GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURITY ATTACKS IN WIRELESS SENSOR NETWORK

Dhamdhere Shubhangi T.*[1] and Dr. Gumaste S. V[2]
*[1]M.E.Student, SPCOE, Dumbarwadi, Distt: Pune, Maharashtra, India
[2]Professor, SPCOE, Dumbarwadi, Distt: Pune, Maharashtra, India

ABSTRACT

A feasible network can be consist of small, inexpensive sensor with several attributes due to development of software, hardware and its technology. Wireless Sensor Networks are rapidly gaining interests of researchers from emerging technology, industry and defense. Security is one of major issues for wireless sensor networks (WSN) because of various their vital situations. This paper focuses on the security attacks and its requirement, Security threats and types of attacks in WSN.

Keywords: *Security attacks, wireless sensor network and Cryptography concepts.*

I. INTRODUCTION

Due to data acquisition and data processing abilities Wireless Sensor Networks (WSNs) are a new technology can be used increasingly. Wireless sensor networks mostly operate in public and uncontrolled area, Hence Security is the major issue for the wireless sensor network (WSNs) in order to protect the functionality of the networks. Wireless sensor networks are collection of sensor nodes, storage nodes and sink node. In moderns wireless sensor network are used in military, habitat monitoring, battlefield and health monitoring applications today where sensor nodes need to send data to storage node and storage node to sink. With the development of Internet, more and more people need to access and share the remote resources, which bring great challenges for the security of information systems. Security is essential as they can be deployed in hostile environments with active intelligent opposition. Battlefield applications is one of the example where there is need for secrecy of location and resistance to subversion and destruction of the network. The protocol stack used in sensor nodes contains physical, data link, network, transport and application layers [7]. A Physical layer is responsible for carrier frequency generation, signal detection, modulation, and data encryption. A Data link layer is responsible for the data frame detection, multiplexing of data streams and error control. Also it ensuring reliable point-to-point and point-to-multipoint connections. Network layer is responsible for forwarding packets to the destination and assignment of addresses. A Transport layer is responsible for specifying how the reliable transport of packets will take place. A Application layer is responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user. The major contribution of this paper includes classification of security requirement, security Vulnerability and attacks in Wireless Sensor Networks. Section 2 gives the detailed information about the security requirements in Wireless Sensor Networks. Types of attacks are discussed in section 3. Security Vulnerability and their classification are explained in Section 4. Section 5 describes conclusion.

II. SECURITY PRE-REQUISITE FOR WSN

Sensor networks handled sensitive information in a number of domains. A WSN is a special type of network. It shares some resources with computer network, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most important security requirements in WSN are shown in figure 1.

Data confidentiality: Data confidentiality is a property of data, which prevents it from unauthorized users. In this security mechanism information cannot be understood by anyone except intended recipient. This is the most important issue in network security. Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential.

***Data Integrity*:** If a storage node sends an anonymous data to the sink then sink will detect the query as an invalid query The accuracy and consistency of stored data indicated by an absence of any alteration in data between two updates of a data record. Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by modifications.

ISSN 2348 – 8034
Impact Factor- 3.155

Data Availability**:** Availability determines whether the network is available whether a node has the ability to use the resources for the messages to communicate. Availability ensures that services and information can be accessed at the time that they are required.ie. in the presence internal or external attack such as denial-of-service attacks it must ensures that the preferred network services are available. Due to loss of availability, sensor networks suffer from many risks such as denial of service attacks and sensor node capturing. Lack of availability may affect the operation of many critical real time applications.

