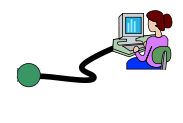
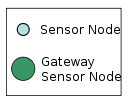
**1.1 Wireless Sensor Network**

Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, enabling control over the activity of the sensors. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer application, such as industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control.

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a micro-controller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoe-box down to the size of a grain of dust. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Sensors integrated into structures, machinery, and the environment, coupled with the efficient delivery of sensed information, could provide tremendous benefits to society. Potential benefits include: fewer catastrophic failures, conservation of natural resources, improved manufacturing productivity, improved emergency response, and enhanced homeland security. However, barriers to the widespread use of sensors in structures and machines continue to exist. Bundles of lead wires and fiber optic “tails” are subject to breakage and connector failures. Long wire bundles represent a significant installation and long term maintenance cost, limiting the number of sensors that may be deployed, and therefore reducing the overall quality of the data reported. Wireless sensing networks can eliminate these costs, easing installation and eliminating connectors. The ideal wireless sensor is networked and scalable, consumes very little power, is smart and software programmable, capable of fast data acquisition, reliable and accurate over the long term, costs little to purchase and install, and requires no real maintenance.





**Figure 1.1: Typical Wireless Sensor Network Architecture**

Selecting the optimum sensors and wireless communications link requires knowledge of the application and problem definition. Battery life, sensor update rates, and size are all major design considerations. Recent advances have resulted in the ability to integrate sensors, radio communications, and digital electronics into a single integrated circuit (IC) package. This capability is enabling networks of very low cost sensors that are able to communicate with each other using low power wireless data routing protocols. A wireless sensor network (WSN) generally consists of a base station (or “gateway”) that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed, and transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data is then presented to the system by the gateway connection.

Wireless Sensor Networks (WSNs) are networks of light-weight sensors that are battery powered used majorly for monitoring purposes. The advances in micro-electromechanical technologies have made the improvising of such sensors a possibility. Recently, WSNs have been heavily researched by several organizations and by the military where we can find some of the applications in battle field surveillance and other security etiquettes. With the recent issues on climate change, WSNs can be utilized to track changes that affect the climate using a network of sensors to gather environmental variables such as temperature, humidity and pressure. One of the numerous advantages of these sensors is their ability to operate unattended which is ideal for inaccessible areas. However, while WSNs are increasingly equipped to handle some of these complex functions, in-network processing such as data aggregation, information fusion, computation and transmission activities requires these sensors to use their energy efficiently in order to extend their effective network life time. Sensor nodes are prone to energy drainage and failure, and their battery source might be irreplaceable, instead new sensors are deployed. Thus, the constant re-energizing of wireless sensor network as old sensor nodes die out and/or the uneven terrain of the region being sensed can lead to energy imbalances or heterogeneity among the sensor nodes. This can negatively impact the stability and performance of the network system if the extra energy is not properly utilized and leveraged. Several clustering schemes and algorithm such as LEACH, DEEC, have been proposed with varying objectives such as load balancing, fault- tolerance, increased connectivity with reduced delay and network longevity. A balance of the above objectives can yield a more robust protocol. LEACH protocol and the likes assume a near to perfect system; an energy homogeneous system where a node is not likely to fail due to uneven terrain, failure in connectivity and packet dropping. But more recent protocols like SEP considered the reverse that is energy heterogeneity where the factors mentioned above is a possibility, which is more applicable to real life scenario for WSN. Thus, energy heterogeneity should therefore be one of the key factors to be considered when designing a protocol that is robust for WSN. A good protocol design should be able to scale well both in energy heterogeneous and homogeneous settings, meet the demands of different application scenarios and guarantee reliability.

Conventional protocol designs do not address these situations. This research explores existing work done in this area. The goal is to present a modified protocol design that is more robust and can ensure longer network life-time while taking other performance measures into consideration. Mathematical modeling and computer simulations are used for proof of concept and testing.

