International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 03, March 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

WIRELESS SENSOR NETWORKS: A SURVEY REPORT

Nitin Panwar[1], Amit Sharma[2]

[1,2]*Asssistant Professor, IIMT College of Engineering, Greater Noida (India)*

ABSTRACT

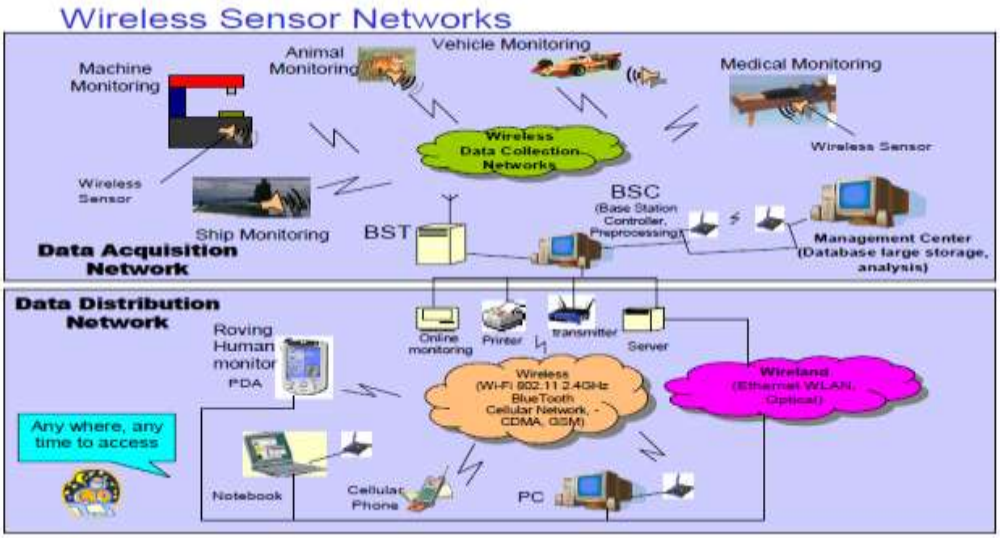
Wireless Sensor network consists of some tiny sensors with general computing elements to monitor the environmental, physical conditions such as pressure, temperature to give the great potential for applications and the ability to transform the human life. However, there have been resources constraints problems such as memory, power consumption of nodes in WSNs. Depending on the resources limitations and used applications of WSNs , security is very important and big challenge in WSNs. In this paper we were doing the survey for the issues comes on associated with the development of wireless sensor networks.

Keywords: Wireless, networks, Security, application.

I. INTRODUCTION

WSN consists of circulated self-governing sensors to monitor physical or environmental conditions. WSN consist of an array of sensors. Each sensor network node has typically several parts: a radio, transceiver, antenna and microcontroller A Base station links the sensor network to another network to advertise the data sensed for future processing. One of the biggest problems of sensor network is power consumption. To solve this issue two methods are defined. First method is to introduce aggregation points. This reduces total number of messages exchanged between nodes and saves some energy. Usually aggregation points are ordinary nodes that receive data from neighbouring nodes, execute processing and then forward the filtered data to next hop.

Smart environments represent the next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world. Sensory data comes from multiple sensors of different modalities in distributed locations. The smart environment needs information about its surroundings as well as about its internal workings; this is captured in biological systems by the distinction between exteroceptors and proprioceptors.



A. Characteristics of WSN [3]

1. Compact size
2. Physical security
3. Power
4. Memory space
5. Bandwidth
6. Unreliable communications

II. TYPES OF WIRELESS SENSORS

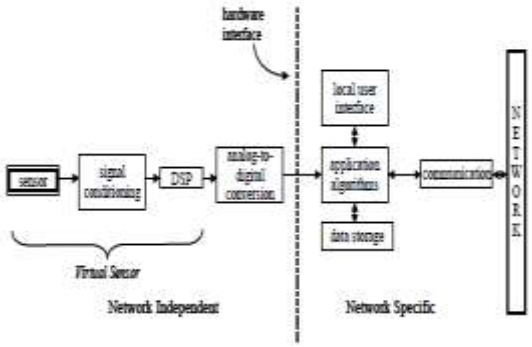
2.1 IEEE 1451 and Smart Sensors

Wireless sensor networks satisfy these requirements. Desirable functions for sensor nodes include: ease of installation, self-identification, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces [IEEE 1451 Expo].

