Security Attacks and Challenges of Wireless Sensor Network

\

[1]Mubashir Tariq(Mubashirtariq9@gmail.com), [2]Faisal Mehmood(faisalmehmood685@uaf.edu.pk),
[3]Muhammad Tahzeeb ul Hassan(muhammadtahzeeb@gmail.com)
4'Muhammad Wasim Abbas Ashraf (wasim_117@hotmail.com)

Abstract— Wireless sensor networks is an emerging field to research and development, due to a large number of application avail benefits from such systems and has lead to the development of tiny, cheap, disposable and self contained battery powered computers, known as sensor nodes or "motes", So the demanding and challenging part of wireless sensor network is security makes it more severe constraints than conventional networks. However, there are several types of sensor network , helps to trace the challenges to make secure network. In this paper, we investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks.

Index Terms— Wireless Sensor Networks (WSNs), Security Attacks And Challenges, Security Mechanism.

I. INTRODUCTION

A group of two or more computing devices linked via a form of communications technology. For example, a business might use a computer network connected via cables or the Internet in order to gain access to a common server or to share programs, files and other information.

A computer network consists of a collection of computers, printers and other equipment that is connected together for the purpose of sharing data.

The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly using wireless networking cards that send and receive data through the air. Connected computers can share resources like access to the Internet, printers, file servers, and others[1].

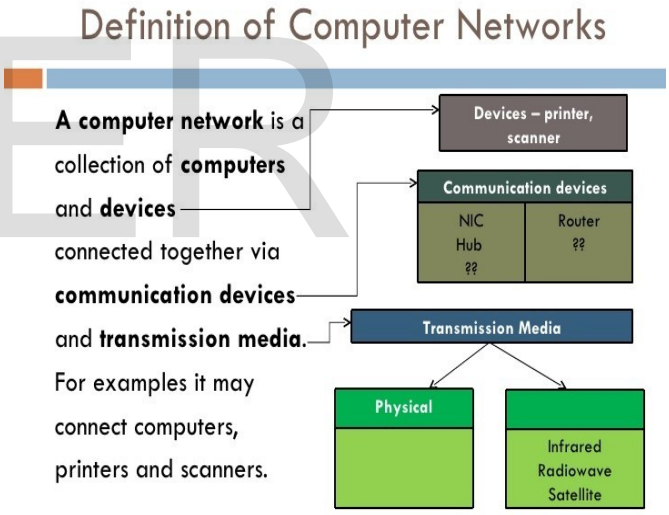

Figure 1: Computer Network[1]

Types of Network

There are two main types of network i.e. wired network and wireless network.

a) Wired Networks

Wired network are those network in which computer devices attached with each with help of wire. The wire is used as medium of communication for transmitting data from one point of the network to other point of the network.

b) Wireless Networks

A network in which, computer devices communicates with each other without any wire. When a computer device wants to communicate with another device, the destination device must lays within the radio range of each other Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

II. WHY USED WIRELESS NETWORKS?

Wireless networks are getting popular due to their ease of use. Consumer/user is no more dependent on wires where he/she is, easy to move and enjoy being connected to the network. One of the great features of wireless network that makes it fascinating and distinguishable amongst the traditional wired networks is mobility [2]. This feature gives user the ability to move freely, while being connected to the network. Wireless networks comparatively easy to install then wired network. There is nothing to worry about pulling the cables/wires in wall and ceilings. These can range from small number of users to large full infrastructure networks where the number of users is in thousands

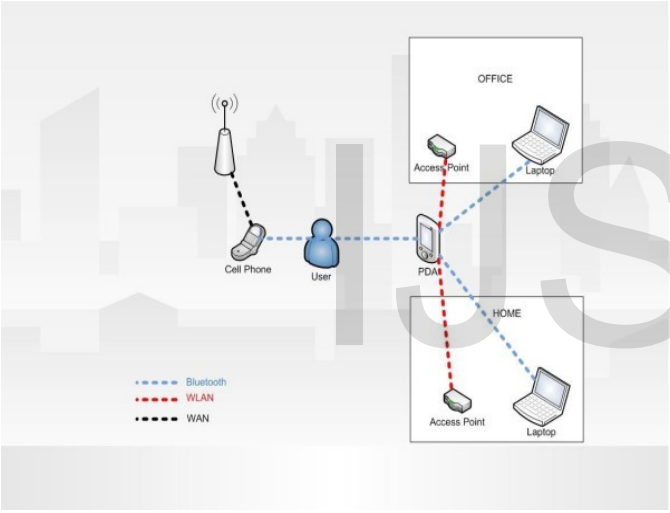

Figure 2: Communications in Wireless Networks [2]

