Excel Journal of Engineering Technology and Management Science
Vol. I No.1 December-January 2012 ISSN 2249-9032

Wireless Sensor Network:
A Promising Approach for Distributed Sensing Tasks

* ***Prof. Madhav Bokare***[1]
HOD, SSBES`s Institute Of Technology and Management ,Nanded.
* ***Mrs. Anagha Ralegaonkar***[2]
Lecturer,SSBES`s Institute Of Technology and Management ,Nanded.

1. INTRODUCTION

Sensor networks are a promising approach for a variety of applications, such as monitoring safety and security of buildings and spaces, measuring traffic flows, and tracking environmental pollutants. The continuous miniaturization process of computing devices featuring wireless technologies influences our everyday life. With the popularity of laptops, cell phones, PDAs, GPS devices, RFID, andintelligent electronics in the post-PC era, computing devices have becomecheaper, more mobile, more distributed, and more pervasive in daily life. The emergence of wireless sensor networks (WSNs) is essentially the latest trend of Moore's Law toward the miniaturization and ubiquity of computing devices. Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components.

2. WIRELESS NETWORK

Mobile computers, such as notebook computers and personal digital assistants (PDAs), are the fastest-growing segment of the computer industry. Many of the owners of these computers have desktop machines on LANs and WANs back at the office and want to be connected to their home base even when away from home or on route. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless networks.

Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using a transmission system called radio waves. AM radio, FM radio, satellite radio, satellite TV, satellite Internet access and broadcast TV is also, in fact, wireless networks. Wireless technology is very convenient. You do not have to worry about running wires in tight places, or obtaining low-voltage permits. The range of wireless technology can be impressive. While the equipment you use may break (just as wired equipment would) the signals themselves never break. In comparison to wireless eventually getting old or corroded, this is a great advantage. Wireless networks have many uses. A common is the portable office. People on the road want to use their portable electronic equipment to send and receive telephone calls, faxes, and electronic mail, read remote files, login on remote machines, and does this from anywhere on land, sea, or air. Another use is for rescue workers at disaster sites where the telephone system has been destroyed. Computers there can send messages, keep records, and so on.
There are four main types of wireless networks:

- Wireless Local Area Network (LAN): Links two or more devices using a wireless distribution method, providing a connection through access points to the wider Internet.

- Wireless Metropolitan Area Networks (MAN): Connects several wireless LANs.
- Wireless Wide Area Network (WAN): Covers large areas such as neighboring towns and cities.
- Wireless Personal Area Network (PAN): Interconnects devices in a short span, generally within a person’s reach.

3. A WIRELESS SENSOR NETWORK (WSN)

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Typically, a sensor node is a tiny device that includes three basic components: a sensing subsystem for data acquisition from the physical surrounding environment, a processing subsystem for local data processing and storage, and a wireless communication subsystem for data transmission. In addition, a power source supplies the energy needed by the device to perform the programmed task.This power source often consists of a battery with a limited energy budget. There are different Sensors such as pressure, accelerometer, camera, thermal, microphone, etc. They monitor conditions at different locations, such as temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, the current characteristics such as speed,

