CHAPTER 1

WIRELESS SENSOR NETWORK

1.1 INTRODUCTION

A hardware device that produces measurable response signals to register changes in physical conditions like temperature, pressure and humidity is called ‘a sensor’. Continual analog signals sensed by sensors are digitized through analog-to-digital (A/D) converters and forwarded to embedded processors for more processing. As sensor nodes are micro-electronic devices powered by limited power source, attached sensors must be small and must consume very low energy (Wang & Balasingham 2010). Sensor nodes may have one or many types of sensors integrated with it.

A sensor network comprises of sensing (measuring), computing and communication elements that ensure the ability to observe and react to events/phenomena in a specific environment. A sensor network has four basic components (Sohraby et al 2007):

1. Assembly of distributed or localized sensors.
2. Interconnecting network (usually wireless-based).
3. Central information clustering point.
4. Computing resources at a central point (or beyond) to handle issues like data correlation, status querying, event trending and data mining.
Sensor network development needs technology from three research areas: sensing, communication and computing (Chong & Kumar 2003). Earlier, sensor networks include radar networks in air traffic control where networks adopt a hierarchical processing structure with processing occurring at consecutive levels till the information about events reaches users.

Sensors combined with machinery, environment, and structures linked to effective sensed information delivery highly benefit the society. Wireless sensors are networked and scalable, consume little power, software programmable, smart and reliable, capable of fast data acquisition and accurate over long terms, cost little and require no maintenance (Potluri & Kadiyala 2012). This capability enables networks of low cost sensors to effectively communicate with others through low power wireless data routing protocols.

1.2 WIRELESS SENSOR NETWORKS (WSNs)

WSNs are similar to ad-hoc wireless networks as the main communication method in multi-hop networking, but many distinctions exist between both. Ad-hoc networks support routing between node pairs (Karlof & Wagner 2003), while sensor networks include specialized communication patterns. Most sensor networks traffic is classified into three categories:

1. **Many-to-one**: Multiple sensor nodes send sensor readings to base station or network aggregation point.

2. **One-to-many**: One node (typically a base station) floods a query or multicasts or control information to many.

3. **Local communication**: Neighbouring nodes send localized messages to discover/coordinate with each other.
Multi-hop network sensors detect events and communicate collected information to a central location where events characterizing these parameters are estimated. The transmission cost is slightly higher than the computation (Bandyopadhyay & Coyle 2003) and hence advantageous to organize sensors into clusters. In clustered environment, data gathered by sensors are communicated to data processing centers through a cluster-heads hierarchy. Processing centers determine parameter’s final estimates using information from cluster-heads. Data processing center can be a particular device or just a sensor itself. As sensors communicate data over smaller distances in clustered environments, energy spent in networks is much lower than that spent when all sensors communicate directly to information processing center.

Every sensor node gets a clear-cut view of the environment in WSNs. A sensor’s view of the environment has been limited in range and accuracy covering an environment’s limited physical area (Al-Karaki & Kamal 2004). Hence, area coverage is an exceedingly designed parameter for WSNs.

1.3 MOBILE WIRELESS SENSOR NETWORKS

Mobile Wireless Sensor Networks (MWSNs) are specific WSNs where mobility has major role in application execution. Of late, mobility was introduced into system function as extensions to stationary sensor network. It does not necessarily mean that every mobile node is aware of global network state and/or node positions. It is to be noted that a mobile node is unable to complete its task (data collection, network instruction and information extraction) when motionless. Mobile connections to big WSN arise in scenarios where energy or bandwidth is a big concern (Sohrabi et al 2000). Low bit-rate data packets are exchanged to relay data to and from network, where there are limited power consumption constraints. Changes in local
topology trigger updates to nodes neighbour list in mobile networks (Kulik et al 2002). When nodes notice that a neighbour list has changed, it spontaneously re-advertises all the data.

Mobile sensor networks can be categorized by flat, 2-tier, or 3-tier hierarchical architectures. Flat or planar network architecture comprises of a set of heterogeneous devices that communicate in an ad-hoc manner.

The two-tier architecture includes a stationary nodes set, and a mobile nodes set (Amundson & Koutsoukos 2009). Mobile nodes form an over-lay network or behave as data mules to move the data through a network.

In three-tier architectures, a stationary sensor nodes set passes data to a mobile devices set which forwards data to an access points set. This heterogeneous network covers wide areas and is compatible with many applications simultaneously.

