CHAPTER 1

INTRODUCTION

1.1 WIRELESS SENSOR NETWORK

Wireless Sensor Network (WSN) is an emerging network model that influences the sensor nodes to sense, monitor and control and communicate in the physical environment. WSN is the most reliable communication platform where remote monitoring is the major objective. In such organizations, energy autonomy will be one of the key challenges which in turn control the network lifetime. Sensors are generally equipped with data processing and communication capabilities. The sensing circuitry measures ambient conditions of the environment surrounding the sensor and transforms them into a stimulating signal. The sensor nodes send such collected data to a command centre (sink) through radio transmitter, either directly or through a relay node. The decrease in the size and cost of sensors are main advantages of sensors. Such interest has motivated intensive research in the past few years addressing the potential of association among sensors in data gathering and processing and the synchronization and management of the sensing action and data movement to the sink. Sensor nodes are constrained in energy supply and bandwidth. Such imperatives consolidated with a typical exploitation of substantial number of sensor nodes have postured many difficulties to the outline and administration of sensor systems.
1.1.1 Evolution of Sensor Networks

Sensor networks are first used during the cold war which took place in the US being operated mainly by humans and the communication path between nodes were done with the help of wires where a numerous acoustic sensors were kept in different locations in the water bed to watch every small and minute movements of the Soviet submarines, They called it the SOund SUrveillance System (SOSUS).

After a few years with more research on these networks held at DARPA (Defense Advanced Research Projects Agency) during a program called Distributed Sensor Network. Their research concentrated mainly on acoustic sensors and their processing methodologies etc.

Later due to large number of extensive research works done in this field, it gave rise to the MEMS (Micro Electro Mechanical System) which has only small and cheaper sensors when compared to its predecessors. Finally as advancements keep pouring in this field more features like power-efficient processors, wireless networking which lead to their usage in dynamic ad-hoc applications.

Nowadays wireless networks provide more bandwidth efficiency, lower cost expense and higher work capabilities when compared with those of wired networks due to standards of IEEE 802.11. In PAN (Personal Area Network), short range sensors within the range of 5-10 m radius are deployed. Furthermore advancements were made in the processors to be capable of processing multiple operations parallel.
1.1.2 Architecture of Wireless Sensor Network

Wireless technologies are used widely in our everyday life since it is spread worldwide. This is because of some features like economical cost, distributed sensing, simple installation and maintenance in industrial applications.

In general, WSN uses sensors to gather the information and process them to publish data in environment. Sensor nodes are designed as small devices with less power consumption sensing, lesser memory to calculate and communicate for easier installation in remote areas. They have capabilities in dynamic sensing, routing, searching, locating and robust to enable flexible topology of the network.

![Figure 1.1 Architecture of WSN](image)

As depicted in Figure 1.1, WSN consists of collection of nodes used to communicate measurements collected in their range. Multiple communication paths between intermediate nodes can be adopted flexibly as the network is implemented in ad-hoc manner that every node can route
independently to its sink. When data is forwarded to the final sink between intermediary nodes, extracting of useful data out of redundant data must be performed.

The sensor network generally consists of huge number of nodes interacting with each other to perform operations like sensing and monitoring things based on the environmental requirements and criteria.

1.1.3 Functional Components

Sensor nodes are composed of four major components: power Supply unit, processor, communication unit and sensor unit. The power supply component consists of a dc-dc converter and a battery has the purpose to power the node. The Communication unit consists of a wireless communication path. Most of the platforms use short-range radio signals, others use laser or infrared. The processing unit has a memory to store data and programs, a microcontroller with ADC (Analog to Digital Converter) to receive signals. In the sensor unit links between the sensor nodes to the environment is present.

A power layer is necessary to maintain resources of a sensor node and also its energy levels. The sensing unit contains a group of sensors, which produces electrical responses to a change in any physical condition. The processing unit helps in determining the computational capability and energy consumption of a sensor node. The different types of processing units are FPGA’s (Field Programmable Gate Arrays), Microcontrollers, etc. The communication unit enables sensors to communicate between the nodes through a path. They can be radio signals, infrared or optical.
1.1.4 Network Model

WSNs are resource limited and they are being deployed densely and are prone to failures. The major components of a WSN are:

- **Sensor Field**: It is the area in which the nodes are placed.
- **Sensor Nodes**: They are in charge of collecting data and transferring information.
- **Sink**: A destination sensor node whose job is to receive process and store the data from other neighbouring sensor nodes in the network.
- **Task Manager**: The task manager is a centralised point of control within the network, which extracts information required. It also assists as a gateway to other networks.
- **Data**: Data is streamed to these workstations through internet, wireless channels etc. So, several thousand nodes are deployed throughout a sensor field to create a multi-hop network connecting all the nodes to the sink through intermediary nodes or directly.

1.1.5 Characteristics and Requirements

The basic Characteristics and Requirements a sensor node must possess are

**Energy efficient**: Since every network consists of plenty of sensor nodes in it, the main requirement for sensor nodes in networks must be energy efficient. Each sensor node has a limited energy to determine its lifetime.
because it is difficult to recharge numerous nodes in a network thus each node must be energy efficient.

**Economical:** Each sensor nodes must be cost effective because WSN generally have thousands of sensor nodes, so it should cost lower to make it economically usable.

**Distributed sensing:** Using a WSN, more data can be collected and compared with just one sensor. Even deploying a sensor with line of sight, it could have obstructions caused by environment. Therefore it provides robustness to environmental obstacles.

**Wireless:** Sensor nodes must be wireless since many applications in the environment are being monitored does not primarily have any infrastructure predefined or installed. Also in case of any fault it would be difficult to rectify it they are being wired.

**Multi-hop:** If every node is being connected to every other node or base station in the same network it would create a chaos in the processing and collision is predominant to take place. To overcome this connection to base station from every node it can be made through multi-hop details making sure that there is a path existing between every node to the base station. Radio signals are proportional to the fourth power of the distance of communication. Radio signals are more energy economic in transmitting many short-distance messages than to a single long distant message.

**Distributed processing:** Every node in a sensor network must able to process local data by using various fusions and filtering algorithms in the environment to acquire and aggregate the local data to convert it into a useful piece of information.
1.1.6 Types of Sensor Networks

WSNs are being used on underground, land and underwater. Depending on environment, sensor networks have to face different challenges. There are five types of WSNs:

- Terrestrial WSN,
- Underground WSN,
- Underwater WSN,
- Multi-media WSN, and
- Mobile WSN

Terrestrial WSNs comprises of hundreds to thousands of monetarily moderate remote sensor hubs being conveyed in a given range in a specially appointed or in a pre-characterized configuration based. In ad-hoc deployment, sensor nodes can be randomly placed in the target area. In pre-planned scenarios, there is grid placement or an optimal placement or 3-d and 2-d placements models. Terrestrial sensor nodes should effectively communicate data back to the base station since battery power is limited and not rechargeable.

