Chapter 2

An Overview of Wireless Sensor Networks

2.1 Introduction

The invention of ubiquitous computing and increase of portable devices have raised the importance of mobile and wireless networking. Wireless networking is an emerging technology that makes the users to access data and services electronically, irrespective of their geographic location. Wireless network is a data communication system, which uses electromagnetic waves to transmit and receive information via air as medium from one place to another place. Basically wireless networks are classified into two types: infrastructure-based networks and infrastructure-less (ad-hoc) networks.

Infrastructure-based networks have fixed BSs called access points which are connected by wires. The mobile nodes communicate with the BS via wireless link when it is inside the communication range of it. When the mobile node moves out of the communication range of a BS, it makes the connection with the other base station for communication. Cellular phone system, wireless local area networks (WLAN), paging systems are some of the example of

Infrastructure-based networks.

The MANET is a collection of autonomous, self-configurable, self-organizing nodes with communication capabilities connected by wireless links [7]. The MANETs do not have predefined infrastructure and the nodes can move freely from one place to another changing the topology constantly. The nodes in MANET communicate each other using multi-hop communication. A MANET is setup for a specific purpose to meet a quick communication need. For example networks utilized in disaster relief operations, networks in difficult locations like large construction sites, battle field, flood relief operations, military operations, where the deployment of wireless infrastructure (access points etc.) is not a feasible option [4]. In such applications, the individual nodes together form a network that relays packets between nodes to extend the reach of a single node, allowing the network to span larger geographical areas than would be possible with direct sender-receiver type of communication.

A WSN is a special type of Ad Hoc network, composed of a large number of sensor nodes spread over a wide geographical area. Each sensor node has wireless communication capability and sufficient intelligence for making signal processing and dissemination of data from the collecting center. The sensor nodes have many constrains such as, low computational power, limited energy and bandwidth [4]. Such constraints influence the deployment of a large number of sensor nodes that have posed many challenges to the design and management of sensor networks.

Some of the similarities between the WSNs and MANETs [7] are:

- Both are distributed wireless networks with no significant network infrastructure.
- Employ ad hoc method of wireless node deployment.
- In majority of application, the nodes communicate each other using multi-hop communication.

- Nodes are battery powered, resulting in concern over the minimization of energy consumption.
- Both uses wireless channel of unlicensed spectrum and hence prone to interference by other radio waves operating in the same frequency.
- Self-configuration is necessary because of the distributed nature of the networks

In spite of similarities among WSNs and MANETs, there are also some fundamental differences between these two networks. The differences listed here are:

- The number of sensor nodes in a WSNs is in the order of several hundreds to thousands compared to small number in MANETs.
- Nodes are densely deployed in WSNs.
- Nodes in WSNs are prone to failure due to physical and environmental conditions.
- The topology of a WSN changes very frequently due to nodes failure.
- In Most of the applications, sensor nodes use broadcast communication paradigms whereas MANETs are based on point-to-point communications.
- In WSNs, nodes are resource constrained i.e limited power, computational capabilities, and memory.
- Nodes in WSNs may not have global unique identification because of the large number of nodes.
- In most of the WSNs applications, mobility of sensor nodes are relatively low or nil as compared to MANETs.
- Data rate is very low in WSNs.

