(AGUIJET) 2018, Vol. No. 7, Jul-Dec **e-ISSN: 2455-0442, p-ISSN: 2455-6734**

A Brief Review of Design Issues and Security Attacks on Wireless Sensor Networks: Last Five Years Study

Nagesh Kumar
Department of Computer Science & Engineering
School of Science & Technology
A P Goyal Shimla University, Shimla, Himachal Pradesh, India
engg.nagesh2@gmail.com

ABSTRACT

The collection of sensor nodes which are deployed in the area of interest and communicate wirelessly constitute of a wireless sensor networks. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. The sensor nodes have extreme resource limitations, unreliable communication medium and that too in unattended environments. This makes it very difficult for the implementation of the existing security approaches to WSNs due to the complexity of the existing algorithms. In this paper various issues and requirements concern with the security of WSNs are discussed and then various security attacks has been classified. Study of these attacks will help in the design of robust and efficient countermeasures for attacks against WSNs.

Keywords— *WSN; Security; Attacks; Threat; Data integrity.*

INTRODUCTION

WSN has a variety of applications like military, health, environment, commercial and agriculture. Due to the large application area of WSN, it needs powerful security mechanism. Security in WSN is a stringent task because sensors are placed in a hostile and unattended environment. In WSN sensor nodes are constrained and communication medium is wireless therefore it has security problems at the level of source, data and networks. Source security includes source authorization and authentication, data security includes data integrity and confidentiality, and network security encompasses network availability and integrity [1] [2].

Applications of WSN in last 5 years has been increased very high, therefore addressing of security concern at every level become important. The need of security in WSN has various reasons like distributed network architecture, open shared wireless communication medium, node deployed in hostile environment, highly vulnerable to malicious attacks, adversary can spoof out the information and can interrupt the network operation.

WSN protocols must ensure confidentiality, authentication, integrity, availability, authorization, nonrepudiation and freshness characteristics in order to protect the information and resources from the attacks in WSN.

WSN are susceptible to variety of security attacks due to its hostile and unattended environment. The classification of security attacks has been presented in this paper on the basis of protocol stack, attacking device, position of attacker, transit information and damage level. The paper is organized as follows. In section II it presents the trust requirements, threat models and security goals in WSN. Section III gives a review of security attacks in WSN. The various security attacks has been given in section IV. The conclusions are given in section V.

DESIGN ISSUES IN WSN

There are different goals and issues which have to be considered to achieve best performance from wireless sensor networks. Most of the issues are due to the application requirements. Also the performance of wireless sensor networks is directly related to the architectural model for a particular application. This section describes such issues and their impact on architecture of wireless sensor networks.

a) Network Parameters

Almost all types of Wireless sensor network architectures assume that all the sensor nodes are stationary objects. There are few setups that also use the mobile sensors [9]. On the other hand, it is sometimes necessary that support the mobility of sink nodes or cluster-heads [10]. So in these mobile nodes the routing becomes challenging task. The route stability becomes the biggest optimization factor in addition to energy, bandwidth etc. Also as presented in [11] the sensed event can also be dynamic or static depending on the application.

b) Node deployment

Node deployment is another factor to be considered which affect the performance of the routing protocols. This is totally application dependent factor. Node deployment can be either deterministic or self-organizing. In deterministic, one can place sensor nodes manually and the routes in the network are predetermined.

c) Energy consumption without losing accuracy

Each data transmission consumes a significant amount of energy and energy is the scarcest resource in the wireless sensor networks. The transmission power of any radio transmitter is proportional to the distance squared or it can be higher if there is presence of some obstacles in the path. Also, multi-hop routing uses less energy than single-hop routing [12].

d) Data Reporting Model

The data reporting models have been presented in [11] which are totally application dependent. The authors in [11] divided the data delivery models in following categories: continuous, event-driven, query driven and hybrid. In the continuous data delivery model, the senor nodes can be active every time and sends data continuously or there can be some time interval has been defined by the base station for the sensor nodes to be active and transmit sensed data. In event-driven and query driven models, the transmission of data is initiated when an event occurs or a query is generated by the base station.

e) Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base station which requires actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption or rerouting packets through regions of the network where more energy is available [11]. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

f) Connectivity

The connectivity in between sensor nodes mostly depends upon the node density. High node density in wireless sensor networks predefines that the sensor nodes are completely isolated from each other. Therefore, connectivity should be high. However, the high connectivity does not assure that the topology will remain constant and it does not prevent the size of the network from shrinking due to node failures. Hence in addition, connectivity between nodes also depends on the random distribution of nodes.

g) Quality of Service

Some application of WSN needs the data to be transmitted in certain period of time form the time the data being sensed; otherwise the sensed data will be useless. Therefore, there is a bound in data delivery time introduces quality of service factor. As the energy gets decreased, The WSN tries to reduce the quality of data transfer to save energy in sensor nodes which then leads to increased lifetime of the network. Therefore, there is a need of routing protocols which can save energy in the network.

