Various Attacks in Wireless Sensor Network and Comparison of Both Attacks

Supreet Kaur[1], Silky Narang[2]

[1]*Department of Computer Science and Engineering, Chandigarh University, Chandigarh, India*
kaursupreet184@gmail.com

[2]*Department of Computer Science and Engineering, Chandigarh University, Chandigarh, India*
silkynarang94@yahoo.com

Abstract - Wireless sensor network consists of a large number of sensor nodes that are wirelessly connected to each other that's called wireless sensor network. These sensor nodes are used to sense and measure various parameters like atmospheric pressure, temperature, humidity and heat etc and therefore its very important to secure them from various attacks. Sensor network initially consists of small or large nodes called sensor nodes. Wireless sensor network are now widely used in many areas such as military, environmental health and commercial applications. In these environments, security issues are extremely important since a successful attack cause a great damage even threatening for human life. Wireless sensor network consisting the large number of low cost elements. Sensors network collaborate with each other to send packets in multi-hop manner. Wireless sensor networks are used for various tasks such as surveillance, widespread environmental sampling, security and health monitoring. WSNs are ready to be attacked in various way such as wormhole attack, Denial of service attack, sybil attack and selective forwarding attack.

I. INTRODUCTION

We present some attacks that discussed in references Group communications refers to either point-to-multipoint or multipoint-to-multipoint communications. Wireless Sensor network are susceptible to wide range of security attacks due to the multi-hop nature of transmission medium. Wireless sensor network have different vulnerability because nodes are generally deployed in a unproducted or hostile environment, even if there is no standard layered architecture of the communication protocol for wireless sensor network, hence there is need to summarize the possible attacks and security solution in different layers with respect to ISO-OSI model Wireless sensor network is an emerging field for research in today's world. Wireless sensor network have vast potential for usage of sensor networks in different areas like military area, disaster management, sensing environment conditions such as temperature humidity etc. In wireless sensor networks, as no. of sensor nodes are used for communication which mainly forms a sensing field and sink (Base station)[1].All communication in a network is performed by sensor nodes so the effect of energy depletion occurs which decreases the network lifetime. So to optimize networks lifetime there is a need of highly energy efficient routing protocols. As a new information acquisition and processing technology, wireless sensor network has a wide range of applications in military, environmental monitoring, smart furniture and space exploration and so on.

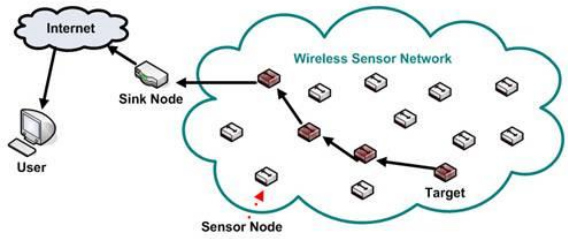

Fig.1.1: Wireless Sensor Network

Wireless sensor network are widely used in many areas such as military, environment, health and commercial applications. Wireless sensor network consisting the large number of low cost resources. Source sensor node in wireless sensor network finds the shortest path to transfer the data in hop to hop and multi-hop manner via other sensor nodes in networks .WSNs are used for various tasks such as surveillance, widespread environmental sampling, security and health monitoring [10]. WSNs are prone to be attacked in various ways.

II. OVERVIEW OF WSNS

In this section, we present an outline of different aspects of WSNs, such as definitions, characteristics, applications, constraints and challenges and comparison different attacks of wireless sensor network.

A. Defination of WSNs

A wireless sensor network is a heterogeneous systems consisting of hundreds and thousands of low-cost and low power tiny sensors to monitor and gather real-time information from deployment model. WSN (wireless sensor network) is made by the convergence of sensor, micro-electro-

mechanism system and networks technologies WSN consist of small nodes with sensing, computation and wireless communication capabilities. Various architectures have been developed for WSN, depending upon the requirement of application. WSN are used in different applications e.g. environmental monitoring, habitat monitoring, home automation, military application etc. In this paper we present the architecture and characteristics of WSN. As viewed from the existing work, the hot spots recent representative routing protocols are analyzed, and their characteristics and application areas are compared. A wireless sensor network is a collection of sensor nodes, linked together via some form of wireless communication network. These sensor nodes are autonomous devices using a variety of sensors (e.g., temperature, sound, vibration, pressure, motion, or pollutant) to monitor the environment in which they are deployed. A number of different node manufacturers exist (e.g., MoteIV and Xbow, which build nodes suitable for deployment in outdoor areas, in buildings, as well as underwater.