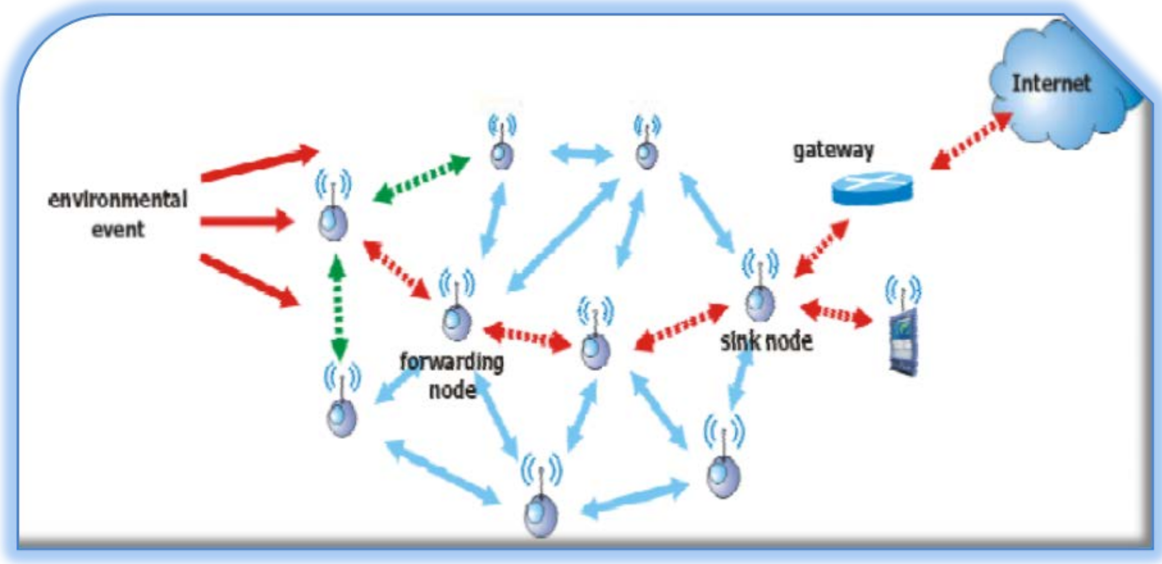

Fig.1 Wireless Sensor Network

direction and size of an object. Normally a sensor nodecombines the abilities to compute, communicate and sense.

3.1 Sensor node architecture:

A sensor node typically consists of five main parts: one or more sensors gather data from the environment. The central unit in the form of a microprocessor manages the tasks. A transceiver (included in the communication module in Figure 2) communicates with the environment and a memory is used to store temporary data or data generated during processing. The battery supplies all parts with energy (see Figure 2). To assure a sufficiently long network lifetime, energy efficiency in all parts of the network is crucial. Due to this need, data processing tasks are often spread over the network, *i.e.* nodes co-operate in transmitting data to the sinks. Although most sensors have a traditional battery there is some early stage research on the production of sensors without batteries, using similar technologies to passive RFID chips without batteries.

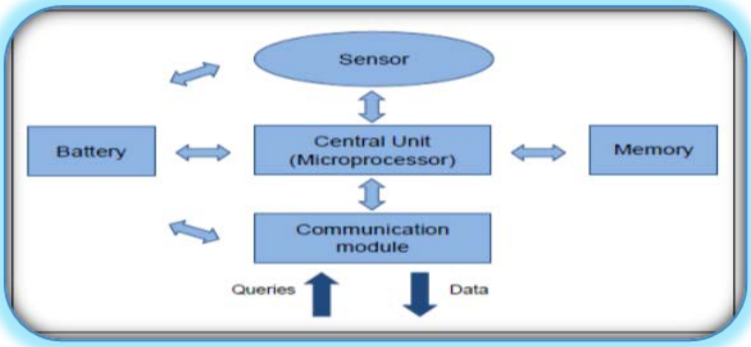

Fig.2 Sensor Node Architecture

The development of sensor nodes is influenced by

- increasing device complexity on microchips,
- high performance, wireless networking technologies,
- a combination of digital signal processing and sensor data acquisition,
- advances in the development of micro-electro mechanical systems (MEMS), and
- Availability of high performance development tools.

3.2 CHARACTERISTICS of WSN:

The main characteristics of a WSN include

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

- Unattended operation
- Power consumption

3.3 FIELDS OF APPLICATIONS OF WIRELESS SENSOR NETWORK:

1.Security and Surveillance:

Because most of the elemental knowledge of sensor networks is basic on the defense application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the Defense Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing. Now wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. In the battlefield context, rapid deployment, self-organization, fault tolerance security of the network should be required. The sensor devices or nodes should provide services like Battlefield surveillance, Reconnaissance of opposing forces, Targeting, Battle damage assessment, Nuclear, biological and chemical attack detection reconnaissance.

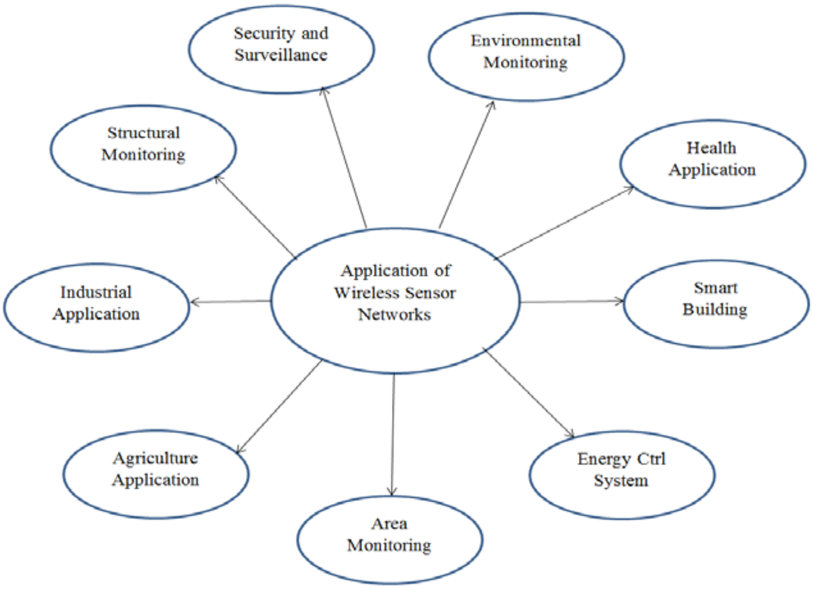

Fig. 3 Fields of applications of Wireless Sensor Network

2. Environmental Monitoring:

The term Environmental Sensor Networks has evolved to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests, etc. Some other major areas are listed below.