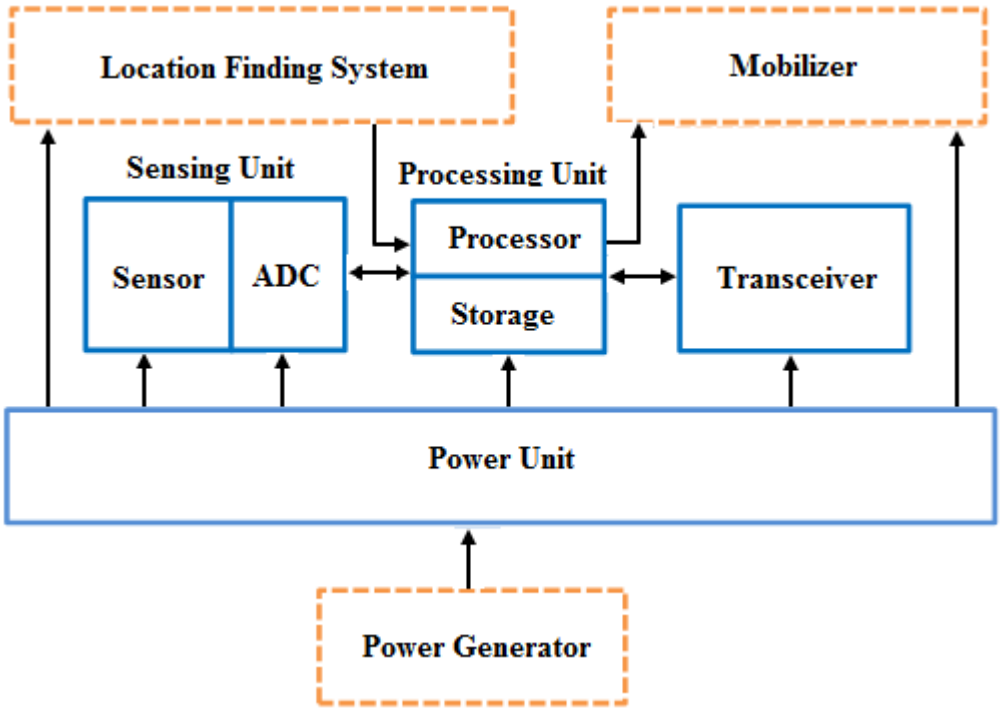

Figure 2.1: Components of a typical Sensor node

2.2 Sensor Node Architecture

A sensor is a transducer which measures a physical quantity such as light, temperature, pressure and humidity. Sensor converts physical quantities into a electrical signal which can be used by a human or by an instrument to take necessary decisions. They self-organize and collaboratively coordinate the sensing process depending on the phenomenon. Sensors are typically small, battery-powered, low cost devices with wireless communication capability. A sensor node in a sensor network capable of performing processing, gathering sensory information and communicating with other connected nodes in the network. A general hardware architecture of a sensor node platform is shown in Figure 2.1 [3]. Basically a typical sensor node made up of following four basic components: *processing unit*, *communication unit*, *sensing unit* and *power unit*. In addition to these, a sensor node may also contain some application specific components: *mobilizer*, *location finding system* and *power generator*.

2.2.1 Processing unit

In a sensor node, the functionality of processing unit is to convert the electrical signals received from the sensor into an intelligible message format, schedule tasks, process data received, execute the algorithms for data forwarding and control the functionality of other hardware components in the sensor node. The processing unit made up of embedded processor [8] which include Microcontroller, Digital Signal Processor (DSP), Field Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC).

2.2.2 Communication unit

The communication unit has both a transmitter and a receiver for establishing wireless communication between sensor nodes. The communication unit which combines both transmitting and receiving tasks are called transceiver. The most essential task of transceiver is to convert the digital bit stream coming from microcontroller into radio waves and vice versa. The Radio Frequency (RF) based wireless communication suits to most of WSN applications. Transmit, Receive, Idle and Sleep are the operational states of transceiver. The commercially available transceiver incorporates all the circuitry required for modulation, demodulation, amplification, filtering, mixing and so on.

Some of the standard radio transceivers [4] used in various sensor nodes include RFM TR1000 family from RF Monolithics, CC1000 and CC2420 family from Chipcon, TDA 525x family from Infineon, IEEE 802.15.4, LMX3162 from National Semiconductor, RDSSS9M from Conexant systems.

2.2.3 Sensing unit

Sensing unit [9] consist of two subunits: sensors and analog to digital converters (ADCs). Sensor is a transducer which produces a measurable electrical signal

to a change in a physical phenomena such as temperature, chemical level, light intensity, sound, magnetic fields, image, etc. Sensors can be classified as either analog or digital devices. The sensor produces continuous analog signals, converted into digital signals by ADCs and then fed to the processor for further processing.

