IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary research**
**Website: www.ijdacr.com (Volume 2, Issue 3, October 2013)**

# Operational Parameters of Wireless Sensor Networks

Tomsy Varghese
tomsyvarghese@yahoo.co.in
M. Tech student

Ms. Kanwarpreet Kaur
kanwarpreet27@gmail.com
Assistant Professor

Gyan Ganga College of Technology, Jabalpur (India)

*Abstract:* **Wireless Sensor Networks are the type of ad-hoc networks that have found considerable interest among the researchers and actual users. They provide application in monitoring and control of physical phenomenon by enabling dense and un-tethered deployments at reasonable pricing. The WSN along with its applications have experienced a number of attacks in its timeline. In this paper we review some of the major advances in WSN technologies and the most vulnerable attacks it has faced in its time. We first focus on the algorithms deployed in this segment to make working of WSN better. Then we will discuss the attacks that were introduced to affect the working of network.**

## I. INTRODUCTION

A wireless sensor network is the accumulation of sensor nodes deployed over globe to investigate physical parameters like humidity, temperature, seismic events, vibrations etc. Since the scope of WSN is so broad, there is a considerable variation in hardware/software solution space of WSN technology. A simplified view of hardware/software helps develop a basic understanding of how these systems work. Most WSNs are multihop networks and rely on a communication stack that includes Media Access Control (MAC), routing and transport layers. There are many protocols for each of these layers, but they are not the same protocols found in wired networks or even Wi-Fi networks.

The WSN was initially coined for military and heavy industrial applications in around 1950s. A Sound Surveillance System (SOSUS) was the first network developed by US Military forces to track Russian submarines. This network used submerged acoustic sensors – hydrophones – distributed in the Atlantic and Pacific oceans. 1960s-70s was the period of internet exploration which we see today. The Distributed Sensor Network program (1980) was launched by US Defense Advanced Research Projects Agency (DARPA) to explore the challenges in the implementation of wireless sensor networks. DSN were assumed to have spatially distributed low-cost sensing nodes that collaborated with each other but operated autonomously, with information being routed to whichever node was best able to use the information.

Although the technology for large volume industrial and consumer applications did not exist in the 20th century, both academia and industry recognized the potential for such networks and formed joint efforts to solve the engineering challenges. Examples of these academic/industrial initiatives include:

- UCLA Wireless Integrated Network Sensors (1993)
- University of California at Berkeley Pico Radio program (1999)
- μ Adaptive Multi-domain Power Aware Sensors program at MIT (2000)
- NASA Sensor Webs (2001)
- ZigBee Alliance (2002)
- Center for Embedded Network Sensing (2002)

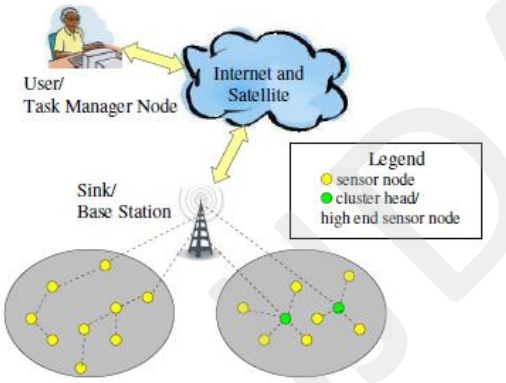
The new wave of research in WSNs started in around 1998 and has been attracting more and more attention

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary research**
**Website: www.ijdacr.com (Volume 2, Issue 3, October 2013)**

and international involvement. In the new wave of sensor network research, networking techniques and networked information processing suitable for highly dynamic ad hoc environments and resource constrained sensor nodes have been the focus.

WSN is a network consisting of numerous sensor nodes with sensing, wireless communications and computing capabilities. These sensor nodes are scattered in an unattended environment (i.e. sensing field) to sense the physical world. The sensed data can be collected by a few sink nodes which have accesses to infrastructure networks like the Internet. Finally, an end user can remotely fetch the sensed data by accessing those networks. Fig. 1 shows the operation sketch of WSNs.




(a) Flat sensor network (b) Clustered Sensor Network

Figure 1: Wireless Sensor Network Operation

In Fig. 1, two kinds of network topologies are shown. The sensor nodes either form a flat network topology where sensor nodes also act as routers and transfer data to a sink through multi-hop routing, or a hierarchical network topology where more powerful fixed or mobile relays are used to collect and route the sensor data to a sink. (Include cluster head definition)

## II. TECHNOLOGIES IN WSN

The WSN has experienced a dramatic growth in last few decades. After the SensIT (Kumar and Shepherd, 2001) program IEEE noticed the low expense and high capabilities that sensor networks offer. According to IEEE 802.15.4 for a device (sensor) there can be at most three operational modes:

- Personal Area Network (PAN) Coordinator: This is the principal controller of the entire network this device identifies its own network, to which other devices may be associated.
- Coordinator: The Coordinator has no capability of creating its own network; A Coordinator does the synchronization services through transmission of beacons. Such a coordinator must be associated to a PAN Coordinator.
- A simple Device: A device (sensor) which is neither a PAN nor Coordinator.

The IEEE 802.15.4 supports two different types of devices.

- *Full Functional Device (FFD)*: A FFD is a device which supports all the three operational modes
- *Reduced Function Device (RFD)*: The RFD is intended for the applications such as a passive infrared sensor, they do not need to synchronize services, they do not need to identify the network, and they are associated with single FFD at a time.

## III. APPLICATIONS OF WSN

The original motivation behind the research of WSN was military applications. For example large-scale acoustic ocean surveillance systems for detection of submarines, self-organized and randomly deployed WSNs for battlefield surveillance and attaching micro-sensors to weapons for stockpile surveillance (Pister, 2000). The applications of WSN in last two decades have also entered in civilian world. Today it is used in some of the following sectors:

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary research**
**Website: www.ijdacr.com (Volume 2, Issue 3, October 2013)**

*A. Environmental Monitoring*

Animal tracking, forest surveillance, weather and flood forecasting use WSN. They collect data like temperature variation, humidity from the distributed sensor nodes over a region without any costly physical setup for forecasting purpose by the concerned authorities.

*B. Health Monitoring*

Health monitoring has gone typically precise by the special kind of sensors used for heart rate monitoring, blood pressure measurement, body temperature, ECG etc. The sensors that are worn on body are a part of Body Sensor Networks (BSN). BSN has allowed inexpensive, remote and continuous health monitoring with real time updates of medical record via internet.

*C. Traffic Control*

The density of traffic can be measured by overhead or buried sensor networks. The traffic lights control has become efficient with the known value of traffic density. However, the traditional communication networks used to connect these sensors are costly, and thus traffic monitoring is usually only available at a few critical points in a city (Chong and Kumar, 2003).

*D. Industrial Sensing*

WSN can be used to sense equipment performance and their failure. In most of the industries the heavy industrial setup is installed and is not replaced over considerable amount of years. The machine performance degrades with span of time and is need to be monitored to prevent accidental incidents like unplanned downtime.

## IV. Future Work

In the future, the wireless sensor networks will have wide range of application areas to make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment and power consumption.