Air pollution monitoring

Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad-hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.

Forest fires detection

A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fires in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; due to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.

Landslide detection

A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. And through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.

3. Health Applications:

Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital. In some hospital even use RFID basic of above named applications to get the situation at first hand.Long-term nursing home: this application is focus on nursing of old people. In the town farm cameras, pressure sensors, orientation sensors and sensors for detection of muscle activity construct a complex network. They support fall detection, unconsciousness detection, vital sign monitoring and dietary/exercise monitoring. These applications reduce personnel cost and rapid the reaction of emergence situation. Applications in this category include tele-monitoring of human physiciological data, tracking and monitoring of doctors and patients inside a hospital, drug administrator in hospitals.In the Smart Sensors and Integrated Microsystems (SSIM) project, retina prosthesis chips that consisting of 100 micro sensors are built and implanted within human eye. This allows patients with no vision or limited vision to see at an acceptable level. The wireless communication is required to suit the need for feedback control, image identification and validation.

Some other similar applications include Glucose level monitors, Organ monitors, Cancer detectors and General health monitors. The idea of embedding wireless biomedical sensors inside human body is promising, although many additional challenges exist: the system must be ultra safe and reliable; require minimal maintenance; energy-harnessing from body heat. With more researches and progresses in this field, better quality of life can be achieved and medical cost can be reduced.

4. Smart buildings:

Along with developing commercial application of sensor network it is no so hard to image that Home application will step into our normal life in the future. After one day hard work one come back home. At the front door the sensor detects someone is opening the door, then it will tell the electric kettle to boil some water and the air condition to be turned on. He/she sits in the sofa lazily. The light on the table automatically turned on because the pressure sensor under the cushion has detected your weight. The TV is also on. One sensor has monitored that someone is sitting in front of it. When he turned down the temperature of the air condition. At the sometime five sensors in every corner in the room are measuring the temperature. Originally there is also sensor in the air condition. But it can only get the temperature at the edge of the machine not the real temperature in the room. So the sensors in the room will be detecting the environment. The air condition will turn to sleep mode until all the sensors get the right temperature. The light on the corridor, in the washing groom and balcony are all installed with sensor and they can be turned on or turn out automatically. Even the widows are also attached with vibratory sensors connected to police to against thief.

5. Energy Control System:

Societal-scale sensor network can greatly improve the efficiency of energy-provision chain, which consists of 3 components, the energy-generation, distribution, and consumption infrastructure.

6. Area monitoring:

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A civilian example is the geo-fencing of gas or oil pipelines.

7. Agriculture Applications:

- **Agriculture**

  Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing. Irrigation automation enables more efficient water use and reduces waste.

- **Greenhouse monitoring**

  Wireless sensor networks are also used to control the temperature and humidity levels inside commercial greenhouses. When the temperature and humidity drops below specific levels, the greenhouse manager must be notified via e-mail or cell phone text message, or host systems can trigger misting systems, open vents, turn on fans, or control a wide variety of system responses.

8. Industrial applications:

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors. There are many opportunities for using wireless sensor networks within the water/wastewater industries.

9. Structural monitoring:

Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc... enabling Engineering practices to monitor assets remotely without the need for costly site visits, as well as having the advantage of daily data, whereas traditionally this data was collected weekly or monthly, using physical site visits, involving either road or rail closure in some cases. It is also far more accurate than any visual inspection that would be carried out.

3.4 ENABLING TECHNOLOGIES:

Operating systems

Operating systems such as eCos or uC/OS used for sensor networks. TinyOS is perhaps the first operating system specifically designed for wireless sensor networks. LiteOS and Contiki are the other new operating systems used for sensor networks.

Hardware standards

A WSN measurement node contains several components including the radio, battery, microcontroller, analog circuit, and sensor interface. In battery-powered systems, one must make important trade-offs because higher data rates and more frequent radio use consume more power. Today, battery and power management technologies are constantly evolving due to extensive research.

Often in WSN applications, three years of battery life is a requirement, so many of the WSN systems today are based on ZigBee or IEEE 802.15.4 protocols due to their low-power consumption. The IEEE 802.15.4 protocol defines the Physical and Medium Access Control layers in the networking model, providing communication in the 868 to 915 MHz and 2.4 GHz ISM bands, and data rates up to 250 kb/s. ZigBee builds on the 802.15.4 layers to provide security, reliability through mesh networking topologies, and interoperability with other devices and standards. ZigBee also allows user-defined application objects, or profiles, which provide customization and flexibility within the protocol.The base stations are one or more components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, long-range Wi-Fi links etc. Many base stations are ARM-based running a form of Embedded Linux.

