International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.02, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Comprehensive Study on Security Attacks and Mitigation Measures in Wireless Sensor Networks

Madhu K P

Assistant Professor, Department of Computer Science and Engineering,
Government Engineering College Idukki, Kerala, India - 685603

ABSTRACT

Wireless Sensor Network (WSN), is a major communication technology that has wide applications in domains like military, disaster management, transportation, agriculture, health, home and industry. Most of these applications usually have a hostile environment. The WSN is designed to serve these requirements in an effective manner. WSNs are prone to both active and passive type of attacks. This paper deals with various attacks on WSNs and a summary of the mitigation measures.

Keywords: Wireless Sensor Networks, security attacks

1. INTRODUCTION

Wireless Sensor Networks (WSN) [1] is a low cost technique for many applications. These networks are deployed in various applications such as environmental monitoring, health observing, habitat watching, disaster detection and management, industrial quality control and protection, transportation, law and order enforcement, agriculture, smart buildings and traffic monitoring [2] [3]. WSNs shares communication channels, adopts multi-hop communication, uses untrusted transmissions, deployed in hostile environments, and avails limited resource. Hence suitable security measures are required [4]. The WSN is vulnerable to various security attacks. The attacks are grouped as active/passive attack, External/Internal attacks, Mote-class/Laptop-class attacks and attacks on Secrecy, Availability, and Stealthy [2].

The paper is organized as follows. Section 2 gives an introduction to WSN. Section 3 discusses about the need for security, security goals and the challenges faced in providing security in WSN. Section 4 explains the various attacks in WSN. Section 5 discusses various mitigation measures.

2. INTRODUCTION TO WSN

WSNs are a distinct type of ad-hoc networks, comprising a large number of heterogeneous sensor nodes and designed to operate in hostile and conditions to sense environmental data such as temperature, humidity, pressure,

light, sound etc. The sensor nodes sense the data, process it and transmit it to a sink node through wireless links. The architecture of WSN [1] is shown in Fig. 1. The major components of a WSN are Sensor Nodes, Sink and Task Manager Node.

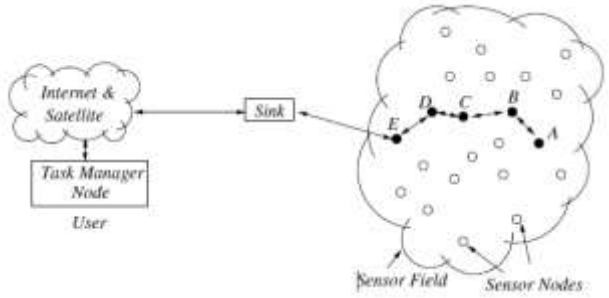

Fig.1: Architecture of WSN [1]

The protocol stack consists of five layers and a group of management planes. The attackers can attack on the different layers [1].

Characteristics of WSN [3]

- Lack of a central node
- Self-organizing nodes
- High scalability
- Dynamic network topology
- Multi-hop routing

3. SECURITY OF WSN

Security of WSNs is really significant as most of these networks are deployed in hostile environments and are vulnerable to attacks.

A. Need for Security

Since the wireless sensor network is used for many security critical applications, the secrecy and privacy of data being transmitted through the wireless medium has to be preserved. Multiple constraints that should be noted while considering a security mechanism for WSN are summarized below.

- **Wireless and Shared nature of Communication Channel:** The broadcasting nature of WSN makes it vulnerable to multiple types of security attacks. The interception, analysis and alteration of the messages transmitted via the wireless channel can be done easily by an attacker. The attacker can easily inject false data into the network that can affect the integrity of data. A jamming or Denial of Service (DoS) attack can be executed by an attacker from inside or outside the network. The attacker can obtain the details of a

legitimate node and replace that node with a malicious node. Security of data transmitted through a wireless communication channel and the security of WSN nodes itself is a great challenge.

