Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

LAYER SPECIFIC CLASSIFICATION OF THREATS TO WIRELESS SENSOR NETWORK

Viralkumar B. Polishwala[1], P. H. Bhathawala[2]

[1]Asst. Professor, Sutex Bank College of Computer App. & Sci., Amroli, Surat

[2] Professor & Head, Department of Mathematics, VNSGU

Abstract—Recent advances in sensing technology, wireless communication, and digital computing techniques have led to the creation and subsequent proliferation of wireless sensor networks (WSNs). In past years WSNs have been applied to many areas like Military, Civilian, Health Care, Acoustic and Video Surveillance, Industrial Process Control as well as Home Intelligence. [1] It can reach to any location on the globe. It is composed of large no of independent sensing nodes which communicates to each other without physical connections. Since large no of users are working on the single channel of wireless the security of WSN become huge concern. It may face challenges for the privacy of data, distribution of information; signal loses and so on at various layers under the OSI model among which the information travels. This paper will provide the survey of such layer specific threats to the WSN since the network is in the base of it.

Keywords—Cryptography, Data Authenticity, Layer-specific Attacks, Network Attacks, Security Threats, Wireless Sensor Networks

I. INTRODUCTION

In the current technology oriented era, networks can work as basic platform for business entity and for personal use. It cannot only play an important role for information storage, but also act as crucial role in the Information process with various techniques to meet the needs of networks users. With powerful ability to handle complex applications, the network can work as a virtual society of real life world, such as virtual university (education), virtual game environment, virtual social network etc. each network either internet or ad hoc wireless sensor network, is vulnerable to malicious activities. Since the wireless sensor networks are made of large no. of sensor nodes with limited resources and one or more base stations or sink (gateway) which are deployed to connect with another network. (Figure - 1)

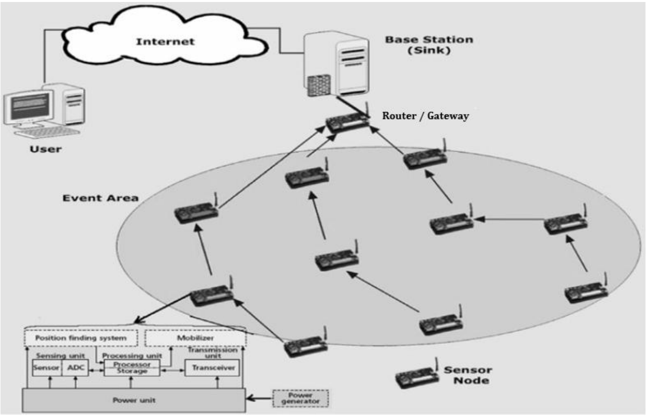

Figure-1 Basic Architecture of Wireless Sensor Network

Since the networks have grown in size and importance both; if the security is compromised than there may be the possibilities of theft of information, loss of privacy as well as bankruptcy of that institution. As the rise of network implies that the security solutions become seamlessly integrated.

This paper is organized as follows: section II describes the basic terms of individuals which are involved positively or negatively in threats to the WSNs, section III describes the possible threats at various OSI Network layers, section IV describes the conclusion of this paper.

II. TYPES OF ATTACKERS

Various type of attackers who threaten the network security on certain areas are described below.[2]

White Hat
It is an individual Security expert who is looking forward for vulnerabilities to improve the network security. They are basically appointed by the owners of the systems to prevent the attacks.

Hacker
It is the most commonly used term to identify the computer programming experts who works maliciously to break down the network system. They accesses the system unauthorized manner to damage the information.

Black Hat
They are the individuals who use their knowledge to break the network system that they are not authorized to use. They do such things for personal or financial benefits.

Cracker
It is more appropriate term for the individual who tries for access the network for destruction of the information and ones privacy.

Phreaker
An individual who enters into the phone network for managing the long distance calls in unauthorized way.

Spammer
This term is used for personnel who send large number of mails by using certain viruses. They enters in home computer and uses such viruses to send emails in bulk size.

Phisher
This term is for individual who uses emails or other tricks to get sensitive information likewise credit card, bank account details or passwords etc.