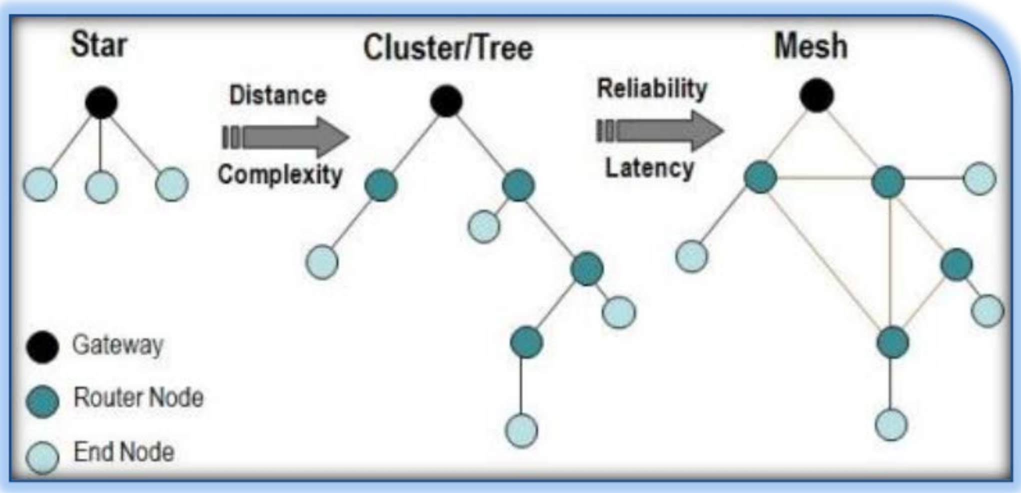

Fig.4 WSN Network Topologies

3.5 SECURITY REQUIREMENTS AND COUNTERMEASURES FOR WSN

Security requirements for WSN mainly include Authentication and Secrecy of the node.

- **Authentication:** Since sensor networks use a shared wireless communication medium, authentication is necessary to enable sensor nodes to detect maliciously injected or spoofed packets. Authentication enables a node to verify the origin of a packet (source authentication) and ensure data integrity, that is, ensure that data is unchanged (data authentication).

- **Secrecy:** Ensuring the secrecy of sensed data is important for protecting data from eavesdroppers. We can use standard encryption functions to achieve secrecy.

- **Countermeasures:** Standard cryptographic techniques can protect the secrecy and authenticity of communication links from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

- ***Key Establishment*** — for two sensor nodes to set up a secret and authenticated link, they need to establish a shared secret key.

- ***Broadcast Authentication*** — in broadcast source authentication possible approach is to use a digital signature, where the source signs each message with a private key and all the receivers verify the message using the public key.

3.6 CONCLUSION:

Sensor nodes are susceptible to physical capture, but because of their targeted low cost, tamper-resistant hardware are unlikely to prevail. Similarly, an attacker can easily inject malicious messages into the wireless network. Many sensor networks have mission-critical tasks, so it is clear that security needs to be taken into account at design time. Security will be important for most applications for the following reasons. Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored. Such unwanted information leakage often results in privacy breaches of the people in the environment.

REFERENCES:

1. A. Perrig *et al.*, “SPINS: Security Protocols for Sensor Networks,” *Wireless Networks J.*, vol. 8, no. 5, Sept. 2002, pp. 521–34.

2. L. Eschenauer and V. D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” *Proc. 9thACM Conf. Comp. and Commun. Security*, Nov. 2002, pp. 41–47.

3. E. Amir, S. McCanne, and R. Katz. An active service framework
and its application to real-time multimedia transcoding. In *SIGCOMM ’98: Proceedings of the ACM SIGCOMM ’98conference on Applications, technologies, architectures, andprotocols for computer communication*, pages 178–189. ACM Press, 1998.

4.Arch Rock Corporation. Sensor network architecture for the ip enterprise. In Proceedings of the 6th international conference on In-
formation processing in sensor networks, demo session, Cambridge.Massachusetts, USA, 2007.
5. K. K. Chang and D. Gay. Language support for interoperable messaging in sensor networks. In Proceedings of the 2005 workshop on Software and compilers for embedded systems, pages 1–9, Dallas, Texas, 2005. ISBN: 1-59593-207-0
6. J. I. Choi, J. W. Lee, M. Wachs, and P. Levis. Opening the sensornet black box. In Proceedings of the International Workshop on Wireless Sensornet Architecture (WWSNA), Massachusetts, USA, April 2007.