International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

WIRELESS SENSOR NETWORK: INTERNET MODEL LAYER BASED SECURITY ATTACKS AND THEIR PANACEA

[1]D. Sowmyadevi, [2]G. Kavitha

Assistant Professor, Dept. of Computer Science,
Sri Ramakrishna College of Arts and Science for Women, Coimbatore, Tamilnadu, India
Assistant Professor, Dept. of Information Technology,
Dr. NGP Arts and Science College, Coimbatore, Tamilnadu, India.

ABSTRACT - *A Wireless Sensor Network is a consisting of widely distributed independent devices using sensor nodes to observe physical or environmental conditions. Today's era, it is implemented in potential applications like healthcare, smart home, logistics, intelligent buildings, aircraft, wind speed and direction, pressure, etc. There are many limitations, untrustworthy communication between the nodes is mostly found in unreachable locations. WSN are highly vulnerable in their security. Generally its applications are mounted in hostile environments to collect different kinds of data, so there are many possibilities to face serious of active and passive attacks due to interaction among the devices in the network, unreliable transmissions, and deployment in open environments. This paper, mainly deals with various types of attacks in WSN and to overcome from these attacks, which speaks a lot about Internet model layered attacks and it analyses the main attacks, and their main characteristics.*

Keywords: Security Objectives, Three Cross Layer, Active and Passive attacks, Cryptography, Internet Model Layer, Denial of Service.

1. INTRODUCTION

WSN consists of many sensor nodes rely on the specific location and type of applications is mounted. A sensor network comprises a collection of small battery-powered devices that monitor and record conditions in many environments. The sensor node plugged with network, like an enterprise WAN or LAN, or a specialized industrial network so that collected information can be transferred to back-end systems for analysis and used in applications. Typically a sensor network follows a tree topology, with nodes sending data to the root of the tree for delivery. WSNs are usually more at risk to various security threats since it uses the unguided transmission medium which leads to more prone to security attacks, but also through traffic analysis, privacy violation, physical attacks and so on [7]. In many applications the data obtained by the sensing nodes need to be authentic. An intruder node could intercept confidential information in the absence of proper security or could send false messages to nodes in the network.

2. OBJECTIVES

Security mechanisms are require to safely transfer the confidential information and resources from attacks and misbehavior. WSNs must support all security objectives such as availability, authenticity, integrity and confidentiality.

Availability: The entire yearned sensor network services are available during communication.

Authentication: It represents the process of giving individuals access to system objects based on their identity. It is also responsible for a genuine communication between two nodes, i.e., a fake node cannot cover-up as a trusted node.

Integrity: It makes sure that a message sent from one sensor node to another is not modified by fake intermediate nodes.

Confidentiality: Transferred data can be understood by the intended receiver not by the intruders.

Robustness: To prevent attacks, Sensor network should be strong enough.

3. ARCHITECTURE OF WSN

The most common WSN architecture follows the OSI architecture model. It includes five layers and three cross layers. The five layers are Application, Transport,

Network, Data Link and Physical layers. The three cross planes are namely Power, Mobility and Task management plane. These layers of the WSN are used to accomplish the network and make the sensors work together. The layered model is essential to raise the complete efficiency of the network, categorizing protocols, attacks and their protections. Fig.1 illustrates the structure of internet model and cross layers in wireless Sensor Networks.

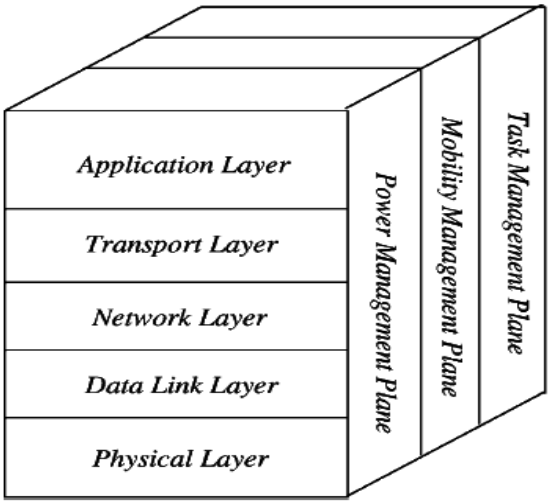

Fig.1: Structure of Internet model and Cross layers.

The Three cross layer's functionalities are,

Power Management Plane: It provides the power to the sensor nodes and maintains the power level among the devices [10].