There are many sensor manufacturers and many networks on the market today. It is too costly for manufacturers to make special transducers for every network on the market. Different components made by different manufacturers should be compatible. Therefore, in 1993 the IEEE and the National Institute of Standards and Technology (NIST) began work on a standard for Smart Sensor Networks. IEEE 1451, the Standard for Smart Sensor Networks was the result. The objective of this standard is to make it easier for different manufacturers to develop smart sensors and to interface those devices to networks.

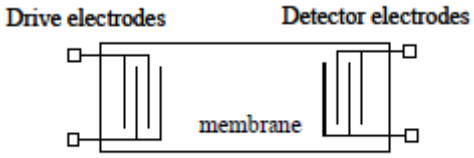
2.2 Smart Sensor, Virtual Sensor.

The figure shows the basic architecture of IEEE 1451. Major components include STIM, TEDS, TII, and NCAP as detailed in the figure. A major outcome of IEEE 1451 studies is the formalized concept of a Smart Sensor. A smart sensor is a sensor that provides extra functions beyond those necessary for generating a correct representation of the sensed quantity.



2.3 Acoustic Wave Sensors

are useful for a broad range of sensing devices [Kovacs 1998]. These transducers can be classified as surface acoustic wave (SAW), thickness-shear mode (TSM), flexural plate wave (FPW), or acoustic plate mode (APM). The SAW is shown in the figure and consists of two sets of interdigitated fingers at each end of a membrane, one set for generating the SAW and one for detecting it.



SAW Sensor

2.4 Some Smart Wsn Measurements

Sensor networks may consist of many different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of conditions. These sensor nodes can be put for continuous sensing, location sensing, motion sensing and event detection. The idea of micro-sensing and wireless connection of these sensor nodes promises many new application areas. A few examples of their applications are as follows:

Measurements for Wireless Sensor Networks		
	Measurand	**Transduction Principle**
Physical Properties	Pressure	Piezoresistive, capacitive
	Temperature	Thermistor, thermo-mechanical, thermocouple
	Humidity	Resistive, capacitive
	Flow	Pressure change, thermistor
Motion Properties	Position	E-mag, GPS, contact sensor
	Velocity	Doppler, Hall effect, optoelectronic
	Angular velocity	Optical encoder
	Acceleration	Piezoresistive, piezoelectric, optical fiber
Contact Properties	Strain	Piezoresistive
	Force	Piezoelectric, piezoresistive
	Torque	Piezoresistive, optoelectronic
	Slip	Dual torque
	Vibration	Piezoresistive, piezoelectric, optical fiber, Sound, ultrasound
Presence	Tactile/contact	Contact switch, capacitive
	Proximity	Hall effect, capacitive, magnetic, seismic, acoustic, RF
	Distance/range	E-mag (sonar, radar, lidar), magnetic, tunneling
	Motion	E-mag, IR, acoustic, seismic (vibration)
Biochemical	Biochemical agents	Biochemical transduction
Identification	Personal features	Vision
	Personal ID	Fingerprints, retinal scan, voice, heat plume, vision motion analysis

A. Area monitoring applications

Area monitoring is a very common application of WSNs. In area monitoring, the WSN is deployed over a region where some physical activity or phenomenon is to be monitored.

B. Environmental applications

A few environmental applications of sensor networks include forest fire detection, green house monitoring, landslide detection, air pollution detection and flood detection.

C. Health applications

Some of the health applications for sensor networks are providing interfaces for the disabled, integrated patient monitoring, diagnostics, drug administration in hospitals, monitoring the movements and internal processes of insects.

D. Industrial applications

WSNs are now widely used in industries, for example in machinery condition-based maintenance. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.

E. Other applications

Sensor networks now find huge application in our day-to-day appliances like vacuum cleaners, micro-wave ovens, VCRs and refrigerators. Other commercial applications includes constructing monitoring product quality, managing inventory, factory instrumentation and many more.

III. SECURITY ISSUES IN WSN

The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network .It is necessary to know and understand these security requirements first before implementing security scheme for WSN.

A. Data Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data . It ensures that data packets received by destination is exactly the same with transferred by the sender and any one in the middle cannot alter that packet[6]. The techniques like message digest and MAC are applied to maintain integrity of the data.

B. Data Confidentiality

Confidentiality is to protect data during communication in a network to be understood other then intended recipient. Cryptography techniques are used to provide confidentiality. Data confidentiality is the most important issue in all network security.

