CHAPTER 2

BACKGROUND OF NETWORK ROUTING

2.1 ROUTING

Wireless sensor networks are extremely versatile and can be deployed to support a wide variety of applications in many situations, whether they are composed of stationary or mobile sensor nodes. The way these sensors are deployed depends on the nature of the applications. In environmental monitoring and surveillance applications, for example, sensor nodes are deployed in an adhoc fashion so as to cover the field to be monitored. In health care applications, smart wearable wireless devices can be attached to the human body to monitor vital signs of the patients. Once deployed, sensor nodes organize themselves into an autonomous wireless adhoc network, which requires very little or no maintenance. Sensor nodes then collaborate to carry out the tasks of the applications for which they are deployed (kazemsohraby et al 2010).

Despite the disparity in the objectives of sensor applications, the main task is of WSN is to sense and collect target data, process such data and transmit the information back to the sink. Efficient achievement of this task requires the development of energy - efficient routing protocol to set up paths between the source node and the sink. The path election must be such that the life time of the network is maximized. The characteristics of the environment within which sensor nodes typically operate, coupled with sever resource and energy limitation, make the routing problem very challenging.
Routing is the process of forwarding the data packets over the network from source to destination by selecting the best path. Many routing protocols are proposed in the area of wireless sensor networks by researchers to overcome the issues faced during transmission phase.

In the following sections, the primary challenges, design goals, strategies and various techniques have been proposed for routing in wireless sensor networks are discussed (KazemSohraby et al 2010).

2.2 ISSUES AND CHALLENGES IN ROUTING

Although WSNs share many commonalities with wired and adhoc networks, they also exhibit a number of unique features which distinguish them from existing networks. These unique characteristics bring sharp focus to new routing design requirements that go beyond those typically encountered in wired and wireless adhoc networks. Meeting these design requirements presents a distinctive and unique set of challenges. These challenges can be attributed to multiple factors, including severe energy constraints, limited computing and communication capabilities, the dynamically changing environments within which sensors are deployed, and unique data traffic models and application-level quality of service requirements (KazemSohraby et al 2010).

Designing efficient routing protocols for wireless sensor networks is a challenging task due to several constraints. WSNs are subjected to the limitations of the network resources like limited available energy level and bandwidth (Jamal Al-Karaki & Ahmed Kamal 2004) (Kemal Akkaya & Mohamed Younis 2005). The design challenges involve the following main aspects.
2.2.1 **Restricted Power Capacity**

Since sensor nodes are battery power-driven, they have inadequate energy capability. For network designers, energy constraint poses a huge challenge. For example, in landslide detection, once sensor nodes are deployed, it is not possible to access the sensor nodes and recharge their batteries. Also, when the energy level of a sensor node attains a threshold, it becomes faulty and reduces the lifetime of the entire network. Energy efficient routing protocols should be proposed to enhance the network lifetime for this reason.

2.2.2 **Sensor Locations**

Establishment of best route during the movement of sensor node is another challenge that may lead to efficient routing protocols to handle the location of the sensor nodes. Protocols proposed may have the assumption that the nodes are equipped with location detecting device like global positioning system (GPS) or may use localization methods to find the location of the sensor nodes.

2.2.3 **Limited Hardware Resources**

Sensor nodes face limited processing and storage capacities and so, only limited computation can be performed for a sensor node. Designing of routing protocol should consider the limitations in hardware resources in the development of an energy efficient healthy path between the sender and receiver.

2.2.4 **Node Deployment**

Deployment of sensor nodes in a wireless sensor network is application dependent and it may be of manual or random. This behaviour
affects the entire performance of the network and finally it may lead to the implementation of efficient routing protocol to allow connectivity and to reduce the power consumption.

2.2.5 Network Features and Unpredictable Environment

The environment in which the sensor network operates is usually dynamic and unreliable. Topology gets changed due to the mobility of node. Managing the topology of the network due to node failure, node insertion is another one issue in routing which affects the performance of entire network. Also, the medium where the signal travels is of wireless which is error prone and, as a result the link existing between the sensor nodes may get weak. So that a routing protocol should act effectively possess topology management schemes even in unreliable environment.