Mobile sensor devices, in general, are more powerful than those static regarding battery power as mobile sensor node consume much energy to move (Ho et al 2009). Besides, energy consumption for movement is much larger than key operations. Path breakage in mobile WSNs occurs frequently due to shadowing, channel fading, node mobility interference and power failure. Rerouting or alternative routing may be necessary when a path breaks. In hindsight, it results in packet loss and large delay (Huang et al 2008).

In WSNs, there can be some Global Positioning System (GPS)-enabled mobile nodes, called seeds, which can afford to offer location information needed by other mobile nodes. But the number of seeds cannot be too many on account of economic reason. A mobile node has to get three reference nodes, usually seeds, to do triangulation. However, it is not that always a node can get enough seeds information, especially when Dynamic
Reference Localization (DRL) limits the seed flooding scope to reduce network load. Each seed in DRL has its own values of $hd$ (hopdistance) and $fh$ (flooding-hop) to reflect the current conditions around the seed (Hsieh & Wang 2006). DRL has to update seeds dynamically to maintain its location correctness. Dynamic seed information is beneficial to location accuracy, when nodes are irregularly distributed.

1.4 APPLICATIONS

Wireless sensors and WSN are now in the forefront of the scientific community due to increasingly smaller devices ensuring many applications. Irrespective of exact platform type, known applications are categorised under military applications, environmental monitoring, commercial or human-centric applications in addition to robotics applications (Arampatzis et al 2005). Since most applications fundamentally focus on monitoring, distributed sensing enables parameterization of physical environment and its integration to established information propagation forms. Medical research and healthcare greatly benefit from sensor networks: vital sign monitoring and accident recognition being natural applications. A major issue is care for the elderly, especially if affected by cognitive decline: a sensor and actuators network can monitor and aid them in their daily needs.

An application in Civil Engineering is smart buildings: wireless sensor and actuator networks integrated in buildings ensure distributed monitoring and control, improve living conditions and reduce energy consumption, through control of temperature and air flow. Military applications are plentiful, an example being Defence Advanced Research Project Agencies (DARPA’s) self-healing minefield (Puccinelli & Haenggi 2005), a self-organizing sensor network where peer-to-peer communication between anti-tank mines help to respond to attacks and redistribute mines to
heal breaches, complicating enemy troops progress. A sample of commercial and military applications includes (Vaish 2009):

- Environmental monitoring (e.g. traffic, habitat and security)
- Industrial sensing and diagnostics (e.g. appliances, factory and supply chains)
- Infrastructure protection (e.g. power grid and water distribution)
- Battlefield awareness (e.g. multi-target tracking)
- Context-aware computing (e.g. intelligent home and responsive environment)

Permitting sensors to increase applications which use static WSNs, Animals could be attached with sensors to track their migration patterns, feeding habits. Sensors can be attached to unmanned aerial vehicles for surveillance/environment mapping. Such nodes maintain network access to static nodes distributed in an environment with static nodes being suspended by the cable or distributed at surface (Pon et al 2005). Tracking and monitoring doctors and patients inside a hospital: Each patient has a small, light weight sensor nodes attached to them (Akyildiz et al 2002). Doctors can carry a sensor node, allowing other doctors to locate them.

Sensor nodes are also used to detect and identify threats in geographic regions with threats being reported to remote end users through the net for analysis (Akyildiz et al 2002).

Due to sensors reduced computing, radio and battery resources, WSN routing protocols are expected to fulfil the following (Villalba et al 2009):
- **Autonomy**: Assuming that a dedicated unit controlling radio and routing resources does not come in a WSNs way as it could be easily attacked. As there will be no centralized entity to make routing decisions, routing procedures are transferred to network nodes.

- **Energy Efficiency**: Routing protocols must prolong network life while ensuring good connectivity to ensure intra node communication.

- **Scalability**: As WSNs have 100s of nodes, routing protocols must work with these nodes.

- **Resilience**: Sensors may unexpectedly stop operating for environmental reasons or due to battery consumption.

- **Device Heterogeneity**: Though WSNs civil applications rely on homogeny nodes, introduction of various sensors could reap benefits.

- **Mobility Adaptability**: WSNs different applications could make nodes cope with own mobility, sink mobility or mobility of event to sense.

