RESEARCH ARTICLE OPEN ACCESS

Study of Wireless Sensor Networks Security Issues and Attacks

Menaka Chandra[1], Ankit Naik[2], Chayya Chandra[3]
Research Scholar[1&3], Lecturer[2]
Department of Computer Science and Engineering
Kirodimal Institute of Technology
Raigarh
Chhattisgarh – India

ABSTRACT
Wireless sensor network is the interesting field which are used in various field such as motivate by military application such as battlefield surveillance. Today such network are used in many industrial and consumer application, such as industrial process monitoring and control, machine health monitoring and disaster management, habitat monitoring, home automation, Systems building, traffic surveillance, smart home, mass public etc. This paper discusses Definition of WSN, its type, Architecture of WSN, attacks in WSN & Security issues.

Keywords: - Wireless sensor network, Type of WSN, Attack in WSN, Security goals in WSN.

I. INTRODUCTION

A wireless sensor network (WSN) of spatially distributed autonomous sensor to monitor physical and environmental condition, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location. The more modem network are bi-directional , also enabling control of the sensor activity. The development of wireless sensor network was motivate by military application such as battlefield surveillance. Today such network are used in many industrial and consumer application, such as industrial process monitoring and control, machine health monitoring and so on.

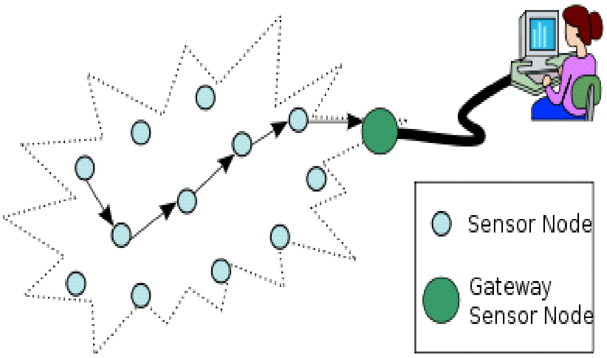

Fig 1 Nodes in WSN

The WSN is built of “nodes” from a few to several hundreds or even thousands, where each node is connected to one (or sometime several) sensors. Each such sensor network has typically several parts : a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensor and an energy source, usually a battery or an embedded from of energy harvesting.

II. TYPES OF SENSOR NETWORKS

A. *Terrestrial WSNs[1]*

In these, nodes are distributed in a given area either in an ad hoc manner (sensor nodes are randomly placed into the target area by dropping it from plane) or in pre-planned manner (sensor nodes are placed according to grid placement, optimal placement, 2-d and 3-d placement models). Since battery power is limited and it cannot be recharged, terrestrial sensor nodes must be provided with an optional power source such as solar cells.[2]

B. Underground WSNs[1]

In these, sensor nodes are buried underground or in a cave or mine that monitors the underground conditions. Sink nodes are deployed above the ground to forward the gathered information from the sensor nodes to the base station. These are more expensive than the terrestrial sensor networks because proper nodes are to be selected that can assure reliable communication through soil, rock, water and other mineral contents. [2]

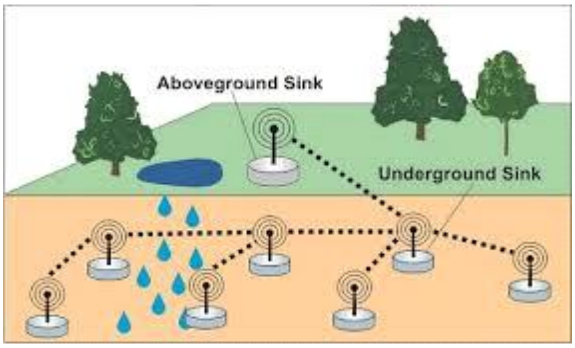

Fig 2 Underground WSN

C. Underwater WSNs[1]

In these, sensor nodes and vehicles are located underwater. Autonomous vehicles are used for gathering the data from the sensor nodes. Sparse deployment of nodes is done in this network. Main problems that come under this while communicating are limited bandwidth, long propagation delay and signal fading issue.[2]

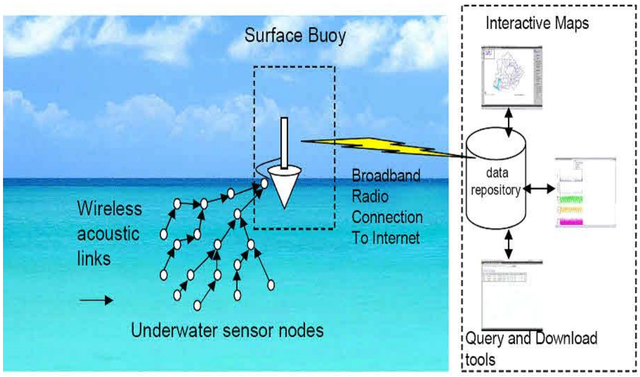

Fig 3 Underwater WSN

D. Multimedia WSNs [2]

In these, low cost sensor nodes are equipped with cameras and microphones. These nodes are located in a pre-planned manner to guarantee coverage. Issues in these networks are demand of high bandwidth, high energy consumption, quality of service provisioning, data processing and compression techniques, and cross layer design. [2]

