SURVEY: WIRELESS SENSOR NETWORK ATTACKS.

Shikha Maan
Assistant Professor Department of Information Technology
Silver Oak College of Engineering & Technology, Ahmedabad, India

Abstract : Wireless Sensor Network (WSN) is being emerged as a prevailing technology in future due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks, since once deployed these networks are unattended and unprotected. Some of the inherent features like limited battery and low memory make sensor networks infeasible to use conventional security solutions.. Some of the data attacks in sensor nodes are wormhole, jamming, selective forwarding, sinkhole and Sybil attack. In this paper, we discussed about all these attacks and some of the mitigation schemes to defend these attacks

Keywords-wsn,sinkhole,wormhole,mitigation

I. INTRODUCTION

Setting up of fixed access points and backbone infrastructure is not always feasible because infrastructure may not be present in a disaster area or war zone and infrastructure may not be practical for short-range radios. Ad hoc networks do not need backbone infrastructure support, are easy to deploy and are useful when infrastructure is absent, destroyed or impractical. Popular ad hoc networks are mobile ad hoc networks, vehicular ad hoc networks and wireless sensor networks. While WSNs come from wireless ad hoc networks, important distinctions exist between them and these differences greatly affect the system designs including security designs.[1]

A sensor can be as simple as a button, but more widely deployed, more complex sensors include weather sensors (barometers, anemometers, thermometers), accelerometers and GPS units, light sensors, As well as medical sensors (blood glucose, heart rate, etc.), industrial sensors (monitoring of the production line, etc.) and many others. Actuators are electronically controlled systems that affect the physical world. [2]

This paper will lead readers into this area by presenting a survey of various potential attacks and solutions in WSNs.

II. BACKGROUND

A. Security Goals: When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services:

- Confidentiality: Confidentiality refers to data in transit to be kept secret from eavesdroppers. Here symmetric key ciphers preferred for their low power consumption.
- Integrity: Integrity measures that the received data is not altered in transit by an adversary.
- Authentication: Authentication enables a node to ensure the identity of the peer with which it is communicating.
- Availability: The service should be available all the time.
- Data Freshness: It suggests that the data is recent, and it ensures that no old messages have been replayed.
- Non-repudiation**:** It denotes that a node cannot deny sending a message it has previously sent.
- Authorization: It ensures that only authorized nodes can be accessed to network services or resources.

These goals are not ensured by traditional security techniques. Therefore, new security measures are needed to address the specific security challenges of wireless sensor networks.

B. SECURITY CHALLENGES:

We summarize security challenges in sensor networks as follows:

[1] minimizing resource consumption and maximizing security performance.

[2] Sensor network deployment renders more link attacks

[3] Wireless communication characteristics render traditional wired-based security schemes unsuitable.

[4] Large scale and node mobility make the affair more complex.

[5] Node adding and failure make the network topology dynamic

III. WSN APPLICATIONS

We can classify the usage of WSN into defense applications, forest applications, and domestic applications [5].

A. Defense applications

WSNs can be an integral part of defense command, security control, data communications, computation, intelligence, targeting systems such as surveillance etc.

B. Forest applications

Certain environmentally usage of sensor networks (SN) comprise recording and detect the activities of minor birds and insects, monitoring environmental conditions, animals, earth monitoring and exploration.

C. Medical Science applications

Certain of the applications of health for SN are diagnosing the patients, tracking location and movement of patients and doctors inside hospital etc.

D. Industrial applications

Certain industrial applications of WSNs are make virtual keyboards, environmental control in office constructions, robot control, interactive toys, monitoring product quality etc..

IV. ATTACKS ON WSN

A. Internal Attacks

These are mainly done because of the compromised nodes. These compromised nodes continuously seek to disrupt or parallelize the network. Based on kind of activity performed by attacker, it can be further classified as: Outside Attack- in which, an attacker can replace/introduce new malicious node from outside. Inside Attack- in which, an attacker can capture any node; reprogram it, to act as malicious node.

