SIES Graduate School of Technology
RISE WITH EDUCATION

Techscience
IT Magazine

Security Attacks and Challenges of Wireless Sensor Network

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. 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.

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. Figure 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.

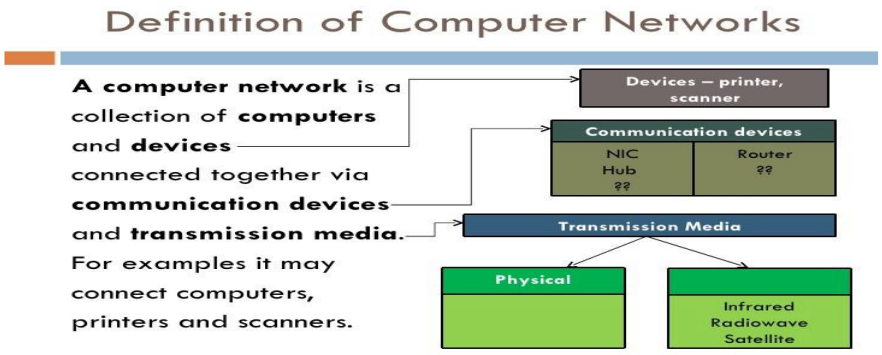

Figure1.Definition of Computer Network

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.

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 . 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.

Wireless Network includes a larger advantage in today's communication application like environmental, traffic, military and health observation. To realize these applications it's necessary to possess a reliable routing protocol. The self-organizing nature of MANETs makes them suitable for many applications and hence, considerable effort has been put into securing this type of networks. Secure communication in a network is determined by the reliability of the key management scheme, which is responsible for generating, distributing and maintaining encryption/decryption keys among the nodes. In this paper various key management schemes for MANETs are discussed. This research work proposes a novel secure Identity-Based Key Management protocol making use of cryptographic and Information Theoretic Security.

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 [2]. 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.

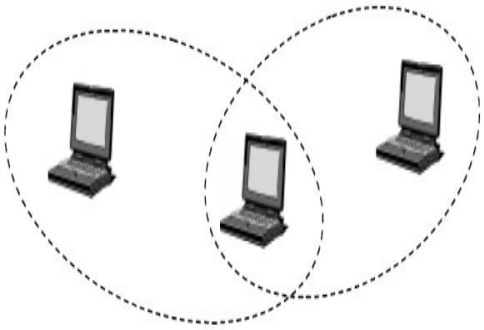

Figure 2.Simple ad-hoc networks

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 rely 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.

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 . 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"

A wireless sensor and actuator network 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.

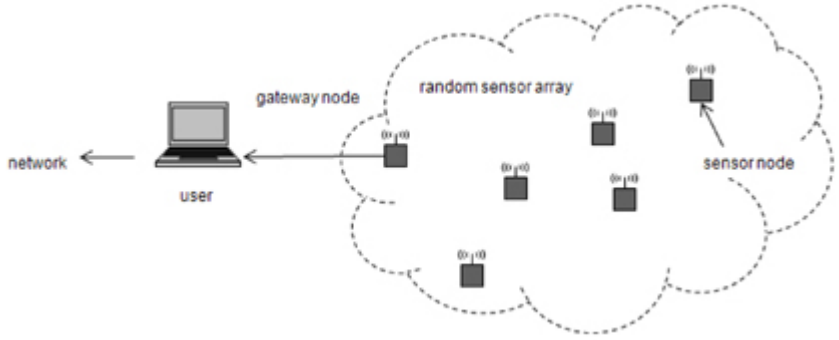

Figure 3. Wireless sensor network.

Wireless sensor networks use three basic networking topologies; point-to-point, star (point-to-multipoint), or mesh. 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.

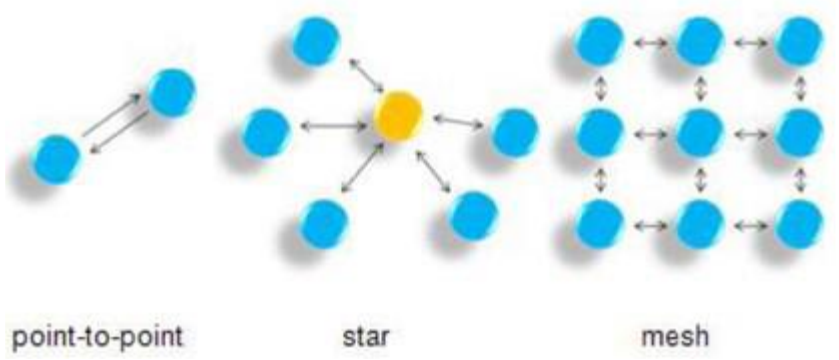

Figure 4. Basic wireless network topologies