SECURITY HACKS AND CHALLENGES IN WSN

D.Vinotha, Assistant Professor,
PRASHANT KUMAR, [UG] **Student**

Department of computer Science and Engineering,
PRIST Universit.y

ABSTRACT

Internet of things is emerging technologies used in which provides applications on smart city, smart grid, industrial automation, agriculture, and smart home applications. Wireless Sensor Networks are used to monitor, physical or environmental conditions like sound, pressure, temperature, and co-operate passed data through the network. The challenging portion of a wireless sensor network is security. In order to secure the network from hacking, it provides various types of services to overcome the challenge which helps to secure the network. The purpose of this paper to explore the impact of wireless sensor network involving security hacks and its challenges to overcome it. This paper also represents the security requirements and characteristics of a wireless sensor network.

KEYWORDS : Internet Of Things, Wireless Sensor Networks (WSN), Security Attacks and Threats, Security Challenges, Security Mechanisms.

I.INTRODUCTION

A Collection of two or more devices in a wireless network. Internet of Things is the most emerging and promising area of technological advance In the future. Wireless sensor network (WSN), Cloud services, Middleware, Radio Frequency Identification(RFID), etc., A computer network consists collection of computers, printers and other equipment that is connected together for the purpose of sharing data can be done via cabling, most commonly (Ethernet cable)or wireless using send and receive data through the air.

The common communication is the using technologies ZigBee and 2G/3G/4G cellular, but there are also several new emerging networks. Wi-Fi, Bluetooth, options.Thread as an alternative for home automation applications, and Whitespace TV technologies being implemented in major cities for wider area IoT-based use cases. WSN's are typically self-organizing and self-healing. A Wireless Sensor Network can be defined as a network device that can communicate the information gathered from a monitored field through Wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like Wireless Ethernet.

I.1 WIRELESS SENSOR NETWORK

A wireless sensor network is a computer network that uses wireless data connections between networks. Wireless telecommunications networks are generally implemented and administered using radio communication. Example:-wireless network includes cell phone network, Wireless Local Area Network(WLAN) wireless sensor network. Satellite communication network and terrestrial microwave networks

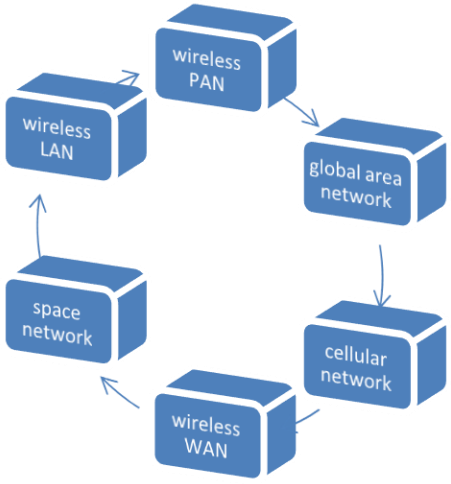

Fig:1 Types of Wireless Network

1.2 Wireless PAN

Wireless Personal Area Network (WPAN) to connect devices within a creativity small area, that is generally within a person's reach.

For example:-

- Bluetooth
- Infrared
- Zigbee also supports WPAN application.

1.3 Wireless LAN

The use of Spread-Spectrum of OFDM technologies may allow users to move around with local coverage area and still, remain connected to the network.

Produces using the IEEE 802.11 WLAN.

1.4 Wireless ad hoc network

Distance Sequenced Distance Vector Routing, Associatively, Based Routing, Ad hoc On-demand Distance Vector routing and dynamic source routing.

1.5 Wireless MAN

WiMAX is a type of wireless MAN and is described by the IEEE 802.16 standard.

II. NETWORK TOPOLOGY

Network topology is the arrangement of the elements (links, nodes, etc) of a communication network. Type of telecommunication network, including command and control radio networks industrial field buses and computer network. The physical topology is the placement of the various components of the network (E.g.: device location and cable installation) while logical topologies illustrate how data flows within a network. Distance between nodes, physical interconnection transmission rates, or signal types may differ may be confidential. A network's physical topologies are a particular concern of the physical layer of the OSI model. A wide variety of physical topologies have been used in LANs including ring, mesh, and star.

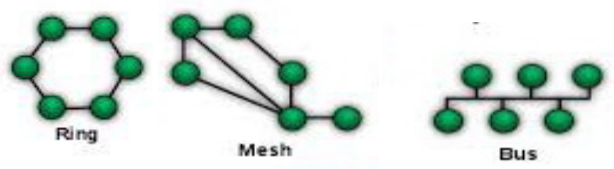

Fig 2: Types of Topologies.