- **Multi-hop communication:** Wireless Sensor Networks rely on multi-hop communication and thus the intermediate sensor nodes may modify or destroy the data send by other nodes. Sometimes the intermediate nodes drops the packets selectively which is very difficult to identify.
- **Untrusted transmissions:** An attacker can easily capture and modify the data send by a node if the data is not properly encrypted. All the encryption schemes used in traditional networks cannot be used in WSN due to its resource constraints.
- **Loopholes in communication protocols:** Most of the protocols developed for wireless sensor networks does not provide a full-fledged security mechanism. Since the code of these protocols are publicly available, an attacker can easily find a loophole [5].
- **Deployment in hostile and unattended environments:** Most of the wireless sensor applications uses a massive deployment of sensor nodes in harsh and hostile environments such as forest, sea etc. These sensor nodes are kept untouched or unattended for a long period of time. An attacker can physically access the node to get information, ruin the sensor node or change the sensor node by a malicious node. Also an attacker may intercept the signals from sensors, extract important information or modify the information.
- **Limited resources:** The resource constrained WSN nodes are a barrier to provide a strong security mechanism for WSN. The two major constraints are on memory and battery power. When strong security mechanisms have to be implemented, the memory and battery power requirement also increases. This makes it difficult to implement powerful cryptographic algorithms developed for traditional networks in WSN.
- **Immense Scale:** While implementing a strong security mechanism in WSN, the scale of the network plays a crucial part. The network performance in terms of computation, communication and energy efficiency has to be preserved while scaling the network by maintaining the same security features. The resource constraints are a barrier for scaling the network beyond a limit.

B. Security Goals

The goals of WSN security techniques are summarized as below.

- **Confidentiality:** Confidentiality is related to data security, secure channel and security of sensor information like keys and sensor identities. Encryption is the standard approach used to achieve data confidentiality.
- **Integrity:** Guarantees that a message is not altered or modified while transmitting through wireless medium by an adversary. This safeguards the WSN from false data injection or the modification of messages.

- **Availability:** The network is available for the nodes to communicate and resources are available for communication. Adding security to WSN should not affect the availability.
- **Freshness:** Data freshness indicates that the stream of data coming from sensor nodes are recent. That is, a sensor node is not sending or replaying any old data. The data freshness can be weak and is acceptable for sensor readings, but a strong one is required for time synchronising data [4].
- **Self-Organization:** The sensor nodes are independent and self-organizing based on the situations like frequent path breaks, security attacks and power losses. All the processing shall be distributed. Self-organization is a great challenge and its absence makes the wireless sensor network vulnerable to various attacks [4].
- **Time Synchronization:** Time synchronization is important for multi-hop networks to synchronize the local clocks of sensor nodes. Some applications demand synchronization between groups of nodes.
- **Secure Localization:** Localization enables to locate the faults with accurate location information. The location information sent by a node through the wireless medium may be easily manipulated. Thus localization schemes must be designed with security in mind [4].
- **Access Control:** Access control is provided to prevent malicious nodes joining a WSN. This gives to the legitimate participants a means to detect the messages coming from external sources of the network [6].

4. SECURITY ATTACKS ON WSN

Vulnerability to multiple security attacks exists in a WSN due to its sharing of communication channels, multi-hop communication, untrusted transmissions, deployment in hostile environments, and limited resource availability. Basically attacks are classified as active and passive attacks.

A. Active Attacks

An intruder will try to listen, monitor and alter the message transmitted on the network. The most common active attacks are given below [1] [7] [8].

- **Routing Attacks:** Routing attacks target the network layer of the protocol stack of WSN. The most common routing attacks are summarized as follows.
    - **Selective Forwarding:** All nodes in WSN try to forward the information they received. Selective forward attack is carried out by creating malicious nodes and they may refuse to forward certain messages by dropping them. One solution for this attack is to use multiple paths to send data.
    - **Spoofed Routing Information:** In a wireless sensor network, every node performs a routing or forwarding operation for other nodes in the sensor network. A malicious node may alter or spoof that routing information while routing.

- **Sink hole/ Black hole:** An opponent moulds a node that looks extra powerful and every node belongs to the network is attracted to it. A path through this node is advertised as a shortest path so that all nodes send packets to this node and ends up in a black hole and the attacker can do anything with the sensor data.
- **Sybil attack:** In Sybil attack, the attacker copies the identities of legitimate nodes and becomes part of the network. After that these nodes can affect the activities done in that network like routing operation, data storage and aggregation etc.
- **Worm hole:** A worm hole is executed by retransmitting the network messages continuously, usually done through a low delay link. The attacker records the messages in some location and later retransmits it into the network causing the network to be jammed and also affecting the integrity of data.
- **Hello flood:** The attacker uses high power transmitter to broadcast HELLO packets and the nodes receiving these packets assumes that the sender is a neighbour of it and try to transmit messages through this attacker node and thus spoofed by attacker.
- **Acknowledgement Spoofing:** An attacker node captures packets transmitted from other nodes in the network and the ACK to be sent is spoofed.