Underground WSNs consists of a numerous sensor nodes kept underground or a cave to monitor underground actions. More sink nodes are located on ground to extract information from sensor nodes to base station. Underground WSN are very costly when compared with other networks because it must have a clear communication in the path consisting of rocks and debris. It is difficult to create wireless network in underground. It uses batteries with limited energy.
Underwater WSNs consists of large number of sensor nodes and vehicle being deployed underwater. Underwater sensor nodes are costlier to maintain so only a fewer nodes are being used in the network and communications are done with the help of acoustic waves.

Multi-media WSNs is used in nursing by pursuing of data and events in multimedia like video, audio, and images. It consist plenty of low cost sensor nodes equipped with cameras and mics.

Mobile WSNs consists of a group of sensor nodes that are mobile and interact with the environment. They are able to sense, compute and communicate like static nodes. The main difference is that every mobile node is able to reposition and organize itself in any network.

1.1.7 Challenges in WSN

Energy: In general the sensors to perform operations use some form of power. The various functions performed by sensors include data collection, processing of data, data communication and hearing the medium for any future operations. So batteries are being incorporated into the sensors for providing power to them which can be charged and recharged based on the demands after they are consumed. Here the main disadvantage is that it is very difficult for recharging the batteries or replaces the batteries in the sensors due to certain conditions based on the demography. It is also difficult to design or develop or implement any protocols to be energy efficient in WSN.

Self-Management: Without any human intervention WSN must work when they are deployed. To perform this every node must manage on certain criteria’s such as network configuration, maintenance and adaptation. The
most important criteria are fault tolerance where it must be able to repair itself in case it occurs.

**Lifetime:** Lifetime of the network is determined by the properties of the sensor nodes. It can change from hours to years for different applications. Energy efficiency is an important issue for network lifetime.

**Quality of Service Requirements:** Quality of Service (QoS) aspects that are to be considered is real time constraints (degree of coverage, required time for reporting data etc.), robustness, resistance and other issues.

**Network Topology:** There are several network topologies like star, tree and mesh considering the design of a sensor network. Topology is very crucial since network characteristics like capacity, latency, and robustness are directly affected by the choice of topology. Moreover, important decisions such as routing and processing of the data sensed should be made according to the network topology.

**Hardware and Software Issues:** Sensor Networks generally made up of hundreds or thousands of sensor nodes in a single network. So everyone prefers nodes to be cheap in order to make it economical. Flash memory is advised to be used in sensor networks as it is inexpensive. The central processing unit of sensor node determines energy consumption and computational capabilities of a node. In order to provide the flexibility for CPU implementation large number of micro-controller, microprocessor and FPGAs are available. For saving of power, microcontroller should have three states: active, sleeps and idle. Further energy consumption for FPGA cannot be reduced; moreover separate block cannot be made for it. Deployment of FPGA to reduce power consumption is a great challenge. Along these lines, other than being practical, different issues resemble the radio scope of one
sensor hub must be high going from 1 to 5 km. Radio range is basic for guaranteeing system availability and information gathering in a system as nature being observed might not have an introduced foundation for correspondence. Programming in WSN ought to be equipment free other than being light and less vitality devouring. Calculations and conventions ought to be outlined such that they ought to be less perplexing and be useful in diminishing vitality utilization.

**Operating System:** Operating System for WSNs should be less complex than the general operating systems. It should have an easy programming paradigm. Application developers should be able to concentrate on their application logic instead of being concerned with the low level hardware issues like scheduling, pre-empting and networking. Various Operating Systems developed for Sensor nodes include TinyOS, Mantis Operating System and Nano-Qplus.

**MAC Layer Issues:** Medium Access Control (MAC) solutions have direct impact on energy usage and the primary reasons for energy waste found at the MAC layer. Power saving forward error control technique is not easy to implement due to its high computing power requirements and the fact that long packets are normally not practical.

**Security:** WSN is not only deployed in the battlefield and military applications and also for surveillance tasks like building monitoring and burglar alarms. A WSN deployed in critical systems such present in airports and hospitals. Confidentiality is required in sensor systems to watch data between the sensor hubs of the system or between the sensors and the base station; else it might bring about listening stealthily on the correspondence. False information can change the way a system could be anticipated. Uprightness of information ought to be kept up. Data should not change and
accurate data must reach at user end. The other threats present in sensor networks include spoofing and modifying routing information and also passive gathering of information, sinkhole attacks or denial- of- service attack and jamming.

**Architecture:** It is a set of rules and regulations designed for implementing functionalities along with interfaces, protocols and desired hardware. Due to the lack of Network architecture, it slows down the progress in the field. Sensor network architecture should be durable and scalable. Though number of hubs are expanded QoS is not diminished, it must be adaptable to meet the extensive variety of target application situations since the remote sensor systems don't have a settled arrangement of correspondence conventions that they should stick to. The architecture must decouple the data path speed and the radio transmission rate because direct coupling between processing speed and communication bit rates can lead to suboptimal energy performance.

**Calibration:** Calibration is the movement of modifying the raw sensor readings got from the sensors into revised values by contrasting it and some standard qualities. Physical calibration of sensors in a sensor network is a time overwhelming and challenging task due to failure of sensor nodes and arbitrary noise which makes manual calibration of sensors too expensive.

**Fault Tolerance:** Sensor network should persist functional even if any node fails while the network is operational. Networks should be able to self-repair its connectivity and other related issues in case of any fault. To overcome this well- efficient routing algorithm is designed to change the overall configuration of network.

**Decentralized Management:** WSNs are usually infeasible to adapt on centralized algorithms to implement management solutions like topology or
routing. Therefore nodes must collaborate with its neighbouring nodes to make local decisions without global knowledge. Thus the results of distributed algorithms are not optimal.

**Limited Memory and Storage Space:** A sensor node is a device with minimal amount of memory allocated for the code. In order to build an effective mechanism, it is requires to reduce the code size of algorithm. Common sensor type has 16bit, 8 MHz RISC CPU with 10K RAM, 48KB program memory and 1024KB flash storage. With this limitation, the software built for the sensor must be small.

**Physical Attacks:** The sensors are being deployed in an environment open to bad weather etc. A sensor may suffer a physical attack in such an environment which is much higher than the PCs, which are located in a secure place and mainly face attacks from networks. Physical securities of the sensor nodes cannot be assured. Attackers can modify node hardware and also replace it with malicious or dummy sensor.

**Formation of Knowledge:** Challenges for data interpretation and formation of knowledge includes problems like addressing noisy data and developing new techniques for inference. Uncertainty in interpreted data causes users not to trust the system. Developing techniques that convert this raw data into usable knowledge in an energy efficient manner must be designed.

**Robustness:** Each node should be constructed to be robust. In a typical deployment, hundreds of nodes will have to work together for many years. To achieve this, the system is designed such that it tolerates and adapt to node failures. Apart from this each node designed to be individually robust. By separating framework usefulness into segregated sub-pieces, each capacity can be completely tried in seclusion before consolidating them into a total application. To encourage this, framework segments ought to be as free as
would be prudent and have interfaces that are restricted, keeping in mind the end goal to forestall unforeseen associations. It is normal for offices to have existing remote gadgets that work on at least one frequency. The capacity to keep away from congested frequencies is basic with a specific end goal to ensure an effective arrangement.