PROBLEM STATEMENT

The application of WSN is still not in mature phase. Research is in progress to design and optimize WSN. Researchers raised many security issues in past. Nodes are deployed in hostile area with large numbers. Unattended and hazardous deployment of nodes forces nodes to be low cost, therefore less reachable and prone to attacks. Traditional methods such as cryptographic authentication is not sufficient to secure WSN from attacks. Security problems in WSN can be explained by describing trust requirements, threat model and security goals.

a. Trust Requirements

As WSN uses content based addressing instead of node centric addressing, therefore, survival of network depends on cooperative and trusty nature of its nodes. The term trust and security are used interchangeably when defined secures WSN system. Sometimes trust is confused with repudiation but trust is yet to have a formal definition. The trust is very important issue in networks environment because interaction between nodes is there all the time. The trust can be understood in better way by considering different domains. The trust in social science and e-commerce is concerned with the relationships among individuals in society. The trust in distributed and pear-2-peer (P2P) networks are distributed as users keep track of their peers' behaviors and exchange information. Trust in ad-hoc networks vulnerable to various attacks due to node leave and join network very often in shared wireless medium [13].

Trust in WSN plays very crucial role because nodes in WSN has less energy which drains out very quickly and number of nodes shrinks and grows very rapidly. The operation of WSN is highly depends upon the trusty and cooperative nature of the nodes. Trust in WSN has challenging field of research due to its nature.

b. Threat Model

Robust and wireless nature of sensor node have a various security attacks when it is deployed for military and surveillance applications. The traditional security architecture is not applicable for WSN because of the wireless communication and constrained resources. The WSN threat models are generally categorized into active/passive, external/internal, laptop class/mote class and function and are evaluated on the basis of various parameters. The attacks based on damage and access level is of active or passive types. The attacks based on the attacker location is of external or internal type [17]. The attacks based on the attacker's functional capabilities is of laptop class or mote class type and the attack function is of secrecy or availability.

c. Security Goals

The various applications of WSN such as military, event detection and surveillance etc., wireless nature of communication, hostile environment and constrained resource needed security. Therefore the WSN have the security goals like confidentiality, integrity, authentication, access control, availability, secrecy, efficiency, scalability, freshness, survivability, reliability, self-organization, secure localization and time synchronization.

SECURITY ATTACKS IN WSN

WSN is one of the most emerging technology for performing different tasks in various application areas such as military, environment monitoring, health monitoring etc. WSN are vulnerable to security attacks due to placement of nodes in a dangerous environment and broadcast nature of transmission. It is impossible to protect nodes from physical and logical attacks in large WSN. Various types of security attacks has been shown in fig (1).

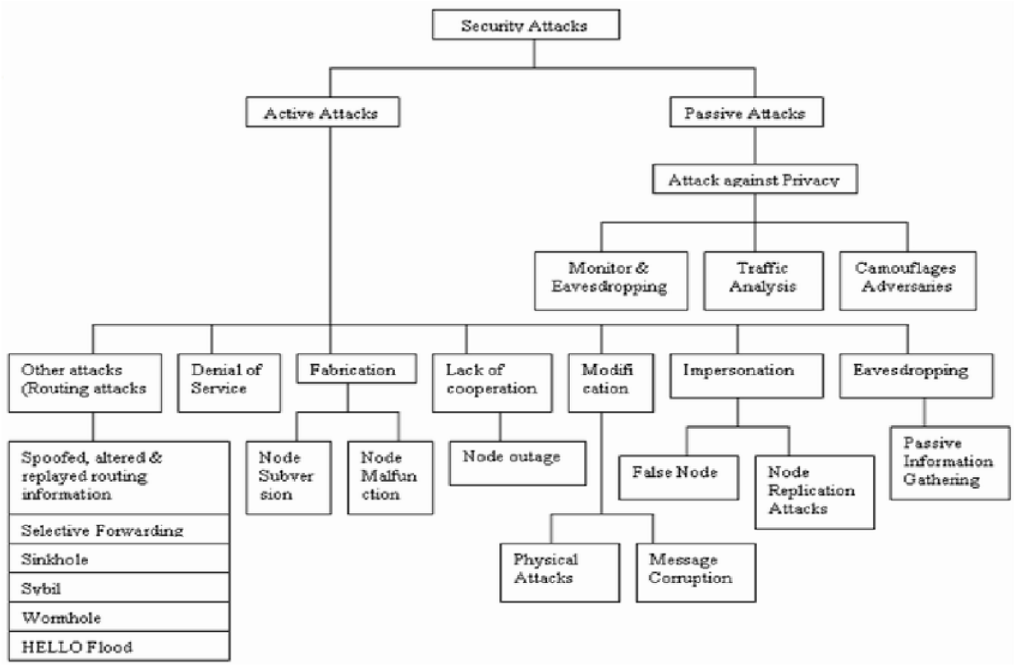

Figure 1. Security attacks in WSN

Most of the WSN are deployed for monitoring critical task where security is most important. WSN detects the data/information in their surroundings, and it is often easy to produce information other

