A Review on Wireless Sensor Networks- Security Issues and Disputes

K.Priyadharshini
Assistant Professor, Department of Information Technology
G.Venkataswamy Naidu College,Kovilpatti,India

Abstract

Today world is evolving around wireless devices. Therefore wireless sensor networks are becoming prominent area for research and development. Due to a massive variety of software avail benefits from such structures and has cause the improvement of tiny, reasonably-priced, disposable and self contained battery powered computers, known as sensor nodes or "motes". So the traumatic and hard a part of wireless sensor community is security makes it extra excessive constraints than conventional networks. However there are many kinds of sensor networks, that helps to find out the challenges to make the network secure. There are many technologies that are really developed for the security of wireless sensor networks. In this paper we inquire issues related to security and disputes in wireless sensor networks. We find out the security issues and survey proposed security mechanisms for wireless sensor networks.

Keywords - *Wireless Sensor Networks (WSNs), Security issues and disputes, security Mechanisms*

I. INTRODUCTION

A group of more than two computing devices linked via a form of communications era. For example, an enterprise would possibly use a laptop community linked through cables or the internet with a view to advantage get admission to a common server or to proportion packages, files and other data.

A computer network consists of a set of computers, printers and other device that is linked collectively for the cause of sharing facts. The relationship among computer systems can be finished thru cabling, maximum typically the Ethernet cable, or wirelessly the use of Wi-Fi networking cards that send and acquire data via the air. Connected computers can share resources like get right of entry to the internet, printers, record servers, and others.

A. Types of Network

There are two important types of network i.e. wired network and wireless network [2]

1. Wired Networks

Wired network are the ones wherein pc gadgets attached with each with assist of cord. The cord is used as medium of communiqué for transmitting information from one point of the network to other point of the community.

2. Wireless Networks

A network in which, computer devices communicates with each different without any cord. While a computer device wants to talk with another device, the vacation spot device should lays within the radio range of each different [2] devices.

Users in wireless networks transmit and get hold of facts the use of electromagnetic waves. Recently wireless networks are becoming increasingly famous because of its mobility, simplicity and very low priced and price saving set up.

Fig 1. Computer Networks

II. WHY USE WIRELESS NETWORKS?

Wi-Fi networks are becoming famous due to their ease of use. Patron/consumer is not any greater depending on wires wherein he/she is, smooth to transport and experience being linked to the network. One of the superb functions of wireless network that makes it charming and distinguishable among the conventional stressed out networks is mobility [2]. This selection gives user the ability to move freely, whilst being linked to the network. Wireless networks comparatively clean to install then stressed out community. There may be not anything to fear approximately pulling the cables/wires in wall and ceilings. These can range from small wide variety of usersto huge complete infrastructure networks in which the wide variety of users is in heaps.

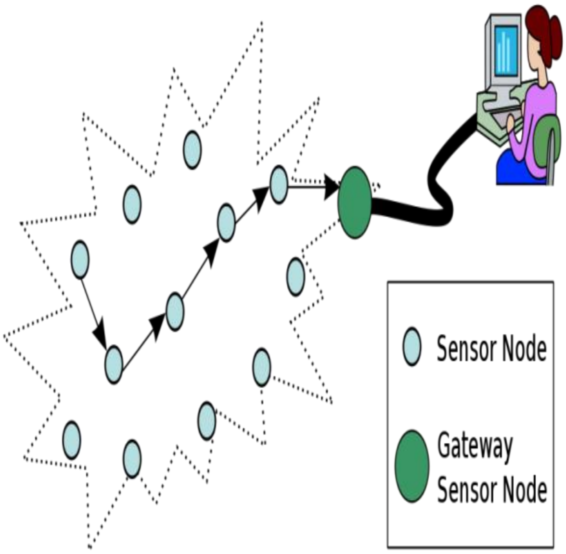

Fig 2. Communications in Wireless Networks

A. Wireless ad-hoc Network

A wireless ad-hoc community includes a collection of nodes that communicate with each different via wireless links without a pre-mounted networking infrastructure. It originated from battlefield communication applications, wherein infrastructure networks are frequently not possible [3]. Due to its exibility in deployment, there are many capacity packages of a wireless ad-hoc community. For instance, it could be used as a communication network for a rescue-crew in an emergency caused by disasters, such as earthquakes or floods, where infrastructures may additionally were damaged.

B. Manet

A mobile ad hoc community is formed by using cellular hosts. Some of those cellular hosts are willing to forward packets for neighbors. All nodes are capable of moving and can be linked dynamically in an arbitrary way. The duties for organizing and controlling the network are dispensed among the terminals themselves. in this form of networks, a few pairs of terminals might not be able to speak at once with every other and need to depend upon some other terminals so that the messages are delivered to their locations [4][5]. Such networks are frequently referred to as multi-hop or keep-and-ahead networks.

It is also used to provide a communication system for people who are pedestrians or travel by vehicles in a city. An 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. An important application of wireless ad-hoc networks is the 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.

