sensors nodes are used for monitoring different environment in the cooperative manner and compute the data for analyzing. The two components of wireless sensor network: aggregation and base station. Aggregation collects the information from their nearby sensors, integrate them and send them to the base station for processing. The WSN nature of communication is unprotected and unsafe because of deployment in hostile environment, limited resources, an automated nature and untrusted broadcast transmission media, the most of security techniques are not sufficient in WSN network and security is a vital required for networks. The main objective of this paper is to review different issues such as confidentially, authenticity and availability.

The challenges of security in WSN are totally different from traditional network security due to inherent resources and computing constraints. Sensor nodes are often deployed in large accessible areas that present the added risk of physical attack. Most of the early proposed network techniques in the past assumed that all nodes are cooperative and trust worthy. However, this is not the case for many sensor network applications today, that require a certain amount of trust in the application.

II. WSNs Security Issues

This section we discuss various issues concern with the security of WSNs including limitations, unreliability, etc. the signals along with communicating and performing simple computational tasks. Common functions of WSNs are broadcasting, multicasting, routing, forwarding and route maintenance. WSNs have many constraints from which results in new challenges. The sensor nodes have extreme resource limitations and unviable communication medium and the too in unattended environment which make it very difficult for the employed of the existing security approaches due to the complexity of the algorithms working for sensor platform. In order to effectively implemented approaches, required amount of data memory, code space, and energy is required . However, due to small size of sensor nodes, these resources are limited.

A. Limited memory and storage

The memory of tiny sensor nodes usually ranges from 2KB to 256 KB. While storage ranges from 32 KB to 2 GB.

B. Limited power

Energy (power) is the biggest constraint in wireless sensor capabilities. It is of the main reason that nodes are subjected to failures, or more general, it due to environment changes. Therefore, the energy consumption must be minimized for long file, the necessities both the power efficiency of the hardware along with the efficiency of security and other routing protocols as show in *Table 1*.

Layer	**Attacks**
Application layer	Repudiation data corruption
Transport layer	Session hijacking , SYN flooding, wormhole, black hole, location disclosure attacks
Data link layer	Traffic analysis, monitoring disruption
Physical layer	Jamming , interceptions, eaves dropping
Multi-layer	DoS, impersonation, replay, man-in-the-middle.

Table I. *attacks in network layers*

A. Sensor networks: the limitations

A distributed sensor network consists of thousands low cost and low power small sensors as show in Figure 1. The sensors are embedded devices that are worked via wireless media, usually integrated with a physical environment , and are capable of acquiring and processing the signals along with communicating and performing simple computational task.

B. Unreliability of Communication

One of the major threads to sensor security is the very nature of the wireless communication medium, which is inheriting insecure. The wireless medium is open and accessible to anyone unlike wired networks, where a device has to be physically connected to the medium.

C. Cryptography and Non-Cryptography Related Attacks

Some attacks are non-cryptography related, and others are cryptographic primitive attacks. Figure 2 shows cryptographic primitive attacks. Physical layer attacks Wireless communication is broadcast by nature. A common radio signal is easy to jam or intercept. An attacker could overhear or disrupt the service of a wireless network physically. Eavesdropping: Eavesdropping is the intercepting and Table 1 Security Attacks on Each Layer of threading of messages and conversations by unintended receivers. The mobile hosts in mobile ad hoc networks share a wireless medium.

The majorities of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be overheard, and fake messages can be injected into network. Interference and Jamming: Radio signals can be jammed or interfered with, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse. Jamming equipment is readily available. In addition, jamming attacks can be mounted from a location remote to the target networks.