In addition to a wide array of sensor nodes and sensing technologies, there is also a wide array of wireless technologies. For both in building and outdoor environments, Zigbee is among the more popular wireless technologies. Underwater deployments use acoustic modems for their communication (see e.g. underwater video systems).

B. ARCHITECTURE OF WSN

Most common architecture for WSN follows the OSI Model. Basically in sensor network we need five layers: application layer, transport layer, network layer, data link layer and physical layer. Added to the five layers are the three cross layers planes as shown in Fig.2

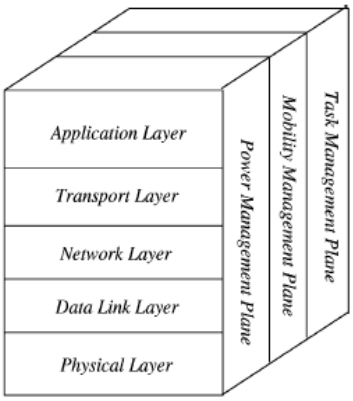

Fig.2: WSN architecture

- Physical layer provide an interface to transmit a stream of bits over physical medium. Responsible for frequency selection, carrier frequency generation, signal detection, and Modulation. IEEE 802.15.4: proposed as standard for low rate personal area and WSN with low: cost, complexity, power consumption, range of communication to maximize battery life. Use CSMA/CA, support star and peer to peer topology.
- The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access, and error control.
- The major function of network layer is routing. Threats in the network layer mostly aim at disturbing data-centric and energy efficient multi-hop routing, which is the main design principle in WSNs.
- The function of transport layer is to provide reliability and congestion avoidance where a lot of protocols designed to provide this function are either applied on the upstream (user to sink, ex: ESRT, STCP and DSTN), or downstream (sink to user, ex: PSFQ and GARUDA). This layer is specifically needed when a system is organized to access other networks.
- Application layer Responsible for traffic management and provide software for different applications that translate the data in an understandable form or send queries to obtain certain information. Sensor networks deployed in various applications in different fields, for example; military, medical, environment, agriculture fields.

C. ROUTING PROTOCOLS IN WSN

Many routing protocols have been proposed for WSNs. These have been classified into three categories, namely:
- Data-centric protocols
- Hierarchical protocols
- Location-based protocols

Data-centric protocols are query-based and use the concept of naming of desired data to eliminate many redundant transmissions.

Hierarchical protocols cluster the nodes so that cluster heads can aggregate and reduce the data to save energy.

Location-based protocols use position information to send the data to only the desired regions rather than to the whole network. The more important ones among these are SPIN, LEACH, PEGASIS, TEEN and APTEEN.

D. TYPES OF WIRELESS SENSOR NETWORK

1. Terrestrial wireless sensor networks
- Ad-Hoc (unstructured)
- Preplanned (structured)

2. Underground wireless sensor networks
- Preplanned
- More expensive equipment, deployment, maintenance

3. Underwater wireless sensor networks
- Fewer sensor nodes (sparse deployment)

- More expensive than terrestrial
- Limited bandwidth
- Signal fading

4. Multi-media wireless sensor networks

- Sensor nodes equipped with cameras and microphones
- High bandwidth/low energy, Qos, filtering, data processing and compressing techniques

5. Mobile wireless sensor networks

- Ability to reposition and organize itself in the network
- Start with initial deployment and spread out to gather information Deployment, localization, self organizations, navigation and control, coverage, energy, maintenance, data process etc.

E. WSNs Characteristics

- Ad-hoc based networks and hop-by-hop communications.
- Constant or mobile sensors(mobility)
- Low reliability and wireless communication and immunity.
- Non-central management,infrasture-less.
- Self organization.
- Resource limited sensor.
- Open hostile-environment nature.
- Limited power supply.
- Energy harvesting.
- Small scale sensor nodes.
- Harsh environmental conditions.
- Node failure
- Mobility of detected events.
- Unattended operation.
- Large scale deployment.
- Dynamic network topology.
- Cross layer design.