Most of these attacks are revolved using the layered approach. OSI model is consists of 7 protocols. The approach of layers stack is consisting 5 protocols which are Application Layer, Transport Layer, Network Layer, Data Link Layer and Physical Layer. The layer stack works with three planes which are; Task Management, Mobility Management and Power Management. Collectively theses layers and planes constructs Wireless Layered Architecture. [5][Figure-2]

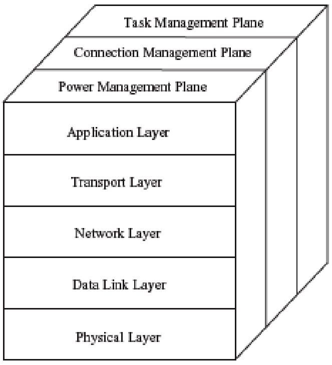

Figure-2 OSI Layered Plane for WSNs

III. LAYERED SECURITY THREATS

The security threats at various layers of OSI model can be classified as follows:

A) Security threats at Physical Layer

The physical layer is liable for signal transmission and reception over a physical communication medium, including frequency generation, signal modulation, transmission and reception, data encryption, and so on. The data is broadcasted in wireless networks. The attacker use radio signals to disrupt or overhear the service of the network physically. Threats at this layer are: Jamming / Interference and eavesdropping.

Jamming / interference: By using noise and pulse the data signals can be easily interfered or may be lost totally. The attackers normally use transmitters or jamming equipments to target the data signal or disrupt the communication over network. Such devices can be managed from remote locations to targeted location.

Eavesdropping: Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. The term *eavesdrop* derives from the practice of actually standing under the eaves of a house, listening to conversations inside. VoIP systems that don't use encryption make it relatively easy for an intruder to intercept calls.

The attacker effectively uses the LAN environments with Hubs and Switches an wireless environment.

B) Security threats at Data Link Layer

The data link layer is liable for data stream multiplexing, data frame creation and detection, medium access, and error control in order to provide reliable point–to–point and point – to – multipoint transmissions. One of the most important functions of the data link layer is medium access control (MAC). The primary objective of MAC is to fairly and efficiently share the shared communication resources or medium among multiple sensor nodes in order to achieve good network performance in terms of energy consumption, network throughput, and delivery latency.

Most common threats on Data link layer would be MAC address alteration and MAC Flooding attacks. Network device or host under MAC Flooring attack will be taken all the CPU resource. By MAC address alteration, traffic flow can be changed easily, once attacker finds a security hole on the switch.

MAC Flooding attacks are dumping massive MAC addresses were created by auto tool. It makes overflow of MAC table (CAM table) on the switch. The switch is running in malfunction or getting slow (crashing).

ARP attack is another pattern of data link layer threat. First, attacker finds a LAN port and sniffing a live traffic to choose victim. They pick an active MAC address which is actively communicating to server or other host. By using MAC duplicator/Hacker's tool, intercept communication and collect important information such as login/password and so on.

C) Security threats at Network Layer

The network liable is responsible for routing the data sensed by source sensor nodes to the data sink(s). In a sensor network, sensor nodes are deployed in a sensing region to observe a phenomenon of interest. The observed phenomenon or data need to be transmitted to the data sink. In general, a source node can transmit the sensed data to the sink either directly via single – hop long – range wireless communication or via multihop short – range wireless communication.
Threats at this layer are wormhole attack, blackhole attack, sinkhole attack, sybil attack and acknowledgement spoofing attack.

Wormhole Attack: It is the one of the most severe security attack on the network layer. In this kind of attack the attacker generates a fake route which is shorter than the originsl one within the network only. [Figure-3] The routing mechanism works on the knowledge of the distance between the nodes so it won't be able to work properly. There may be one or more malicious nodes and tunnel among them exists. The attacker captures the packets sent over the network by using such malicious node and then transmits the packet on other node locally. The attacker doesn't require to have deep knowledge about the network or compromising any legitimate nodes or cryptography techniques.