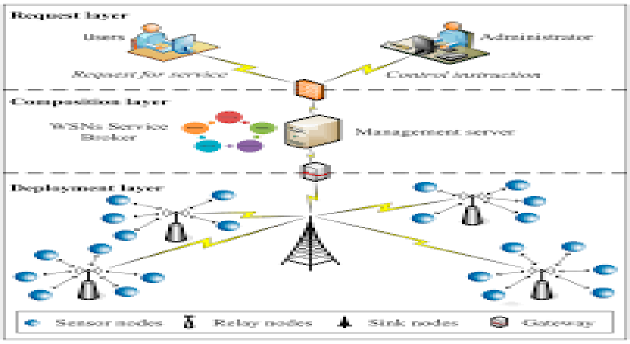

Fig.1. *Security Issues in WSNs*

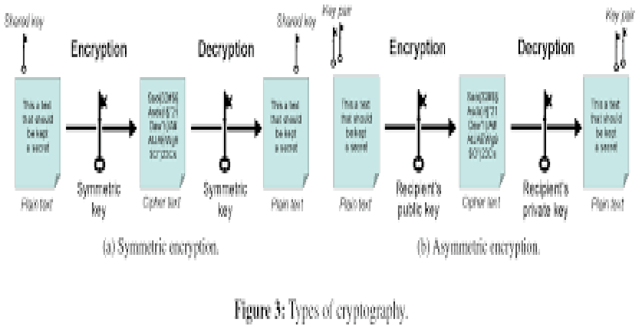

Fig. 2.*Types of cryptography*

III. Conclusions

Thinking like the attacker people understands better their goals and intensions. Now, popularity of WSNs increases, and takes attentions. This will help them to protect their systems and networks better for the future intrusions. It will help us to create better intrusion detection systems. This paper treats security challenges in WSNs, which differ from the ad hoc networks with more severe restrictions in terms of energy, computation capabilities and communications. Consequently, the solutions of security must thus be adapted. In the case of WSN, security has been an increasingly significant subject. Due to resource limitations, it is quite impossible to provide a strong security to a WSN. In the present paper, attacks and defenses referenced from 1997 till 2013 have been summarized and particular solutions were proposed. As all WSNs attacks and counter attacks have been presented the extensive study could offer a review of the relevant topic for future research on WSN security. Future work should focus on finding a solution for combinational link layer attacks, designing the MAC36 protocol, or securing WSNs links against collision and DoS attacks. More comprehensive research is also necessary to measure the efficiency of algorithms in terms of resources available.

References

[1] Prabhudutta Mohanty, Sangram Panigrahi, Nityananda Sarma, Siddhartha Sankar, “Wireless Sensor Network Security” 2005-2010. JATIT.

[2] V. S. Bagad, I. A. Dhotre, “Information Security” First Edition, 2009.

[3] Padmavathi G, Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks” IJCSTS, 2009. [4] Rajni Sharma, Chander Diwakar, “Security Analysis of Wireless Sensor Networks.” 2012. Volume 2, Issue 2, IJREAS.

[5] Dr. Shahriar Mohammadi, Hossein Jadidoleslamy, “A Comparison of Link Layer Attacks on Wireless Sensors Network.” International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.1, pg 35-56, 2011.

[6] Sheela D. Naveen K,C and Mahadevan G, A non-cryptographic method of sink hole attack detection in wireless sensor networks, Recent International Journal

of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.4, No.6, December 2013.

[10] Madhavi, S. and K. Duraiswamy, “Flooding Attack Aware Secure AODV” Journal of Computer Science, 2013.

[11] Kashyap Patel , Mrs.T.Manoranjitham, 2013. “Detection of Wormhole Attack In Wireless Sensor Network” India International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 5, May – 2013.

[12] Lingxuan Hu and David Evans, 2004. “Using Directional Antennas to Prevent Wormhole Attack”,In Proceedings of the Network and Distributed System Security Symposium, pp. 131-141.

[13] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003. “Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks”. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE, pp. 267-279.

[14] Srdjan Capkun, L.evente Buttyan, and Jean-Pierre Hubaux, “SECTOR: Secure Traking of Node Encouters in Multi-hop Wireless Networks”. In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32.

[15] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liangmin, “Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks’ IEEE 2009. pp.226-232.

[16] Guorui Li, Xiangdong Liu, and Cuirong Wang, “A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks”, 2010. pp.554-558.

[17] X. Pu, Z. Yan, S. Mao, Y. Zhang and Y. Li, “The sequential mesh test for a proportion,” in Journal of East China Normal University, 2006, No. 1, pp. 63-71.

[18] Wazir Zada Khan Yang Xiang Mohammed Y Aalsalem, , “Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks” International Journal of Computer Network and Information Security (IJCNIS), 2011.