F. APPLICATIONS OF WIRELESS SENSOR NETWORKS

The applications for wireless sensor networks are broad. Commercial and industrial applications include monitoring equipment to which it is difficult to attach wired sensors, or in older buildings where it is difficult to retrofit a wired network. Environmental monitoring (e.g., coastal monitoring) applications abound due to the ease of deployment, and the minimal impact on the environment. Sensor networks not only eliminate the need for wires, but also do not typically require large power supplies. Common applications for sensor networks include: environmental monitoring, habitat monitoring, acoustic detection, seismic detection, military surveillance, inventory tracking, medical monitoring, smart space, etc. See e.g. Monitoring biodiversity in dunes, beaches and salt marshes, instrument and sensors to measure environmental parameters.

Environmental applications

- Air pollution monitoring
- Flood and oceans detection
- Forest fire detection
- Precision agriculture

Military applications

- Monitoring, tracking, surveillance of borders.
- Nuclear, biological and chemical attack detection
- Battle damage assessment

Health applications

- Drug administration
- Remote monitoring of physiological data
- Tracking and monitoring doctors and patients inside a hospital

Home applications

- Automated meter reading
- Home automation
- Instrumented environment

Commercial application

- Monitoring vibration that could damage the buildings structures
- Monitoring traffic flow and road condition

III. NETWORK TOPOLOGIES

Wireless sensor network may consists of tens hundreds or thousands of devices network topologies must be considered in its design. The most common network topologies used in wireless sensor networks are star, tree mesh or hybrid networks that combine the other ones. Each of these topologies presents its own set of challenges, advantages and disadvantages are discussed below

Topology	Power usage	Communication range
Star	Low	Short
Tree	Low	Long
Mesh	High	Long
Hybrid	Low(typically)	Long

Fig.3: Network Topologies

A. Star topology

The most popular topology for business today,the star topology consists of all of the nodes on a network connected to a central switch or hub.A node is a device attached to the network such as computer. Each node on the network has a cable back to the central switch. If one cable fails to a node, only that node (computer) is affected. You can combine several switches or hubs to create several stars, all connected together.The Star topology is very inexpensive to maintain versus other topologies. 10BaseT is an example of Star topology. Think of the star topology as a big wheel. At the center of the wheel is a switch or hub and each spoke going out from the center goes to a node.

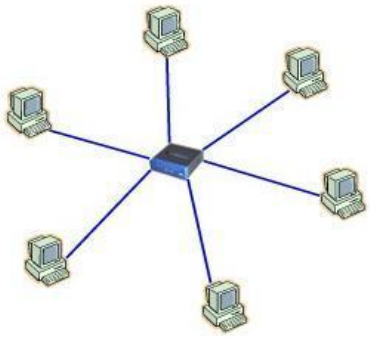

Fig 3.1 Star topology

B. *Bus Topology*

Bus topology is one which all of the devices on the network are connected with a single cable with terminators on each end. This single cable is often referred to as a backbone or trunk. The typical Bus network uses coax as its cable. Coax is a cable similar to what you use for your cable TV. Coax is also referred to as 10Base2.

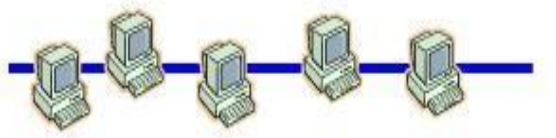

Fig 3.2 Bus topology

C. Mesh topology

A mesh topology is one which all of the nodes are directly connected with all of the other nodes. A mesh topology is the best choice when you require fault tolerance, however, it is very difficult to setup and maintain the mesh topology.

There are two types of mesh network: full mesh and partial mesh. A full mesh is one which every workstation is connected to the other ones in the network. In a partial mesh, the workstations have at least two NICs with connections to other nodes on the network. Mesh networks are commonly used in WANs.

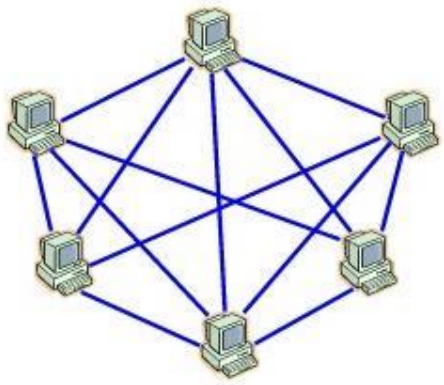

Fig 3.3 Mesh topology

D. Ring topology

The ring topology is one which the network is a loop where data is passed from one workstation to another. Ring topology find with the token ring topology. Token ring networks are defined by IEEE 802.5 and were primarily developed by IBM. The token ring network is designed to transmit a token, or a special frame, designed to go from node to node around the ring.