Mobility Management Plane: It detects the mobility of the sensor nodes and keeps track of neighboring nodes.

Task Management Plane: It is responsible for assigning the tasks to the sensor nodes to extend network lifetime and increase energy efficiency [10].

The five Internet Model layer's functionalities are,

Application Layer: It defines a standard set of services and interface primitives available independently for the programmer based on their platform.

Transport Layer: It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components.

Network Layer: It is responsible for routing the packets in the selected path over network.

Data Link Layer: It provides multiplexing of data streams, data frame detection and MAC.

Physical Layer: It is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium and handles the encryption and decryption process.

4. COMPONENTS OF SENSOR NODES IN WSN

It enables wireless connectivity within the network, connecting an application platform at one end of the network with one or more sensor devices in Wireless Sensor Network. It made up of software and hardware components, which consists of four parts [10].

i. Sensors Connected to each node by a wired connection. Sensors which measures the water pressure, flow rate, electrical connectivity and a range of weather variables like light, air, temperature, wind and humidity.

ii. Nodes collect the data from sensors and transmit that to a 'base station' computer using a one way or two-way radio signals. It contains several technical components. These include the radio, battery, microcontroller, analog circuit, and sensor interface. The Fig.2 represents the components of sensor nodes and its interfaces.

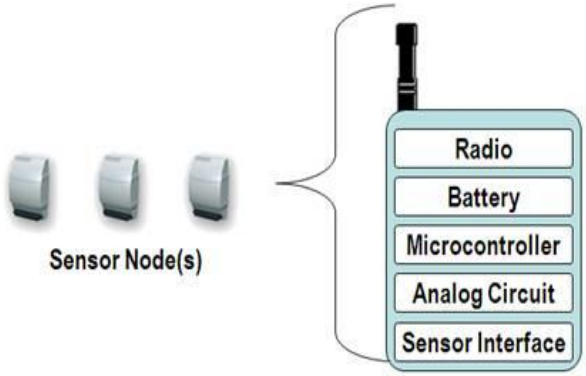

Fig.2: Components of Wireless Sensor Node and its devices

iii. Base Station computer connects the system to the internet, so that data collected by the nodes, then transmitted to the base station computer and data will be available in the internet.

iv. Graphical user interface is the web based software package that allows the data collected by the sensor nodes which can be accessed, interpreted and viewed.

While establishing a WSN the above mentioned components are not same for all wireless sensor application.

5. CLASSIFICATION OF ATTACKS IN WSN

Generally attacks are happening either by passively or actively through intruders. An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access. Traffic can be overheard by any adversary in the radio range which affects the network communication between source and destination. Because of the vulnerable structure of WSNs and the nature of DoS attacks it may be difficult to distinguish between an attack and a network failure. This paper mainly represents possibilities of attacks in Internet Model of WSN.

5.1 Passive and Active Attacks:

Attacks can be classified into two major categories namely passive attack which include unauthorized reading of a message of file and traffic analysis and active attacks, such as modification of messages or file and Denial of services.

There are two types of passive attacks are release message contents and traffic analysis. Examples of passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of adversary is to obtain information that is being transmitted.

Eavesdropping: Secretly listening real-time interception of a private communication. Such as a phone call, instant message and videoconference or fax transmission.

Traffic analysis: The process of intercepting and examining messages in order to deduce information from patterns in communication.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. When the messages are exchanged neither the sender nor the receiver is not aware that a third party has read the message. It can be prevented by encryption of data.

Active attacks are difficult to prevent due to wide verity of potential physical, software and network vulnerabilities. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

Jamming: It is a subset of denial of service (DoS) attacks in which malicious nodes block genuine communication by causing planned interference in networks.

Impersonation: An adversary assumes the identity of one of the genuine parties in a system.

Replay Attack: A valid data transmission is maliciously or fraudulently repeated or delayed. It can be prevented by using digital signatures which include time stamps. It is also called as playback attack.

5.2 Internal and External Attacks:

According to the domain of attacks, attacks can be classified into external and internal attacks. External attacks are happened by nodes that do not belong to the domain of the network [2]. Internal attacks are compromised nodes, which are truly part of the network. It is more severe when compared with external attack. Since the insider knows precious and secret information, and possesses privileged access rights.

5.3 Cryptography and Non Cryptography Related Attacks:

Cryptography deals with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages. There are two types of cryptographic approaches are symmetric and asymmetric algorithm. Symmetric algorithm makes use single public key and Asymmetric algorithm makes use of private and public key. Generally it is a method of storing and transmitting data in a particular form, so that only those for whom it is intended can read and process it.