**Heterogeneity:** It is a group in which all the nodes are not identical and do not have same capability i.e. some node are more powerful than others. Example of heterogeneous group is cluster architecture in which group of nodes form a cluster and each cluster has Cluster Head (CH) which is responsible to gather data from less powerful node.

**Multimedia Communication:** Multimedia information is collected and communicated by the sensor network. Notwithstanding information exchange modes commonplace of scalar sensor networks, multimedia information incorporates snapshot and spilling multimedia content. Preparing and conveyance of multimedia substances are not self-deciding and their correspondence majorly affects the reachable QoS. It request high data transmission for transmission.

**Real Time Operation:** Must achieve Real-time performance can be achieved by Many real-time WSNs over extremely long lifetimes. While energy harvesting has demonstrated guarantee as an empowering innovation for long-running remote sensor systems, it likewise acquaints new difficulties with ongoing processor scheduling because of fluctuating energy sources and restricted limit of energy stockpiling.

**Synchronization:** Time Synchronization in a sensor network aims to provide a common timescale for local clocks of nodes in the network. A global clock is used to process and analyse the data properly and forecast future system behaviour. Applications make use of a global clock synchronization to
monitor environment and tracking the desired goals. Energy exploitation in some synchronization patterns are more due to energy starving equipment’s like GPS (Global Positioning System) receivers or NTP (Network Time Protocol). Sensors need to be synchronized with each other, as it may lead to inaccurate data estimation. Some synchronization protocols have high accuracy so they need more resources which results in energy loss. So, synchronization needs to be implemented correctly based on the application.

**Deployment:** Implementing the WSN in real world location. It is very laborious and cumbersome activity depends on the demographic location of the application. At locations which are hard to reach, sensors are dropped from helicopter or may be in some locations sensors are placed according to some topology. Energy management issues like battery recharge and changing are challenges in real world scenarios. Deployment of sensor networks results brings about system congestion because of numerous simultaneous endeavours made by a few sensor nodes. Low information yield is an issue in real time situation as system conveys inadequate measure of data.

Various research issues and challenges pertaining to WSNs that have been experienced by the researchers are presented in this work. Sensor networks have many challenges, but its vast number of applications lures researchers to investigate more into it. A thorough investigation reveals that WSN is a multidisciplinary field. The other side it demands a scalable architecture from hardware engineers to maintain good QoS and on the other hand it demands for energy efficient algorithms from software engineers to make its execution practical and feasible. Energy saving is main concern and various research issues ultimately deals in minimizing it. Finally, a holistic approach and coordinated effort is required from the research fraternity to make it a reality.
1.1.8 Applications of Industrial WSN

Applications of WSN is generally categorized into mainly

- Event-Detection - Where sensors are used to detect the occurrences of any events.
- Spatial Process Estimation - In this sensors are used to estimate physical phenomena.

Given below are few scenarios where the WSN are applied:

**Area monitoring:** It is an event-detection application where sensors are widely spread and monitored. An example for this is in military conditions to detect the intrusion of enemies into the boundary specified.

**Health care monitoring:** It is a spatial process estimation application where a patient’s complete body is diagnosed in a regular interval period and estimate their effect of illness and future diagnostics is done. This is done by sensors being utilized as two types either being incorporated in wearable devices like watches etc., or by implanting the sensors into the patient’s body and monitoring them to maintain their health and fitness.

**Environmental/Earth sensing:** Many applications are present in monitoring environmental parameters, examples of a few are mentioned below.

**Air pollution monitoring:** Remote sensor networks have been sent to screen the centralization of unsafe gasses for residents. The Ad-hoc wireless links are used instead of wired installations, which is easier for testing different areas.

**Forest fire detection:** A network of sensors can be installed in forests to detect the fire accidents. These sensors measure temperature and humidity which have occurred due to fire in the forest. The other applications can be
landslide detection, natural disaster prediction, monitoring the quality of water, etc.

**Machine health monitoring:** WSN has been developed for machinery Condition-Based Maintenance (CBM) as they offer significant cost savings and enable new functionality. Wireless sensors can be placed in locations connected to heavy working machineries, such as rotating machinery and untethered vehicles to detect and monitor its lifetime and for flaws in it.

**Data centre monitoring:** Due to the high density of server racks in a data centre, often cabling and IP addresses are an issue. To avoid this problem numerous racks are being deployed with wireless temperature sensors to observe the intake and outtake of the rack temperatures. ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) recommends us to use around six sensors per rack and meshed wireless technology is advantageous than the cabled networks.

**Data logging:** WSNs are being used in collection of data to monitor the environment information which is easy to monitor the temperature in fridge to level of water in overflow tanks present in nuclear power plants. This statistical information is used to show how systems are working. The advantage of WSNs over conventional loggers are the "live" data feed that is possible.

**Water monitoring:** Checking the quality and level of water has many activities which includes monitoring quality of underground, surface water and ensure the infrastructure of country’s water.

**Structural health monitoring:** WSNs are used in monitoring the condition of civil infrastructure and geo-physical processes of real time and over long periods through data logging by using interfaced sensors.
**Wine production:** WSNs are used for monitoring wine production in the field as well as in the cellar.

**Industrial monitoring:** Industrial Wireless Sensor Networks (IWSN) is a developing class of WSN that countenances specific imperatives connected to the particularities of the mechanical generation. In these terms, IWSNs faces a few difficulties, for example, the reliability and robustness in brutal situations, and also the capacity to legitimately execute and accomplish the objective in parallel with the various modern forms.

IWSN applications can be classified into three groups based on the precise necessities of the industrial fabrication:

1. Environmental Sensing
2. Conditional Monitoring
3. Process Automation

A reduced cost and easy installation and deployment of the wireless components are the main reasons for considering wireless solutions in industrial applications. This has resulted in an increased popularity among industry and especially companies interested in the area of industrial process automation.

Industrial automation applications can be categorized into two distinct fields: (1) Process Automation (PA) (batch processing) and (2) Factory Automation (FA) (discrete automation). Some applications are hybrid of the two.

PA is often involved in monitoring and control of fluids (e.g., oil, gas, water, etc.).
Typical applications include: chemical manufacturing, pulp & paper, oil & gas, glass & mineral, to name a few. The PA applications usually transmit process values at regular intervals and normally involve non-critical closed-loop control whose latency requirement usually is not stringent (>100 ms). This allows nodes to reduce power consumption by carrying out aggressive duty cycling of their radios and sensor sampling operations. PA involves using computer technology to monitor performance values and quality of outputs. This is done with the help of sensors that collect data on temperatures, pressure, and vibration and so on. Human to machine interfaces, supervisory and control systems are placed at its higher level for processing data and configuration. The lower level, field network where sensor nodes are installed might be in a remote place with harsh environment (Jianping et al. 2008).

Hence the issue of high reliability and safety of communication of sensor-to-sensor (within the field network) and sensor-to-host (between field network and plant network) are very crucial.