2.2.4 Power unit

The electronics of the sensor node is powered [5] by using either stored energy or harvesting energy from other potential sources such as light, vibration, heat and radio frequency signal. Energy supply is necessary to support network operation from a few hours to months or even years. Most of the existing commercial and research platforms rely on batteries, which dominate the node size. Batteries are the obvious energy storage medium, ranging from the small coin cell to large sealed lead acid batteries (AA, AAA types) which include lead acid, lithium, NiCad, NiMH, and thin-film. Rechargeable batteries are typically not desirable due to lower energy density, higher cost and in most of the applications recharging is simply impractical.

2.2.5 Application specific units

In addition to the basic units, sensor nodes might have some additional application specific units such as location finding systems, mobilizer and power generator. In most of the application, WSN routing techniques and sensing tasks require the information of location. So location finding systems or Global Positioning System (GPS) are used to estimate the geographical position with certain level of accuracy. Some applications require the sensor node to move to carry out the assigned task. In such cases the sensor nodes equipped with mobility unit called mobilizer. The power generator which supplies continuous power to a node have some additional functionality.

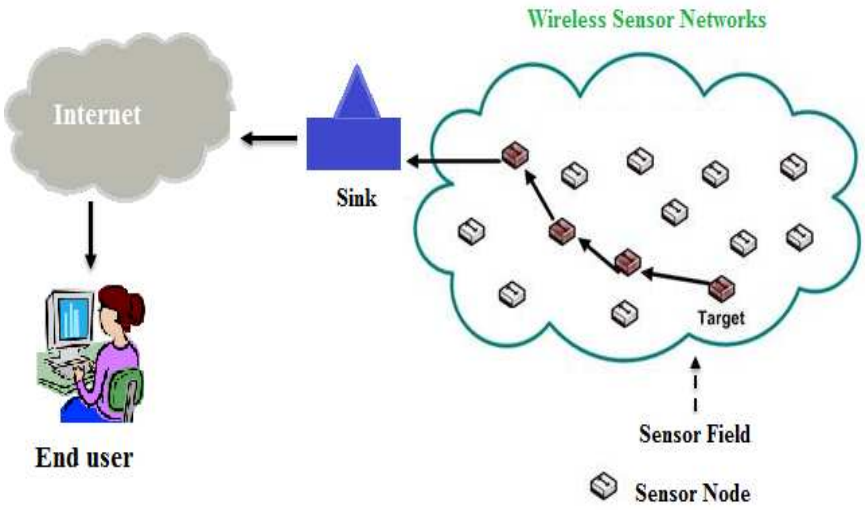

Figure 2.2: Typical Wireless Sensor Network Architecture

2.3 Wireless Sensor Network Model

A WSN [3] is a group of hundreds to thousands of low cost, autonomous devices with inbuilt sensors, which could either have a predefined location or randomly deployed for monitoring various environmental and physical conditions at various places and times. Sensor nodes usually collect the information from their surrounding environment and send their data using multi-hop communication approach to the main collecting center called BS (sometimes they are also referred to as sinks).

A typical WSN model is as shown in Figure 2.2 [3]. Sensor field is an area where the nodes are deployed to collect the information about the surrounding environment. Each of the sensor node is capable of sensing and sending data to the requested nodes or to the external BS. A BS may be static or mobile and can collect the information from the sensor nodes and perform complex data processing. Usually, BSs are rich in computational power, memory and energy when compared to sensor nodes. The BSs are able to connect the sensor network to an existing communication infrastructure (for example internet) where the remote user can access the data reported by the sensor nodes.

2.4 Constraints in Wireless Sensor Networks

A WSN consists of a large number of spatially distributed sensor nodes which are inherently resource constrained. These nodes have limited computational capability, very low data storage capacity, and low communication bandwidth. These limitations are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is difficult to directly employ the conventional routing protocols in WSNs. The major constraints of a WSN are explained in the following sections.