- **DoS Attacks/ jamming:** DoS (Denial of Service) affects the availability of data from a sensor network due to intentional or unintentional interruption in the network. A malicious node can intentionally jam the network using well calibrated antennas and powerful transmitters. Although all layers of protocol stack are vulnerable to jamming attacks, physical layer attacks are easy to execute and are very common in WSN.
- **Physical attacks:** Physical attacks include destruction of sensor nodes, extracting sensitive information/secrets, changing program codes, replace with a malicious node and tamper with the associated circuitry.
- **Node Replication Attacks:** The attacker creates a replica of a valid node with an id similar to a legitimate node. This replicated node can perform malicious activities within the sensor network such as alteration and destruction of packets which results in a degradation of performance of the entire network.
- **Node Outage:** A node may stop its working due to battery failure or by some other reasons. This situation is called node outage and it can degrade the performance of network. Efficient and robust protocols for WSN are required to handle the situation of a cluster head failure.
- **Node malfunction:** A faulty node can originate information that can compromise the correctness of sensor networks particularly if it is an information accumulating node like a cluster head or a sink node.
- **Passive Information Gathering:** This type of attack utilizes high end receivers and well calibrated antennas to acquire information from WSN. It allows the intruder to discover the sensors and crash them.

- **False Node:** The attacker node is added in WSN in order to inject incorrect values so as to stop the flow of actual data.
- **Node Subversion:** This type of attack controls a node and will try to disclose the key information like cryptographic and configuration specific data, thereby compromising the entire sensor network.

B. Passive Attacks

An attacker monitors, listens and analyses the traffic. The most common passive attacks are explained below [1] [7] [8].

- **Monitor and Eavesdropping:** This attack mainly affects the confidentiality and privacy. The attacker monitors and analyses the traffic, but does not make any modification to the messages. These monitored traffic may give some control information about the sensor network configuration thus enabling the attacker to plan an active attack. This type of attacks are difficult to detect because it does not alter any messages.
- **Traffic Analysis:** The attacker analyses traffic to determine actions in a WSN and also to uniquely identify specific sensors such as cluster head. By analysing the traffic patterns an attacker may get many useful data about the network. These information can be used by an attacker to carry out a DoS attack.
- **Camouflaged Adversaries:** It is a passive attack on privacy. This attack is carried out by adding a malicious sensor node or compromising a valid sensor node of a WSN. This type of camouflaged nodes can misroute packets by successfully pulling the traffic from other nodes to it.

C. Security Attacks at each Layer of WSN

Various attacks on each layer are summarized as below.

- **Physical Layer:** Denial of service attack (Jamming), Tampering, Radio interference
- **Data Link Layer:** Denial of service attack (Jamming), Collision, Continuous Channel Access (Exhaustion), Unfairness
- **Network Layer:** Denial of service attack, Selective Forwarding, Wormholes, Sinkholes, Sybil attacks, Hello Flood Attacks, Acknowledgement Spoofing
- **Transport Layer:** Denial of service attack (Flooding), Desynchronization Attacks
- **Application Layer:** Attacks on reliability

5. MITIGATION MECHANISMS

The security mechanisms helps to detect a WSN under attack and provides mechanisms to block and recoup from future attacks. Multiple security schemes are available to protect the WSN from different attacks and they can be grouped as high-level and low-level mechanisms.

A. Low-Level Mechanisms

Different low-level security schemes are used for the security of WSN, some of them are described below.