On the other hand, control systems for FA are PLC (Programmable Logic Controller), which mainly deals with on/off signal and its origin is a relay sequence. FA applications, which involve machines (e.g. robots) that perform discrete actions, for example, assembly process for automotive, consumer products, and electronics. The FA applications generate ‘burst’ data, and are highly sensitive to any signal delays (1–50 ms). Thus, in FA applications, some performance metrics (e.g. real-time capability and reliability) have been assigned higher priority than reducing power consumption.

Consequently, using wireless technologies in FA field is much more challenge than in PA field. Meanwhile, most of the advantages (such as low power requirements, mesh routing potentialities to elaborate network
distance and reliability) of WSNs directly relate to the PA applications. Therefore using WSNs in the PA applications have attracted a significantly more attention than FA applications (Quan & Jin 2016).

Communication protocols for industrial automation have high demands on reliability and robustness. As the technologies of WSN are developed rapidly, there is a trend to adopt low power, cost and rate standards for ambient intelligence of industrial automation application. The popular industrial WSN standards: ZigBee, Bluetooth, WirelessHART, ISA100.11a. The PA industry is adopting wireless technologies, but in such harsh environments technologies like Bluetooth and ZigBee are not reliable enough. An alternative to Bluetooth and ZigBee is WirelessHART that can cope with the noisy environment but instead imposes very high demands on the hardware.

1.2 INDUSTRIAL WIRELESS STANDARDS

Wireless innovations have been broadly embraced and incorporated with industrial PA by a few associations demonstrates to have incredible advantages. Reliability, Flexibility and Cost-effectiveness of automation arrangements and cost decrease, Simplicity of upkeep of industrial plant are all huge benefits brought close by adjusting automation frameworks remotely. Communication protocols for industrial automation have high demands on reliability and robustness. Moving from wired communication to wireless communication involves many advantages but also some disadvantages. Installing cables to every sensor is a tedious and expensive task and this is one of the biggest reasons why companies are looking into wireless solutions. This becomes evident from the increasing amount of wireless standards developed for this application area.
As the technologies of WSN are developed rapidly, there is a trend to adopt low power, cost and rate standards for ambient intelligence of industrial automation application. ZigBee with the upper layer specification built upon IEEE 802.15.4 which is a major standard of low-rate wireless PAN operating in the 868/915MHz and 2.4 GHz ISM bands comes out as one of few low-power/cost monitoring and control based wireless standards together with Bluetooth. Bluetooth and ZigBee are wireless standards designed for general-purpose. WirelessHART and ISA100.11a are specifically targeted at wireless industrial communications.

1.2.1 Requirements of Industrial WSN

The IWSN dominion is a subgroup of the WSAN (Wireless Sensor and Actuator Network) dominion and has requirements specific to the industrial domain

- Energy Efficiency
- QoS

Recent advancements in wireless sensor technology lead to optimization and improvement in product development and it processes. Industrial Wireless Sensor Networks (IWSN) is an advanced extension of WSN that faces specific constraints linked to the industrial production. Therefore IWSN requires reliability, latency, updating rate, transmission range, integration etc., which makes it versatile, east to access, economical and energy efficient.

Reliability: It is a measure of how the accurate data which reaches its destination. Reliability is used in addition with stability. It represents how data packets transmitted in the network. The transfer in IEEE 802.15.4 is an acknowledge-based system. The transmitter expects to receive an ACK from
the receiver for each transmitted packet. It is possible to achieve 100% reliability with no data loss along with 90% stability.

**Latency:** Latency is a measure of time delay. It is defined as the time it takes from when a data packet is transmitted from the originating sensor to reach its final destination. A poor link increases the number of retransmissions and latency. Hop-count is another factor which increases latency. In an IEEE 802.15.4 based mesh sensor network every sensor is a Full-Function Device (FFD).

**Sensor Data Update Rates:** Update rate of the sensor data affects consumption of power, a trade-off between update rate and battery lifetime is required.

**Wireless Transmission Range:** All flow lines in the process must be within radio range of one wireless gateway. In general, the sensors require a radio range of 25 meters.

**Power Consumption:** There are factors which affect the power consumption of a wireless sensor node, i.e. Update Rate, Routing Activity, Link Quality; Low power consumption is required to increase the intervals.

During the last 13 years, standardized radio technologies like Wireless LAN / WLAN (IEEE 802.11), IEEE 802.15.4 and Bluetooth technology (IEEE802.15.1) have become the dominating technologies for industrial applications. Table 1.1 shows the comparison between the IEEE 802.15.4 standard with the most popular wireless technologies such as IEEE 802.11 commonly known as Wi-Fi and Bluetooth. It is nowadays widely accepted that the IEEE 802.15.4 offers the best basis for wireless sensor applications.
Table 1.1 Comparison between IEEE 802.15.4 and the most well-known wireless technologies

<table>
<thead>
<tr>
<th>Parameter</th>
<th>IEEE 802.15.4</th>
<th>IEEE 802.11 (Wi-Fi)</th>
<th>Bluetooth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Frequency</td>
<td>2.4GHz/ 868 MHz / 915 MHz</td>
<td>2.4GHz / 5 GHz</td>
<td>2.4GHz</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>250 kbps</td>
<td>Up to 54 Mbps</td>
<td>720 kbps</td>
</tr>
<tr>
<td>Typical average Consumption</td>
<td>1µA</td>
<td>2-20 Watts</td>
<td>5000 µA</td>
</tr>
<tr>
<td>Network Size</td>
<td>Up to 65536</td>
<td>Up to 250 nodes</td>
<td>Up to 8 nodes</td>
</tr>
<tr>
<td>Range</td>
<td>30–300ft (10-100m)</td>
<td>50-100 meters</td>
<td>30–300ft (10-100m)</td>
</tr>
<tr>
<td>Battery Lifetime</td>
<td>5-10 yrs.</td>
<td>1 week</td>
<td>1 week</td>
</tr>
<tr>
<td>Main Application</td>
<td>Monitoring Control</td>
<td>High speed Internet</td>
<td>Device Connectivity</td>
</tr>
<tr>
<td>Advantages</td>
<td>Low Power, cost</td>
<td>Speed</td>
<td>Convenience</td>
</tr>
</tbody>
</table>

1.2.2 Bluetooth

- Bluetooth is a standardized protocol for sending and receiving data via a 2.4GHz wireless link. It’s a secure protocol, and it’s perfect for short-range, low-power, low-cost, wireless transmissions between electronic devices.

- It is widely used in Short-range office applications.

- Bluetooth provides useful features such as channel hopping and time slots which increase the reliability of the system.

- The standard does not make any effort to guarantee an end-to-end wireless communication delay. Bluetooth is predominantly
designed for point-to-point communication and is entirely unable to scale to handle high-volume node networks.

- Bluetooth Networks (commonly referred to as Piconets) use a Master/Slave model to control when and where devices can send data. In this model, a single master device can be connected to up to seven different slave devices. Any slave device in the piconet can only be connected to a single master.

- Bluetooth wireless devices have limited battery lifetime compared to other energy efficient wireless standards.

- Bluetooth is not suitable for industrial applications as it does not meet the strict industrial requirements regarding security, scalability and power consumption.

