Security Issues and Challenges in Wireless Sensor Network - Review

K.Gowri
Asst. Professor in Department of Computer Science, Kovai kalaimagal College of arts and Science, Coimbatore

***Abstract*- Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. A sensor network comprises a group of tiny, typically battery-powered devices and wireless infrastructure that monitor and record conditions in any number of environments -- from the factory floor to the data center to a hospital lab and even out in the wild. A wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. Wireless sensor network is one of the growing technology for sensing and performing the different tasks. In this paper we present a survey of security issues in WSNs. First we outline the constraints, architecture of wireless sensor network, Challenges of WSN, and attacks in WSNs.**

***Index Terms*- Architecture of wireless sensor network, Challenges of WSN, and attacks in WSNs.**

I. INTRODUCTION

The improvement in wireless communications and electronics has enabled the development of low-cost sensor nodes that are small in size and communicate unbound short distances. . The sensor networks can be used for various application areas (e.g., health, military, home). The assembly of network consists of sensing entity, computing and processing entity and wireless communication entity. There are two types of motes- sink mote and the sensor motes. The sink node is also called base station. It instructs the sensor nodes about the type of data to be collected from the area under surveillance. The sensing unit of WSN which consists of the sensor nodes gathers the information and reports back to the sink node. The storage and processing of data takes place in the computing unit[1].

The WSN is distributed and highly vulnerable wireless communication, anyone can intercept into the network and therefore the risk of transmitting the data securely has in-creased. There is a chance of eavesdropping, tempering with data etc. Because sensors do not have high computation re-sources, therefore, traditional methods with huge computation for data transmission are unsuitable for WSN [2].

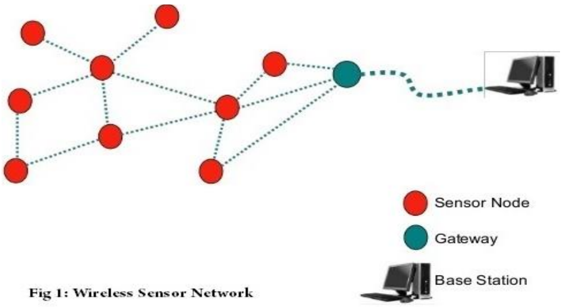

Fig 1: Wireless Sensor Network

1.1 *Architecture of Wireless Sensor Network*

- Sensor nodes With limited capabilities deployed in the sensor field communicate to a powerful BS that links them to the Internet and a central manager for processing the sensed data.
- Communications to the BS have to go through several sensor nodes first, because all sensor nodes will not be typically able to communicate directly with the BS.
- This may be due to limited communication range, distance from the BS, intermittent sensor activity, and so on.

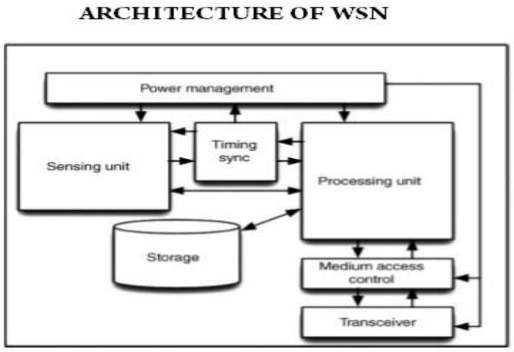

Fig 2: Architecture of WSN

1.2 *Characteristics of Wireless Sensor Network*

- Self – Organization
- Concurrency processing

- Low cost
- Restricted energy resources
- Tiny
- Small radio range

1.3 Advantages of a WSN

- It avoids a group of wiring
- It Can provide accommodation new devices at any time
- Network travels can be carried out without immovable infrastructure.
- Flexible to go through physical partitions
- It can be accessed through a centralized monitor
- Implementation pricing is inexpensive.

1.4 Wireless Sensor Network Challenges

- Fault Performance
- Scalability
- Production Cost
- Operation Environment
- Quality of Service
- Data Aggregation
- Data Compression
- Data Latency
-

A .Fault performance:

Some sensor nodes may fail due to lack of power, have physical damage. The failure of sensor nodes should not affect the overall task of the sensor network. This is the fault tolerant issue. Fault tolerant is the ability to sustain sensor network functionalities without any interruption due to sensor node failures.