The basic intention of an attacker is to find the plaintext from ciphertext by using one of the keys of sender or receiver. The cryptographic attacks are Analytic, Implementation, Statistical, Meet-in-the-Middle and Replay attack to discover encryption key or the encryption algorithm used.

5.4 Various Attacks in Internet Model Layer:

According to the five layers of the Internet model the attacks are further classified. Table1 presents a classification of various security attacks on each layer. Attacks can occur at any layer such as physical, link, network, transport, and application of WSN layers etc. Most of these routing protocols are not designed to have security mechanisms and it makes it even easier for an attacker to break the security [6]. In the following section deals with the layer wise attacks in WSNs.

WSN Layer	Attacks
Application	Data corruption, Denial-of-Service, Cloning
Transport	Flooding , Session hijacking
Network	Hello Flood, Selective Forwading , Wormhole, Sybil, Sinkhole , location disclosure attacks
Data Link	Collision, Exhausting
Physical	Jamming, Tampering, Sybil

Table 1: Security Attacks on Each Layer of the Internet Model

5.4.1 Physical Layer:

Attacks like jamming of radio signal, tampering with physical devices are found in this layer.

Jamming: Adversary nodes disrupt the communication frequencies of required sensor network. If only one frequency is used throughout the network then jamming can affect the whole sensor network. Due to this, Energy consumption is increased at nodes. Thus the communication channel is Jammed. To handle these Issues symmetric key algorithms are used.

Tampering: Attacker can take out sensitive information like message or cryptographic key. The sensors nodes are also tempered or swap to create a fake node which the attacker operates which means physically modifying and destroying sensors nodes. To remove this issue Tamper-proofing, hiding and protection are required.

Interference: Malcious sensor nodes produce collisions or interferences in the transmission. To remove this issue blacklisting and channel hoping are used.

Sybil: In this attack, one adversary sensor nodes assumes multiple identities to all other sensor nodes in the WSN. This reduces the effectiveness of WSN. The physical devices need to be protected from Sybil attack. Sybil attack affected the following protocols and algorithms:

1. Network topology maintenance
2. Fault-tolerant
3. Distributed storage
4. Geographic routing protocol

5.4.2 Data Link Layer:

Collision: An attacker induces minute change in data packet will result in checksum mismatch [1]. Then the packets will be rejected as invalid. This may cause retransmission of data packets. To avoid collision, error correcting code, CRC and time diversity techniques are used.

Exhaustion: The nodes are continuously disturbed using repeated collision method by an attacker. Due to this energy level of a node is quickly decrease. To avoid Exhaustion, protect the network ID and limited the data rate.

Spoofing: When a malicious node impersonates another device on a network in order to commence attacks against network hosts, steal data, spread malware or bypasses access controls. An adversary is able to spoof link layer acknowledgements, after overhearing the packets [4]. This issue can be resolve by using various paths, for re-sending the messages.

Sybil: To block the Sybil attack at link layer the security keys need to be changed regularly . This is a popular attack of DOS. Voting and data Aggregation are two types of Sybil attacks.

a) Voting: An adversary try to find out the outcomes of any voting depending on the number of identities of the adversary owns.

b) Data Aggregation: A spiteful node may act as dissimilar Sybil nodes and these may give much harmful reinforcement to make the collective information a false one.

Traffic Analysis: An attacker analyzed the communication channel of sensor network to damage to the sensor network.

5.4.3 Network Layer:

Wormhole: An attacker can easily launch the wormhole attack without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms. It is caused due to formation of a low - latency link that is formed so that packets can travel from one to the other end faster than normally via a multi-hop route.

Sybil: In this attack, one adversary sensor nodes assumes multiple identities to all other sensor nodes in the WSN. This reduces the effectiveness of WSN. A fake node

appears at several places at same time. Sybil attacks are prevented by changing the security keys and resetting the network devices.

Sinkhole: An attacker establishes a malevolent, stare more attractive to adjacent nodes by unfaithful routing information. A malevolent sensor node works as a black hole. That's why Sinkhole attack is also called Black hole attack.

Selective Forwarding: In the multi-hop networks all nodes exactly forward received data, but the attacker developed a malevolent sensor nodes which selectively forward only certain data and drop others data [4].

There are two methods to protection from Selective Forwarding.