1.2.3 **ZigBee**

- ZigBee is a specification for a cost-effective, low rate and low-power wireless communication protocol for home automation, monitoring and control. ZigBee is secured by a 128-bit AES (Advanced Encryption Standard) encryption algorithm.

- It is a short range wireless networking which is scalable, Self-organizing and secure, while providing battery life up to two years.

- In a ZigBee network, all nodes share the same channel, and frequency agility is minimal.

- There is no frequency hopping, and the only option is to scan for a channel with the least amount of interference at start up.
- Parameters like network strength, reliable message distribution, verification and integrity are all important for industrial use.

- Since the whole network shares the same static channel, there is no frequency diversity which makes it highly susceptible to both unintended and intended jamming. This also means that the severe frequency selective diminishing due to the metal-rich propagation environments in plants potentially can stop all ZigBee communication.

- Moreover the static channel will increase nosiness for other systems like wireless-LAN and increase delay as the network size grows and collisions forces retransmissions.

- There is no route diversity meaning that in case of a connection is destroyed; a new path from source to destination must be set up which cause increases in both delay and overhead and route-discovery will eventually consume all bandwidth available in environments with unstable routes.

- Furthermore, the lack of robustness also means that ZigBee is less suited for control applications (Tomas et al. 2008).

1.2.4 International Society of Automation (ISA) 100.11a

The design criteria for ISA100.11a include:

- Flexibility,
- Support for multiple protocols,
- Use of open standards,
- Support for multiple applications,
- Reliability (error detection, channel-hopping),
- Determinism (Time Division Multiple Access(TDMA), QoS support),
- Security.

ISA supports Connectionless UDP service, Security, end-to-end encryption and data integrity. ISA100 Standard that is a family of industrial wireless standards covering different applications such as process applications, asset tracking and identification, and so on. ISA100.11a is the first standard of ISA100 family with the specification for PA including the management and security coverage. The ISA100.11a follows the same OSI (Open System Interconnection) layer description methodology as WirelessHART does, however many of its protocol suite specifications appear to vary from those of WirelessHART. It provides great methods of security such asymmetric cryptography and object-based application layer security. Additionally, ISA 100.11.a establishes means of reliability though frequency diversity, network robustness and reliable message delivery. ISA 100.11a is regarded as the great competitor of WirelessHART. It is designed to satisfy optimally the industrial requirements of security, reliability, scalability and power consumption. However, it does exclude a backwards compatibility with the current industrial innovation, making all the more exorbitant its foundation in the process business. Application Layer, Currently no procedure control application layer is indicated by ISA100 to work with the ISA100.11a correspondence convention stack. ISA100.11a determines just an arrangement of administrations for client applications and not a procedure robotization application. Just the System Management application is indicated.
1.2.5 WirelessHART

WirelessHART (Wireless Highway Addressable Remote Transducer) is a Wireless Mesh Network Communications Protocol intended to address the issues for process computerization applications. WirelessHART was created to fulfill the existing gap in the industrial wireless standardization. WirelessHART that was officially released by the HART Communication Foundation in September 2007 is the first open wireless communication standard for process control and related applications. WirelessHART is an extension to the HART protocol that adds the wireless medium alongside the 4-20mA analog instrumentation wiring.

The basic network device types include:

- Field devices - Field Devices are located at a plant level and connected to the industrial process with full functionality and routing capability.
- Routers – All devices must have the ability to route packets in the wireless mesh.
- Adapters - Bind wired HART devices into the wireless mesh.
- Hand-held devices – Devices carried by mobile users such as plant engineers and service technicians.
- Access points – Points that connect wireless mesh to the gateway.
- A simplex or redundant gateway – Bridge between the host applications.
- A single network manager (may be redundant) that may reside in the gateway device or be separate from the gateway;
- A security manager that may reside in the gateway device or separate from the gateway.

Highway Addressable Remote Transducer (HART) is a protocol for bi-directional communication between a host application and intelligent field instruments. The HART protocol operates in a master-slave fashion. All communication is initiated by the master. A master can either be a control station or an operating device. There can be most extreme of two masters, Essential Master -regularly the control framework — and Optional Master - a handheld terminal or a portable PC. Slaves (e.g. HART field gadget) react just to command messages from a master. After the culmination of an exchange the master will sit tight for a settled time before sending another command. This empowers the other master to soften up so two masters can alternate speaking with the field gadgets.

WirelessHART is a first open and interoperable wireless standard to address the critical needs of real-world industrial applications. WirelessHART is a secure and robust mesh networking technology operating in 2.4GHz ISM radio band. WirelessHART utilizes IEEE 802.15.4 compatible Direct Sequence Spread Spectrum (DSSS) radios with channel hopping on a packet by packet basis (Song et al. 2010).

WirelessHART standard provides the idea of Frequency Hopping Spread Spectrum (FHSS) and Channel Blacklisting, i.e. disallowing the use of determined channels. Channel Backlisting used to ban channels when certain channels have high interference. Frequency hopping and channel blacklisting allow to achieving high network robustness and a high reliability required in industrial applications. Its channels are numbered from 11 to 26 with a 5MHz gap between two adjacent channels. WirelessHART to hop across the 16 channels defined in the IEEE802.15.4 standard in order to avoid interference.
The Network Manager (NM) is the centralized “brain” of the WirelessHART network. It is the application responsible for forming and configuring the network, scheduling communication between devices, managing the routing in the network and monitoring and reporting the health of the network. There is only one active NM per WirelessHART network. The NM acts as a commander and controller of the whole network by building and maintaining wireless mesh network (Anna et al. 2008). It is also responsible for identifying the best paths and managing distributing resources, scheduling communication for every device in WirelessHART network. The NM utilizes the Application Layer commands for configuring and managing the entire WirelessHART network as illustrated in Figure 1.2.

Figure 1.2 Architecture of WirelessHART Network with Protocol Layer Features

The main objectives of the wireless HART standard are:

- Backward compatibility, i.e., supports existing HART technology.
- More flexibility for installing and operating PA equipment. Reliable, easy-to-use and simple communications.
Secure communication protocol standard that utilizes a time synchronized, self-organizing, and self-healing mesh network architecture.

Interoperability, i.e., allow HART-enabled devices from different industrialists to work together.

Figure 1.3 Comparison of Protocol Architecture

The differences on protocol architectures of the standards and functions at each protocol layer are shown in Figure 1.3. As shown in figure, all of these standards are based on the IEEE 802.15.4 standard, which is widely used standard for short-range connectivity characterized by low-power consumption and low cost (Willig et al. 2005). These features make it appealing for the connection of sensors/actuators on mobile equipment or within distributed sensor networks. The WirelessHART physical layer is based mostly on the IEEE STD 802.15.4-2006 2.4GHz DSSS physical layer with a data rate of up to 250 Kbits/s. The WirelessHART Data Link Layer Protocol Data Unit (DLPDU) establishes the mechanisms for a reliable and secure communication at the Data-Link Layer (DLL). The WirelessHART
DLL extends the functionality of the MAC by defining a fixed 10-ms time slot, synchronized frequency hopping and TDMA to provide collision-free and deterministic communications. The network layer responsibilities consists of several functions including packet routing, ensuring secure end-to-end communications and encapsulating the transport layer information exchanged across a network (Jian & Jin 2010). WirelessHART transport layer ensures an end-to-end packet delivery for all the communications that require acknowledgment such Request/Response traffic. The application layer defines various device commands, responses, data types and status reporting. The NM utilizes the application layer commands for configuring and managing the entire WirelessHART network.

