Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Some issues and challenges of Wireless Sensor Networks

**Himani Chawla**
CSE Dept.
Maharishi markandeshwar university
Ambala, Haryana, India

***Abstract-- Sensor network consists of tiny sensors with general purpose computing elements to cooperatively monitor physical or environmental conditions, such as temperature, pressure, etc. They have a great potential for long term applications and also have the ability to transform human lives in various aspects. 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 investigate issues and challenges associated with development of wireless sensor networks.***

***Keywords -- Wireless sensor networks, Security, applications, WSN.***

## 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.

### *A.* Characteristics of WSN[3]

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

## II. Applications of WSN

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:

### *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. When the sensors detect the event being monitored (sound, vibration), the event is reported to the base station, which then takes appropriate action (e.g., send a message on the internet or to a satellite). Similarly, wireless sensor networks can be deployed in security systems to detect motion of the unwanted, traffic control system to detect the presence of high-speed vehicles. Also WSNs finds huge application in military area for battleeld surveillance, monitoring friendly forces, equipment and ammunition, reconnaissance of opposing forces and terrain, targeting and battle damage assessment .

### *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. They can also be used for tracking the movement of insects,

 

birds and small animals, planetary exploration, monitoring conditions that affect crops and livestock and facilitating irrigation.

### *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 or other small animals, telemonitoring of human physiological data, and tracking and monitoring doctors and patients inside a hospital.

### *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. They can also be used to measure and monitor the water levels within all ground wells and monitor leachate accumulation and removal.

### *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 smart oce spaces, 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.WSN should take the following major security requirements which are basic requirements for any network into consideration of secure mechanism:

### *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. By providing data integrity we are able to solve the Data integrity attacks. Data integrity is achieved by means of authentication the data content .

### *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. Every network with any security focus will typically address this problem first Data confidentiality of the network means that data transfer between sender and receiver will be totally secure and no third person can access it(neither read nor write) .Confidentiality can be achieved by using cryptography: symmetric or asymmetric key can be used to protect the data.

### *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. Availability ensures that sensor nodes are active in the network to fulfill the functionality of the network.

### *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. In asymmetric cryptographic communication digital signatures are used to check the authentication of any message or user while in symmetric key, MAC (Message Authentication Code) are used for authentication purpose .

### *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. The freshness is achieved by using mechanisms like nonce or timestamp should add to each data packet.

## 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.This results maximum traffic to flow towards these fake nodes. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction.

### *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 tunneled 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. This may cause congestion and retransmission of packets squandering the energy of innocent nodes.

### *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. To avoid this, the attacker smartly forwards the selective data. To figure out this type of attack is a very tedious job.

### *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, topology maintenance and misbehavior detection. The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide the routing algorithms by constructing many routes from only one node.

### *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. Malicious node can get authority to the sensitive information and thus can harm the network .

## V. CONCLUSION

In this paper, various applications of WSN along with the knowledge of security issues & attacks of WSN are discussed. This paper can be helpful for research scholars who are working in this field. Security is an important requirement and complicates enough to set up in different domains of WSN.

Adding security in a resource constrained wireless sensor network with minimum overhead provides significant challenges, and is an ongoing area of research. 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, pp-01-06

 