2.2.6 Data Aggregation

A sensor node in a network may receive the same data repeatedly from various sensor nodes in the network. The redundant data reduces the energy level of the sensor and so the similar data can be aggregated to reduce the number of transmissions thereby achieving energy efficient routing protocols.

2.2.7 Scalability

Protocols available for routing should have the ability to scale with the network size (Shio Kumar Singh et al 2010). The sensor network is densely deployed. In mobile sensor networks, the nodes mobility suddenly rise or down the network size.
2.3 TAXONOMY OF ROUTING PROTOCOLS

Routing protocols of WSNs can be classified into several types based on different criteria. A classification tree of routing protocols is shown in Figure 2.1 (Jamal Al Karaki & Ahmed Kamal 2004, Tilak et al 2002). Some of the classes, their properties, and the basis of classifications are discussed below. The classification is not mutually exclusive and some protocols fall in more than one class. The routing protocols for WSNs can be broadly classified into:

i. Mode of functioning

ii. Network structure

iii. Participating style of nodes.

![Classification of Routing Protocols Diagram]

Figure 2.1 Taxonomy tree of routing protocols

2.3.1 Based on Mode of Functioning

Wireless sensor routing protocols can be classified into three categories based on the mode of functioning. They are:
2.3.1.1 Proactive routing

This is a table driven routing protocol. Every node maintains the network topology information in a base called the routing table. Changes in the network are updated frequently in the routing table to avoid improper routing. Based on the table, a routing path is established through which the data gets forwarded. Whenever a node requires a path to the destination, it runs an appropriate path-finding algorithm on the topology it maintains. The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol is an example for proactive routing protocol.

2.3.1.2 Reactive routing

It is a on-demand routing protocol with no routing table being maintained. The nodes obtain the path when required, by using some control packets like route request and route reply for connection establishment process. The Threshold sensitive Energy Efficient sensor Network (TEEN) is an example for reactive protocol.

2.3.1.3 Hybrid routing

It combines the best feature of proactive and reactive approaches. Nodes within the certain distance from the node concerned, or within a particular geographical region, will use the proactive approach. The nodes beyond this zone use the reactive approach. Adaptive Periodic Threshold sensitive Energy Efficient sensor Network (APTEEN) is an example for hybrid protocol.
2.3.2 Based on Participating Style of Nodes

2.3.2.1 Direct communication

The packets are sent directly to the base station by the nodes. Due to this behaviour the energy drains out quickly. An example for direct communication protocol is SPIN (Sensor Protocols for Information via Negotiation).

2.3.2.2 Flat

If a node wants to transmit the data, it first searches the route to the base station and then transmits it. Nodes close to base station drain out quickly compared to other nodes. Rumour routing is an example for flat protocol for routing.

2.3.2.3 Clustering protocols

In this approach the entire sensor field is divided into many clusters and the data is forwarded through the cluster head. The cluster head from each cluster may communicate directly or through other cluster heads to the base station. TEEN protocol is an example of the clustering approach.

2.3.3 Based on Network Structure

2.3.3.1 Data centric

In data centric routing approach the query raised is based on data and thus it eliminates the redundant transmission. SPIN is the example for data centric protocol.
2.3.3.2 Hierarchical

Based on the energy, the hierarchy is made and the higher energy nodes play the main role of processing and data forwarding and other nodes only participate in sensing process. LEACH, TEEN protocols are example for hierarchical based routing.

2.3.3.3 Location based

It is a location based routing protocol. Location information can be received from a location finding device and an optimal path can be found out to forward the packets. Geographic and Energy-Aware Routing (GEAR) is an example for location based routing protocol.

2.4 ROUTING PROTOCOL METRICS

In a wireless sensor network, the overall performance of routing to find best path can be measured using the following metrics. The existing routing metrics are classified as Topology based, Signal strength based, Beaconing based, Mobility aware and Energy aware metrics.