**1.2 CHARACTERISTICS OF WIRELESS SENSOR NETWORK**

The main characteristics of a WSN include:

* Energy constraints for nodes using batteries
* Ability to cope with node failure
* Mobility of nodes
* Dynamic network topology
* Communication failure
* Heterogeneity of nodes
* Scalable to large scale of deployment
* Easy to use
* Ability to withstand harsh environment conditions

**1.3 WSN TCHNOLOGY**

WSN represent a paradigm shift in wireless networks. They are being regarded as the enabling technologies for future surveillance-oriented application. A standard wireless sensor network consists of a large number of tiny sensor nodes. A sensor node basically consists of the following modules:

* The sensing module that collects information from the environment.
* The communication module that sustains wireless data communication between nodes.
* The processing module that processes the information provided by the sensor module or received from neighbor nodes.

These tiny sensor nodes work collaboratively to form a network (WSN). The network senses a given environment, perform in-network computation and communicate with a base station when a targeted event happens. The major handicap of these devices is resource constraint; low memory, limited power supply and limited processing capabilities. This directly affects the WSN at large. Due to the limitations, detection capacity in sensors diminishes with the increasing distance between the node and the phenomenon .

Memory

Communication System

Embedded

Processor

Sensor

Power Supply

**Figure 1.2 Typical Wireless Sensor Network Node Architecture**

A WSN is characterized by the following features:

* The network relay on a collection of tiny sensors to observe and influence the real world.
* The sensors have a modest and sometimes non-renewable power budget and do not necessarily need to be active at all times. So sensors can be dynamically added to or removed from the network.
* There is no infrastructure (wireless).
* It is a self organized network.
* Multi-hop communication is used and the network topology changes dynamically.

Among contemporary networks, WSN are closely related to Mobile Ad hoc networks (MANETs). They have a number of characteristics in common; network topology is not fixed, power is an expensive resource and nodes are connected to each other by wireless communication links.

* WSNs are mainly used to collect information while MANETs are designed for distributed computing rather than information gathering
* Usually a WSN is deployed by the owner whilst MANET could be run by several unrelated units.
* The number of nodes in WSNs can be several orders of magnitude higher than that in MANETs.
* WSN nodes are quite cheaper than those in MANETs, and are usually deployed in thousands.
* Power resource of WSN nodes could be very limited; however nodes in MANETs can be recharged.
* WSN’s are more limited in their computational and communication capabilities compared to MANET.
* Due to some of these differences, protocols used in MANETs can not be applied directly in WSNs.

**1.4 APPLICATION OF WIRELESS SENSOR NETWORK**

Wireless Sensor Networks (WSN) offers a rich, multi-disciplinary area of research, in, which a number of tools and concepts can be applied to address a whole diverse set of applications. Sensor networks may consist of many different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of conditions. These sensor nodes can be put for continuous sensing, location sensing, motion sensing and event detection. The idea of micro-sensing and wireless connection of these sensor nodes promises many new application areas. A few examples of their applications are as follows:

**1.4.1 AREA MONITORING APPLICATIONS**

Area monitoring is a very common application of WSNs. In area monitoring, the WSN is deployed over a region where some physical activity or phenomenon is to be monitored. When the sensors detect the event being monitored (sound, vibration), the event is re-ported to the base station, which then takes appropriate action (e.g., send a message on the internet or to a satellite). Similarly, wireless sensor networks can be deployed in security systems to detect motion of the unwanted, traffic control system to detect the presence of high-speed vehicles. Also WSNs finds huge application in military area for battled surveillance, monitoring friendly forces, equipment and ammunition, targeting and battle damage assessment.

**1.4.2 ENVIRONMENTAL APPLICATIONS**

A few environmental applications of sensor networks include forest fire detection, green-house monitoring, landslide detection, air pollution detection and food detection. They can also be used for tracking the movement of insects, birds and small animals, planetary exploration, monitoring conditions that affect crops and livestock and facilitating irrigation.

**1.4.3 HEALTH APPLICATIONS**

Some of the health applications for sensor networks are providing interfaces for the disabled, integrated patient monitoring, diagnostics, drug administration in hospitals, monitoring the movements and internal processes of insects or other small animals, telemonitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital.