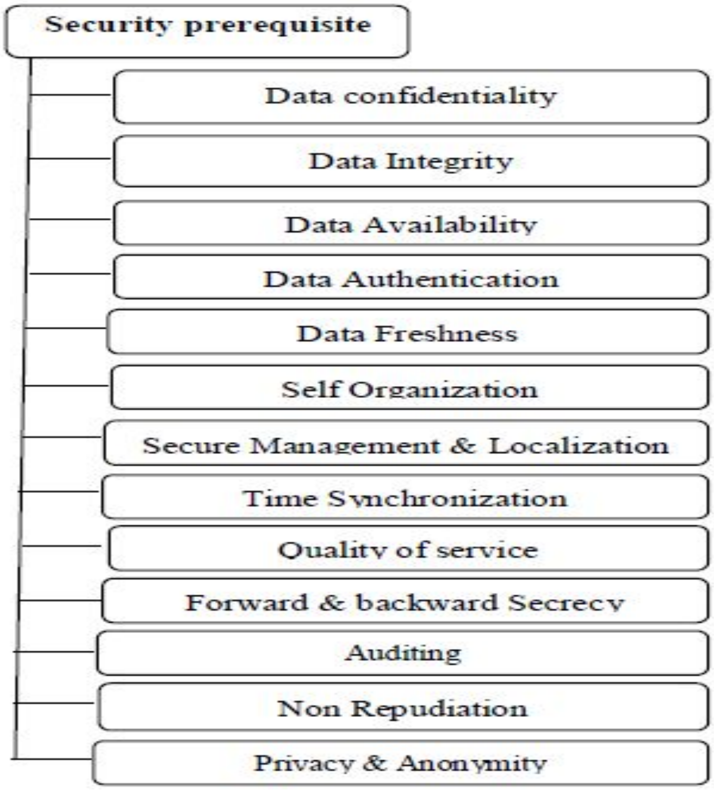

Fig: 1: Security Prerequisite for WSN

Data Authentication**:** Authentication ensures that the communication from one node to another node is actual, that is a malicious node cannot modify data in a network. Authentication ensures the reliability of the message. Attacks in sensor networks does not modify data, also can inject additional false packets [1].

Data Freshness: Freshness ensures that no resource can replay old messages. It implies that the data is fresh. To preserve confidentiality and data integrity, there is necessity of the freshness of each message. Data freshness objective ensures that data is recent, so that they can obey message ordering and have not been reused.

Self Organization: Each node in a WSN should be self-healing and self organizing. This characteristics of a WSN also poses a great challenge to security. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [4].

Secure Management & Localization**:** In the case of wireless sensor networks, secure management on base station or storage node level is required; since sensor nodes securely communicate with the base station. Key distribution to sensor nodes is used to establish encryption and routing information. In many situations, it becomes necessary to accurately and automatically locate each sensor node in a WSN. For example, a WSN designed to locate faults would require accurate locations of sensor nodes which identifies the faults.

Time Synchronization: In most of the applications, sensor networks require time synchronization. Any security mechanism for WSN should also be time-synchronized. Time synchronization is a vital part of infrastructure in any distributed system. In sensor networks, a convergence of factors makes robust and flexible time synchronization.

Quality of Service: Quality of Service have different meanings and perspectives. QoS is defined as the quality as apparent by the user while in the networking area. QoS is accepted to evaluate the service quality that the network offers to the applications/users.

Forward and Backward Secrecy*:* When sensor node leaves the network then sensor should not be able to read any future messages. It shows that the current key should not compromise any future key.ie. No consequent session keys can be recovered. While backward secrecy means even if an adversary recovered an adjacent subset of keys, it is impossible to recover the previous keys. i.e. no previous session keys can be recovered.

Auditing: A major function of wireless sensor networks is to sense data and to collect data. The Energy Auditing project is the application of battery powered wireless networks to measure potential sources of energy.

Non repudiation**:** It denotes that a node cannot refuse sending a message it has previously sent. It is the assurance that someone cannot deny something. Typically, non- repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Privacy and anonymity: Sensor networks are tools for collecting information, and an resource can gain access to sensitive information by accessing stored sensor data or by eavesdropping on the network. Resources can use data to derive sensitive information if they know how to correlate multiple sensor inputs. The main privacy problem, however, is not that sensor networks enable the collection of information that would otherwise be impossible. In fact, much information from sensor networks could probably be collected through direct site observation.