### 1.5 HARDWARE ARCHITECTURE OF SENSORS

The core of the architecture is a central computational engine that is timeshared across application and protocol processing. Ideally, it includes hardware support for efficient, fine-grained concurrency. As is typical in microcontroller designs, the data path is connected to the rest of the system components through a shared interconnection. In advanced designs, this may be a combination of specialized buses. Memory, I/O ports, analog-to-digital converters, system timers and special purpose hardware accelerators are
attached to this interconnection (Hill & Culler 2002). The interaction between the core and its peripherals are through a memory-mapped interface with support for processor interrupts. The peripheral devices signal interrupts upon the completion of a task with the result stored in shared memory.

Besides providing the core a flexible, high bandwidth, low latency connection to the peripherals, the interconnect also allows the individual peripherals to interact with each other. In particular, the special-purpose hardware should be able to stream data into the shared memory for buffering or automatically recording the value of the system timers when an event occurs. The amount of shared memory dedicated to each operation can be set dynamically to meet application requirements. Figure 1.1 is the Hardware architecture of sensors.

![Hardware Architecture of Sensors](image)

**Figure 1.1  Hardware architecture of sensors**

The architecture is said to be free from any specific radio or processing technology but details how computation and communication are brought together (Hill 2003). It is mainly meant for communication subsystem which ensures a flexible, application specific optimization of communication protocols while ensuring high bandwidth and efficiency simultaneously.
1.5.1 Controller

There are several WSN-specific controller implementations that have been proposed by the research community. These controllers try to exploit the WSN-specific characteristics such as event-centric behaviour and asynchronous communication to achieve a lower energy per instruction (Pasha et al 2012). The operating frequency range of some of these controllers is also quite limited (e.g., a Phoenix processor can operate at around 100 KHz). Moreover, all of these processors are manually designed and optimized and no automatic design tool exists for them.

MSP430G2553 series which are ultra-low-power mixed signal microcontrollers have built-in 16-bit timers, up to 24 Input/Output (I/O) touch-sense-enabled pins, a versatile analog comparator with built-in communication capability through use of universal serial communication interface and a 10-bit analog-to-digital converter.

1.5.2 Memory

Data memory has been a very scarce resource in sensor networks. Thus, its efficient utilization is necessary. Allocation of a memory to the dynamic data structures becomes a herculean task on the sensor node as the memory requirement varies depending on the size of the data structure. WSN applications with increasing application domains require efficient dynamic memory allocation techniques to be designed.

1.5.3 Sensors and Actuators

Sensors convert physical parameters to electric outputs (Peura & Webster 2009). An electric output from a sensor is desired due to its advantages in further signal processing. Generally speaking, sensors are
resistive, capacitive and inductive. Sensors are machines that receive and respond to signals which can be produced by energy like heat, light, motion, or chemical reaction.

When a sensor detects one or more signals (an input), it carefully converts them to input signal’s analog/digital representation.

**Sensor examples**

- Hot-wire anemometers – to measure flow velocity
- Accelerometers – to measure acceleration
- Gas sensors - to measure concentration of specific gas
- Humidity sensor
- Temperature sensors, etc.

**Actuator**

An actuator converts electric signals to physical outputs. There are so many actuator types like piezoelectric, electromagnetic, electrostatic and electro-thermal.

**Actuator examples**

- Motors – to produce torque
- Relays – to actuate a device

**1.5.4 Communication Devices**

A communication device exchanges data between nodes and the communication medium between nodes are through radio frequencies which
fit wireless sensor applications requirements as it provides long range and high data rates and acceptable error rates at reasonable energy use. A transmitter and a receiver are required for actual communication in sensor nodes where the task is converting a bit stream from a microcontroller to radio waves.

The transceiver ensures an interface permitting a Medium Access Control (MAC) layer to frame transmissions and hand over the packet from the sensor node’s main memory to transceiver. In the reverse direction, incoming packets are streamed into buffers accessible through MAC protocol. Sensor network communication is split into local coordination and sensor-base communication (Lu et al 2002). Before forwarding information to base stations, local area sensors coordinate to aggregate data and generate reliable results.

Sensor network communication can suffer from “hot regions”, i.e., areas of serious network congestion. Hot regions are due to many related events that synchronously trigger large data flows to a base station. Among sensors a coordination service handles dynamic group management and data aggregation.