**1.4.4 INDUSTRIAL APPLICATIONS**

WSNs are now widely used in industries, for example in machinery condition-based maintenance. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors. They can also be used to measure and monitor the water levels within all ground wells and monitor leach ate accumulation and removal.

**1.4.5 OTHER APPLICATIONS**

Sensor networks now find huge application in our day-to-day appliances like vacuum cleaners, micro-wave ovens, VCRs and refrigerators. Other commercial applications includes constructing smart ocean spaces, monitoring product quality, managing inventory, factory instrumentation and many more.

**1.5 ISSUES IN WIRELESS SENSOR NETWORK**

A sensor node, also known as a mote is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. Sensor nodes are small in size, low power, low cost. Despite plethora of applications of WSN, these networks have several restrictions e.g., limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSN is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. In order to design an efficient routing protocol, several challenging factors should be addressed meticulously. The following factors are discussed below:

|  |
| --- |
|  |

**Node deployment**: Node deployment in WSN is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths; but in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. Hence, random deployment raises several issues as coverage, optimal clustering etc. which need to be addressed.

**Energy consumption without losing accuracy**: Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime. In a multi hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

**Node/Link Heterogeneity**: Some applications of sensor networks might require a diverse mixture of sensor nodes with different types and capabilities to be deployed. Data from different sensors, can be generated at different rates, network can follow different data reporting models and can be subjected to different quality of service constraints. Such a heterogeneous environment makes routing more complex.

**Fault Tolerance**: Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

**Scalability**: The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

**Network Dynamics**: Most of the network architectures assume that sensor nodes are stationary. How-ever, mobility of both BS‘s and sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, besides energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS.

**Transmission Media**: In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network. As the transmission energy varies directly with the square of distance therefore a multi-hop network is suitable for conserving energy. But a multi-hop network raises several issues regarding topology management and media access control. One approach of MAC design for sensor networks is to use CSMA-CA based protocols of IEEE 802.15.4 that conserve more energy compared to contention based protocols like CSMA (e.g. IEEE 802.11).

**Coverage**: The coverage of a WSN node means either sensing coverage or communication coverage. Typically with radio communications, the communication coverage is significantly larger than sensing coverage. For applications, the sensing coverage defines how to reliably guarantee that an event can be detected. The coverage of a network is either sparse, if only parts of the area of interest are covered or dense when the area is almost completely covered. In case of a redundant coverage, multiple sensor nodes are in the same area.

**Data Aggregation**: Sensor nodes usually generate significant redundant data. So, to reduce the number of transmission, similar packets from multiple nodes can be aggregated. Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. It is incorporated in routing protocols to reduce the amount of data coming from various sources and thus to achieve energy efficiency. But it adds to the complexity and makes the incorporation of security techniques in the protocol nearly impossible.

**Data Reporting Model**: Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. In wireless sensor networks data reporting can be continuous, query-driven or event-driven. The data-delivery model affects the design of network layer, e.g., continuous data reporting generates a huge amount of data therefore, the routing protocol should be aware of data-aggregation .

**Quality of Service:** In some applications, data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime. Hence, energy-aware routing protocols are required to capture this requirement.

**Routing:** Multi hop routing is a critical service required for WSN. Because of this, there has been a large amount of work on this topic. Internet and MANET routing techniques do not perform well in WSN. Internet routing assumes highly reliable wired connections so packet errors are rare; this is not true in WSN. Many MANET routing solutions depend on symmetric links (i.e., if node A can reliably reach node B, then B can reach A) between neighbors; this is too often not true for WSN. These differences have necessitated the invention and deployment of new solutions. For WSN, which are often deployed in an ad hoc fashion, routing typically begins with neighbor discovery. Nodes send rounds of messages (packets) and build local neighbor tables. These tables include the minimum information of each neighbor’s ID and location. This means that nodes must know their geographic location prior to neighbor discovery. Other typical information in these tables include nodes’ remaining energy, delay via that node, and an estimate of link quality.