2.4.1 Topology Based Metrics

In Topology Based routing, the network topological information considered for selecting the best path depends on the number of neighbours of each node, number of hops and/or paths towards a particular destination. The metrics always consider connectivity information which is available locally by the routing protocol, without requiring additional passive or active measurements. The topology-based metrics do not consider any Qos based parameters.
(i) **Hop count**

The hop count is the number of network devices between the starting node and the destination node. The number of point-to-point link in a transmission path. Since each link is terminated at a network device such as a router or gateway, the processing performed within the device to determine how to forward the packet adds overhead to the transmission. The ease of implementation has made hop count the most widely used metric in wired networks. It is the default metric in many wireless sensor networks routing protocol.

### 2.4.2 Signal Strength Based Metrics

The signal strength can be viewed as a good indicator for measuring link quality since a packet can be transferred successfully when the signal strength is more than the threshold value. This can be measured by the Received Signal Strength Indicator (RSSI). The Signal based techniques exclude 'bad' quality links from the routing process. It is reported that high signal strength implies low packet loss, however low signal strength does not necessarily imply high packet loss.

### 2.4.3 Beaconing Based Metrics

Probing or Beaconing techniques eliminate the issues in topology based routing. These techniques have various challenges such as packet sizes of beacon packets or beacon packets in the network should be equal to the data so that what the beacon measures is as close to the target as possible. Beacon packets should not give any priority in the network. The Beaconing based metrics have proved promising in the context of wireless sensor networks. They measure directly the quantity of interest, rather than inferring
it from indirect measurements, and do not rely on analytical assumption. Some of the beacon based metrics are discussed below.

(i) **Per-hop Round Trip Time (RTT)**

The per-hop Round-Trip Time (RTT) metric is based on the bidirectional delay on a link. In order to measure the RTT, a probe packet is sent periodically to each neighbouring node with time stamp. Then each neighbour node returns the probe immediately. This probe response enables the sending node to calculate the RTT value. The path RTT metric is the summation of all links RTT in the route. The RTT metric is dependent on the network traffic.

(ii) **Per-hop packet pair delay**

The per-hop packet pair delay is designed to overcome the problem of distortion of RTT measurements arising from queuing delays and it consists of periodic transmission of two probe packets with different sizes back-to-back from each node. The neighbour node calculates the inter-probe arrival delay and reports it back to the sender. This metric is less susceptible to self-interference than the RTT metric, but it is not completely immune, as probe packets in multi-hop scenario contend for the wireless channel with data packets. Both the RTT and Packet pair metrics measure delay directly, hence they are load-dependent and prone to the self interference phenomenon. Moreover, the measurement overhead they introduce is $O(n^2)$, where $n$ is the number of nodes.

(iii) **Expected Transmission Count (ETX)**

The Expected Transmission Count (ETX) is one of the first routing metrics based on active probing measurements specifically designed for
MANETs. For overcoming the drawbacks of RTT and Packet pair techniques, the authors propose Expected Transmission Count (ETX) metric which is first routing metric based on active probing measurements designed for wireless sensor networks. ETX estimates the number of transmissions required for sending a packet over a link. Minimizing the number of transmissions optimize the overall throughput and energy consumption. The expected number of transmissions is defined as

$$ETX = \frac{1}{d_f d_r}$$  \hspace{1cm} (2.1)

Where $d_f$ and $d_r$ are expected forward delivery ratio and reverse delivery ratio respectively which are measured using link-layer broadcast probes.

(iv) Expected Transmission Time (ETT)

Expected Transmission Time (ETT) metric incorporates the throughput into its calculation. Let $S$ be the size of the probing packet and $B$ the measured bandwidth of a link, then the ETT of this link is defined as

$$ETT = ETX \times \frac{S}{B}$$  \hspace{1cm} (2.2)

2.4.4 Mobility-Aware Metrics

Mobile aware metrics need to consider the changing nature of the network parameters like distance, position, link quality. There is a need for regular updating of routing parameters to balance the mobility of the nodes. The metrics largely use signal strength measurements and their rate of variation to infer the stability of links and routes. Mobility-aware metrics aim at the selection of routes with higher expected lifetime to minimize the routing overhead related to route changes and their impact on throughput. The
metrics largely use signal strength measurements and their rate of variation to infer the stability of links and routes.

