Advanced Science and Technology Letters
Vol.134 (CIA 2016), pp.146-151
http://dx.doi.org/10.14257/astl.2016.134.25

Study on Security Issues in Wireless Sensor Network

Yiguang Gong[1], Feng Ruan[1], Zhiyong Fan[1], Tao Li[2], Jin Wang[3]

[1] School of Information & Control, Nanjing University of Information Science & Technology, Nanjing, China

[2] School of Electronic & Information Engineering, Nanjing University of Information Science & Technology, Nanjing, China

[3] School of Information Engineering, Yangzhou University, Yangzhou, China

Abstract. Security issues become more and more important in recent years for wireless sensor networks (WSNs). In this paper, we summarize the security architecture and requirements, then introduce several attacks and defenses. In addition, we also summarize key management and several typical key management methods, which benefit researchers greatly to realize the situation and trend of state-of-the-art of wireless sensor network security.

Keywords: Wireless sensor network, security, attack, key management

1 Introduction

Sensor network mainly consists of a large number of small, low-cost, battery-powered, with wireless communications and monitoring ability of sensor nodes. Wireless sensor networks have a wide range of applications. Akyildiz, et al. proposed that the applications of sensor networks divided into military applications, health applications, home applications, and some other commercial applications [1].

Many sensor networks have mission-critical tasks, so it is definite that security needs to be taken into consideration at the time of design. Actually, the lack of effective security mechanism has become the main obstacle to sensor network applications [2, 3]. A wireless sensor network can gather messages via its sensors, do communicate and computations wirelessly with other sensor nodes [4]. While a wireless sensor network is an ad hoc networks in which the nodes self-organized without any preexisting infrastructure, important differences exist between them. Thus, security in wireless sensor networks is quite complicated.

In this article we summarize the security architecture and requirements. Then we discuss attacks and countermeasures. In addition, we explore key management in sensor network security and introduce several typical key management methods. Our goal is to provide a deeper understanding of current security issues and defense for attacks in wireless sensor network.

ISSN: 2287-1233 ASTL

2 Security Architecture and Requirement

2.1 Security Architecture

Sensor network is vulnerable to various attacks and has numerous potential safety hazard. Fig.1 is security architecture. In this paper, we mainly introduce attack technique, security defense and key management. The protocol stack of wireless sensor network is composed of hardware layer, operating system layer, middleware layer and application layer.

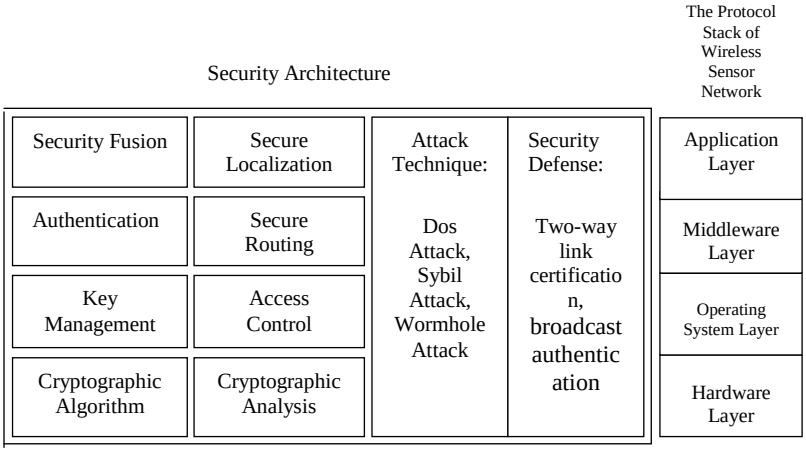

Fig. 1. Security Architecture

2.2 Security Requirements

The security level and requirements are variant in different scenarios of sensor networks. When cope with security in wireless sensor networks, we mainly devote to the problem of achieving some of all of the following security targets:

(1) Availability: Availability makes sure that the network can accomplish basic tasks while under attacks. A variety of attacks can compromise the availability. In consideration of availability in sensor network, it is crucial to achieve graceful degradation [5].
(2) Confidentiality: Confidentiality ensures that confidential information will not be exposed to unauthorized users. Confidentiality makes that an adversary cannot know the message context even it intercepted communication signals.
(3) Integrity: Integrity ensures that information will not be altered in transit by an adversary [6], [7].
(4) Non-repudiation: Non-repudiation signifies message sources cannot deny sending information it has sent previously.
(5) Freshness: Freshness could classify as data freshness and key freshness. Freshness guarantees that users achieve messages needed within schedule time.

(6) Authentication: Authentication is concerned with assuring that communication of nodes are authentic [6], [7].

3 Attack and Defense

3.1 Attacks in Wireless Sensor Network

In wireless sensor networks, a large-scale individual sensors are affected by security compromise. An attacker can eavesdrop messages by any sensor nodes due to the broadcasting of the nature of communication. Therefore, security is an important issue here. The main attacks in wireless sensor networks are as follows:

A. Wormhole Attack

Wormhole attack, also known as tunnel attack, needs two distant malicious nodes to send messages directly through a high-quality and high-bandwidth private tunnel established together. In a wormhole attack, an adversary records data packets or location messages in one part of the tunnel and transfers stolen messages to a different part of the tunnel. The wormhole attack can destroy the integrity and confidentiality of messages. Fig.2 shows a situation of wormhole attack.