- **Key establishment and trust setup:** Different cryptographic techniques can be used to ensure security in WSN. The major challenge in these techniques is the overhead and security of processing the cryptographic keys. The main characteristics of sensor nodes is that they have limited computational power and memory, thus cryptographic primitives used in traditional networks are too expensive. Key establishment is a challenge with large scale networks which contains hundreds or thousands of nodes. If public key cryptographic algorithms are used, the compromised key leads to attack against all the nodes in the network thus affecting the security of entire system.
- **Secrecy and Authentication:** Most of the security critical applications demand the protection of data sent by the sensor nodes against traffic analysis, injection, modification, and interception of packets. Cryptography is the standard defence used to provide authentication and secrecy of data. Various cryptographic algorithms are used in WSN viz. public key cryptography, symmetric key cryptography and hybrid cryptographic techniques. Key distribution and storage are the major challenges in symmetric key cryptography. The key should be distributed to all the nodes in a secured manner. The constraints of WSN also impose challenges to the use of the most efficient cryptographic algorithms that are available for traditional networks.
- **Privacy:** Some applications demands privacy of data. Privacy can be preserved by informing the existence of WSN and by ensuring the confidentiality of data. The data acquisition and transfer must be done in a secure way [8].
- **Robustness to communication denial of service:** Denial of Service or jamming is an active attack in which the attacker strive to disturb the communication of legitimate nodes by sending a powerful signal. It is very important to detect and take countermeasures against jamming attacks as fast as possible. Although various mechanisms are available to detect and prevent jamming attack in WSN, efficient methods implemented in hardware are required.
- **Secure routing:** In any sensor network, the sensor nodes performs two important functions - Routing and data forwarding. Different routing protocols are available for this purpose, but they suffer from many security vulnerabilities [8]. The attacker can inject false data or he can spoof the routing information. An attacker node can perform selective forward attack by dropping some packets at irregular intervals.
- **Resilience to node capture:** In many applications there is a possibility of capturing the sensor nodes to modify their programs or replacing them with another node. Also cryptographic information can be exploited by the attacker. This is due to the deployment of sensor nodes in easily accessible locations. This type of node capture attacks are very difficult to detect. Highly secured packaging for sensor nodes can

prevent such attacks, but it is very expensive. An Algorithmic approach is preferred as the solution for this type of attack [8].

A. High Level Mechanisms

Some of the High-level security mechanisms used for the security of wireless sensor networks are given below.

- **Secure group management:** In a WSN nodes are usually grouped into clusters. These clusters are capable of performing data aggregation and analysis. The mobility of nodes that belongs to a group have to be efficiently managed. Group management protocols are required to accomplish the management of these groups. Group key establishment and transmission is a challenging task.
- **Intrusion detection:** Efficient and accurate intrusion detection system has to be developed for WSN. It is difficult to identify a compromised network node than an external attacker. The solution for intrusion detection should be feasible in terms of energy, communication, memory and cost requirements. Establishing secure groups and using powerful cryptographic algorithms can tackle the intruders.
- **Secure data aggregation:** One of the major task in a WSN is the aggregation of data from various sensor nodes. The point at which data aggregation take place depends mainly on the architecture of WSN that serve a particular application. False data injection and routing attacks may affect the data aggregation. All aggregation locations and data transmission must be secured.

6. CONCLUSION

This comprehensive study on WSNs explains the architecture, characteristics, various security challenges and attacks on WSNs and various mitigation measures.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"A survey on sensor networks", IEEE Communication Magazine, Aug 2002.

[2] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy,"A comparison of physical attacks on wsn", International Journal of Peer to Peer Networks, April 2011.

[3] David Culler, Deborah Estrin,"Overview of sensor networks", IEEE Computer Society, 2004.

[4] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudharyi,"Wireless sensor network security: A survey", Security in Distributed, Grid, and Pervasive Computing, 2006.

[5] Yun Zhou, Yuguang Fang, Yanchao Zhangf,"Securing wireless sensor networks: A survey", IEEE Communications Surveys and Tutorials, 2008.

[6] Sahabul Alam 'and Debashis De,"Analysis of security threats in wireless sensor networks", International Journal

of Wireless and Mobile Networks, April 2014.

[7] Abdul Wahid, Pavan Kumar, ”A survey on attacks, challenges and security mechanisms in wireless sensor network”, International Journal for Innovative Research in Science and Technology, January 2015.

[8] Dr. G. Padmavathi, Mrs. D. Shanmugapriya,”A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security, Vol 4, No 1 and 2, 2009.

[9] A. Perrig, J. Stankovic, and D. Wagner, ”Security in wireless sensor networks”, Communications of the ACM, vol. 47, no. 6, pp. 5357, 2004.

[10] Madhumita Panda,”Security Threats at Each Layer of Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[11] Abhishek Pandey, R.C. Tripathi,”A Survey on Wireless Sensor Networks Security”, International Journal of Computer Applications, Volume 3, No.2, June 2010.

[12] Yang Xiao et. al, ”A Survey of Key Management Schemes in Wireless Sensor Networks”, Computer Communications, Special Issue on Security on Wireless Adhoc and Sensor networks, 2007.

[13] Nusrat Fatema, Remus Brad,”Attacks and Counteattacks on Wireless Sensor networks”, International Journal of Ad hoc, Sensor and Ubiquitous Computing, Vol.4, No.6, December 2013.

[14] Mohamed Lamine Messai,”Classification of Attacks in Wireless Sensor Networks”, International Congress on Telecommunication and Application, April 2014.