1.6 NETWORK ARCHITECTURE

Sensor clustering is based on proximity (in a communication sense) of sensor units to each other (Kottapalli et al 2003). Most WSN architecture follows the Open System Interconnection (OSI) model. Sensor networks have five layers: application, transport, network, data link and physical layers (Alkhatib & Baicher 2012). Three cross layer planes are added to these five layers. Figure 1.2 shows the Architecture of WSN.
Node architecture aims at lowering the cost, increasing flexibility, providing fault-tolerance, improving development and conserving energy. Sensor nodes have a processing unit (MCU-Micro Controller Unit), sensing unit, communication unit and power supply where a node is divided into five blocks with each block having a specific task (Jangra 2010). There are no stable, unified and mature networking’s and system architectures to construct various applications, as applications and research prototypes are integrated to maximize performance.

Network life is the time duration before any sensor group dies which occurs when sensors in a group fail to provide minimum Quality of Monitoring (QoM) or when associated Aggregation Relays node runs out of battery power. To get network life, given each Energy Aware Routing (EAR) node’s battery capacity, energy consumption should be calculated in one recurrent cycle.

1.6.1 Single-hop Networks

Henceforth, a single-hop WSN, without base-station, accurately represents networks used in hot-spot networks, smart-rooms, emergency
environments and in-home networking. When a base-station is an intermediary, direct one-hop transmissions are made two-hop unnecessarily (Shah et al 2005). The base-station must serve as access point to wired Internet and not as peer-to-peer transmissions relay between mobile nodes in wireless networks.

A simple approach uses single-hop broadcast in order to send a message to neighbours and to repeat forwarding a packet on receiving one. To avoid a packet circulating endlessly, a time-to-live value, decremented on each retransmission has been added. Furthermore, the application discards irrelevant packets for a neighbourhood. Though this is a straight-forward solution to communication problems, it does not fulfil its task under network conditions (Schnaufer et al 2006) as a single-hop broadcast is unacknowledged and also it can be destroyed by collisions. Additionally, nodes can re-send a packet, when neighbours and then their neighbours try to re-broadcast it.

Network data aggregation is not required in single-hop (Saha & Bajcsy 2003). Each node independently transmits data to a central processing and logging unit, eliminating sensor nodes complicated aggregation logic. Difficulties in measuring single-hop delay in real networks are many (Papagiannaki et al 2002):

- Timestamps should be accurate to ensure calculation of transit time through routers.
- Data amount for in-depth analysis reaches hundreds of gigabytes. Data from input and output links must be matched to compute time in router.
1.6.2 Multi-hop Networks

In multi-hop wireless networks (Li et al 2005), communication between two nodes goes through many consecutive wireless links and uses routing techniques similar to wired networks.

Unlike wired networks, with a fixed network topology (except in failures), each wireless network node can potentially change network topology by adjusting transmission power to control neighbours. Topology control aims at designing power-efficient algorithms, maintaining network connectivity and optimizing performance metrics like network life and throughput.

Topology control problem is formalized as follows (Li et al 2001): Given a set $V$ of mobile nodes located in the plane. Each node $u \in V$ is specified by coordinates, $(x(u), y(u))$ at any point in time. Each node $u$ has a power function $p$ where $p(d)$ gives minimum power needed to establish communication link to a node $v$ at distance $d$ away from $u$, assuming that maximum transmission power $P$ is same for all nodes and maximum distance for two nodes to communicate directly is $R$, i.e. $p(R) = P$. If every node transmits with power $P$, then induced graph is $G_R = (V,E)$ where $E = \{(u, v) | d(u, v) \leq R\}$ [where $d(u, v)$ is Euclidean distance between $u$ and $v$].

There are many approaches to improve upon multi-hop wireless networks capacity like directional antennas, improved MACs and channel switching. The shortest path algorithm does not perform well when network nodes have multiple radios (Draves et al 2004). Let us consider a two-hop path, where both hops interfere with each other. i.e., only one hop operates at a time assuming that every hop has a bandwidth of $B$. When packet losses are ignored, then anticipated transmission packet time along each hop will be equal. This is denoted by $T$ and it is inversely proportional to $B$. Due to
interference, maximum bandwidth a flow achieves on this path is equal to B/2. As T is inversely proportional to B, the reduced bandwidth idea along the path is captured by giving path a weight equal to sum of packet transmission times on interfering hops; here it is 2*T.