2.4.1 Energy

Sensor nodes are generally battery-powered devices. The WSN is deployed to operate in remote or hostile environments. It is difficult to replace or recharge batteries in such environment. Energy is one of the biggest constraints for a WSN. In general, energy consumption in sensor nodes can be divided into three parts: (i) energy consumption by sensing unit, (ii) energy consumption for communication among sensor nodes, and (iii) energy consumption due to computation. It is found that each bit transmitted in WSNs consumes about as much power as executing 800 to 1000 instructions [10]. Thus, communication between sensor nodes consumes most of the available power, much more than that of the sensing and computation. Current small batteries provide about 100mAh of capacity, powering a small Amtel processor for 3.5 hours (if no power management techniques are be applied). The new generation of sensor platforms use about 2 microJ per bit of data transmitted.

2.4.2 Computation

The processing unit in a sensor node performs computational tasks related to both locally sensed information as well as information communicated by other

sensors. In order to meet large scale deployment of sensor nodes and also due to economic constraints, low cost embedded processors such as microcontrollers are often selected when designing sensor nodes. These embedded processors significantly constrained in terms of computational power. Due to the constraints of such processors, devices typically run specialized component-based embedded operating systems, such as TinyOS. In sensor node, more power is consumed for communication than computations. Since the power for computations is even more constrained than the total quantity of power, this limits the adoption of complex algorithms, which is computationally expensive.

2.4.3 Memory

Majority of the sensor nodes are made up of microcontroller as a processing unit. These have small amount of storage in the form of random access and read-only memory include both program memory and data memory. There is usually not enough space to run complex algorithms after loading the operating system and application code. In the Smart Dust project, for example, TinyOS consumes about 4K bytes of instructions, leaving only 4500 bytes for applications [10].

2.4.4 Communication

Wireless sensor node includes a low data rate, short-range wireless radio transceivers (10 to 100kbps, less than 100 m) [11]. In spite of limited capability, these radios are likely to improve in sophistication over time including improvements in cost, spectral efficiency, tunability, immunity to noise, fading, and interference. Radio communication is often the most power intensive operation in a WSN device, and hence the radio must incorporate energy-efficient sleep and wake-up modes to extend the node lifetime.

2.5 Unique Characteristics of WSNs

Even though the WSNs exhibit some similarities with the other wireless networks like cellular networks and mobile ad hoc networks, there are several characteristics that distinguish WSNs from other communication networks [3]. Some of these characteristics are given in the following section.

2.5.1 Communication paradigm

The WSNs differ from the traditional wired and wireless networks in terms of service provided by them. It is not possible to have global addressing as like in wired networks. Since the WSNs have relatively large number of nodes, this increases the overhead of ID maintenance. The WSNs are data-centric, which means that messages are not sent to individual nodes but to geographical locations or regions based on the data content.

2.5.2 Application specific

In traditional wired and wireless networks, a node may have multiple applications and the network should be able to serve each application according to Quality of Service (QoS) in terms of throughput, latency, and reliability as required. Conversely, a WSN is deployed to perform a specific task, e.g. environmental monitoring, target tracking, or intruder alerting. This makes it possible to use application-dependent node platforms, communication protocols, data aggregations and in-network processing and decision making [12].

2.5.3 Resource constraints

A typical WSN node combines low cost with small physical size and is battery powered. Thus, the sensor nodes are tightly constrained in computation, communication, storage capacity, and energy resources. Therefore, they require

efficient energy management techniques to prolong the network lifetime [3,12].

2.5.4 Dynamic topology

The WSNs are subject to a large number of uncertainty factors [3]. The wireless communications are inherently unreliable due to frequent node failure, simple modulation techniques and environmental interferences. The unreliability is especially evident in WSNs because of harsh operating conditions e.g. due to environmental changes in outdoors, node mobility, and nodes dying take place due to depleted energy sources. As a result, the unreliability causes network dynamics due to link breaks even when nodes are stationary.

2.5.5 Network size and density

In some of the WSNs application, the number of nodes is in the order of thousand to more than ten thousands as compared to other wireless networks. The density of nodes can be high, depending on the application requirements for sensing coverage and robustness via redundancy [13].