Anonymity is the state of being un-identifiable within a set of objects. Untraceability refers to the inability of an adversary in tracing individual data flows back to their origins or destinations [3]. Unlinkability means preventing an adversary from learning the identities of the source and the destination at the same time.

III. TYPES OF ATTACK

There are two types of attack:

Passive Attack**:** A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include monitoring of unprotected communications, traffic analysis, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the discovery of information or data files to an attacker without the consent or knowledge of the user.

Active Attack: In an active attack, the attacker tries to bypass or break into secured systems. This can be done through viruses, worms, or Trojan horses. Active attacks include attempts to avoid or break protection features, to introduce malicious node, and to alter the information.

IV. SECURITY VULNERABILITIES IN WSN

Due to the broadcast nature of the transmission medium, Wireless Sensor networks are weak to security attacks. Moreover, wireless sensor networks have an additional vulnerability because nodes are often placed in a dangerous environment where they are not physically protected. Wireless Sensor Networks are vulnerable to various types of attacks. These are classified into two types:

1. Physical Vulnerability

2. Technological Vulnerabilities

Physical vulnerabilities**:** Due to the deployment nature in public and hostile environments renders more link attacks ranging from passive eavesdropping to active interfering, sensor nodes would be highly exposed to capture. WSN can extent up to thousands of sensor nodes without any fixed infrastructure. This implies the need to develop simple, flexible, and scalable security protocols. And addition of new nodes and failure make the network topology dynamic and the solutions more complex Physical vulnerability is categorized as Authentication and secrecy attack and network availability attack shown in fig 2.

Attacks on secrecy and authentication: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as replay attack, spoofing of packets, eavesdropping, modification and packet replay attacks.

Replay Attack**:** A replay attack occurs when an attacker copies a messages between two parties and replays that message to one or more of the parties. A replay attack can be prevented using a strong digital signature which include time stamps and addition of unique information from previous transaction.

Eavesdropping**:** Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, and videoconference or fax transmission. The term eavesdrop comes from the practice of actually standing under the eaves of a house, listening to conversations inside. This is the most common attack to privacy. By probing to the data, the resources could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information.

Node Replication attack **:** Nodes replication attacks are one of the most mighty attacks. when an attacker compromising a node, it uses its secret cryptographic key to successfully occupy the network. Practically, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the nodeID of an existing sensor node. in this approach a node is replicated to disrupt a sensor network's performance. Packets can be corrupted or misrouted resulting in a disconnected network, false sensor readings etc. If an attacker can achieve physical access of the entire network, it can copy cryptographic keys to the replicated sensor nodes [7].

Traffic analysis: Traffic analysis is the process of intercepting and examining messages in order to realize information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted.

Passive monitoring: attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks. The purpose of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is necessary. A DoS attack can be any event that eliminates a network's capacity to perform its expected functions [5].

a) Denial of services

b) Software stealing

c) Hardware Stealing

d) Modification of data

e) Damage a system by code

f) Corrupt data by code

g) Illegally User Privileges

Technological vulnerabilities**:** Security services in WSNs must consider the hardware constraints of the sensor nodes:

1. Energy: energy consumption in sensor nodes can be categorized into three parts: energy for the sensor transducer, Energy for communication, energy for microprocessor computation.

2. Computation: Complex cryptographic algorithms cannot be used in WSNs because of sensor nodes's processors are not generally powerful.

3. Memory: There is usually not enough space to run complicated algorithms after loading OS and application code.

4. Transmission range: the communication range of sensor nodes is limited and need to preserve energy. Each bit transmitted in WSNs consumes about as much power as executing 800-1000 instructions. Thus, communication is more costly than computation in WSNs.

5. Wireless communication: Anyone can monitor or participate in communications by configuring at the same frequency band.