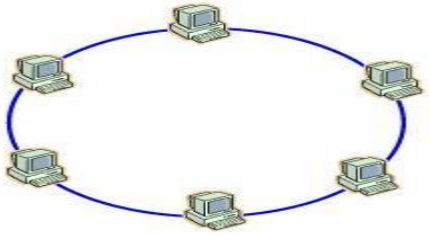

Fig 3.4 Ring topology

IV. DIFFERENT ATTACKS OF WSN

Wireless sensor network are susceptible to wide range of security attacks due to the multihop nature of the transmission medium. We can classify the wireless sensor attacks in two categories: Active attack and Passive attack Aims of the Active attack is to obtain information and have the monitoring or eavesdropping nature and transmitted data will not be modified in passive attack. Unlike Passive attack, attackers modifies the transmitted data. Different attack consisting in the different layers

- Wormhole Attack
- Sybil Attack
- Denial of Service Attack
- Jamming Attack
- Collision

A. Wormhole Attack

The wormhole attack is very dangerous and damaging though protection is there even the path information is confidential, authenticated and encrypted [7] .In wormhole attack two opposite nodes are connected through low latency link called wormhole link. A low latency can be realized through a network cable or other kind of wired link. When the wormhole link is established, the packets one end of link tunnels them through wormhole link and replays the packets other end of the link. Node X and Y are two end points of the wormhole link, node X receives packets and tunnel them through wormhole link and replays the packets at node Y and vice versa.

Node X and Y are two opposite nodes and connected via a network cable. Both nodes, node X and node Y are two end points of the wormhole link. Node X receives packets and tunnels them through the wormhole link and replays the packets at node Y and vice versa. At last we see nodes in the neighborhood of node X and all nodes in the neighborhood of Y are their neighbors and vice versa

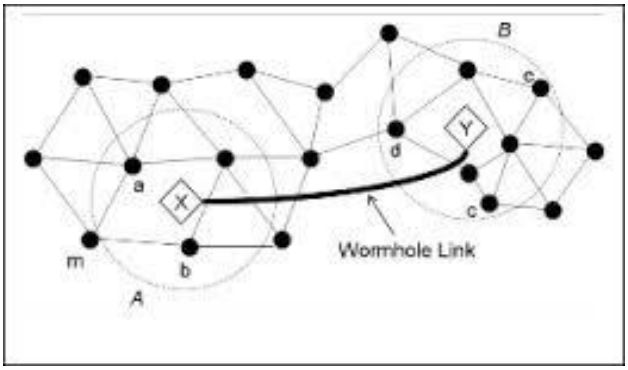

Fig. 4.1: Warmhole Attack

B. Sybil Attack

The Sybil attack is very vulnerable attack to wireless sensor network [8]. This attack create multiple identities from the same malicious nodes and introduced by Douceer peer to peer and several ways to create sybil attack in sensor network based upon communication and fabricated identities.It shows the one node is communicate with the other nodes. There are three different types of Sybil attack taxonomy-

Direct vs Indirect Communications

In Direct communication, Sybil nodes directly communicate with legitimate nodes but indirect communication it cannot directly communicate with nodes.

Fabricated vs Stolen Identities

Attacker creates arbitrary new identities in fabricated, but in stolen, attackers assign legitimate identities to Sybil nodes.

Simultaneity

It consisting simultaneous or non- simultaneous. In Simultaneous, attacker participates with all the identities at one time, but in non- simultaneous, attacker present a large number of identity over a period of time.

Types of Sybil Attack

- Distributed storage
- Routing
- Voting
- Data Summarization

C. Jamming Attack

Jamming node interrupt the entire network randomly because using the nature of interference on radio frequencies, that it can be change the behavior of node become a out of service.

D. Collision Attack

The node A, B, C are both communicate with each other at same time for transmitting the packets,In this case altering of packet transmission in between the nodes, signal collisions has been take place, it leads to not able to communicate with each other.

E. Sinkhole Attack

This type of attack that number of attacker nodes will be covers the certain region by wrongly manipulated information.

