Chapter 2

State of the Art on Routing Protocols for Wireless Sensor Networks

2.1 Introduction

2.2 Limitations, Characteristics of WSN Routing and Routing Challenges in Wireless Sensor Networks

2.3 Routing Protocols for Wireless Sensor Networks

   2.3.1 General Routing (Non-Secure) Protocol

       2.3.1.1 Flat Network Routing Protocol
       2.3.1.2 Hierarchical Routing Protocol
       2.3.1.3 Location based Routing Protocol

   2.3.2 Secure Routing Protocol

2.4 Conclusion
In this chapter, a literature survey on the general routing and secure routing protocols for Wireless Sensor Networks is reported. The unique characteristics and limitations of Wireless Sensor Networks are discussed. The routing challenges regarding routing in Wireless Sensor Networks are also mentioned. Taxonomy of the current routing protocols is also included. This chapter includes a global view of the research in the area of routing and secure routing in Wireless Sensor Networks.
2.1 Introduction

A wireless network uses wireless radio as the communication medium. A wireless network enables users to access information and related services irrespective of their physical and geographical locations. There are basically two broad classes of wireless networks namely infrastructure-based and infrastructure-less networks. Infrastructure-less networks are popularly known as ad-hoc networks. Infrastructure-based networks consist of several fixed Base Stations covering a particular geographic region. In infrastructure-based networks, fixed Base Stations are connected by wires and the mobile hosts or users can connect to the fixed Base Stations through wireless links. Such an arrangement gives mobility to the users and enables the users to move around within the communication range of the Base Station and still they get the access to the network. Whenever a mobile host moves out of the communication range of the currently connected Base Station, the mobile host may connect to another Base Station in its proximity for remaining connected to the network and for further communication. In infrastructure-based networks a backbone (wired network) remains active throughout the operations of such networks.

In contrast to the infrastructure-based networks the infrastructure-less networks consist of only the mobile hosts connected by the wireless links. There is no fixed Base Station and no wired links and such a network is completely ad-hoc in nature. These networks are self configuring in nature. The hosts can move freely and they organize themselves into a network in an arbitrary fashion. The infrastructure-less networks need minimal configuration and these are possible to deploy quickly. The expenditure involved against such deployments is also minimal in comparison to that of infrastructure based networks. Such networks are very useful in emergency situations such as disaster relief operations, military applications etc.

Wireless sensor network is a kind of ad hoc network, which contain hundreds or thousands of sensor nodes equipped with sensing, computing and communication circuitry. Each sensor node consists of such electronic circuitries which give them ability to sense different parameters of their deployment environment (i.e., environment sensing), perform necessary computations (i.e., processing of signals), and also communicate with other sensor nodes and the external Base Station or Sink node (i.e, networking for data communication). The deployment of the sensor nodes may happen either randomly or in a planned manner depending on the application type. Such networking platforms promise a fault-tolerant and free of maintenance mechanism for gathering different kinds of data from the areas of interest. However, the sensor nodes are constrained in many aspects such as limited energy supply, limited computing power, limited bandwidth for communication etc. Such constraints pose different and many challenges against the development and management of wireless sensor networks. The limited energy supply to the sensor nodes imposes necessity of energy-conserving communication protocols and due to the limited computing power of the sensor nodes, the wireless sensor networks can not run highly sophisticated network protocols. Moreover, since the available bandwidth for communication among the sensor nodes is limited, the inter sensor communication becomes constrained. All these constraints of
wireless sensor networks put challenges at all the layers of the protocol stack but one common observation is that it is necessary to have energy-awareness at all layers of the protocol stack. There has been research effort for optimal use of the available energy in wireless sensor networks. In [41][42], focus is on system level power awareness such as dynamic voltage scaling. There are several reported research results on energy efficiency in the medium access control layer. These are energy efficient medium access control protocols for wireless sensor networks [43][44][45]. At the network layer, main aim is to find out energy efficient mechanism for route set up through which data can be forwarded from the source node towards the Base Station (or Sink node) with reliability and with minimum overall energy expenditure. The network lifetime needs to be optimized. Reliability in packet routing is well studied for wired network. Multi-path routing is a mechanism to ensure reliability. In [46][47][48][49][57] multi-path routing protocols are proposed for wired networks. As these are table driven routing protocols, they demand significant memory space at each intermediate router. As a whole, routing in communication network is an important issue and also a challenging task [18].