1.6.3 Multiple Sink Networks

A sink normally has higher capacity as well as cost than usual sensor nodes. Sinks can be sensors themselves or devices such as Preserving Data Aggregations (PDAs) or gateways to other larger networks (Poe & Schmitt 2008). For large-scale WSNs, a single-sink model is not scalable, since message transfer delays as well as energy consumption of the sensor nodes becomes prohibitive, due to the fact that many nodes would be far away from sink and thus many hops must be traversed before the sink is reached. As a result, response times become too much and the lifetime of WSN becomes very short. Therefore, it is sensible enough to deploy multiple sinks so that messages reach their destination with fewer hops and consequently response times are decreased and energy can be saved.

Sink nodes amount and exact locations directly affect sensor network life. Hence, for economically feasible investment, a designer must concentrate on correct sink nodes placement (Oyman & Ersoy 2004). Sink nodes exact location is easily found as soon as clustering algorithm is completed. When Euclidean distance is the clustering metric, the center of mass of nodes in a cluster reveals sink nodes location. Depending on routing algorithm’s priorities, power aware distance metrics are also utilized.

Multi-sink WSN design involves deployment of hundreds or thousands of homogenous and energy-limited sensor nodes in areas where information is collected. As a result, sensor nodes sense nearby environment and send information to sinks that are not energy/computing power limited (Huang et al 2010).
1.7  ROUTING PROTOCOLS IN WSN

Sensor data routing is a challenge in WSN research involving multi-hop communications and was studied as part of network layer problems (Akkaya & Younis 2003). Despite similarities between sensor and Mobile Ad-Hoc Networks (MANETs), ad-hoc networks routing approaches proved unsuitable for sensors networks due to varied routing requirements for ad-hoc and sensor networks in various aspects. For example, sensor network communication is from multiple sources to one sink, which is not so in ad-hoc networks.

1.7.1  Data Centric Protocols

Sources send data to sink, but routing nodes enroute scan data content and perform some aggregation/consolidation on data originating from various sources. It helps to consider some scenario classified regarding type and dynamics of data sent by sources (Krishnamachari et al 2002):

1. All sources send completely different information (no redundancy).
2. All sources send identical information (complete redundancy).
3. The sources send information with some intermediate, non-deterministic, level of redundancy.

Data-centric paradigm promises to combine the applications needed to access data (instead of individual nodes) with a natural framework for network processing (Parvin & Rahim 2008). In many applications of WSNs, it is tough to select an explicit set of sensor nodes to be queried precisely because of lack in global identification, along with arbitrary deployment of sensor nodes. This consideration has paved the way for data-centric routing,
which is entirely different from traditional address-based routing where routes are created between addressable nodes.

Sensor Protocols for Information via Negotiation (SPIN) a data-centric routing protocol sends messages through network by negotiation. When a node $A$ wants to send a message, it first sends an Advertisement message (ADV). ADV is used to broadcast meta-data which is a description of the data that is ready to be sent; another node $B$ which receives the ADV and receives the data and then sends Request (REQ) back to $A$ to request data; at last, the node $A$ sends the data to $B$ (Zhao et al 2010).

SPIN’s advantage over blind flooding/gossiping data dissemination methods is in its avoidance of implosion, overlap and resource blindness. Implosion occurs in highly connected networks using flooding and so every sensor receives redundant data copies wasting much energy for larger messages. On the other hand, in SPIN short ADV messages suffer from the implosion problem, but the costly transfer of data messages is greatly reduced (Perillo & Heinzelman 2004).

Overlap is due to redundant nature of the sensor data. So, two sensors with common data send their data, leading to data transmission redundancy and energy waste. SPIN solves this by naming data so that sensors request only data or parts of it they are interested in. Finally, there are three mechanisms in SPIN whereby a sensor low on energy will not advertise its data to save its dwindling energy. Hence, SPIN solves resource blindness through sensors and making decisions based on available resources at current level.

Generally, SPIN protocols are “controlled” flooding protocols, whose aim is addressing “broadcast storms,” overlap problems and resource blindness of usual flooding protocols (Zhong et al 2007). SPIN protocols use
data negotiation and resource-adaptive ideas. Nodes using SPIN perform metadata negotiations prior to every data transmission ensuring no redundancy of data transmission.

