International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.295-302
http://dx.doi.org/10.14257/ijsia.2016.10.8.25

Security Architecture and Requirements for Wireless Sensor Networks

Yiguang Gong[1], Feng Ruan[1], Zhiyong Fan[1], Jianmin Hou[1], Ping Mei[1] and Tao Li[2]

[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*

Abstract

Recently, with the wider application and development of wireless sensor networks (WSNs), security issues become essential for many sensor network applications including environment monitoring, traffic controlling, military sensing, patient status monitoring and so on. In this paper, we summarize the security architecture and requirements, enumerate attacks and countermeasures in wireless sensor networks. In addition, we also summarize key management and introduce several typical key management methods. Which benefit researchers greatly to realizing the situation and trend of state-of-the-art of wireless sensor networks security.

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

1. Introduction

Sensor network is consist of a large number of small volume, low-cost, battery-powered, with wireless communications and monitoring ability of sensor nodes. In order to achieve the purpose of monitoring the physical world, these nodes are densely deployed in monitoring area, Wireless sensor networks have a wide range 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. Though a big differences between sensor network and ad hoc network, their starting point are same. All of them need to solve the confidentiality, integrity, authentication of messages and access control, *etc*. [5, 6]. The differences between sensor networks and ad hoc network are as the following [1, 7]:

- Compared with ad hoc nodes, sensor nodes are densely deployed in monitoring area.
- The number of nodes in a sensor network is much larger than the nodes in an ad hoc network.
- Compared with ad hoc network, designing sensor network must take scalability into consideration due to its large quantity of sensor nodes.
- Due to the infertile circumstance and energy constraints, sensor nods are easy to failures.

ISSN: 1738-9976 IJSIA

- In contrast to general ad hoc network, the topology of sensor network changes quite frequently because of the node removing, joining or mobility.
- Sensor nodes have severely constrained in memory storage, power resources and computational capacities.
- Due to the large amount of sensors, sensor nodes may not have global identification.
- In sensor network, there is no guarantee that the physical security of deployment area.

In this article we summarize the security architecture and requirements, then 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.

The reminder of this paper is organized as follows. In Section 2, security architecture and security requirements are described. Section 3 gives a short introduction of attacks and defenses. In Section 4, we focus on key management. Finally, we summarize this paper.

2. Security Architecture and Requirement

2.1. Security Architecture

Sensor network is vulnerable to various attacks and has numerous potential safety hazard. Figure 1 is security architecture. The security architecture composed of security fusion, authentication, key management, cryptographic, secure localization, secure routing, access control, cryptographic analysis, attack technique and security defense. 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.

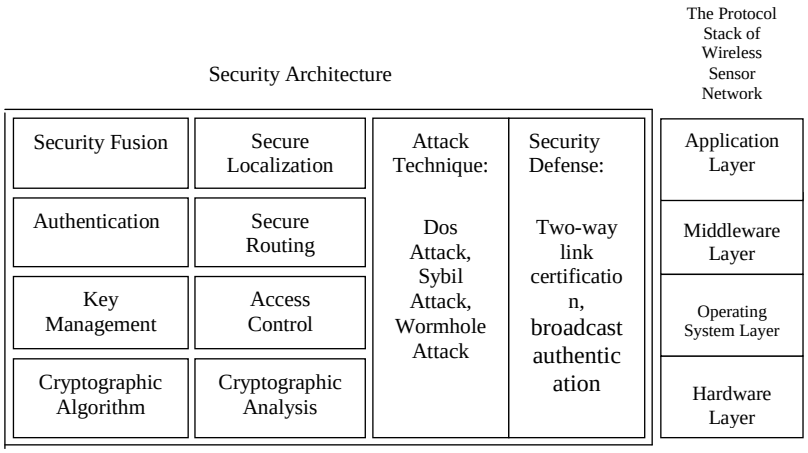

Figure 1. Security Architecture

2.2. Security Requirements

The security level and requirements are variant in different scenarios of sensor networks. For example, security requirement of military and civilian in sensor network are different. 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 [8].

(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 [9], [10].

(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 [9], [10].

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

(B) Sybil attack

(C) Denial of Service (DoS)

(D) Hello Flood attack

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.

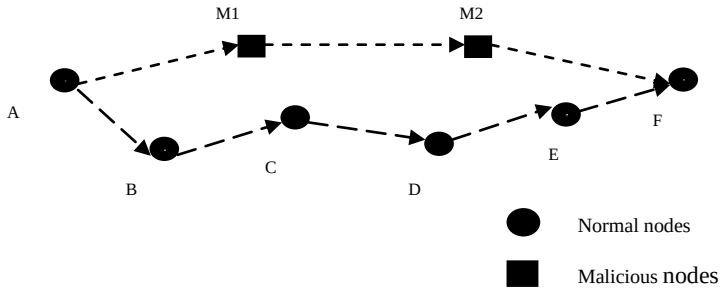

Figure 2. Situation of Wormhole Attack

Figure 2 shows a situation of wormhole attack. A and B, not in each other's communication radius, are two distant normal nodes in wireless sensor networks. M1 and M2 are the wormhole attack nodes. B, C, D and E are intermediate nodes.