2.5.6 Deployment

In some of the applications, sensor nodes are used to operate in the harsh or hostile environments. In such applications, to avoid tedious network planning of a large number of nodes, WSNs are often randomly deployed. This hinders the maintenance, and makes the node replacement impracticable [14]. This necessitates network self-configuration and autonomous operation.

2.6 Key Design Challenges

Sensor networks are characterized by a powerful combination of distributed sensing, computing and communication. Despite the innumerable applications

of WSNs, these networks offer numerous challenges mainly the stringent energy constraints, limited computing power, communication range, and storage space of sensor nodes. The primary design goals of WSNs is to carry out data communication while trying to extend the lifetime of the network and prevent connectivity degradation by employing aggressive energy efficient techniques. The design of routing protocols in WSNs is influenced by several challenging factors. These factors must be properly dealt before efficient communication can be achieved in WSNs. In the following sections, we describe some of the challenges and design issues that affect data routing process in WSNs.

2.6.1 Network longevity

The WSNs are typically deployed to measure certain physical phenomenon that range from fractions of a second to a few months or even year. A typical alkaline battery, for example, provides about 50 watt-hours of energy can last less than a month of continuous monitoring the environment. In a large network and deployment in possibly hazardous environment, replacing batteries is not feasible. Improvements in battery design and energy harvesting techniques will offer only partial solutions. This is the reason that most protocol are designed explicitly with energy efficiency as the primary goal.

2.6.2 Responsiveness

Extending network lifetime can be achieved by forcing the nodes to operate in a duty-cycled manner with periodic switching between sleep and wake-up modes. The synchronization of sleep and wake-up schedules is challenging itself, since long sleep periods can reduce the responsiveness and effectiveness of the sensors. In event driven applications, certain events in the environment must be detected and reported rapidly, the latency introduced by sleep schedules must be kept within strict bounds.

2.6.3 Fault tolerance

Fault tolerance is the ability to maintain the sensor network functionalities without any interruption due to node failures. Sensor node may fail due to lack of energy, physical damage, or environmental interference. The failure of sensor node should affect the overall performance of network. If many nodes fail, the routing protocols must establish new links and routes the data to the destination node or sink.

2.6.4 Scalability

For many envisioned applications, the combination of fine granularity sensing and large coverage area implies that WSNs networks have the potential to be extremely large scale (hundreds or thousands or even millions of nodes). Any routing protocols must be scalable to work with large number of nodes.

2.6.5 Heterogeneity

The sensor nodes in the WSNs may have heterogeneous device capabilities (with respect to computation, communication, and sensing). This heterogeneity can lead to a number of important design consequences. For example, the presence of a small number of devices of higher computational capability along with a large number of low-capability devices can dictate a two-tier, cluster-based network architecture, and the presence of multiple sensing (i.e. temperature, humidity, pressure, etc.) modalities require pertinent sensor fusion techniques.

2.6.6 Self-configuration

Because of large number of sensor nodes deployed in remote environments, WSNs are inherently unattended distributed systems, the ability of individual

sensor nodes to self-organize is vital. The nodes in a WSN expected to configure their own network topology, localize, synchronize, calibrate themselves and coordinate inter-node communication. Self-organization should be done in a way to improve the performance while reducing the power consumption of the entire sensor network.

2.6.7 Privacy and security

The large scale, prevalence, and sensitivity of the information collected by WSNs give rise to the final key challenge of ensuring both privacy and security. The need for security and privacy is evident in certain applications e.g. health care and military applications [15].

2.6.8 Data reporting

Data reporting in WSNs is dependent on application and time criticality of the data. Data reporting can be either event-driven (i.e. react immediately to sudden and drastic changes in the sensed attribute), time-driven (i.e sending data periodically), query-driven(i.e. react when the query is made available), and may also be hybrid-driven(i.e combination of more than on type). The data reporting greatly influences the network lifetime in terms of energy consumption and route calculations.