(i) **Link associativity ticks and path average degree of association stability**

Sensor nodes transmit beacon packets at fixed time intervals and calculate the received number of probes from their neighbours. These values serve as indicators of the actual stability of the link. Low values of associativity ticks imply mobile nodes in high mobility state, whereas high associativity ticks, beyond some threshold value are obtained when a mobile node is stable.

(ii) **Link affinity and path stability**

The affinity of a link is related to the received power over that link, its rate of change and a threshold, determining whether the link is broken or not. Each node calculates the strength of the signal received periodically. The route is selected as long as the estimated value for its stability exceeds the required time to transfer data, whose estimate equals the time required to transmit data over the link capacity.

**2.4.5 Energy-Aware Metrics**

Energy consumption may represent an essential constraint in wireless mesh networks. Sensors as well as small and battery operated wireless devices have restricted battery lifetime and are most vulnerable to the energy constraints. The total energy consumed when sending and receiving a packet is influenced by various factors such as the wireless radio propagation environment, interference from simultaneous transmissions, MAC protocol operation, and routing algorithm. The main objective of energy aware metrics
is to minimize overall energy consumption and to maximize the time until the first node runs out of energy.

(i) **Minimal Total Power routing (MTPR)**

Minimal Total Power Routing metric (MTPR) is meant to minimize the overall energy consumption. It is computed using the distributed Bellman-Ford algorithm. The average transmission power of the nodes in the path is considered for computing MTPR. A disadvantage of this packet-oriented metric is that it does not directly take into account the nodes remaining battery lifetime. It is quite probable that seeking for routes that minimize the per-packet energy consumption, one might end up with nodes that forward traffic from multiple concurrent flows and consume their battery power much faster than other nodes.

(ii) **Minimum battery cost routing (MBCR)**

The Minimum Battery Cost Routing is based on the remaining battery capacity of the node. The ratio of battery capacity is defined as

\[
R_{brc} = \frac{\text{Battery remaining capacity}}{\text{Battery full capacity}}
\]  

(2.3)

(iii) **Min-Max Battery Cost Routing (MMBCR)**

The objective of MMBCR metric is to avoid low residual energy nodes in the routing path. The idea is to select a path, which minimizes the maximum power required at any node in a network.

The above routing metrics can be considered to measure the efficiency of the routing protocol for wireless sensor network.
2.5 ROUTING ALGORITHM CLASSIFICATIONS

Routing algorithms can be classified based on the updated routing mechanism, topology and utilization of resources.

2.5.1 Adaptive Routing Algorithm

Due to the mobility of nodes, the network topology gets changed. Adaptive routing algorithm change their routing decisions based on the optimized parameters distance, number of hops and estimated transit time. It needs to recompute the route continuously.

2.5.2 Non-Adaptive Routing Algorithms

These algorithms are termed as static routing algorithms that will decide the route based on the measurements of current traffic and topology and it’s computed in advance. Maintaining routing table is easy for smaller networks in the case of static routing compared to dynamic.

2.6 EXISTING ROUTING ALGORITHMS

Various routing algorithms are proposed for efficient data delivery. Routing refers to delivery of data to the correct destination without any loss. For successful delivery, link quality and the energy levels of sensor nodes through which the data has to travel get assessed. Here some of the algorithms are focussed that help link quality assessment and cluster head based data forwarding.

2.6.1 Cluster Based Routing

In cluster based routing approach, the entire sensor network is split into many clusters and one cluster head among several clusters is elected
based on some criteria. The cluster head is fully responsible for routing the packets to the destination.