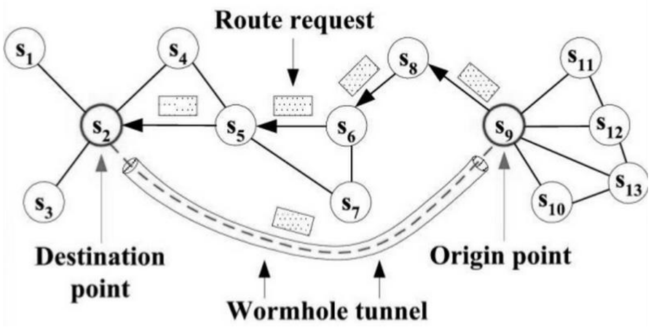

Figure-3 Wormhole Attack on Network

The tunnel is either the wired link or high frequency links, which creates an illusion that the two end pointsof the tunnel are very close to each other.

Blackhole Attack: A malicious node's routing protocol is used by the attacker to advertise itself for intercepting the packet located at the destination node by creating the shortest path.[15] The hostile node advertises its availability of fresh routes without checking the routing table. So the attacker node always possesses its availability to routing the pockets and keeps the packets with it. When the routing protocol is used the forged route restricts the sending of the packets to the original recipient. One such situation is depicted in the following figure. [Figure-4]

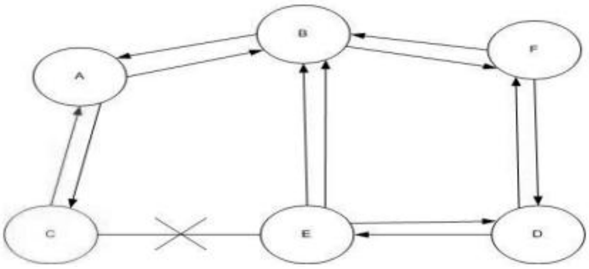

Figure-4 Black hole Attack on Network

Sinkhole Attack: One of the least talked but one of the most effective network security technique is sinkhole attack. The attacker node tries to attact the data to itself from all the neighbouring nodes. [Figure-5] It generates the fake routing information. The atacker node attempts to draw all network traffic to itself. Thereafter the attacker node silently drops or alter the data packet. This attack increases the network overhead, decreses the network lifetime due to energy consumption, and at the end destoys the network,[14]

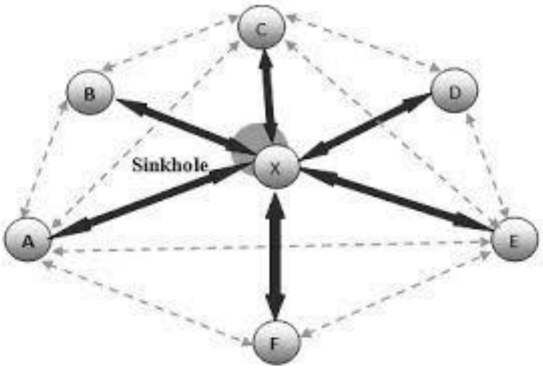

Figure-5 Sinkhole Attack on Network

Sybil Attack: A sybil attack is a security attack on peer to peer network; where the attacker node is illegitimately takes on multiple nodes identity. [Figure-6] The additional identities are known as sybil nodes. The attack targets the reputation system of the P2P program and allows the hacker to have an unfair advantage in influencing the reputation and score of files stored on the P2P network. Several factors determine how bad a Sybil attack can be, such as whether all entities can equally affect the reputation system, how easy it is to make an entity, and whether the program accepts non-trusted entities and their input. Validating accounts is the best way for administrators to prevent these attacks, but this sacrifices the anonymity of users.

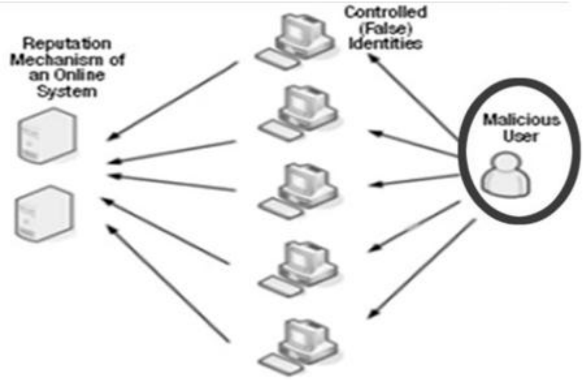
Reputation Mechanism of an Online System
Controlled (False) Identities
Malicious User

Figure-6 Sybil Attack on Network

Acknowledgement Spoofing Attack: By using some specific programs the attacker node sends an acknowledgement of recieveing the data packet sent over the neighbouring nodes which results in falsifying the data and then gains the illegitimate advantage of it.