### 1.2.6 Comparison of Industrial Wireless Standards

The Table 1.2 depicts briefly the distinct features of the communication protocols described. The Table 1.3 (http://www.mouser.in/applications/rf-sensor-networks) briefly discussed various Protocols Used in Industrial Wireless Networks and their standards, descriptions, advantages and disadvantages.

**Table 1.2 Comparative tables including the main features of Bluetooth, ZigBee, WirelessHART and ISA100.11a**

<table>
<thead>
<tr>
<th>Features</th>
<th>Bluetooth</th>
<th>ZigBee</th>
<th>ISA100.11a</th>
<th>Wireless HART</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Optional</td>
<td>High</td>
<td>Very high</td>
<td>Very high</td>
</tr>
<tr>
<td>Reliability</td>
<td>Low</td>
<td>Very Low</td>
<td>Very high</td>
<td>High</td>
</tr>
<tr>
<td>Power consumption</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>scalability</td>
<td>Limited</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>(8 device)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Standard &amp; Operating Frequency</td>
<td>Description</td>
<td>Example Modules</td>
<td>Advantages</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>ZigBee</td>
<td>IEEE 802.15.4ISM band 2.4GHz and 900MHz</td>
<td>A mesh-networking standard for control and monitoring; building/home automation, embedded sensing. Distance range of up to 50 m.</td>
<td>Silicon Labs, NXP, Panasonic</td>
<td>Low-cost, power efficient, easy solution for small networks. Use is widespread.</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>IEEE 802.15.1ISM band 2.4GHz.</td>
<td>Replaces serial connections like RS-232 and RS-485 and Ethernet over short distances (&lt;100m)</td>
<td>Murata, Panasonic</td>
<td>Bluetooth Low Energy</td>
</tr>
<tr>
<td>Wi-Fi – Low Power</td>
<td>IEEE 802.11a/b/g/n/ac 2.4 GHz and 5GHz. (inconsistent worldwide)</td>
<td>Mature wireless standard developed for commercial/consumer use. Maximum distances from 100 – 200m.</td>
<td>Murata, Microchip</td>
<td>Higher information rate. Develop innovation; no bridges required to outskirt to the web.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Standard &amp; Operating Frequency</td>
<td>Description</td>
<td>Example Modules</td>
<td>Advantages</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ISA-100.11a</td>
<td>IEEE 802.15.4ISM band 2.4GHz.</td>
<td>A multi-vendor standard for reliable and secure wireless connectivity for non-critical control and monitoring. Low-data-rate, very low power consumption. ISM band 2.4GHz. Range of 600m.</td>
<td>RFM Microchip Panasonic</td>
<td>Can scale above 250 nodes per network. An accepted standard. Created specifically for industrial controls. 600m range.</td>
</tr>
<tr>
<td>WirelessHART</td>
<td>IEEE 802.15.4ISM band 2.4GHz.</td>
<td>A multi-vendor standard specifically designed for process monitoring and control; mesh networking with large numbers of sensors/nodes. Range is less than 100 feet.</td>
<td>RFM Panasonic</td>
<td>Designated as an International standard. Built on a 30-year old HART technology. An accepted standard. Created specifically for industrial controls.</td>
</tr>
</tbody>
</table>
For the existing IWSNs, the preferred standards among adopters in 2012 versus 2014 are given in Table 1.4 (Hatler 2015). Compared with these two; there has been a slight increase in interest of ISA100.11a as well as a decline in the number of WirelessHART adopters. However, WirelessHART is still the most preferred standards for IWSN.

Table 1.4 Preferred Standards among Adopters in 2012 versus 2014 (Quan & Jin 2016).

<table>
<thead>
<tr>
<th>Elements</th>
<th>Percentage in 2012</th>
<th>Percentage in 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>WirelessHART</td>
<td>27%</td>
<td>25%</td>
</tr>
<tr>
<td>ISA 100.11a</td>
<td>10%</td>
<td>11%</td>
</tr>
<tr>
<td>Hybrid Strategy</td>
<td>22%</td>
<td>16%</td>
</tr>
<tr>
<td>Standards for factory automation</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>Other</td>
<td>23%</td>
<td>28%</td>
</tr>
<tr>
<td>N/A</td>
<td>5%</td>
<td>8%</td>
</tr>
</tbody>
</table>

In conclusion, WirelessHART is the chosen wireless solution as it is specifically designed to fulfill the industrial requirements of wireless communications and moreover, it provides a backward compatibility with the widely-used and proven-to-be-effective HART technology in the process industry in contra position with ISA 100.11.a.

1.3 CHALLENGES IN WSN FOR IMPROVING NETWORK LIFETIME

WSNs are emerging ad-hoc networks consist of small sensor nodes that sense, measure, observe, or monitor physical environmental phenomena. Sensors are small devices with limited computation power, limited bandwidth and limited power supply. Power supply is a scarce, core resource in sensors.
Low energy consumption is very important for sensor nodes, since the sensor nodes are powered by limited power batteries. In order to reduce the energy consumption, a clustering and data aggregation approach has been extensively used. Sensor nodes have limited transmission range as well as limited processing and storage capabilities. When the nodes have to send the data in multiple hops, a routing path must be established between the node and the sink. The routing path is determined by a routing protocol. The routing protocols have to ensure reliable multi-hop communication under the limited resources of a WSN. In WSN, the clustering is basically described by data aggregation by each CH, which fundamentally decreases the movement cost. The hierarchical show requires two primary techniques: (1) periodic determination of CHs; and (2) task of every node to one.

Moreover, the network lifetime should be measured not only by the time that the first or the last node dies, but also by the period of time that the network is available for providing services and operating appropriately. Since the network is usually dense and many nodes are redundant, the death of a few nodes does not affect the network. Thus, network lifetime is firmly together with the network performance.

### 1.3.1 Data Aggregation in WSN

One of the major issues with WSN is that one need to increase the lifetime of network. Generally lifetime of the network is defined as the time whenever the first node fails to send its information to base station. This issue can be resolved by implementing data aggregation technique as it decreases data traffic and further saves energy by merging multiple incoming packets into a single packet whenever the sensed information are highly correlated. With the point of decreasing Power utilization, data gathering is the worldwide procedure of get-together and routing data through a multi-hop system and preparing information at middle nodes. It endeavors to gather the
most basic and imperative information from the sensors nodes and make it accessible to the base station in an energy efficient way with least information idleness and least conceivable data transfer capacity. The main aim of data aggregation algorithms are gathering and aggregating the data in an energy efficient way and improving the network lifetime.

Key Points in data gathering are as per the following:

- Nodes sense attributes over the whole system and route to adjacent nodes.
- Node can get distinctive adaptations of same message from a few Neighbouring nodes.
- Communication is typically performed in the aggregate.
- Neighbouring nodes report comparable information.
- Combine information originating from various sources and routes to evacuate excess.