### 1.7.2 Hierarchical Protocols

Similar to a cellular telephone network, sensor nodes in a hierarchical routing approach send their data to central cluster-head and the cluster-head then forwards the data to the desired recipient (Parvin & Rahim 2008). Hierarchical routing aims at efficiently maintaining sensor nodes energy consumption by involving them in multi-hop communication in a specific cluster and through performing data aggregation and in undergoing fusion to decrease messages transmitted to the sink. A node in each cluster is selected as leader or cluster head. Schemes for hierarchical routings differ in the method of cluster-head selection and the behaviour pattern of nodes in inter and intra-cluster domain (Villalba et al 2009).

Hierarchical routing protocols reduce energy consumption by localizing communication within clusters and aggregate data to reduce transmissions to Base Station (BS). Low Energy Adaptive Clustering Hierarchy (LEACH) is a popular routing protocol using cluster based routing to minimize energy consumption; the following section describes the LEACH protocol, its architecture, analysis and simulation (Shukla 2013).

LEACH is a cluster-based protocol including distributed cluster formation. It randomly selects some sensor nodes as cluster-heads, rotating this to distribute energy loads evenly among network sensors. In LEACH, cluster-heads compress data from nodes belonging to respective clusters and send aggregated packets to BS to reduce information to be transmitted to BS.
Nodes take autonomous decisions in LEACH to form clusters using a distributed algorithm without centralized control. This needs no long-distance communication with the BS and distributed cluster formation is possible without knowing the location of any network nodes. Additionally, global communication is not needed to set up clusters. Cluster formation algorithms should ensure that nodes are designed as cluster-heads approximately the same number of times, assuming that all nodes start with same energy to prolong network lifetime (Malik et al 2013).

Cluster-head nodes also spread through network, to minimize the distances for non-cluster-head nodes. A sensor node chooses a random number, r, between 0 and 1 and threshold value be $T(n)$:

$$T(n) = \frac{p}{1 - p} \times (r \mod p)$$

If random number is less than a threshold value, $T(n)$, the node becomes a cluster-head for the current round. The threshold value is calculated based on the equation 1.1 that incorporates the desired percentage to become a cluster-head, the current round, and the set of nodes have not been selected as a cluster-head in the last $1/p$ rounds, $p$ is cluster-head probability.

### 1.7.3 Location Based Protocols

Most sensor network routing protocols need location information for sensor nodes (Akkaya & Younis 2005). This is needed to calculate distance between two nodes to estimate energy consumption. As sensor networks have no addressing schemes like Internet Protocol-addresses and as they are spatially deployed regionally, location information is used to route data energy efficiently.
An adaptive fidelity algorithm is Geographic Adaptive Fidelity (GAF) (Rathi et al 2012) where many sensor nodes are in an observed area of which only a few are permitted to transmit messages. The other nodes sleep. Thus, GAF reduces nodes needed to form a network saving battery. Each node uses location information to associate itself to a virtual grid (Agrawal & Raut 2013). Nodes in same grid square are equal regarding packet forwarding taking turns to sleep and being awake to balance energy consumption. GAF is dependent on an underlying ad-hoc routing protocol.

Hierarchical Geographical Adaptive Fidelity (HGAF) saves more battery by enlarging GAF cell through the addition of a layered structure to choose an active node in each cell. GAF saves battery power by enlarging cell size. Connectivity between active nodes in two neighbouring cells is ensured as active nodes work as cluster-heads to deliver packets between cells. GAF needs an active node in all areas whose maximum size is $R^2/5$ due to this limitation.

To obtain $R^2/5$ through an upper bound on how much GAF may extend network lifetime we next consider a very simple analytical model. Assume that $n$ nodes are evenly distributed in a area with topography size $A$. Nominal radio range for each node is $R$. According to equation $r^2 + (2r)^2 \leq R^2$ or $r \leq R/\sqrt{5}$, the grid size can be set as $R/\sqrt{5}$ which is the maximum size of a virtual grid.

1.7.4 QoS Based Protocols

QoS based protocols ensure sensor nodes balance between energy consumption and pre-determined QoS metrics like delay, energy, reliability and bandwidth, before delivering data to sink node. Sensor nodes have low processing capability, low memory power and limited transmission energy in addition to energy constraints. Hence the constraints impose an important requirement on wireless sensor network QoS support mechanisms including
simplicity. Traffic flows from many sensor nodes to a small subset of sink nodes in most WSN applications. QoS mechanisms must be made for unbalanced QoS-constrained traffic.