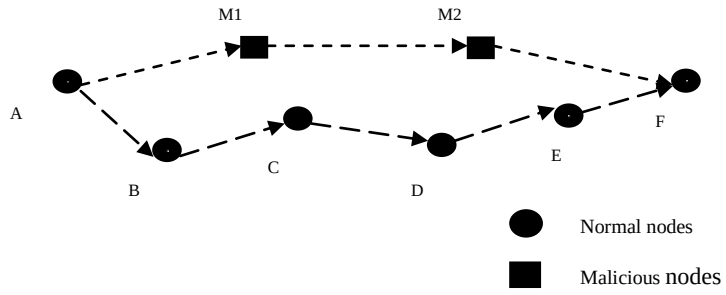

Fig. 2. Situation of Wormhole Attack

B. Sybil Attack

The Sybil attack was first proposed by Douceur in the setting of peer-to-peer networks [8]. However, Newsome, et al.in [9] showed that Sybil attack is also a menace to routing mechanism in sensor networks. Sybil attack was defined as a malicious device or node having multiple identities. Due to the immature authentication mechanism of WSN, Sybil attack utilizes a single malicious device or node to forge and pretends to be legitimate nodes.

C. Denial of Service Attack

Denial of Service (DoS) [10] is meant not only for that the adversaries attempt to disrupt, subvert, or destroy sensor networks, but also for any event that diminishes or eliminates sensor network's capability to perform its excepted function. At physical layer, Denial of Service attacks impede communication by jamming or tampering of the packet. At link layer, it is by generating collision data, exhaustion of resources and attempting to get an unfair share of the resource in sensor networks. At network layer, it occurs by the greediness of packets, neglecting and misdirection. At transport layer, this attack could be occurred due to malicious flooding and de-synchronization.

D. Hello Flood Attack

In Hello Flood attack [11], it is assume that a node which receives such a packet is within a radio range of the sender [12]. An attacker wastes large enough transmission power to broadcast routing or other massage. And then every other nodes in a big area of the network convinced that the attacker is its neighbor. Thus, a large number of nodes will respond to route messages from adversaries and attempt to use the route. However those packets sent from the nodes which are away from the adversary would be forgotten. Therefore the network is left in a state of chaos.

3.2 Attack Defenses in Wireless Sensor Network

Security issues mainly come from attacks. Tab. 1 is attacks and defenses in wireless sensor network.

Table 1. Attacks and defenses in Wireless Sensor Network

Attacks	Defenses
External attack and link layer security	Encryption and authentication in link layer
Sybil attack	authentication
Hello flood attack	Two-way link certification
Selective forwarding	Multipath routing technology Routing technology based on the clues
Wormhole and sinkhole	Due to defensing difficultly, we must consider them when designing, i.e. routing based on geographical location
Certification broadcast and flood	broadcast authentication, i.e. μTESLA

Under physical attacks, the idea of confronting physical attacks is that the nodes in wireless sensor network implement destroy themselves including all data and keys.

This is a feasible solution when having enough redundant information. We can detect neighbors regularly to discover physical attacks.

In order to prevent Denial of Service attack, we can utilize those mechanisms include pushback, payment for network resources, identification of traffic and strong authentication. Virtual currency systems [13, 14] compensate for the service of a node by credit or micro payments. For forwarding the message of another node, this node receives a virtual payment deducted from the destination node or the sender.

About Sybil attack, there are several defense mechanisms for it in sensor network [9]. The basic idea is to associate every node's identity with the keys assigned through utilizing the key pre-distribution process. Only when a node has the corresponding keys of spoof identity S, the node can succeed. Otherwise it cannot survive validation or establish a communication with other nodes.

4 Conclusion

The research of sensor network security faces huge challenges. In this paper, we introduce security architecture and analyze security requirements. Based on the sensor network protocol model, we review many types of attacks and provide defenses for those attacks. Key management is very important in sensor network security, we suggest taking a system application environment and secure resilience into consideration when designing key management schemes. In this article, we just introduce a few approaches about sensor network security, and more studies are needed in sensor network.

References

1. Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks, IEEE Commun. Mag 40, 102-114. (2002)
2. Perrig, Adrian, J. A. Stankovic, Wagner, D.: Security in wireless sensor networks, Commun ACM, Communications of the ACM 47(6), 53-57. (2004)
3. Hu, F., Sharma, N. K.: Security considerations in ad hoc sensor networks, Ad Hoc Networks 3(1), 69-89. (2005)
4. Oreku, GS., Pazynyuk, T.: Security in Wireless Sensor Networks, Springer Publishing Company, Incorporated. (2015)
5. Shi, E., Perrig, A.: Designing secure sensor networks, IEEE Wireless Communications, 11, 38-43. (2004)
6. Tanenbaum, A. S.: Computer Networks, 4th ed. NJ: Prentice Hall. (2003)
7. Stallings, W.: Cryptography and Network Security: Principles and Practice, International Annals of Criminology 46(4), 121-136. (2003)
8. Douceur, J R.: The Sybil Attack, Peer-to-Peer Systems, First International Workshop, 251-260. (2002)
9. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil attack in sensor networks: Analysis and defenses, International Symposium on Information Processing in Sensor Networks, 3, 259–268. (2004)
10. Ghamgin, H., Akhgar, M. S., Jafari, M. T.: Attacks in Wireless Sensor Network, Chinese Journal of Scientific Instrument. (2011)

11. Singh, Y., Attacks on wireless sensor network: a survey, International Journal of Computer Science & Management Studies 12. (2012)
12. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: Attacks and countermeasures, Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 293-315. (2003)
13. Blazevic, L., Buttyan, L., Capkun, S., Self-organization in mobile ad hoc networks: the approach of Terminodes [J]. IEEE Communications Magazine, 39(6), 166-174. (2001)
14. Buttyan, L., Hubaux, J.-P.: Nuglets: A virtual currency to stimulate cooperation in self-organized mobile ad hoc networks, Swiss Federal Institute of Technology. (2001)