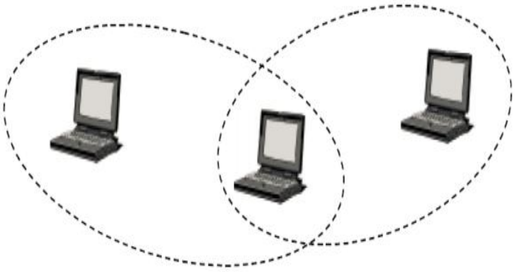

Fig 3. Simple ad-hoc networks [3]

c. Wireless Sensor Networks

Wireless Sensor Networks includes man or woman nodes which might be able to have interaction with their environment by way of sensing or controlling bodily parameter; these nodes should collaborate in order to satisfy their tasks as generally, a single node is incapable of doing so, and that they use wireless verbal exchange to allow 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. WIRELESS SENSOR NETWORK INTRODUCTION

Both wireless sensor network and a simple actuator network is a collection of tiny randomly distributed 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 an ability to provide an efficient and reliable communications via a wireless network. WSANs are typically self-organizing and self-healing. Self-organizing networks allow a new node to automatically join in the network without the need for any intervention action.

Wireless sensor networks are generally self-organizing and self-repairing. Self-organizing networks will allow a new node to automatically join the network without any need for human intervention. Self-repairing networks allow nodes to reconfigure their link associations and find alternative pathways around failed or powered-down nodes.

Wireless sensor networks use three main networking topologies; point-to-point, star (point-to-multipoint), or mesh (figure 4). Point-to-point network topology is simply a dedicated link between two points. Star network is a collection of point-to-point links, with a central master node.

In the mesh network topology, each node has many pathways to every other node, providing the most resiliency and flexibility.

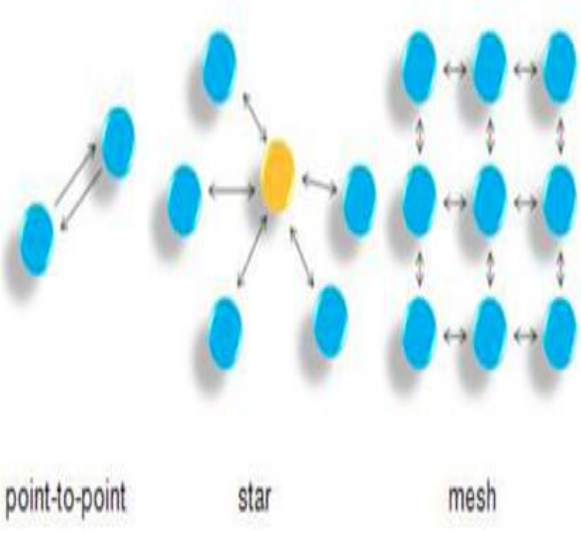

Fig 4. Basic wireless network topologies

A. Components of Wireless Sensor Network

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

Sensor Field

A sensor field can also be considered as an area in which all the nodes are placed. Sensor Nodes: Sensors nodes are considered as the heart of the network. They are the in charge collection of data and routing of those information back to a sink.

a. Sink

A sink is a sensor node with the particular task of receiving, processing and storing data from the other sensor nodes. Sinks are also known as data aggregation points.

b. Task Manager

The task manager which is also known as the 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 may be either a laptop or a workstation.

B. 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

IV. ATTACKS ON SENSOR NETWORKS

Wireless Sensor networks are prone to security assaults because of the broadcast nature of the transmission medium. Moreover, wireless sensor networks have an extra vulnerability because nodes are regularly positioned in a opposed or risky surroundings in which they are no longer physically protected. Essentially attacks are classified as active attacks and passive attacks.

A. Passive Attacks

The monitoring and listening of the communication medium by unauthorized persons are known as passive attack. The Attacks against privacy is passive in nature. Some of the more common attacks [9] against sensor privacy are: Monitor and Eavesdropping, Traffic Analysis, Camouflage Adversaries.

B. Active Attacks

The unauthorized attackers monitors, listens to and also they modifies the data stream in the communication medium 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 really used to find, prevent and recover from the security attacks. These can be separated as high level and low-level.

A. Low-Level Mechanism

A Low-level security primitives for securing sensor networks will include, 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

A High-level security mechanisms for securing a sensor network, 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 sensor network is very difficult to configure and connect to other networks.It is very difficult to find out failures or connection discards in wireless sensor networks.

A. Wireless Medium

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

B. Ad-Hoc Deployment

The ad-hoc nature of sensor networks have no structure can be statically defined. The network topology is will subject to change due to node failure, addition, or mobility. Nodes may be deployed due to airdrop

C. Hostile Environment

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

D. Resource Scarcity

The severe resource limitations of sensor devices provide 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 measures must be scalable to a very large networks while maintaining high computation and communication efficiency.

F. Unreliable Communication

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

VII. CONCLUSION

The deployment of sensor nodes in an unattended environment makes the networks prone. Wireless sensor networks are an increasing number of being utilized in army, environmental, health and commercial programs. Sensor networks are inherently specific from traditional stressed out networks as well as wireless ad-hoc networks. Safety is an critical function for the deployment of Wireless Sensor Networks. This paper summarizes the assaults and their classifications in Wireless sensor networks and also an attempt has been made to discover the security mechanism widely used to address the ones attacks. The challenges of wireless Sensor Networks also are in short mentioned. This survey will with a bit of luck inspire destiny researchers to give you smarter and more robust safety mechanisms and make their community safer.

REFERENCES

[1] AnjuBala"Security Attacks and Challenges of Wireless Sensor Network"International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2018, Volume 3, Issue 1 ,ISSN : 2456-3307.

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

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

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

[5] Ian F. Akykildiz, Weilian Su, Yogesh Sankara subramaniam, and ErdalCayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002.

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

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

[8] TahirNaeem, 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.

[9] 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/papessensor-ids.pdf .

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