2.6.1.1 Low Energy Adaptive Clustering Hierarchy (LEACH)

It is a clustering based protocol which randomly elects its cluster head based on the energy of sensor nodes. It is self-adaptive and self-organised. This protocol randomly elects the cluster head and performs periodic re-election. Each iteration of cluster heads is termed as round and it uses round as unit and each unit is divided into two phases namely set-up and steady state phase. The LEACH protocol process is shown in Figure 2.2.

At the set-up stage, each sensor node chooses a random number between 0 and 1. A threshold value $T(n)$ is calculated using Equation (2.1) and if the value is less than the threshold for node ‘n’ then the sensor node acts as a cluster head. The threshold can be calculated as

$$T(n) = \begin{cases} 
\frac{p}{1 - P(r \mod \left(\frac{1}{p}\right))} & \text{if } n \in G \\
0 & \text{otherwise} 
\end{cases} \quad (2.4)$$

Where

- $p$ – desired percentage of nodes which are cluster heads.
- $r$ – current round
G – set of nodes that has not been elected as cluster head in past \((1/p)\) rounds.

The LEACH clustering is shown in Figure 2.3

![Figure 2.3 Clustering in LEACH](image)

Once the cluster head is elected, it advertises its selection to all the other nodes, which choose their cluster heads based on the received signal strength. The cluster heads then assign TDMA for their members. The data transmission in steady state takes place based on the schedule assign to cluster members. The cluster heads aggregates the data received from its members and aggregated data is forwarded to the base station. This protocol utilises the available energy of all sensor nodes equally (Siva Ram Murthy 2012) (Chunyao et al 2013).

2.6.1.2 **Hybrid Energy Efficient Distributed Clustering (HEED)**

It is one of the most effective cluster based protocol where the cluster head is elected based on two parameters. The primary parameter used is residual energy of sensor nodes and the secondary parameter is node degree and node proximity to achieve power balancing (Wail Mardini et al 2014). It extends the basic scheme of LEACH protocol. The clustering process is
divided into a number of iterations, and in each iterations, nodes which are not covered by any cluster head double their probability of becoming a cluster head. Since these energy-efficient clustering protocols enable every node to independently and probabilistically decide on its role in the clustered network, they cannot guarantee optimal elected set of cluster heads (Ossama Younis & Sonia Fahmy 2004). HEED operation carried out in three phases namely, initialization phase, processing phase and finalization phase. In the initialization phase, sensors put their probabilities to become CHs and, in the processing phase in which the sensors go through many steps to elect the CHs and the finalization phase in which each sensor join the least communication-cost CH or announce itself as a CH. The re-clustering in HEED is triggered dynamically at the beginning of each round which is a predefined period of time; the round in HEED can be in the range of seconds, minutes or even hours depending on the application at hand (Wail Mardini et al 2014). In HEED if Cluster node is near to the base station then node directly communicate with the base station and discharge quickly and energy is wasted that is used for formation cluster head (Roshani Kushavaha et al 2014). The diagrammatic representation of HEED protocol is shown in Figure 2.4.

![Figure 2.4 Diagrammatic representation of HEED protocol](image-url)
2.6.1.3 A Cluster-Head Election Algorithm for WSN using a Takagi-Sugeno Fuzzy System (CHEATS)

This protocol considers the use of residual energy and distance of node to the base station for the election of cluster head. This algorithm changes the set up phase and maintains the steady phase of LEACH. During the set up phase, base station broadcasts “hello” message to all the nodes in the network and each node calculate its distance based on received signal strength and adjust its transmission power to the distance. Then it finds its probability of becoming a cluster head using fuzzy logic.

2.6.2 Link Quality Based Routing

Routing a packet to the destination depends not only on the characteristics and behaviour of sensor nodes, but also on the quality of communication wireless link virtually connecting two nodes. Once the packet is transmitted by a source, it may fail to reach the destination due to collisions, traffic, path break, interference etc. in addition to energy drop and mobility criteria. In view of these constraints, link quality during routing has to be estimated for efficient delivery. Some of the software based link quality existing estimators are discussed below.