A sensor node must route traffic according to QoS requirements as stated below:

1) Priority level based route traffic.
2) Reduce delay to relay event-based packets.
3) Ensure event alerts delivery.
4) Deliver periodic data reporting packets with a best effort policy.

The routing protocol prevents congestion and is energy-efficient to prolong network life. Every data reporting packet includes the following fields:

(i) Source sensor id
(ii) Source sensor location
(iii) Sink id
(iv) Sink location
(v) Next hop
(vi) Reporting type
(vii) Reporting attributes/event
(viii) Reporting time

The last has the time when data was recorded by source sensor.
Quality-Based Reimbursement Program (QBRP) is a QoS based routing protocol that simultaneously meets application requirements for high reliability of delivery, low latency, uniform energy consumption and fault tolerance. It uses interactions among sensors advantageously to ensure better QoS WSN solutions.

Sequential Assignment Routing (SAR) is a WSN routing protocol that first introduces QoS in routing decisions. The aim of SAR algorithm is to reduce average weighted QoS metric throughout network lifetime. Another wireless sensor network QoS routing protocol that ensures soft real-time end-to-end guarantees is SPEED that ensures avoidance of congestion during network congestion.

Diff-MAC is a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based QoS-aware MAC protocol with differentiated services and hybrid prioritization. Diff-MAC aims at increasing the utilization of the channel with effective service differentiation mechanisms while providing fair and fast delivery of the data. Primary application field of the Diff-MAC is wireless multimedia sensor networks which commonly carries QoS-constrained heterogeneous traffic.

Equalizer-MAC (EQ-MAC) is designed to provide QoS support for cluster based single-hop sensor networks by service differentiation and uses a hybrid medium access scheme. The protocol is composed of two parts: Classifier- MAC (CMAC) and Channel Access MAC (CA-MAC).

1.8 PROBLEM STATEMENT

Energy usage in WSN is critical as it may not be possible to replace or recharge batteries in nodes. Network life expectancy is based on the energy available in the nodes. Routing in WSN are mostly based on proactive or
reactive methods; in the former, routes are stored in routing tables whereas in the latter, routes are discovered when required.

Data aggregation algorithm’s goal is in gathering and aggregating data energy efficiently so that network life is enhanced. In WSN there are the routing protocols that minimize the used energy, extending subsequently the life span of the WSN. In densely deployed WSN networks, maintaining routing tables necessitates huge amount of memory. To mitigate the necessity of the routing tables, hybrids methods based on proactive and reactive are used. Clustering of the network into a hierarchical network is another possible solution.

QoS is accepted as service quality that a network provides applications/users. QoS is an assurance to provide measurable service attributes to end-to-end users/applications regarding delay, fairness, available bandwidth, jitter and packet loss. A network must ensure QoS while maximizing network resource use. To achieve this, a network has to analyze application requirements and use varied network QoS mechanisms. It is seen from literature that achieving required QoS is Non-deterministic Polynomial (NP) hard and solving it with Evolutionary Algorithm is an emerging research area. But not much was done in WSN to achieve QoS using EA techniques. This work aims at investigating EA techniques and proposing improvements over current techniques.

1.9 OBJECTIVES

Computational Intelligence (CI) consists of adaptive mechanisms that have the ability to generalize, associate and learn new situations, thus enabling intelligent behaviour in complex and changing environments. Most of CI is fundamentally based upon biological intelligence such as neural networks, swarm intelligence, evolutionary algorithms and so on. Researchers
have used CI techniques to address challenges in WSNs successfully. The objective of this research is stated as under:

- To evaluate the performance M-LEACH, GA-LEACH in WSN routing
- To propose an improved WSN routing with Bacterial Foraging Optimization (BFO) technique
- To introduce a novel Hybrid BFO algorithm to avoid local minima
- To identify an improved data aggregation technique using Travelling Salesman Problem (TSP)

1.10 THESIS ORGANIZATION

Chapter 1 discusses the various dimensions of the WSN like the sensors, network architecture and various routing. Chapter 2 reviews the available works in the literature related to clustering in WSN and mainly focuses on the optimization techniques used in WSN.

Chapter 3 throws light on the performance of genetic optimized routing in WSN. Chapter 4 speaks about the proposed BFO technique to improve the WSN routing. Chapter 5 discusses in detail on the improvements implemented using the proposed BFO. Chapter 6 concludes the research work.