The wormhole attack can destroy the integrity and confidentiality of messages, e.g. an attacker can discard received message package, forge or falsify the content of packets when passing the message packets, which results in the loss of data or erroneous data.

B) Sybil Attack

The Sybil attack was first proposed by Douceur in the setting of peer-to-peer networks [11]. However, Newsome, *et. al.,* in [12] 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. In general, the additional identities of malicious devices or nodes are referred to as Sybil nodes.

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. However, normal nodes are unable to distinguish these forged nodes in the networks, the normal nodes actually communication with malicious nodes directly when forged nodes join the neighbor list.

C) Denial of Service Attack

Denial of Service (DoS) [13] 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. Denial-of-Message attack (DoM) [14], where sensor nodes are deprived of broadcast messages, is another type of DoS.

D) Hello Flood Attack

In Hello Flood attack [15], it is assume that a node which receives such a packet is within a radio range of the sender [16]. 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. Protocols depending on localized information exchange between neighboring nodes for flow control or topology maintenance are mainly subject to this type of attack [17].

3.2. Attack Defenses in Wireless Sensor Network

Security issues mainly come from attacks. Table 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 [18-20] 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. Nuglets [18], [19] proposed two models: one is Packet Purse, and another is Packet Trade Model. The benefit of these models are discouraging users from flooding the sensor network and that it is unnecessary to know how many Nuglets loaded into the packet. Sprite [20] encourages mobile nodes to report and cooperate actions honestly by using credit. In this system, the sender prevents a denial-of-service attack to the destination through sending a large number of traffic.

About Sybil attack, there are several defense mechanisms for it in sensor network [12]. 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. Key Management

Key management which is the basis of sensor network security is very important and complex. The dynamic structure, self-organization property and easy node compromise of sensor network increase the difficulty of key management. In the meantime, those reasons cause a broad research issues in this area. The way of all the nodes share a master key can't satisfy the security requirements of sensor networks.

4.1. Basic Key Distribution Scheme

Eschenauer, *et. al.*, firstly proposed basic key distribution scheme [21], the basic idea is that all nodes randomly select several keys from a large key pool as key chain, the neighbor nodes in key chain with the same key can establish secure channel. In this scheme, key pre-distribution consists of three phases: key pre-distribution phase, shared-key discovery phase, and path-key establishment phase.

Key pre-distribution phase: Firstly, generation of a large pool of G keys and of their key identifiers. Secondly, randomly extracting k keys out of G without replacement to establish the key ring of a sensor. Then loading of the different key ring into the memory of each sensor.

Shared-key discovery phase: After key pre-distribution phase, every node discovers its neighbor nodes with which it shares keys in wireless communication range. Only nodes sharing a key are considered that they are connected.

Path-key establishment phase: In the absence of shared key between two nodes, the link key can be established through the path of the shared key.

4.2. q-composite Random Key Pre-distribution Scheme

Based on the Eschenauer's scheme, some researchers propose key pre-distribution schemes because of improving the network resilience to prevent node compromise. Cahn, *et al*. proposed a q-composite random key pre-distribution scheme [22]. Different from the basic key distribution scheme, this scheme requires q common keys between a pair of nodes. It is show that when q is increased, the resilience of network against node compromise is improved. Of course, with the increasing of q, the sensor nodes should store more pre-distribution keys in order to obtain an applicable probability of key-shared within neighbors. On the basis of the above key management protocol in sensor network, Y.zhang *et al.*, proposed a node-to-node neighborhood authentication scheme [23]. Du, *et al.,* [24] proposed a key pre-distribution scheme with a definite node compromise.

4.3. Random Seed Key Distribution Scheme

In order to adopting the random distribution of secret material and a transitory master key, Gandino *et al.,* in [19] proposed random seed key distribution with transitory master key (RSDTMK) scheme, which is a key management scheme for a wireless sensor network node adding without deployment knowledge. This scheme can be considered an integration of both the random key distribution and the transitory master key [25]. This scheme presents two novelties: RSDTMK distributes seeds, instead of keys. In this scheme, every node obtains a ring which is composed of seeds randomly selected from a pool. Compared with the quantity of seeds in the pool, the purpose of this scheme is to increase the quantity of possible keys. The number of possible keys used by RSDTMK is greater and this scheme decreases the effects of compromised secret material.

5. Summary

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.