2.6.9 Connectivity and coverage

The two fundamental issues, which have a great impact on QoS in WSNs are coverage and connectivity [16], these define how well each point in the sensing field is covered while at the same time satisfying the criterion that each node is within the communication range of at least one other node. In most of the practical applications, sensor nodes are randomly distributed to operate in hostile environment, finding an optimal deployment strategy that would minimize

cost, reduce computation and communication, be resilient to node failures and provide a high degree of area coverage, is extremely challenging. Therefore, maximizing coverage as well as maintaining node connectivity in a severely resource constrained environment is a non-trivial optimization problem.

2.6.10 Delay

The information from sensor node must reach the sink within some stipulated time. Time delay is considered as a very important parameter for the measurement QoS, since it influences performance and stability of control systems [17]. The delay jitter can be difficult to compensate for, especially if the delay variability is large. Hence, a probabilistic delay requirement must be considered instead of using average packet delay. Furthermore, the packet delay requirement is important since the retransmission of data packet to maximize the reliability may increase the delay. Outdated packets are generally not useful for control applications [18].

2.7 Some existing WSNs

Currently there is no common WSN platform [19]. Some designs such as Berkeley Motes and their clones have broader user and developer communities. However, many research labs and commercial companies prefer to develop and produce their own devices. Since there is no true killer application for WSNs that would drive the costs down, it is often more convenient and even less expensive to build your own WSN devices than to buy commercially available ones.

History of development of sensor nodes dates back to the Cold War [20]. A system of acoustic sensors were developed by United States of America(the USA) for sound surveillance to detect and track Soviet submarines which is now used by the National Oceanographic and Atmospheric Administration

(NOAA) for monitoring events in the ocean, e.g., seismic and animal activity.

In 1980, the research on sensor networks started with the Distributed Sensor Networks (DSN) program at DARPA (Defense Advanced Research Projects Agency) where Arpanet (predecessor of the Internet) approach for communication was extended to sensor networks. The network was assumed to have many spatially distributed autonomous, low cost sensing nodes that collaborate with each other for information routing to a node, which can make use of the information.

Further, in 1980s, a multiple-hypothesis tracking algorithm based on DSN was developed by Advanced Decision Systems (ADS), Mountain View, CA, which dealt with difficult situations involving high target density, missing detections, and false alarms. MIT Lincoln Laboratory developed the real-time test bed for acoustic tracking of low-flying aircraft for demonstrations.

This interest increases with the DARPA low-power wireless integrated micro-sensors(LWIM) project of the mid-1990s and continued with the launch of the SensIT project in 1998, which focuses on wireless, ad hoc networks for large distributed military sensor systems. Few of them are explained in the following sections.

2.7.1 WINS

The Wireless Integrated Network Sensors (WINS) project was developed by the University of California at Los Angeles in collaboration with the Rockwell Science Center [20]. In 1998, it has been commercialized with the founding of the Sensoria Corporation (San Diego, California). This program covers almost every aspect of WSN design, from MEMS sensor and transceiver integration at the circuit level, signal processing architectures, and network protocol design, to the study of fundamental principles of sensing and detection theory. The group envisions that WINS will provide distributed network and Inter-

net access to sensors, controls, and processors deeply embedded in equipment, facilities, and the environment.

2.7.2 EYES

The Energy efficient Sensor Networks (EYES) was developed by Infineon [4]. This was funded by European Union to develop the architecture and technology to enable the creation of sensors that can be networked to support large number of mobile nodes. The project aimed at supporting various devices such as laptops, PDAs, mobile phones etc. As a result, the EYES network overlaps with both the fields of WSNs and MANETs.

It is equipped with a Texas Instrument MSP 430 microcontroller, an Infineon radio modem TDA 5250, along with a SAW filter and transmission power control; the radio modem also reports the measured signal strength to the controller. The node has a USB interface to a PC and the possibility to add additional sensors/actuators.

2.7.3 PicoRadio

In 1999, the PicoRadio program started at the University of California to support the assembly of an ad-hoc wireless network of self-contained mesoscale, low-cost, low-energy sensor and monitor nodes [21]. The physical layer proposed for the PicoRadio network is also direct sequence spread spectrum; the MAC protocol proposed combines the best of spread spectrum techniques and Carrier Sense Multiple Access (CSMA).