2.1 Wireless ad-hoc Network:

A wireless ad-hoc network consists of a collection of nodes that communicate with each Other through wireless links without a pre-established networking infrastructure. It originated from battlefield communication applications, where infrastructure networks are often impossible. Due to its edibility in deployment, there are many potential applications of a wireless ad-hoc network. For example, it may be used as a communication network for a rescue-team in an emergency caused by disasters, such as earthquakes or floods, where infrastructures may have been damaged.

It may also provide a communication system for pedestrians or vehicles in a city. Another example of a wireless ad-hoc network is a rooftop network, which consists of a number of wireless nodes spread over an area to provide local networking service and access to wired networks, such as the Internet, for residents in the neighborhood. Another application of wireless ad-hoc networks is a sensor network, which consists of a large number of small computing devices deployed in a region that collect data and may send the information to a central server.

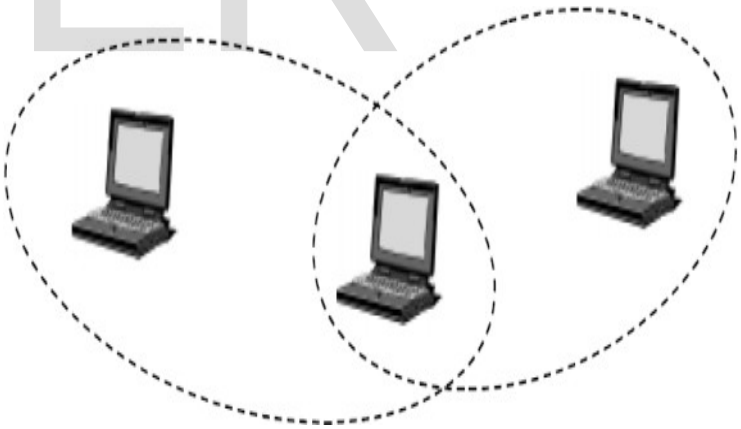

Figure : 3. Simple ad-hoc networks [3]

2.2 Manet:

A mobile ad hoc network is formed by mobile hosts. Some of these mobile hosts are willing to forward packets for neighbors. All nodes are capable of moving and can be connected dynamically in an arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. In this type of networks, some pairs of terminals may not be able to communicate directly with each other and have to

reply on some other terminals so that the messages are delivered to their destinations [4]. Such networks are often referred to as multi-hop or store-and-forward networks. The nodes of these networks function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices. Figure 1.7 shows an example for vehicle-to-vehicle network communicating with each other by relying on peer- to-peer routings.

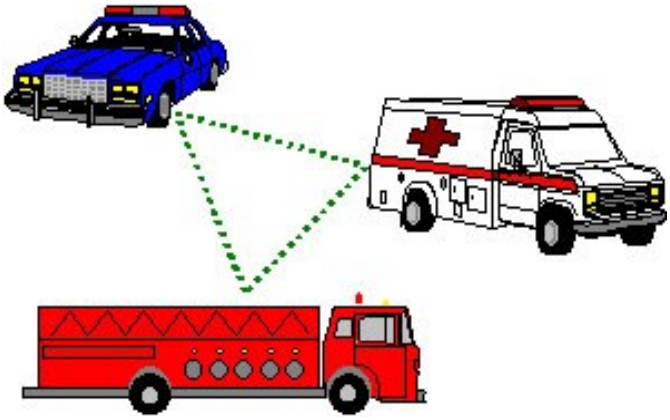

Figure 4. Example of a vehicle-to-vehicle network [4]

2.3 Wireless Sensor Networks

Wireless Sensor Networks consists of individual nodes that are able to interact with their environment by sensing or controlling physical parameter; these nodes have to Collaborate in order to fulfill their tasks as usually, a single node is incapable of doing .So, and they use wireless communication to enable this collaboration [5]. The definition of WSN, according to, Smart Dust program of DARPA is: "A sensor network is a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment".