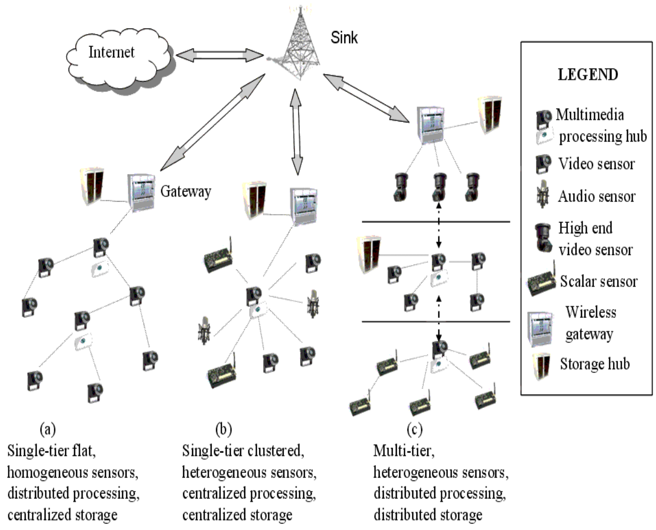
Internet
Sink
Gateway
LEGEND
Multimedia processing hub
Video sensor
Audio sensor
High end video sensor
Scalar sensor
Wireless gateway
Storage hub
(a)
Single-tier flat, homogeneous sensors, distributed processing, centralized storage
(b)
Single-tier clustered, heterogeneous sensors, centralized processing, centralized storage
(c)
Multi-tier, heterogeneous sensors, distributed processing, distributed storage

Fig 4 Multimedia WSN

III. ARCHITECTURE FOR WSN

The typical Wireless Sensor Network consists of the following: -

1. Network manager – The responsibility of the Network Manager is to configure the network, schedule inter-device communication (Configure super-frames), manage routing table, monitor and report network health[6].

2. Security manager – The overall responsibility of the Security Manager is to generate, store, and manage keys[6].

Access point or Gateway Field Device and Host application communication is enabled by the Gateway.

3. Field devices (Sensor motes) – The Field device that is attached to the process, should have the capability to route packets on other devices' behalf. In majority of the situations they define the characteristics of the process or equipment responsible for processing, even controlling them at times. The router is one field device, which is special in nature as it doesn't control the equipment or interface with the process, it even doesn't have the process sensors[6].

IV. ATTACKS ON WIRELESS SENSOR NETWORKS

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks.

Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.[5]

Attacks against Privacy

The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks[8] against sensor privacy are:

Monitor and Eavesdropping

This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

Traffic Analysis:

Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

Camouflage Adversaries

One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.[5]

Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

Routing Attacks in Sensor Networks

The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.[5]

- Spoofed, altered and replayed routing information
- An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information.
- Create routing loops
- Extend or shorten service routes
- Generate false error messages
- Increase end-to-end latency [5]

Selective Forwarding

A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.[5]

Sinkhole Attack

Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes. [5]

Sybil Attacks

A single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault to lerantschemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.[5]

Wormholes Attacks

In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network.[5]

HELLO flood attacks

An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.[5]

Denial of Service

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.[5]

Node Subversion

Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary. [5]

Node Malfunction

A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader [5].

Node Outage

Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route [5].

Physical Attacks

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.[5]

Message Corruption

Any modification of the content of a message by an attacker compromises its integrity.[5]

False Node

A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.[5]

Node Replication Attacks

Conceptually, 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. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.[5]

Passive Information Gathering

An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used. This section explained about the attacks and their classification that widely happens on wireless sensor networks. The next section discusses about the security mechanisms that are used to handle the attacks[5]

V. SECURITY GOALS FOR WIRELESS SENSOR NETWORK

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, no repudiation, and anti-playback [5]. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks.

1. Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks.WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power . Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network. As minimal (or no) human interaction for the sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to time for encryption. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.[4]

2. Steganography

While cryptography aims at hiding the content of a message, steganography. Aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.). The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources of the sensors is difficult and an open research issue.[4]

3. Physical Layer Secure Access

Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop) and hopping [4]

4. Data Confidentiality

Confidentiality is an acceptance of authorized access to information communicated from a certified sender to a certified receiver. A sensor network must not reveal sensor readings to its neighbours. Highly sensitive data is sometimes routed through many nodes before reaching the final node. [1] It ensures that the data should be accessed only by authorized parties. It should not be revealed to others at any cost. The sensor data and routing information both should be maintained in a secret way. It can be attained by using efficient cryptographic techniques. To achieve a secure data aggregation, it is classified as hop by hop and end to end mechanisms. In structured data aggregation method, sensor nodes transmit the encrypted data to the aggregator node. Then it decrypts that data, perform aggregation and again encrypt the data, send to BS. This process leads to more energy consumption and produces delay. In the second method, the aggregator node performs aggregation over encrypted data by using various techniques for example Privacy Homomorphism. The BS can only have the decryption key to decrypt the aggregated data. It provides end to end confidentiality and improves network performance. [3]

5. Data Integrity

Provision of data confidentiality stops the outflow of information, but it is not helpful against adding of data in the original message by attacker. Integrity of data needs to be assured in sensor networks, which strengthens that the received data has not been tampered with and that new data has not been added to the original contents of the packet. Data integrity can be provided by Message Authentication Code (MAC). [1]

6. Data Authentication

An adversary is not only limited to modify the data packet but it can change the complete packet stream by adding extra packets. So the receiver needs to confirm that the data used in any decision-making process comes from the authorized source. Data authenticity is an assurance of the identities of communicating nodes [1] Sensor nodes are transmitting and receiving the data only in wireless medium. It is vulnerable in nature because of various intruders and attacks. Node authentication ensures that the source and destination node should not be compromised. The data should the intended receiver node. Data authentication refers that the transferred data should be the same as the original data sent by the source node. For that, MAC (Message Authentication Code) computation is used. It provides shared secret key between the source and destination.[3]

7. Availability

The availability check is also one of the important factors for energy constrained wireless sensor nodes. Due to the energy depletion, the node accessibility is reduced and it can be a chance of more intruding actions. It ensures the network survivability and prevents the attacks [3]

8. Time Synchronization

Most sensor network applications depend upon some form of time synchronization. In order to skimp power, an individual sensor's radio may be turned off for some time. Moreover, sensors may wish to calculate the end-to-end delay of a packet as it travels between two pair wise sensors [1]

9. Secure Localization

WSN makes use of geological based information for recognition of nodes, or for accessing whether the sensors correspond to the network or not. Some attacks work by investigating the location of the nodes. Attacker may probe the headers of the packets and protocol layer data for this purpose. This makes the secure localization an important feature that must be satisfied during our implementation of security protocol [1]

10. Flexibility

Sensor networks will be used in vigorous arena scenarios where environmental circumstances, hazards and mission may change frequently. Changing mission goals may desire sensors to be eliminated from or injected to a settled sensor node. Moreover, two or more sensor networks may be merged into one, or a single network may be divided in two. Key establishment protocols must be ductile enough to render keying for all potential scenarios a sensor network may encounter [1]

11. Robustness and Survivability

The sensor network should be robust across various security attacks and if an attack conquers, its impact should be reduced. The covenant of a single node must not violate the security of the whole network [1]

12. Data Freshness and Node Localization

The freshness of data greatly prevents the aggregated data from a lot of replay attacks and duplicate messages. Because there is a chance for the replay of old messages. It is a waste of energy only. So the transmitted data should be resent. By achieving data freshness, network performance and energy are effectively used. The location of the destination node is very important for the source node. .[3]

VI. CONCLUSION

In this paper, we present a brief survey on wireless sensor network, its Architecture, its types. Then we discussed about the security in sensor networks. Security is an important requirement and complicates enough to set up in different domains of WSN, discuss various security attacks active attacks and passive attack and also discuss security (availability, integrity, confidentiality, authenticity, cryptography, steganography, physical Layer Secure Access and so on) .

REFERENCE

[1] Aashima single,Ratika Sachdeva," Review on Security Issues and Attacks in Wireless Senso Networks",IJARCSSE,Volume3/Issue4,April2013,PP .529-534
en.wikipedia.org/wiki/wireless_sensor_network.

[2] N.Sugandhi et al.," Analysis of Various Deterioration Factors of Data Aggregation in Wireless Sensor Networks",IJET,Volume5,No1 ,ISSN:0974-4024,Feb-Mar 2013.

[3] Al-Sakib Khan Pathan,Hyung-Woo Lee,Choong Seon Hong," Security in Wireless Sensor Networks: Issues and Challenges",ISBN 89-5519-129-4,Feb.20-22,2006 ICACT2006

[4] Dr.G.Padmavathi Mrs.D.Shanmugapriya, " A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks",IJCSIS, Volume4 ,No.1&2,2009

[5] Anser Ghazaal Ali Alquraishee, Aasim Zafar, Syed Hamid Hasan, "Security Issues in Wireless Sensor Networks",MAGNT ResearchReport(ISSN.1444-939),Volume2 (4): PP.82-91.