### 1.3.1.1 Data Aggregation Strategies

There are many strategies for aggregation in which some of them are listed below (Ameya & Amol 2015):

**Lossless Data Aggregation**: Lossless aggregation refers to concatenating individual data items into larger packets, thus amortizing per-packet protocol overhead. It is effective if the load on the system is not excessive.

**Lossy Data Aggregation**: If the total communication load exceeds system capacity, then the amount of communicated data must be forcibly reduced which is called the lossy aggregation. Example of lossy aggregation is the averaging of sensor values. It can be either temporal or spatial.
Structured Data Aggregation: Structure-based applications require low maintenance since the traffic pattern is unchanging and thus it is suitable for such applications. The approach changes the structure dynamically and acquires high maintenance overhead. However, this technique cannot aggregate the data efficiently.

Structure Free Data Aggregation: Structure free data aggregation technique provides efficient data aggregation without explicit maintenance of a structure. Spatial convergence and the temporal convergence are the necessary conditions for aggregation during transmission.

Centralized Approach: It is an address driven approach. In this every node sends information to a central hub by means of the most limited conceivable route utilizing a multichip wireless convention. The central node likewise called as header node aggregates the information which can be questioned to lessen the excess.

In-Network Aggregation: In-network aggregation is the widespread technique for congregation and directing data through a multi-hop network, prepare data at middle of the road nodes with the objective of diminishing resource utilization, in this manner expanding network period.

Tree Based Approach: In tree based network, the nodes are sorted out as tree topology where sink is considered as a root. Aggregation is completed by developing aggregation tree where source nodes are referred as leaves, and established at sink. Here information stream begins from leaves nodes and end at sink. So here all the middle of the road nodes complete the collection handle lastly exchange to root (sink). The primary point of the tree based approach is developing an energy efficient tree.
**Chain Based Approach:** In this procedure, the nodes are built as chains for information transmission to CH. Every single node in the system sends the detected information just to its neighbor node instead of cluster-head and each of the node aggregates the data to decrease the measure of information exchanged.

**Cluster-Based Approach:** In cluster-based approach, entire network is divided in to number of clusters. Each and every cluster has CH which is elected by cluster members or sinks. CHs is responsible for collecting and aggregating the data from its cluster members and transmit the aggregated to the sink either single hop or Multiple Hop.

### 1.3.1.2 Issues in Data Aggregation

A plan of energy compelled sensors sending over a district is considered, in that each sensor screens its incorporating area and once in a while makes data. The systematic gathering and transmission of detected data to a base station for further handling is the fundamental operation in such a system. Sensors can complete in-system aggregation or combination of data packets reroute to the base station when data gathering. In such sensor framework, the lifetime is the time in which the data can be assembled from every one of the sensors to the base station. In data gathering, from agreed energy constraints of the sensors growing the system lifetime is a major hazard. The data aggregator node or the CH combine the data to the base station and the malicious attacker may attack this cluster node. The base station cannot guarantee the precision of the cumulative data sent to it, if a CH is compromised. Due to the uncompromised nodes, the existing systems may send several copies of aggregate results to the base station and the power consumption at these nodes is increased (Maraiya et al. 2011).
1.3.2 Efficient Routing Techniques in WSN

Sensor nodes are capable of sensing, processing and transmitting the data to a base station or a sink. If the sink is within the transmission range of the node, it transfers the data in single hop. But if the sink is far off, the node sends the data in multiple hops. Sensor nodes have a limited transmission range as well as limited processing and storage capabilities. When the nodes have to send the data in multiple hops, a routing path must be established between the node and the sink. The routing path is determined by a routing protocol. The routing protocols have to ensure reliable multi-hop communication under the limited resources of a WSN. The design space in routing algorithms in WSNs is quite large and classifies the routing algorithms for WSNs in many different ways.

Routing protocols plays an important role in discovering and maintain the routes in WSN. Three kinds of algorithm can be executed as centralized algorithm, distributed algorithm and location based algorithm. Autonomy, Energy Efficiency, Scalability, Resilience, Device heterogeneity and Mobility adaptability are the requirement to be considered while designing the routing protocols. Routing protocols can be roughly classified according to the criteria: Hierarchy role of nodes in the network and data delivery model. The algorithms in WSNs usually realize the following specifications that are Attribute-based, Energy Efficiency, Data Aggregation, and Addressing Scheme, Location-based, Multipath Communication and QoS and also presented how the attribute-based, the geographic and the multipath techniques are usually applied into WSNs for the following routing protocols such as SPIN, Directed Diffusion, Rumor, COUGAR, ACQUIRE, LEACH, PEGASIS, TEEN, SHRP and SAR (Luis Javier et al. 2009).

In hierarchical routing protocols all nodes are organized as different levels. The higher layer is responsible for data aggregation and management
work. The lower layer nodes are responsible for sensing and collecting the information. Hierarchical routing protocols are proved to be more energy efficient than flat where all nodes play the same role in terms of data aggregation and forwarding data packets. Routing protocols in large scale network are classified in to three categories that are control overhead reduction; energy consumption mitigation and energy balance (Changle Li et al. 2011).

Depending on the network structure, routing in WSNs can be classified into flat based or data centric routing, hierarchical based or cluster based routing and location based routing. The three main goals of existing data routing in WSNs are including energy conservation, fast delivery and fault-tolerance. The data routing approaches in WSNs according to their main goals are Energy Efficient approaches - Energy balancing, Energy consumption reduction, Delay aware approaches –Hard-Delay aware approaches, Soft Delay-Aware approaches and Fault-Tolerant approaches – Fault prevention and Fault recovery. Ali & Abdul (2012) explored some energy efficient routing protocols such as LEACH, Direct Diffusion, Gossiping, EESR and their enhancements (Mohammad et al. 2012).

Marjan Radi et al. (2012) presented a comprehensive taxonomy on the existing multipath routing protocols, which are especially designed for WSNs and explain the operation of different protocols in detail, with emphasis on their advantages and disadvantages. The performance gains that can be achieved through using multipath routing approaches are reliability and fault tolerance, load balancing and bandwidth aggregation, QoS improvement. Each multipath routing protocol includes several components such as Path discovery, Path Selection and Traffic Distribution, Path Maintenance to construct multiple paths and distribute network traffic over the discovered paths. The existing multipath routing protocols classified into
three main categories: alternative path routing, multipath routing for reliable
data transmission, and multipath routing for efficient resource utilization,
based on the employed path selection and traffic distribution mechanisms.

1.3.3 Need for Clustering in WSN

Clustering is an approach to reduce communication between nodes
and therefore minimize energy consumption. A research shows that clustering
improves total performance of WSNs, such as communication overhead and
network longevity etc.

Clustering hundreds of nodes into many controllable smaller groups
may eventually increase the performance of the network. Partitioning a
network into many clusters will reduce the amount of traffic and the amount
of energy consumed in network. Since energy efficiency is very important for
network lifetime, clustering becomes crucial. If a sensor node needs to reduce
its energy consumption, it should send its data packets to CHs firstly, instead
of sending them directly to the sink. The sensor nodes could be grouped
together based on their energy levels, sensed data types, proximity to each
other or many other parameters.