III. INTRODUCTION TO WIRELESS SENSOR NETWORKS

A wireless sensor and actuator network (figure 1.5) is a collection of small randomly dispersed devices that provide three essential functions; the ability to monitor physical and environmental conditions, often in real time, such as temperature, pressure, light and humidity; the ability to operate devices such as switches, motors or actuators that control those conditions; and the ability to provide efficient, reliable communications via a wireless network.

WSANs are typically self-organizing and self-healing. Self-organizing networks allow a new node to automatically join the network without the need for manual intervention. Self-healing networks allow nodes to reconfigure their link associations and find alternative pathways around failed or powered-down nodes.

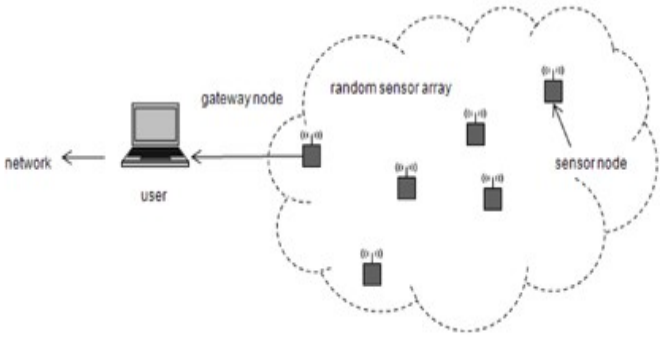

Figure 5. Wireless sensor network.[5]

Wireless sensor networks use three basic networking topologies; point-to-point, star (point-to-multipoint), or mesh (figure 1.6). Point-to-point is simply a dedicated link between two points. Star networks are an aggregation of point-to-point links, with a central master node.
In the mesh topology, every node has multiple pathways to every other node, providing the most resiliency and flexibility.

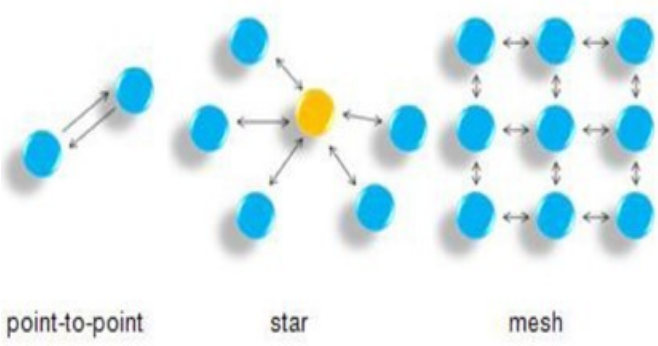

Figure 6. Basic wireless network topologies[6].

3.2 Components of Wireless Sensor Network

Basically, each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment.

- **Sensor Field***:* A sensor field can be considered as the area in which the nodes are placed.

- **Sensor Nodes:** Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink.

- **Sink:** A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. Sinks are also known as data aggregation points.
- **Task Manager:** The task manager also known as base station is a centralized point of control within the network, which extracts information from the network and disseminates control information back into the network. The base station is either a laptop or a workstation.