**Security:** Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive.

**1.6 ENERGY CONSTRAINTS IN WSN**

Due to the energy constraints wireless sensors usually have a limited transmission range. As low power, low cost, and longevity of transceivers are major requirements in wireless sensor networks, optimizing their design under energy constraints is of paramount importance. Energy conservation in WSN is critical and has been addressed by substantial researchers. Generally energy conservation is dealt with on five different levels:

1. Efficient scheduling of sensor nodes between sleep and active nodes.
2. Energy efficient routing, clustering and data aggregation.
3. Efficient control of transmission power to ensure an optimal trade-off between energy consumption and connectivity.
4. Data compression (source coding) to reduce the amount of uselessly transmitted data.
5. Efficient channels access and packet retransmission protocols on the Data Link Layer.

**1.7 WIRELESS SENSOR NETWORK ARCHITECTURE**

Sensor nodes are normally scattered in a sensing field, every sensor has the capability of sensing, processing in form of aggregating and communicating the data to the sink or base station using various schemes. The underlying protocol scheme in the OSI model for WSNs includes the application layer, transport layer, network layer, data link layer and the physical layer. The protocol stack shown in Figure1.4, combines power and routing awareness, integrates data with networking protocols to communicates power efficiently through wireless medium, and promotes cooperative efforts of sensor nodes.

The application layer supports different application software depending on the task. The transport layer maintains the data flow, while the network layer does the routing of data from the transport layer. Depending on the deployment of the sensors, they can be either mobile or static, if the former then the data link layer, specifically the MAC protocol design must have power control mechanism, forwarding mechanism and should be able to perform communication confidentiality through encryption-decryption techniques. Finally, the task of the physical layer involves modulation and demodulation of radio carrier stream, forward error-correction (FEC) and performing efficient synchronization between the sender and receiver. The power, mobility, and task management planes were proposed to monitor the power, movement, and task distribution among the sensor nodes. Most often sensor network protocols are designed with two basic kinds of architectures; the layered and the clustering architectures; these architectures are discussed in the next sections.



**Figure 1.3 Protocol Stack diagram**

The design of a layered architecture would normally consist of a base station and sensors scattered in the field. The layers of sensor nodes around the base station constitutes nodes that are in a single hop count to the base station, while nodes that are farther away can be multiple hop count to the BS depending on the size of the network, this is shown in Figure 1.5. One of the earliest protocols to complete the implementation of the layered architecture is the UNPF (Unified Network Protocol Framework), designed for a multi-hop infrastructure network architecture. The UNPF protocol is unified in the sense that it combines three different protocol structures: the network organization, medium access control (MAC) and the routing protocol to achieve the objectives of a robust protocol.

Three-hop layer

Two-hop layer

One-hop layer

BS

Coverage area

**Figure 1.4 Layered architecture**

Sensor node

**1.8 CLASSIFICATION OF WIRELESS SENSOR NETWORK**

A simple classification of Wireless sensor networks based on their mode of functioning and the type of target application is given below.

**1.8.1 Proactive Networks**

The nodes in this sort of network periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest. Hence, they collect the data for the relevant parameters at regular intervals. They are well suited for applications requiring periodic data monitoring. Some known instances or protocols of this kind are the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol [17], some improvements on LEACH such as [23, 24] and PEGASIS (Power-efficient gathering in sensor information systems)[22].

**1.8.2 Reactive Networks**

The nodes of the networks according to this scheme react immediately to sudden and drastic changes in the value of a sensed attribute. They are well suited for time critical applications. Typical instances of this sort of networks are [16,18].

**1.8.3 Hybrid Networks**

The nodes in such a network not only react to time-critical situations, but also give an overall picture of the network at periodic intervals in a very energy efficient manner. Such a network enables the user to request past, present and future data from the network in the form of historical, one-time and persistent queries respectively. Such kind of network takes advantages of Proactive and Reactive networks. Some instances of this kind of networks are [19, 20, 21].