1. Using several paths to send data and
2. Detect the malevolent sensor node then disastrous.

Hello Flood: The sensor nodes transmit the HELLO packet to broadcast themselves to their neighbors. The receiving nodes, which accept such message, should be inside a radio range of the sender. In this type of situations the hypothesis may be phony. To prevent the Hello flood attack, Authentication and verification of bidirectional link are required.

Acknowledge Spoofing: Sometimes acknowledgements are required in routing algorithm used by sensor network. An adversary node can spoof the Acknowledgments of overheard packets intended for adjacent nodes in order to supply fake message to those adjacent nodes.

5.4.4 Transport Layer:

Flooding: It is designed to bring a network or service down, by flooding with large amounts of traffic. That it cannot, longer process genuine connection requests. By flooding a server, it eventually fills the servers' memory buffer and once this buffer is full, no further connections can be made, and thus resulting in a Denial of Service. To overcome this problem use a client puzzles.

Session Hijacking: It is the exploitation of a valid computer session to gain unauthorized access or services in a computer system that is present in the cookie. It is also known as cookie hijacking.

5.4.5 Application Layer:

Denial-of-Service (DoS): The process of destroying or destructing the sensor network which leads to consumption of bandwidth or consumption of processor time, obstructing the communication, disruption of service to a specific system, routing information, physical components etc. As a result, it makes the system or service unavailable for the user. This attack progressively reduces the functionality as well as the overall performance of the wireless sensor network.

Malicious code attacks: It is an application security threat that cannot be efficiently controlled by antivirus software. It can spread by itself through the network to make the mail server overload by sending email messages, stealing data and passwords, deleting document, email files or passwords and even reformatting hard drives. The other terminologies represent malicious code is attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content.

Repudiation attacks: A transaction or communication happens in the network. Later information is not available when the user claims for it.

Cloning: Adversaries may easily capture and compromise sensors nodes to deploy unlimited number of clones in the sensor network. These clones have legitimate access to the sensor network and easily participate in the sensor network operations. That a legitimate node resulting in a large variety of insider attacks or even taking over the entire networks. If it is not detected the sensor network is unshielded to attackers. So it is severe to destruct.

6. CONCLUSION

In Wireless Sensor Networks, security is an essential feature and its attacks are still a big challenge. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. The Sinkhole and Wormholes creates a lot of challenge to protect the routing protocol proposal. The detection and solution of these attacks are not easy. This paper summarizes the architecture, components, the attacks and their classifications. Also an attempt has been made to overcome the issues arises in the security mechanism. Hopefully this paper motivates future researchers to come up with smarter and more robust security mechanisms and make their network safer.

7. REFERENCES

[1] Rupinder Singh, Dr. Jatinder Singh, Dr. Ravinder Singh, "Attacks In Wireless Sensor Networks: A Survey", International Journal of Computer Science and Mobile Computing,IJCSMC, Vol. 5, Issue. 5, May 2016, pg. 10 – 16.

[2] Teodor-Grigore Lupu, "Main Types of Attacks in Wireless Sensor Networks", Recent Advances in Signals and Systems, ISBN: 978-960-474-114-4, ISSN: 1790-5109.

[3] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy , "A Comparison Of Physical Attacks OnWireless Sensor Networks" , International Journal of Peer to Peer Networks (IJP2P) Vol.2, No.2, April 2011

[4] Payam P R, Maysam G, Sassan P3, Jasem T4, Hamidreza H, and Pasha P R, "Types of Attacks Penetrating Wireless Sensor Networks and Strategies to Overcome Them", International Conference Data Mining, Civil and Mechanical Engineering (ICDMCME'2015) Feb. 1-2, 2015.

[5] Kamaldeep K, Parneet K, Er. Sharanjit S," Wireless Sensor Network: Architecture, Design Issues and Applications", International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014.

[6] 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 APRIL.

[7] 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 ISSN: 2277.

[8] S.Nithya, K.VijayaLakshmi, V.PadmaPriya, " A Review of Network Layer Attacks and Countermeasures in WSN", *IOSR* Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735. Volume 10, Issue 6, Ver. III (Nov - Dec .2015), PP 10-15

[9] Pitipatana Sakarindr And Nirwan Ansari, "Security Services In Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, And Wireless Sensor Networks", IEEE Wireless Communications Volume: 14 Issue: 5.

[10] R. Rathika, D. Sowmyadevi , " Wireless Sensor Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 1, January 2016, ISSN: 2277.

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