B. External Attacks

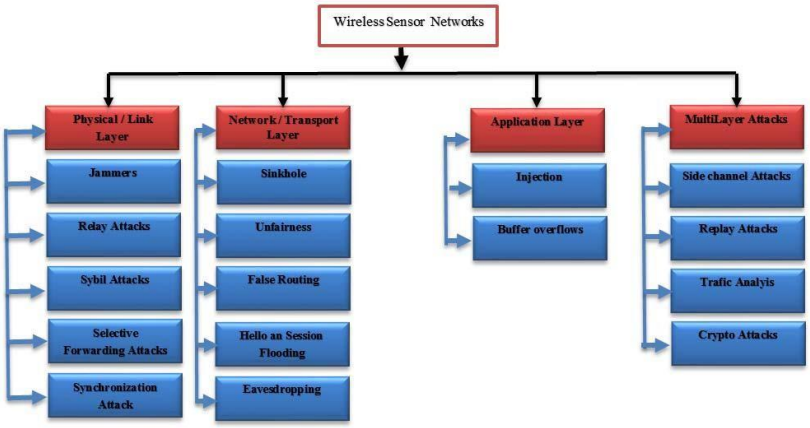

Fig 1 Attacks in WSN

In these attacks, the attacker node isn't always an authorized participate of SN. Depend on the conduct of attacker node, it could be categorized as:

1. **Passive Attack**- it comprise eavesdropping on or monitoring packets swapped within a WSN. It involves only unauthorized listening to the routing packets. Generally, encryption is the standard solution to defend against these attacks.

2. **Active Attack**- it include few changes of the data steam or the making of a wrong stream. Also, it results in disrupting network functionalities by introducing DOS attacks, Jamming attacks & Power Exhaustion.

A. Device Level Capability Attack

This class of attacks is categorized depend on the capability of the device that is being used for attacking. An attacker may attack the WSN either using a sensor device (Sensor Level) or more powerful laptop device (Laptop Level). An adversary can highly damage the system if he/she uses Laptop Class attack having more powerful computation, storage and battery life. Beside the above mentioned classifications, an attacker may utilize one or more of the subsequent attack techniques such as.

B. Eavesdropping

In which an attacker silently listen to media for communiqué amid two parties and don't modifies the data. It's a passive technique.

C. Radio jamming

In this attack, the attacker tries to disrupt the communication by sending few radio waves at the similar frequency resulting in interference or collisions of packets over network. Jamming can be intermittent or continuous depend on the time for which network is kept jammed.

D. Message's injection

In this the attacker transmits many false messages over network in lieu of corrupting the packet data or to simply exhaust network.

E. Message's replication

In this the attackers capture and resend the same packet many times to same or different sensor and at different times in sequence to make receiver foolish.

F. Node compromise (Destruction or theft)

This includes physical capturing of a node in sequence to disrupt network by breaking the communication path or reprogramming a node so that it acts as a spy in network.

G. Denial of Service (DoS)

In this the attacker will regularly sends packet in sequence to disrupt services or battery power by using malicious nodes. This is an active type of attack.

H. HELLO Flooding

We know that HELLO message is used for discovering neighbors. In this form of attack, the attacker uses more powerful nodes to send HELLO messages to far away sensor nodes so that they trust that the malicious node is their neighbor and they will transfer future packets to it.

I. Black Hole Attack

In this attack a node tries to become receiver of packets of neighboring nodes by altering their routing table and it will never forward the packets to correct destination.

J. Selective Forwarding (Gray Hole Attack)

in this attack, the attacker will insert node of malicious in the n/w which tries to change the routing and capture data just like black hole attack but unlike it will selectively forward data (not all) and so difficult to detect.

K. Wormhole Attack

This kind of attack is done with at least two malicious nodes which have high bandwidth between them either wired or w irelessly. These malicious nodes will show other normal nodes that they provide the shorter path to the target even if they are lying far away in the network. So, the node will forward data to the malicious node that can be captured by attacker easily.