D) Security threats at Transport Layer

In general, the transport layer is liable for reliable end – to – end data delivery between sensor nodes and the sink(s). Due to the energy, computation, and storage constraints of sensor nodes, traditional transport protocols cannot be applied directly to sensor networks without modification.
Most common threats at this layer are session hijacking attack and SYN flooding.

Session Hijacking Attack: This attack is cause by interuppting already established TCP session during packet transmission. The attacker controls a session established between two nodes. Since most authentication processes are carried out only at the start of a session, once the session between two nodes gets established, the adversary node disguises as one of the end nodes of the session and hijacks the session.

SYN Flood Attack: A normal three way handshake exchange among the client and server can be describes as: 1) client requests with synchronize message (SYN) to the server 2) Server replies with synchronize acknowledges message (SYN-ACK) to the client 3) client responds with the acknoledgement of connection establishment, the attacker send repeated SYN requests to the every port on the server by using some fake IP. The server, unaware of the attack, receives multiple, false requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port. The client does not respond with the acknowledgement message to the server while the server waits for having the acknowledgement from the client for quite long. The server can't do anything except waiting to get connection timeout. Such attack is also known as Half open attack which results in server malfunction or crash sometimes..

E) Security threats at Application Layer

The application layer includes a variety of application – layer protocols that perform various sensor network applications, such as query dissemination, node localization, time synchronization, and network security.

The main attack at this layer is attack on relaibility.
Attack on reliability: If an attacker is able to put an attacker node intermediate on the communication path which can change the data available on the packet, big question rises on the reliability of the data packet.

IV. CONCLUSION

Many wireless sensor networks collect sensitive information. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. In this paper we have discussed the threats and vulnerabilities to WSNs and we have summarized the OSI layer based categories of such threats. Theses threats could even prone to collapsethe entire systems and networks, so adding security in layered WSNs with minimum overheadprovides significant challenges.

REFERENCES

[1] https://en.wikipedia.org/wiki/Wireless_sensor_network
[2] TEODOR-GRIGORE LUPU, "Main Types of Attacks in Wireless Sensor Networks", RASS, Page:180-185, 2009.
[3] WaltenegusDargie, Christian Poellabauer, "Fundamentals of Wireless Sensor Networks- Theory and Practice", Wiley Pub., 2010.
[4] KAZEM SOHRABY, DANIEL MINOLI, TAIEB ZNATI, "Wireless Sensor Networks – Technology Protocols and Applications", Wiley & Sons Pub., 2007.
[5] Mohammed Lamine Messai, "Classification of Attacks in Wireless Sensor Networks", ICTA, 2014.
[6] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, page. 681 – 688, 2004.
[7] I. Khemapech, I. Duncan and A. Miller. "A survey of wireless sensor networks technology", In PGNET, Proceedings of the 6th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting, June 2005.

[8] K.Venkatraman, J. Vijay Daniel, G.Murugaboopathi, “Various Attacks in Wireless Networks : Survey ”, IJSCE, Page:208-211, 2013.

[9] Mahsa Teymourzadeh, Roshanak Vahed, Soulmaz Alibeygi, Narges Dastanpor, “Security in Wireless Sensor Networks : Issues and Challenges”, IJCNCS, Page: 329-334, 2013.

[10] Navjot Sidhu, Monika Sachdeva, Krishan Kumar, “ Wireless Sensor Networks challenges and Attacks : A Review ”, ICCCS, Page: 106-109, 2014.

[11] Sona Malhotra, Rahul, “Security Threats in Wireless Sensor Networks”,JGRCS, Page:99-101, 2011.

[12] Kalpana Sharma, M. K. Ghose, “Wireless Sensor Networks – An overview on Its Security Threats”, IJCA, Page:42-45, 2010

[13] Madhumita Panda, “Security Threats at each layer of Wireless Sensor Networks”, IJARCSSE, Vol.3, Page: 61-67, 2013.

[14] Anitha S. Sastry, Shazia Sulthana, Dr. S. Vagdevi, ”Security Threats in Wireless Sensor Networks in Each Layer ”, IJANA, Vol.04, Pages 1657-1661, 2013.

[15] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, International Conference on Advaificances in Space Technologies.