Types of communication network

Digital wireless communication is not a new idea. Earlier, morse code: wireless used communication network. Modern digital wireless better performance system.

It is divided into three wireless networks.

- **System interconnection(short-range radio)**
- **Wireless LANs(Ethernet) called IEEE 802.11**
- **Wireless WANs Low bandwidth wireless WANs**

Three generation

- **Analog and for voice only.**
- **Digital and for voice only.**
- **Digital and is for both voice and data.**

Internetwork

Techniques of connecting different network process.

Uses of wireless network

A wireless local area network(LANs) uses radio waves to connect devices such as laptops and mobile phones to connect the internet and to your business network and its application. A wired network uses cables to connect devices, such as a laptop or desktop computer, to the internet or another network. A wireless network allows devices to stay connected to the network but roam untethered to any wires.

Communication in the wireless network

A wireless network is a computer network that uses wireless data connections between network nodes. Wireless telecommunications network is generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

Applications of wireless sensor network

A wireless sensor network can be defined as a network of devices that can communicate information gathered from a monitored field through a wireless link. Data is forwarded through multiple nodes and with a gateway. Data is connected to other networks like wireless Ethernet.

III .SECURITY MECHANISM

A mechanism that is designed to detect, prevent, or recover from a security attack.

Different types of security mechanisms are:

1. Routing control
2. Traffic padding
3. Encipherment
4. Access control
5. Digital signatures
6. Data integrity

Routing control

Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Traffic padding

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Encipherment

Encipherment is the process of translating plain text into cipher text. The use of mathematical algorithms to transform data into a form that it is not readily intelligible. Cryptography technique is used for enciphering.

Security mechanisms

A mechanism that is designed to detect, prevent, or recover from a security attack.

Security service

A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security attack

Any action that compromises the security of information.

Vulnerabilities

Vulnerabilities are weak points or loop nodes insecurity that an attack exploits in order to gain access to the network or to resources on the network.

Attacks

Attacks are an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. There are two types:

1. Passive attack
2. Active attack

IV. TYPES OF ATTACKS

1. Physical layer attacks.
2. Link layer attacks.
3. Network layer attacks.
4. Transport layer attacks.

Physical Layer Attack

Attacks on wireless networks are the most popular and easy to do, because of the nature itself of wifi.

Link Layer Attacks

The link layer in the TCP/IP model is a descriptive realm of networking protocols that operate only on the local network segment (link) that a host is connected to such protocol packets are not routed to other networks.

Network Layer Attacks

Network-Layer Attacks that exploit the basic network protocol in order to gain any available advantage. These attacks generally involve “SPOOFING”.

Transport Layer Attacks

This attack provides data delivery, flow control, and error recovery services to end hosts on the Internet.

V. VARIOUS TYPES OF SECURITY MECHANISMS

- Digital integrity
- Traffic padding
- Access control
- Notarization

VII.CONCLUSION

Due to continuing the growth of WSN's, the need for more effective security mechanisms is also increasing. The security concerns of the sensor network should be addressed from the beginning of designing the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for the secure working of wireless sensor networks. In the paper, we discuss various requirements and issues concern with the security of WSN's. We also discuss various attacks that are possible in WSN's. A detailed study of countermeasures for these attacks is required in order to minimize or eliminate their impact. More efficient and robust techniques for the countermeasures of various types of WSN attacks should be proposed in order to made WSNs more secure and their extensions in other fields.

VIII. REFERENCES

[1] L. In and K. Lee, "The Internet of Things (IoT): Applications, Investments, and challenges for enterprises," Business Horizons, ScienceDirect, vol. 58, no. 4, pp. 431-440, 2015.

[2] G. Gordana, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S.Tomović, and M. Radonjić, "The IoT Architectural Framework, Design Issues and Application Domains," Wireless Personal Communications, Springer Science and Business Media, pp. 1-22, 2016.

[3] K. Nacer, M. R. Abid, D. Benhaddou and M. Gerndt, "Wireless Sensors Networks for Internet of Things," Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), EEE Ninth International Conference on, pp. 1-6, 2014.

[4] I. Gudymenko, K. Borcea-Pfitzmann, and K. Tietze, "Privacy implications of the Internet of Things," In Constructing Ambient Intelligence, Springer Berlin Heidelberg., vol. 277, pp. 280-286, 2012.

[5] A. Sahabul and D. Debashis, "Analysis of security threats in wireless sensor network," International Journal of Wireless & Mobile Networks, arXiv preprint arXiv, vol. 6, no. 2, pp. 35-46, 2014.