L. Sinkhole Attack

In this attack the malicious node reside near the BS and it tries to imaginary to be closest node to the BS so that other surrounding usual node will change themselves and forward info to the malicious node.

M. Sybil Attack

In this attack the adversary tries to have several individualities to different nodes and thus can be in more than one place at single time. Here it tries to be voted as the cluster head. A Sybil attacks is extensive risk to Geographic Routing Protocols.

N. Infinite Loops-

In this attack two or more malicious node tries to circulate packets infinitely in the n/w in sequence to exhaust power of the network.

O. Message Alteration

In this attack the node of malicious will capture and modify packets on the network. It can add false data or delete data so that packet will become corrupted.

P. Sleep deprivation torture

In this attack, the malicious node will prevent a node from sleeping by sending messages to it or asks for calculation. This is complete so that the node will consume its power quickly [4].

V. SECURITY ISSUES IN WSN

A. Data Integrity

It's very vital in SN to ensure the data reliability. It ensures that data packets that are accepted thru the target are exactly the ones transfer thru the source and any one can't modify that packet in amid.

B. Data Confidentiality

Confidentiality means to protect data during communiqué in a n/w to be implicit other than intended receiver. Cryptography techniques are used to provide confidentiality. It's a most significant issue in network security.

C. Data Availability

These services are always available in the n/w even under the attack such as Dos. Availability is of primary importance to maintain an operational network. Availability ensures which a sensor node remains always active in the n/w to fulfill the functionality of the network.

D. Data Authentication

The data accepted thru target has not been modified during the transmission. It's reached via asymmetric or symmetric mechanisms in which target and source nodes share secret keys.

E. Data Freshness

The data accepted thru the target is mostly current and fresh data and no challenger can replay the old info. It's reached thru utilizing mechanisms as nonce or adding timestamp to all data packet [5].

VI. CONCLUSION

In this paper, survey is given on existing attacks in wireless sensor network. This paper will help in understanding over view of attacks countermeasures in wireless sensor networks, and find their way to start secure designs for network designs.

REFERENCES

[1] NM. Nair, JS. Terence, "Survey On Distributed Data Storage Schemes In Wireless Sensor Networks", Indian Journal of Computer Science and Engineering (IJCSE), Vol.4, No.6, pp.1-6, 2015.

[2] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Science direct, Vol.52, Issue.12, pp.2292– 2330, 2008.

[3] AS. Mandloi, V. Choudhary, "An Efficient Clustering Technique for Deterministically Deployed Wireless Sensor Networks", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, pp.6-10, 2015.

[4] Sanchita Gupta, Pooja Saini, "Modified Pairwise Key Pre-distribution Scheme with Deployment Knowledge in Wireless Sensor Network", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.21-23, 2015.

[5] N. Meenaksi, P. Rodrigues, "Tsunami Detection and forewarning system using Wireless Sensor Network - a Survey", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.76-79, 2014.

[6] Chanchal Yadav, SS. Hegde, NC. Anjana, Sandeep Kumar,"Security Techniques in Wireless Sensor Networks : A Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Issue.4, pp.289- 295, 2015.

[7] Jaydip Sen, "A Survey on Wireless Sensor Network Security", International Journal of Communication Networks and Information Security, Vol.1, No.2, pp.1-16, 2016

[8] Xiaoliang Menga, Xiaochuan Shia, Zi Wangb, Shuang Wua, Chenglin Liu, "A grid-based reliable routing protocol for wireless sensor.networks with randomly distributed clusters",elsevier, Vol.51, NO.11, pp.47–61, 2016.

[9] Hacene fouchal, javier biesa, elena romero, alvaro araujo, octavio nieto taladrez, "a security scheme for wireless sensor networks", 2016 IEEEGlobal Communications Conference (GLOBECOM), Washington, pp.1-5,2017.

[10] Gagandeep Kaur, Deepali, Rekha Kalra,"Improvement and analys security of WSN from passive attack", 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, pp.420-425, 2017.