A node would randomly select a channel (e.g., a code or time slot) and check for activity. If the channel were active, the node would select another channel from the remaining available channels, until an idle channel was found and the message sent. If an idle channel was not found, the node would back off, setting a random timeout timer for each channel. It would then use the

channel with the first expired timer and clear the timers of the other channels.

2.7.4 ScatterWeb

The ScatterWeb platform [22] was developed at the Computer Systems and Telematics group at the Freie University at Berlin. This consist of several family of nodes, starting from a relatively standard sensor node (based on MSP 430 microcontroller) and ranges up to embedded web servers. These nodes equipped with a wide range of interconnection possibilities such as Bluetooth and a low-power radio mode, also connections for I2C or CAN are available.

2.7.5 Mica Mote family

The Mica Mote family of nodes developed at the University of California at Berkeley [4], starting in the late 1990s, in partial collaboration with Intel, over the years. They are commonly referred as the Mica motes, with different versions such as Mica, Mica2, Mica2Dot. They are commercially available via the company Crossbow in different versions and different kits. TinyOS is the usually used operating system for these nodes. All these nodes feature a micro controller belonging to the Atmel family, a simple radio modem (usually a TR 1000 from RFM), and various connections to the outside. In addition, it is possible to connect additional boards to the node to enable a wider range of applications and experiments. Sensors are connected to the controller via a I2C bus or via SPI, depending on the version.

2.8 Applications of WSNs

Advances in the field of MEMS and communication technology have enabled the development of a new and modern technology that has already been implemented in a wide variety of scenarios, and its applications are growing every day [23]. Although most of today's sensors networks are still wired, wireless

sensors offer significant advantages over wired sensors. The main disadvantages with wired sensor networks is cost and delays in deployment. WSNs become more popular, since they can operate autonomously without the need for an existing infrastructure. This great benefit can be seen even more clearly when looking at the many problems that the use of WSN technology solves. The applications of WSN technology have been categorized into four main groups are: environmental, health care, military, and additional applications. Each of these groups is explained in the following sections.

2.8.1 Environmental Applications

Today, the world is more concerned about climate change, global warming, and diminishing natural resources. The use of autonomous WSNs in environmental applications is becoming more and more important. The WSNs can greatly contribute to the development of hazard response systems, natural disaster detection systems, energy-monitoring systems and many more.

Meteorological Monitoring: The WSNs can be used to collect large amount of information about rainfall, wind speed and direction, air temperature, barometric pressure, relative humidity and solar radiation. These data can be stored in data bases and it becomes useful to forecast the weather and also to predict more accurately or detect harsh natural phenomena [24].

Geological Monitoring: Geological monitoring refers to the control, supervision and study of several geological magnitudes. The changes in these magnitudes help in understanding the earth's state. The geological disasters such as earthquakes, tsunamis, volcanic eruptions and landslides, which are related to an underground event [25] can be more accurately predicted by using these features.

Habitat Monitoring: Sensor network solutions for habitat monitoring show enormous potential benefits for the industrial and scientific communities, and

society as a whole, because of their long-term data collection ability at scales and resolutions that are difficult to obtain and their easy interaction with other external networks [26].

Pollution Monitoring: Increase in air, water, noise and radioactive pollution and their devastating effects are the huge concerns of the 21st century. With the fast growing industrial activities, the problem of air pollution is becoming a major concern for the health of the population, the WSN is used to monitor air pollution [27].

Energy Monitoring: The production and consumption of energy resources is very important to the global economy. The advantage of using wireless technology is that the energy waste can often be reduced by something as easy as measuring the temperature or human presence in a room and taking the necessary steps such as switching off a light or turning down the heat [28].

2.8.2 Health Care Applications

WSN technology could potentially impact a number of health-care applications, such as medical treatment, pre- and post-hospital patient monitoring, rescuing people in disasters, and early disease warning systems. Since the health-care domain is a very broad grouping, it has been divided into several categories, few of them are: patient monitoring, disability assistance, drug administration, etc.