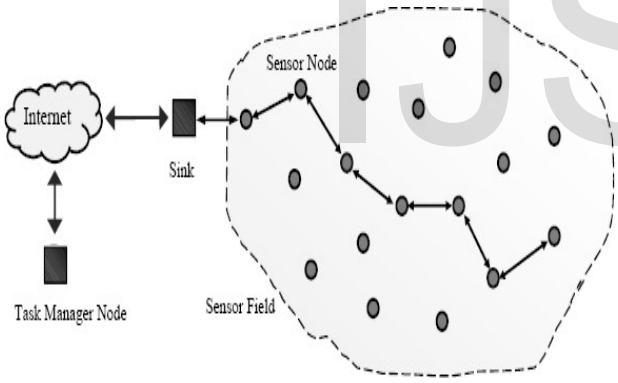

Figure 7. Components of Wireless Sensor Network [7]

3.1 Applications of WSN

1. Area monitoring
2. Air pollution monitoring
3. Greenhouse monitoring
4. Landslide detection
5. Industrial monitoring
6. Forest fires detection
7. Water/wastewater monitoring
8. Volcano monitoring
9. Agriculture
10. Structural monitoring

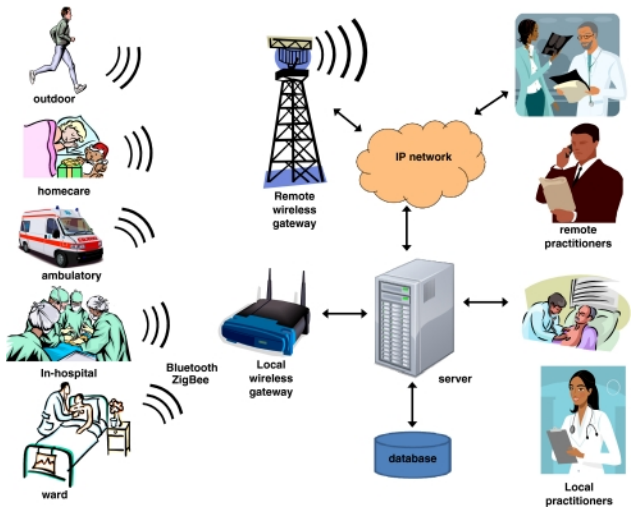

Figure.8. Wireless Sensor Network Applications[8]

IV. ATTACKS ON 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.

A. 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. Some of the more common attacks [8] against sensor privacy are: Monitor and Eavesdropping, Traffic Analysis, Camouflage Adversaries.

B. 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, Denial of Service Attacks, Node Subversion, Node Malfunction, Node Outage, Physical Attacks, Message Corruption, False Node, Node Replication Attacks, Passive Information Gathering etc.

V. SECURITY MECHANISM

The security mechanisms are actually used to detect, prevent and recover from the security attacks. These can be categorized as high level and low-level. Figure 3 shows the order of security mechanisms.

A. Low-Level Mechanism

Low-level security primitives for securing sensor networks includes, Key establishment and trust setup, Secrecy and authentication, Privacy Robustness to communication denial of service, Secure routing, Resilience to node capture etc.

B. High-Level Mechanism

High-level security mechanisms for securing sensor networks, includes secure group management, intrusion detection, and secure data aggregation.

VI. CHALLENGES OF SENSOR

Networks

A wireless sensor network is a special network which has many constraint compared to a traditional computer network.

A. Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple.

B. Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration.

C. Hostile Environment

The next challenging factor is the hostile environment in which sensor nodes function. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices.

D. Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms.

E. Immense Scale

Simply networking tens to hundreds or thousands of nodes has proven to be a substantial task. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

F. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

Unreliable Transfer

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable.

Conflicts

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network.

Latency

The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

G. Unattended

Operation Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main cautions to unattended sensor nodes.

H. Exposure to Physical Attacks

The sensor may be deployed in an environment open to adversaries, bad weather, and so on.

• **Managed Remotely**

Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues.

• **No Central Management Point**

A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

VII. CONCLUSION

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

VIII. REFERENCES

[1]. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004

[2]. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies, Page1043-1045, year 2006

[3]. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier),
Page: 299-302, year 2003

[4]. Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "ASurvey on Sensor Networks", IEEE Communication Magazine, year 2002

[5]. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10- 15, year 2006.

[6]. Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges"Advanced CommunicationTechnology (ICACT), Page(s):6, year 2006

[7]. Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009.

[8]. Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002
http://www.cs.sfu.ca/~angiez/personal/papessenso r-ids.pdf

[9]. Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 –40, year 2006

[10]. Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2,page(s):52-62, year 2009.

[11]. Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[12]. D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2-28, year 2005.