Clustering is a collection of networks consisting of a base station
(also called as Access points) to receive the data that has been sensed by the
sensor nodes. A CH that gathers the cluster nodes sensed information and is
transmitted to the nearest neighbor cluster based on routing mechanisms. The
cluster has two modes: Setup mode and Steady mode. The Setup mode
establishes the advertisement package and sends it to the nearby packets and
broadcasts its presence.

The WSN face vast challenges in implementation. Design goals
targeted in traditional networking provide little more than a basis for the
design in WSNs. Several key attributes have to be considered for designing the Clusters; they include Synchronization, Cost of Clustering, Selection of CHs and clusters, Real-time Operations, Data Aggregation and Repair Mechanisms.

Cluster algorithms can be split into two main categories that are leader first approach and cluster first approach. In the leader first arrangement CH are chosen in view of specific measurements, and they concede to how to allocate different nodes to various clusters. In cluster initially approach all the sensor nodes initially frame clusters and each cluster then choose its CH.

A good clustering approach should have features such as;

- Fault tolerant for node failures
- Reliable for communication between nodes
- Low latency for delays
- Fast reconfiguration for new paths
- Energy saving for network longevity

There are many efficient proposed ways for selecting CHs. However, as a starting point of the selection process, there should be two basic criteria; (1) nodes should have a unique identifier and (2) these identifiers should be uniformly distributed among nodes. Some of the methods used for CH selection are; choosing nodes which are closer to the base station, choosing nodes randomly, or choosing the nodes that have highest or lowest parameters than neighbors in which parameters could be residual energy level, neighbor count, package count, sensed value, unique identifiers etc. However using simple clustering algorithms is not always efficient. If simple clustering algorithms such as selecting nodes with lowest or highest identifiers are applied, same nodes will be selected as CH many
times. This results in quick energy drain of these selected nodes. Therefore, selection of CHs is also crucial to distribute load evenly among other nodes in order to minimize energy consumption.

1.3.4 Load Balancing in WSN

In WSNs, communication efficiency and power consumption are usually the main obstacles to improving service availability and energy efficiency. The power consumption of node and link is highly related with the corresponding traffic volume. One method to solve the trade-off between communication efficiency and power consumption is to distribute the traffic uniformly across the network. Energy-efficiency is a critical issue in WSNs due to the limited capacity of the sensor nodes’ batteries. Therefore large number of researches has been conducted in order to propose algorithms, protocols, and solutions reducing energy consumptions in communications to extend the lifetime of the network. Several research studies have emerged with a main goal: optimization of nodes energy consumption through the use of innovative conservation techniques to improve network performance, including lifetime maximizing. In general, saving energy is ultimately to find the best trade-off between the different energy-consuming activities.

A load balance is extremely crucial for the lifetime of WSNs and a node affording heavier load will consume limited energy more quickly which deduces the efficient lifetime for WSNs. The energy consumption of sensors plays an important role in the network lifetime that became the performance criterion in the WSNs. Clustering can be utilized for load balancing to develop the lifetime of a sensor arrange by lessening energy utilization. Load balancing utilizing clustering can likewise expand arrange scalability. Wireless sensor coordinate with the nodes with various energy levels can drag out the arrange lifetime of the system and furthermore its reliability. Clustering has various favorable circumstances like it decreases the measure
of the directing table, save correspondence transfer speed, extend system lifetime, diminish the excess of information packets, diminishes the rate of energy utilization and so on.

1.4 MOTIVATION OF THE PRESENT THESIS

WSN plays a major role in today’s real world application and particularly the data gathered are important for Industrial applications. For industrial revolutionary monitoring, WirelessHART is the next big technology advancements over ZigBee and Bluetooth specifications. Many industries prefer battery operated field device and particularly vast industries feel recharging of batteries to be labor-intensive. Hence all the sensor nodes are powered with battery supply and when an algorithm with power killing characteristic is deployed, battery power will be exhausted and may isolated from the network until attended. So reliability of the sensor networks arises as a matter of discussion in this case. When it comes in terms of data transfer, Wireless HART follows mesh network, in which data’s are transmitted on different paths. Many evaluations conclude that most of the stored energy dissipates only during the data transmission.

One of the main requirements of automation industry is that WSN should have a very long life time nearly 5 to 10 years without change in battery. Moreover, implementing in-network aggregation of data in wireless HART networks will save energy and thereby prolong the lifetime of network. Wireless-Hart didn’t allow data aggregation because of security. The other industrial standards allow data aggregation in the industrial and PA applications. To the best of the knowledge there do not exist any work dealing with packet aggregation for WirelessHART.
The objective is to develop an energy-efficient packet forwarding approach in WirelessHART to improve the network lifetime. This will help industries to meet their demand for long-term reliable monitoring.

In addition to that, topology of the sensor network plays vital in efficiency of WSNs. Large Networks will have large number of devices that need more hops to reach gateway. As the number of hops increases, so does latency. Node failure occurs when energy of a particular sensor is exploited to its maximum level. So breaking the larger networks into smaller ones, or clusters which reduce overall latency because nodes need to travel only fewer hops which achieves reliable networks with no bottleneck. Hence there is need to develop cluster tree based algorithm, as it is best for energy efficiency among clusters which includes inducing load balance at the CH to improve further efficiency in the cluster tree structure and avoid data packet loss ratio.

1.5 OBJECTIVES OF THE RESEARCH WORK

The High-level objectives of the proposed research work are as follows:

- To analyse the suitable WSN Standards for Industrial environment.
- To design an Efficient Packet aggregation and forwarding using graph routing approach to increase the network lifetime.
- To design a cluster tree topology for data collection with load balance at the CHS in order to improve the QoS with respect to network lifetime.
- To analyse the Performance metric of proposed algorithm with existing approaches.
1.6 ORGANIZATION OF THE THESIS

Chapter 1 provides the background on WSN and the challenges faced while implementing the WSNs in Industrial applications and various Industrial Wireless Standards. The goal of this research work is to enhance the life time of sensor nodes.

Chapter 2 presents the literature review of the research work. The related work on Clustering Algorithms, Data Aggregation, Graph routing Algorithms, MAC Protocol, Load balancing algorithms have been studied and discussed in detail.

Chapter 3 discusses the proposed Energy Efficient Packet Forwarding (EPF) approach to control the excess energy dissipation in the network in order to improve the network lifetime. The routine of node selection and rejection into the data path is monitored periodically using graph routing approach. It also compares the performance of ELHFR, EBGR with the proposed EPF protocol.

Chapter 4 demonstrates the proposed Efficient Cluster tree based algorithm to find an optimal path for data transmission by the formation of a tree structure that helps in overall energy consumption, reduces end to end delay and avoids cluster formation frequently and provides better QoS.

Chapter 5 explores the Load Balanced Algorithm in cluster Tree Structure in order to achieve high throughput by reducing data packet loss.

Chapter 6 concludes this thesis and offers proposals for further research on the theme of the thesis.