Patient Monitoring: The WSNs are mainly used to monitor and track patients in hospitals to avoid the spread of some infectious diseases. The remote patient's blood pressure, body temperature and electrocardiograph (ECG) can be measured by special kinds of sensors which can be knitted into clothes to provide remote nursing, especially for the elderly people [29].

Disability Assistance: In disability assistance applications, smart sensors are implanted to operate within the human body to counteract organ weaknesses

or to monitor important physiological parameters or particular organ viability. The blood glucose level in the diabetic patients can be monitored continuously, controlling the insulin delivery from an implanted reservoir [30]. In cardiology, the value of the implantable cardioverter-defibrillator has increasingly been recognized for the effective prevention of sudden cardiac death [31].

Drug Administration: Sensors are very much useful in drug administration in hospitals. If sensor nodes are attached to medications, the chance of getting and prescribing the wrong medication to patients can be minimized. Computerized systems as described in [32] have shown that they can help to minimize adverse drug events.

2.8.3 Military applications

The unique characteristics of WSNs such as, rapid deployment, self-organization and fault tolerance make them a very promising sensing technique for military applications. The WSNs concept is a better approach for battlefields, because nodes can be used to operate in hostile environment. Some of the military applications of sensor networks are monitoring friendly forces, equipment and ammunition; battlefield surveillance; reconnaissance of opposing forces and terrain; targeting; battle damage assessment; and nuclear, biological and chemical (NBC) attack detection and reconnaissance [3], few of them are summarized below:

Monitoring Friendly forces, Equipment and Ammunition: Head Quarter can constantly monitor the status of friendly troops and their locations by installing small sensors in troops, vehicles, critical equipments and ammunitions. These sensors gather informations about their functioning and send to the sink node which stores, elaborates, and organizes them.

Target Tracking: The WSNs are employed to detect target's positions. They have the ability to adjust the parameters (for example focus, range, and angle)

according to the target motion.

Battlefield Surveillance: The activities of the opposing forces in the inaccessible and critical areas can be rapidly covered with sensor networks. As the operations evolve and new operational plans are prepared, new sensor networks can be rapidly deployed at anytime.

Battle Damage Assessment: The WSNs can be used to assess the battle damage. The battle damage assessment is directly proportional to the number of sensor nodes damaged in the target area. The remaining sensor's functioning can provide information with a precision proportional to the number of alive nodes. This precision can itself be used as a measure of the damages.

Nuclear, Biological and Chemical attack Detection and Reconnaissance: In chemical and biological warfare, it is required to carryout reconnaissance without exposing anyone to nuclear radiation. These sensors act as a biological or chemical warning systems, which provides the forces with critical reaction time, which drops casualties drastically.

2.8.4 Some additional applications

Besides military, environmental, and health applications, sensor networks are employed in variety of applications, few of them are explained below:

Structural Health Monitoring: Life-cycle monitoring of civil infrastructures are critical to the long-term operational cost and safety of aging structures. In this context, WSNs are gaining special attention and attempts are made in this direction to minimize cost and maximize the utility of the system by performing the real time monitoring [33]. The real-time structural monitoring of civil infrastructure with WSNs issues early warning about hazardous structures and impending collapses.

Environmental Control in Buildings/Offices: The temperature and lighting conditions inside building or office can be monitored by embedded sensors,

which drastically decreases energy costs. The information gathered is then used to regulate heating systems, cooling systems, ventilators, lights, and computer servers [34].

Automotive Monitoring: Traffic and transport monitoring are two very important applications of WSN technology. The sensor module detects passing vehicles by measuring disturbances in the earths magnetic field caused by passing vehicles. This disturbance is detectable as far away as 15 meters from the vehicle.

Managing Inventory Control: The sensors can be attached to each item of inventory in a factory warehouse. The exact location of the item can be determined by discreetly attaching sensors to walls or embedded in doors and ceilings. The sensor network locates items, tracks their movements, analyze the correlation between item movements and inventory levels. The end user can tally the number of items in the same category and also can add new inventories simply by attaching sensor to the inventories.