2.6.2.1 Packet Reception Rate (PRR) protocol

This approach either counts or approximates the packet reception rate. It can be computed as the ratio of number of received packets to the number of transmitted packets. It can be calculated as

\[ PRR(w) = \frac{\text{number of received packets}}{\text{number of send packets}} \] (2.5)
By observing the packet reception rate the quality of the link is estimated and, based on the status, route is established. But the disadvantage in this approach lies in its dependence on the adjustment of the time window size. So the links with very low or high PRR can bring out accurate link estimation within narrow window size. But larger window size is required to meet accurate link quality if it possess medium PRR (Cerpa et al 2005) (NouhaBaccour et al 2013).

2.6.2.2 Required Number of Packet Transmissions (RNP) protocol

It is a sender side estimator which finds out the status of the link by observing number of packet transmitted and re-transmitted required before reception. For each transmitted and retransmitted ‘w’ packets, RNP is calculated using Equation (2.3) which is given by

\[ RNP(w) = \frac{number\ of\ transmitted\ and\ retransmitted\ packets}{number\ of\ successfully\ received\ packets} - 1 \quad (2.6) \]

This protocol uses Automatic Repeat Request (ARQ) protocol where a node repeats its transmission until it is successfully received. For characterizing the link quality RNP is better than PRR. The drawback in RNP is due to link asymmetry, the packet delivery is not estimated properly. So that this approach is unstable and not reliable (NouhaBaccour et al 2013).

2.6.2.3 Window Mean with Exponentially Weighted Moving Average (WMEWMA)

It is a receiver side link quality estimator. To smoothen PRR it uses EWMA filter, thus providing a metric that resists transient fluctuation of PRRs and is responsive to major link quality changes. It is given by

\[ WMEWMA(\alpha, w) = \alpha \times WMEWMA + (1-\alpha) \times PRR \quad (2.7) \]
Where $\alpha$ – smoothing factor which controls the smoothness. It varies from 0 to 1.

### 2.6.2.4 Expected Transmission Count (ETX) protocol

It is a receiver initiated protocol which approximates the packets retransmission count. Each node in the network explicitly broadcasts the probe packets to collect the statistical information. Bidirectional link quality is estimated i.e., estimating uplink quality from the sender to the receiver side ($\text{PRR}_{\text{forward}}$) and downlink quality from receiver to sender side ($\text{PRR}_{\text{backward}}$) by considering symmetry level of the link. It is calculated using the Equation (2.8)

$$
ETX(w) = \frac{1}{\text{PRR}_{\text{forward}} \times \text{PRR}_{\text{backward}}} 
$$

(2.8)

The drawback in ETX is in overloaded networks its monitoring fails to work.

### 2.6.2.5 Four-bit

In four-bit link quality estimator, to find the status of the link four factors are considered into account: two bits from network layer, one bit from link layer and one bit from physical layer. To strengthen this four bit link quality estimation RSSI and PRR information gets combined and filtering mechanisms are added to reduce routing losses. It is given by

$$
\text{fourbit}(w_a, w_b, \alpha) = \alpha \times \text{fourbit} + (1 - \alpha) \text{estETX} 
$$

(2.9)

Where

- estETX corresponds to estETX$_{up}$or estETX$_{down}$
- $w_a$ – received probe packets
- $w_b$- transmitted/re-transmitted data packets.
The four-bit LQE is shown in figure 2.5

![Diagrammatic representation of four-bit LQE](image)

**Figure 2.5 Diagrammatic representation of four-bit LQE**

The probability of decoding error is indicated by white bit from physical layer and for each successful transmission link layer provides the acknowledgement (ack) bit. The pin bit and compare bit are related to network layer. The pin bit applies to link table entries. When the network layer sets the pin bit on an entry, the link estimator cannot remove it from the table until the bit is cleared.

A link estimator can ask a network layer for a compare bit on a packet. The compare bit indicates whether the route provided by the sender of the packet is better than the route provided by one or more of the entries in the link table. Using this approach the data transmission can be more accurate and more reliable in wireless sensor networks thus making the network long term and stable (An Zhou et al 2015) (NouhaBaccour et al 2013).