B. Scalability:

The number of sensor nodes deployed in the sensing area may be in the order of hundreds, thousands or more and routing schemes must be scalable enough to respond to events.

C. Production costs:

Since the sensor networks consists of large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the networks and hence the cost of each sensor node has to be kept low.

D. Operation environment:

We can set up sensor network in the interior of large machinery, at the bottom of an ocean, in a biologically or chemically contaminated field, in a battle field beyond the enemy lines, in a home or a large building, in a large warehouse, attached to animals, attached to fast moving vehicles, in forest area for habitat monitoring etc .

E. Quality of service:

The quality of service means the quality service required by the application, it could be the length of the life time, the data reliable, energy efficiency.

Data Aggregation: Data aggregation is a combination of data from different sources by using functions such as min, max, and average.

F. Data Compression:

Reducing the size of the data is called data compression.

G. Data latency:

These are considered as the important factors that influence routing protocol design. Data aggregation and multi-hop relays cause data latency

II. ATTACKS IN WSN

Attacks can take place at any layer such as physical, link, network, transport, and application etc. Most of these routing protocols are not planned to have security mechanisms and it makes it smooth easier for an attacker to break the security.

A. Physical layer attacks

- Jamming – It is caused due to interference with the radio frequencies of the network's devices which is an attack on the availability of the sensor network. It is different from normal radio propagation in the way that it is unwanted and disruptive, thus resulting in denial-of-service conditions.
- Tampering – It is also called node capturing in which a node is compromised, it is easy to perform and is pretty harmful. Tampering is physically modifying and destroying sensors nodes.

B. Link layer attacks

- Collision – It is caused in link layer that handles neighbor-to-neighbor communication along with channel arbitration. Entire packet can be disrupted if an adversary is able to generate collisions of even part of a transmission, CRC mismatch and possibly require retransmission can be caused by a single bit error.
- Exhaustion – Exhaustion of a network's battery power can be induced by an interrogation attack. A compromised node could• repeatedly send thus consuming the battery power more than required.

C. Network layer attacks

- Wormhole attack - In this type of attack, malicious nodes make a tunnel which is hidden from the other genuine nodes. The data packets are sent from one malicious node to another via that tunnel, that is, the malicious node attract the packets from one area and passes them to other malicious node in another area [3]. Tunnel can be made through many ways such as in-band and out-of-band. To launch this attack, there is no need to compromise the other genuine network nodes. Therefore, this operation can extremely affect the routing procedures and the localization and can also launch attacks such as eavesdropping, replay attacks etc. against traffic packets. This attack can be established by using following techniques: wormhole using encapsulation, packet relay, high power transmission, out-of-band channel [4]. This attack occurs at network layer. In Figure 3, The tunnel is either the wired link or a high frequency links. This creates the illusion that the two end points of the tunnel are very close to each other.

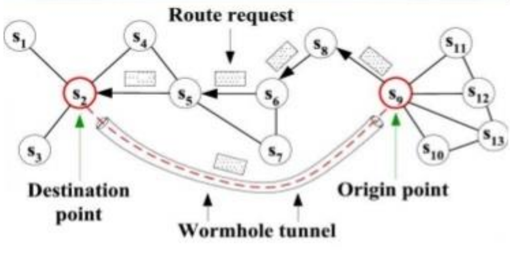

Fig 3: Wormhole attack

- Sybil Attack - In Sybil Attack, a single attacker makes and presents different identities to the other nodes in the sensor network. It can also be considered that "It can be in more than one place at once" [6]. Malicious nodes are known as Sybil nodes. This attack is used against redundancy mechanism of distributed systems. In WSNs, Sybil attack is generally used to attack several types of protocols [7]. This is a serious threat to a locality based protocols in which locality information is exchanged for efficient routing.
- Sinkhole Attacks - In sinkhole attack, a malicious node advertises fake routing information to attract the network traffic [10]. Network layer is affected by this attack. The neighboring nodes are forged by the attackers. The opponent attracts the nearby motes by using attractive bandwidth or path and fools the motes. The fooled motes route data to the compromised node resulting in packet dropping. This may further lead to selective forwarding or blackhole attack.