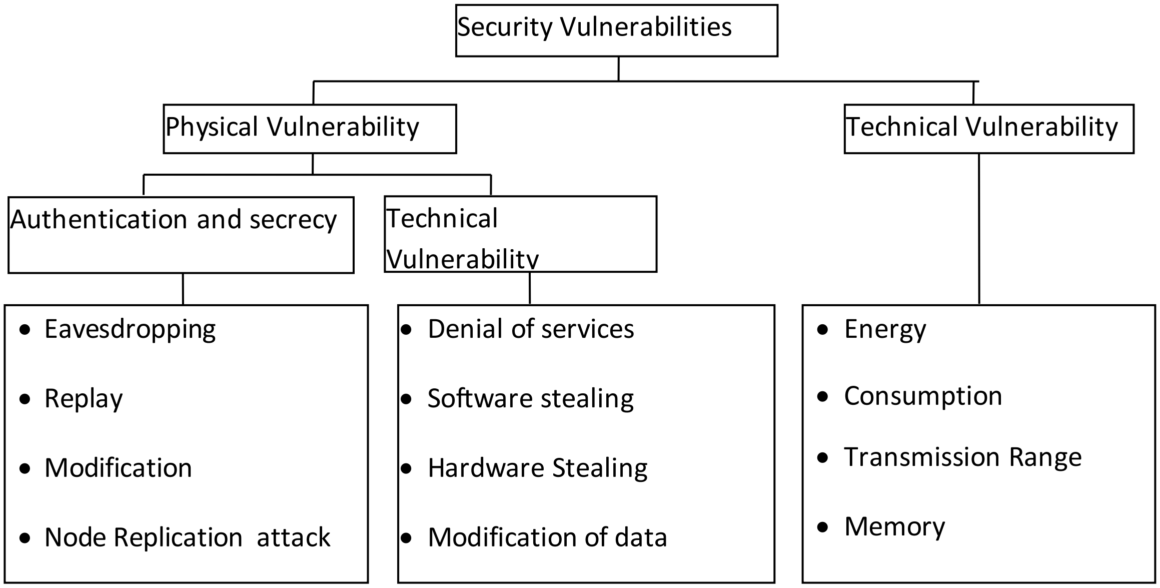

Fig: 2: Security Vulnerability on Wireless sensor networks

V. CONCLUSION

The exploitation of sensor nodes in an hostile environment makes the networks vulnerable. Wireless sensor networks are rapidly used in military, environmental, health and commercial monitoring. This paper analyzed security attacks, security threats, its requirement and vulnerability for processing and collecting the information in WSN and also presents the security objective that need to be achieved.

REFERENCES

1. *F. Akyildiz et al., ―A Survey on Sensor Setworks,‖ IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.*
2. *Y. Wang, G. Attebury, and B. Ramamurthy, ―A Survey of Security Issues in Wireless Sensor Networks,‖ IEEE Commun. Surveys*
3. *Adrian Perrig, John Stankovic, David Wagner, ―Security in Wireless Sensor Networks‖ Communications of the ACM, Page53-57, year 2004*
4. *F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ―A survey on sensor networks‖, IEEE Communications Magazine, Vol.40 No. 8, pp. 102-114, August 2002.*

5. *Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, ―Security in wireless sensor networks: issues and challenges‖ Advance Communication Technology (ICACT), Page(s):6, year 2006*

6. *Zia, T.; Zomaya, A., ―Security Issues in Wireless Sensor Networks‖, Systems and Networks Communications (ICSNC) Page(s):40 – 40,*

7. *N.Shanti, Lganesan and K.Ramar, ―Study of Different Attacks On Multicast Mobile Ad-Hoc Network.*

ABOUT AUTHORS

[1] Ms. Dhamdhere Shubhangi T., ME student, Department of Computer Engineering, SPCOE-Dumberwadi, Otur.

[2] Dr. S. V. Gumaste, currently working as Professor and Head, Department of Computer Engineering, SPCOE-Dumberwadi, Otur. Graduated from BLDE Association's College of Engineering, Bijapur,Karnataka University, Dharwar in 1992 and completed Post-graduation in CSE from SGBAU, Amravati in 2007. Completed Ph.D (CSE) in Engineerng & Faculty at SGBAU, Amravati. Has around 22 years of Teaching Experience.