C. Data Availability

Availability ensures that the services are always available in the network even under the attack such as Denial of Service attack (Dos). The researchers proposed different mechanisms to achieve this goal. Availability is of primary importance for maintaining an operational network. Data Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate.

D. Data Authentication

Data Authentication of a sensor node ensures the receiver that the data has not been modified during the transmission[7]. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys.

E. Data Freshness

Data freshness is very important in wireless sensor networks. Because an attacker can send an expire packet to waste the network resources and decrease in network lifetime. Freshness ensures that the data received by the receiver is the recent and fresh data and no adversary can replay the old data.

IV. ATTACKS IN WSN

This paper focus on the security of WSNs, providing security services in these networks and preventing DOS attacks which is most challenges security issues for these networks. The most vulnerable attack in terms of exhaustion of resources in WSN is Denial of Service attacks (DOS). Denials of Service attacks are specific attacks that attempt to prevent legitimate users from accessing networks, servers, services or other resources by sending extra unnecessary packets and thus prevent legitimate network users from accessing services or resources.

A. Black hole attack

Also known as sink holes attack occurring at the network layer. It builds a covenant node that seems to be very attractive in the sense that it promotes zero-cost routes to neighbouring nodes with respect to the routing algorithm.

B. Wormhole attack

In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer. The whole traffic of the network is tunnelled in a particular direction at a distant place, which causes deprivation of data receiving in other parts of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location.

C. Selective forwarding attack

Selective forwarding is a network layer attack. In this, an adversary covenants a node, that it scrupulously forwards some messages and plunge the others. This hampers the quality of service in WSN. If the attacker will drop all the packets then the adjoining nodes will become conscious and may evaluate it to be a flaw.

D. Flooding

Flooding also occurs at the network layer. An adversary constantly sends requests for connection establishment to the selected node. To hit each request, some resources are allocated to the adversary by the targeted node. This may result into effusion of the memory and energy resources of the node being bombarded.

E. Sybil attack

This again is a network layer attack. In this, an awful node presents more than one character in a network. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. The Sybil attack is efficient enough to stroke other fault tolerant schemes such as dispersity, multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, and topology maintenance and misbehaviour detection.

F. Node replication attack

Every sensor node in a network has a unique ID. This ID can be duplicated by an attacker and is assigned to a new added malicious node in the network. This assures that the node is in the network and it can lead to various calamitous effects to the sensor network. By using the replicated node, packets passing through malicious node can be missed, misrouted or modified. This results in wrong information of packet, loss of connection, data loss and high end-to-end latency.

V. CONCLUSION

In this paper, we have discussed about most of the security issues and attacks on the wireless sensor network. This paper can be helpful for many research scholars who are working on the wireless sensor networks and also help to describe all the physical and climatic conditions for the wireless sensors. There is currently enormous research potential in the field of WSN.

REFRENCES

[1] Neha rang , Anuj gupta , " Wireless Sensor Networks : A Overview", *IJMCS*, Vol.1,iss.2, 2013.

[2] C. Karlof , D. Wagner , " Secure routing in wireless sensor networks : attacks And countermeasures", *In proc. Of the 1st IEEE Int. workshop on sensor network Protocols and applications (SNPA'03)* , pp. 113-127, May 2003.

[3] Aashima singla , Ritika sachdeva , " Review on security issues and attacks in Wireless sensor networks", *IJARCSSE*, vol. 3, iss. 4, 2013.

[4] Kriti Jain, Upasana Bahuguna, "Survey on Wireless Sensor Network", IJSTM, Vol. 3, Issue 2, pp. 83-90, Sept 2012.

[5] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", IJCIT, vol. 2, issue 1, pp. 62-67, 2011

[6] Tin win maw,Myo hein jaw, " A secure for mitigation of DoS attack in cluster Based wireless sensor networks", IJCCER , vol. 1,Issue 3,2013

[7] Prajeet Sharma, Niresh Sharma, Rajdeep Singh, "A Secure Intrusion detection System against DDOS attack in Wireless Mobile Ad-hoc Network",IJCA, Vol. 41– No.21, March 2012.

[8] Snehlata Yadav, Kamlesh Gupta, Sanjay Silakari, "Security issues in wireless Sensor network",Journal of information system and communications,vol.1,issue 2, 2010, pp01_06.