Acknowledgements

This paper is a revised and expanded version of a paper entitled "Study on Security Issues in Wireless Sensor Network" presented at CIA 2016 Philippines, May 19-21. This work was supported by the National Natural Science Foundation of China (71503136, 61304089). It was also supported by the China Special Fund for Meteorological Research in the Public Interest under grant GYHY201306070, and by the Priority Academic Program Development of Jiangsu Higher Education Institutions.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks", IEEE Commun. Mag, vol. 40, no. 102-114, **(2002)**.
[2] A. Perrig, J. A. Stankovic and D. Wagner, "Security in wireless sensor networks", Commun ACM, Communications of the ACM, vol. 47, no. 6, **(2004)**, pp. 53-57.
[3] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks", Ad Hoc Networks, vol. 3, no. 1, **(2005)**, pp. 69-89.
[4] Oreku G. S. and Pazynyuk T., "Security in Wireless Sensor Networks", Springer Publishing Company, Incorporated, **(2015)**.
[5] S. Slijepcevic, "On Communication Security in Wireless Ad-Hoc Sensor Networks", IEEE Int Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, **(2002)**, pp. 139-144.

[6] R. Shaikh, "Securing Distributed Wireless Sensor Networks: Issues and Guidelines", Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on IEEE. **(2006)** February.
[7] X. Chen, "Sensor network security: a survey", IEEE Communications Surveys & Tutorials, vol. 11, no. 2, **(2009)**, pp. 52-73.
[8] Shi E. and Perrig A., "Designing secure sensor networks", IEEE Wireless Communications, vol. 11, **(2004)**, pp. 38-43.
[9] A. S. Tanenbaum, "Computer Networks", 4th ed. NJ: Prentice Hall, **(2003)**.
[10] W. Stallings, "Cryptography and Network Security: Principles and Practice", International Annals of Criminology, vol. 46, no. 4, **(2003)**, pp. 121-136.
[11] Douceur J. R., "The Sybil Attack", Peer-to-Peer Systems, First International Workshop, **(2002)**, pp. 251-260.
[12] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses", International Symposium on Information Processing in Sensor Networks, vol. 3, **(2004)**, pp. 259–268.
[13] H. Ghamgin, M. S. Akhgar and M. T. Jafari, "Attacks in Wireless Sensor Network", Chinese Journal of Scientific Instrument, **(2011)**.
[14] Mccune J. M., Shi E. and Perrig A., "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts", Proceedings of the 2005 IEEE Symposium on Security and Privacy IEEE Computer Society, **(2005)**.
[15] Y. Singh, "Attacks on wireless sensor network: a survey", International Journal of Computer Science & Management Studies, vol. 12, **(2012)**.
[16] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, **(2003)**, pp. 293-315.
[17] A. Hamid, Mamun-Or-Rashid and Hong C. S., "Defense against lap-top class attacker in wireless sensor network", ICACT. **(2006)** January.
[18] Blazevic L., Buttyan L. and Capkun S., "Self organization in mobile ad hoc networks: the approach of Terminodes[J]", IEEE Communications Magazine, vol. 39, no. 6, **(2001)**, pp. 166-174.
[19] L. Buttyan and J.-P. Hubaux, "Nuglets: A virtual currency to stimulate cooperation in self-organized mobile ad hoc networks", Swiss Federal Institute of Technology, **(2001)**.
[20] S. Zhong, J. Chen and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks", in Proc. IEEE INFOCOM. **(2003)** March.
[21] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", ACM Conference on Computer and Communications Security, **(2002)**.
[22] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks", Symposium on Security & Privacy IEEE, **(2003)**.
[23] Y. Zhang, "Securing sensor networks with location-based keys", Wireless Communications and Networking Conference, 2005 IEEE, **(2005)** April.
[24] W. Du, J. Deng, Y. S. Han and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks", ACM Trans Inform. System Security (TISSEC), **(2005)**, pp. 228–258.
[25] F. Gandino, B. Montrucchio and M. Rebaudengo, "Key Management for Static Wireless Sensor Networks With Node Adding", IEEE Transactions on Industrial Informatics, vol. 10, no. 2, **(2014)**, pp. 1133-1143.

Authors

Yiguang Gong, He is a lecturer at Nanjing University of Information Science & Technology. He received the B.S. and M.S. degree in the China University of Geosciences, and PHD in Nanjing University of Aeronautics and Astronautics. His research interests mainly include web information extraction, machine learning, embedded systems, .Wireless Sensor Networks.

Feng Ruan, He is a lecturer at Nanjing University of Information Science & Technology. He received the B.S. and M.S. degree in the Nanjing University of Information Science &Technology. Now he is PHD student in Computer Science Department of Nanjing University of Information Science & Technology. His research interests mainly include complex system, computer network, routing protocol and algorithm design, data mining, cloud computing.

Zhiyong Fan, He received MSc from Nanjing University of Information Science and Technology (NUIST) in 2007, China. He is a lecturer in the School of Information and Control Engineering at NUIST, China. Now, he is a PhD student in Nanjing University of Science and Technology, China. His current research interests include medical imaging, image processing and pattern recognition.

Tao Li, He is an Associate Professor at School of Electronic & Information Engineering, Nanjing University of Information Science & Technology. He received the B.S. and M.S. degree in Nanjing University of Information Science & Technology, and PHD in Nanjing University of Aeronautics and Astronautics. His research interests mainly include computer network, big data, data mining, and cloud computing.