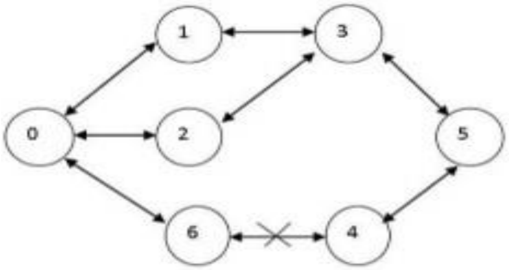

Fig 4: Sinkhole Attacks

- HELLO Flood Attacks- Hello packets are broadcasted to the network by the malicious nodes. High power RF transmitters are used. This is done to make the nodes believe that the malicious nodes are the neighborhood nodes. Thus the unauthorized users have the access to the channel. This results in loss of information as the legitimate user doesn't get the access to the channel. Network layer is affected by the hello packets[16].

D. Transport layer attacks

The objectives of TCP-like Transport layer protocols in WSN include setting up of end-to-end connection, end to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, the mobile node is vulnerable to the classic SYN flooding attack or session hijacking attacks [11] [13]

[14]. Attacks of the transport layer protocol are flooding and de-synchronization. Flooding attack is used to deplete the node's memory by sending numerous requests for connection establishment [12]. In the de-synchronization attack, the attacker node forges packets to at least one or both ends of a connection using different sequence numbers on the packets. In this way, host requests for retransmission of the missed packet frames[15].

E.. Application layer attacks

Denial-of-Service Attack- A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

III. CONCLUSION

This paper things to see the security issue of the WSN. Security is the big challenge in the sensor network. Due to continue development of wireless sensor networks, the require for more efficient security mechanisms is also growing. A complete understanding of the capabilities and restrictions of each of the essential technology is required for secure working of wireless sensor networks. In the paper I discuss various challenges and issues concern with the security of WSNs and also discuss various attacks that are possible in WSNs. Even if there are so many types of attacks and the prospect of having the system compromised people must not provide to the security systems like firewalls, antivirus software, cryptographic systems and software.

REFERENCES

[1] Heena Chawla* , Hardeep Kaur and Charanvir Kaur Review on Security Issues in Wireless Sensor Networks International Journal of Current Engineering and Technology, Vol.6, No.3 (June 2016).

[2] Mishra KB, Nikam CM, Lakkadwala P (2014) Security against black hole attack in wireless sensor network-a review in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on IEEE pp: 615-620.

[3] Mulla RI, Patil R (2016) Review of attacks on wireless sensor network and their classification and security. Imperial J Interdiscipl Res 7: 2.

[4] Patel MM, Aggarwal A (2016) Two phase wormhole detection approach for dynamic wireless sensor networks in Wireless Communications Signal Processing and Networking (WiSPNET), 2016 International Conference on IEEE pp: 2109-2112.

[5] 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.

[6] Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, Joseph Chee Ming Teo, "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs", IEEE Transactions on Information Forensics and Security, Vol. 10, Issue: 3, pp. 613-625, 2015

[7] Gagandeep and Aashima, "Study on Sinkhole Attacks in Wireless Adhoc Network", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Volume 4, Issue 06, pp. 1078-1085, June 2012

[8] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, 2005

[9] Ehab Al-Shaer, "Network Security Attacks I:DDOS", DePaul University, 2007.

[10] Jyoti Ahlawat, Mukesh Chawla and Kavita Sharma, "Attacks and Countermeasures in Wireless Sensor Network", International Journal of Computer Science and Communication Engineering (IJCSCE), pp. 66-69. 2012.

[11] Danny McPherson, BGP Security Techniques, APRICOT, 2005

[12] T.C. Aseri and N. Singla, "Enhanced Security Protocol in Wireless Sensor Networks", International Journal of Computers, Communications & Control, Volume 6, Issue 2, pp. 214-221, June 2011.

[13] Hralambos Mouratidis, Paolo Giorgini, Gordon Manson, Using Security Attack scenarios to Analyse Security During Information System

Design, in the 6th International Conference on Enterprise Information Systems, 2004

[14] Taka Mizuguchi, Tomoya Yoshida, BGP Route Hijacking, APRICOT, 2007.

[15] Jitender Grover , Shikha Sharma Security Issues in Wireless Sensor Network - A Review 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)

[16] Heena Chawla , Hardeep Kaur and Charanvir Kaur Review on Security Issues in Wireless Sensor Networks International Journal of Current Engineering and Technology Vol.6, No.3 (June 2016)