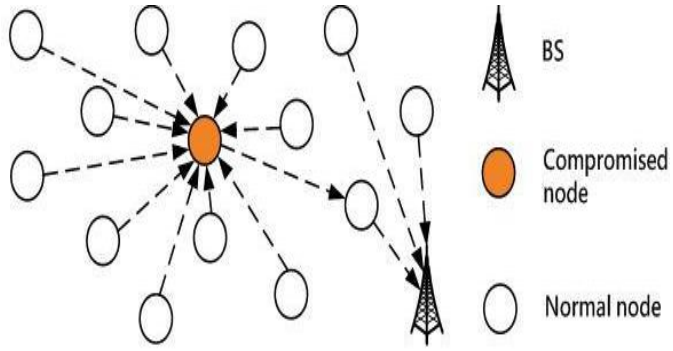

Fig. 4.5: Sinkhole Attack

Comparison of Attacks

Attack/Criteria	Attack Definition	Attack Effects
Black hole	In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages he receives, just as a black hole absorbing everything passing by.	• It can disrupt the communication between the base station and the rest of the WSN, and hence prevent the WSN from serving its purposes. • Throughput of a subset of nodes, around the attacker and with traffic through it, is decreased [1].
Wormhole	A wormhole attack requires two or more adversaries. These adversaries have better communication resources (e.g. power, memory) than normal nodes, and can establish better communication channels (called "tunnels") between them [1].	• False/forged routing information. • Change the network topology. • Packet destruction/alteration by wormhole nodes. • Changing normal messages stream.
Sybil	In Sybil attack, a malicious node attracts network traffic by representing multiple identities to the network [6].	• Confusion and WSN disruption. • Enable other attacks. • Exploiting the routing race conditions.
Sinkhole	Sinkhole is a more complex attack compared with black hole attack [1].	• Attracts almost all the traffic. • Triggering other attacks, such as eavesdropping, trivial selective forwarding, black hole and wormhole. • Changes the base station's position.
Selective forwarding	In Selective forwarding attack, attacker refuses to forward packets or selectively drop them and act as a black hole [7].	• Message modification. • Information fabrication and packet dropping. • Suppressed messages in a certain area. • Routing information modification. • Exhaustion of resources
Hello flood	In Hello Flood Attack, attacker broadcast hello message with strong transmission power to the networks and acts as a fake sink [7].	• Creates an illusion to base station of being a neighbor to many nodes in the networks. • Confuse the network routing badly.[2]
Acknowledgement Spoofing	An adversary can spoof Network layer acknowledgements (ACKs) of overheard packets	• False view/information of the WSN. • Launch selective forwarding attack. • Packet loss/corruption.
False Routing(Misdirection Attack)	Attacker routes the packets to false destination, creates the loops in networks [8].	• False and misleading messages generated; • Resources exhaustion; • Degrade the WSN Performance

V. CONCLUSION

Wireless sensor network vulnerable to wide range of security attacks because of their deployment an open and unprotected environment. This paper introduced the major threats of wireless sensor network. Also compare the different layer attacks. Our approach to better classification of all attacks and compare that's ones. Securing the wireless communication links against eavesdropping and DoS attack.

VI. REFERENCES

[1] A.Cepra,J.Wong,L. Kuang, wireless sensor network in 2005.
[2] W.Znaidi,M.Minier"An Onthogy for attacks in wireless sensor network,"Institute National de Recherche en Informatique et an Automatique ,october2008.
[3] K.sharma and M.K Ghose "wireless sensor network" 2010
[4] Khedo, K., Perseedoss, R., Mungur, A. "A wireless sensor network air pollution monitoring system." International Journal of Wireless and Mobile Netwroks 2010;2(2):31–45.
[5] Sonal. A. Mishra, Dhanashree S. Tijare and Dr. G. M. Asutkar "Design of energy aware air pollution monitoring system using wsn,"International Journal of Advances in Engineering and Technology 2011; 1(2):107–116.
[6] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan " Energy-efficient communication protocol for the wireless wireless microsensor networks,"Proceedings of the 33rd Hawaii International Conference on System Sciences. 2000, p. 3005–3014.
[7] Dong Wormcircle;connectivity-based wormhole detection in wireless ad hoc and sensor networks.In Proceedings of the Parallel and distributed systems.
[8] Yingyingchen, "Detecting and localizing identity-based attacks in wireless sensor network", IEEE Journal, June 2010.
[9] A.Wood and J. Stankovic, "Denial of service in sensor networks," *IEEE Comp.*, vol. 35, no. 10, Oct. 2002, pp. 5462.