than the data detected. Such information leakage is privacy breach. This type of attack in WSN facilitate packet injection and eves-dropping by an adversary and supports various types of attacks mentioned in fig (1). All these factors mentioned above requires security for WSN at design time to ensure WSN operation safely and securely.

A. Passive Attacks

A sort of attacks an attacker is mainly interested in monitoring the unencrypted traffic and communication so that to gain the encryption keys and sensitive information used in other types of attack as well as decrypt the weak encrypted traffic. The examples of such attacks are eavesdropping and traffic analysis etc. [15].

B. Active Attacks

An attacker gets the sensitive information and alter it so that it may be of no use for the other or make it according to their own desire. The attackers will modify the data and then inject this data in the network. Examples of such attacks are node malfunction, wormhole, and sinkhole and Sybil attack etc.

CONCLUSION

The wireless sensor applications are increasing day by day and that's why the requirements for the security becomes essential. The security issues must be addressed while designing the WSN for the applications which require sensitive data flow and to be functional in hostile environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of wireless sensor networks. In this paper, the design issues and security requirements of WSN was discussed. Various security attacks require different kinds of solutions and counter algorithms.

References

1) Chelli P, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures," Proceedings of the World Congress on Engineering 2015, Vol. 1, WCE 2015, July 13 3, 2015, London, U.K.
2) Munish Dhar and Rajeshwar Singh, "A Review of Security Issues and Denial of Service Attacks in Wireless Sensor Networks," International Journal of Computer Science and Information Technology Research, Vol. 3, Issue 1, March 2015.
3) Genita Gautam, Biswaraj Sen, "Survey on different types of Security Threats on Wireless Sensor Networks," International Journal of Computer Science and Information Technologies, Vol. 6, 2015, ISSN: 0975-9646.
4) Kanchan Kaushal and Taranvir Kaur, "A Survey on Attacks of WSN and their Security Mechanisms," International Journal of Computer Applications, Volume 118, No. 18, May 2015.
5) Sahabul Alam and Debashis De , " Analysis of security threats in wireless sensor network," International Journal of Wireless & Mobile Networks (IJWMN), Vol. 6, No. 2, April 2014.
6) Hosam Soleman and Dr. Ali Payandeh , " Self-protection mechanism for wireless sensor networks," International Journal of Network Security & Its Applications (IJNSA), Vol. 6, No. 3, May 2014.

7) Raja Waseem Anwar , Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi, "Security Issues and Attacks in Wireless Sensor Network," World Applied Sciences Journal 30 (10): 1224-1227, 2014.
8) Naser Alajmi, "Wireless Sensor Networks Attacks and Solutions," (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 7, July 2014.
9) Mohamed Lamine Messai , " Classification of Attacks in Wireless Sensor Networks , " International Congress on Telecommunication and Application ' 14 University of A. MIRA Bejaia, Algeria, 23-24, 2014.
10) J. Steffi Agino Priyanka, S. Tephillah and A . M. Balamurugan, "Attacks and countermeasures in WSN," International Journal of Electronics & Communication (IIJEC), Volume 2, Issue 1, January 2014.
11) Dines Kumar, Navaneethan. C, "Protection against Denial of Service (DoS) Attacks in Wireless Sensor Networks," International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), Vol. 2, Issue Special 1 Jan- March 2014.
12) Anser Ghazzaal Ali Alquraishee and Jayaprakash Kar, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks," Contemporary Engineering Sciences, Vol. 7, 2014, no. 3, 135 – 147.
13) Rajkumar , Vani B. A , G. Rajaraman , Dr. H G Chandrakanth, "Security Attacks and its Countermeasures in Wireless Sensor Networks," International Journal of Engineering Research and Applications, Vol. 4, Issue 10, October 2014.
14) Sunil Ghildiyal, Ashish Gupta, Musheer Vaqur, and Anupam Semwal, "Analysis of wireless sensor networks: security, attacks and challenges," International Journal of Research in Engineering and Technology, Volume: 03 Issue: 03, Mar-2014.
15) K .Venkatraman , J. Vijay Daniel , G. Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey," International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-1, March 2013.
16) Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN," International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
17) Jatinder Singh , Dr. Savita Gupta , and Dr. Lakhwinder Kaur, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks," The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.