Though the wireless ad hoc networks and wireless sensor networks share several similarities, the major difference is that the wireless sensor networks suffer from severe resource constraints such as energy supply and bandwidth availability. In other words, the wireless ad hoc networks are resourceful in comparison to the wireless sensor networks. That is the main reason why the protocols and algorithms designed for wireless ad hoc networks are not directly applicable to the wireless sensor networks.

The wireless sensor networks can be time-driven or event-driven depending on the application and time criticality of data reporting. The time-driven wireless sensor networks are those which require periodic data monitoring and data reporting. The event-driven sensor networks react immediately to sudden changes in the value of certain parameters being sensed due to occurrence of some certain event(s). This category of wireless sensor network is suitable for time critical applications. A hybrid of these two types of network is also possible and has got different applications in real life.

It is also necessary to ensure security in the wireless sensor network and at times it becomes extremely important to make the network secure depending on the application type e.g., battle field applications, mission critical applications etc. There are different security threats present at different layers of the protocol stack [84][85]. The network layer suffers from different security threats and design of secure routing protocols is again necessary depending on the application type.

This chapter introduces different general routing and secure routing protocols proposed for wireless sensor networks. The limitations of wireless sensor networks, characteristics of wireless sensor network routing and routing challenges in wireless sensor networks are discussed in this chapter. Taxonomy of the routing protocols is also included. This chapter also introduces current research directions in the area of routing and secure routing in wireless sensor networks.
Chapter 2

2.2 Limitations, Characteristics of WSN Routing and Routing Challenges in Wireless Sensor Networks

In this section different limitations of sensor nodes are discussed. The unique characteristics of wireless sensor network routing are outlined. And the challenges in the design of routing protocols for wireless sensor networks are also mentioned.

a) Some of the limitations of WSN

The wireless sensor networks suffer from several limitations. These are enlisted below:

Limited Energy Supply: The sensor nodes are equipped with battery and those are driven by these batteries. Due to the harsh environment where the sensor nodes are deployed, it is not possible to refuel the battery of a sensor node. Therefore, the available energy level with each sensor node is limited and it has to be utilized optimally.

Limited Computing Capability: The sensor nodes are simple in their architecture and this simple architecture is adapted to keep the cost of the sensor node at low level. So, the simple and tiny sensor nodes cannot perform sophisticated and complex computation.

Limited Storage: The available memory with each sensor node is very limited and this is adapted again to avoid the high cost involved in manufacturing the sensor nodes. Ideally the sensor nodes are of low cost so they are equipped with less memory space as well. Therefore, it is extremely difficult to run those protocols and algorithms which demand high memory space. This implicates the network protocols are algorithms are to be simple enough and lightweight.

Limited Communication Bandwidth: The bandwidth of the wireless communication links connecting sensor nodes is limited; and this fact poses constraints in the communication among the sensor nodes and communication with the Base Station.

Dynamic Topology: The topology of the wireless sensor network is dynamic because of the sudden death of the sensor nodes. When the sensor nodes move the topology of the network becomes even more dynamic. The dynamic topology makes the network protocols unstable and demands frequent changes in the network settings. Thus it may lead to rapid decay in the available energy level.

All these limitations of wireless sensor networks put challenges of extreme level in front of the designers of such network applications.

b) Characteristics of WSN Routing

One of the major design goals of wireless sensor network routing is to prolong the lifetime of the network and maintenance of connectivity among the sensor nodes by employing energy management techniques and energy efficient protocols.
The routing protocols designed for traditional networks cannot be used directly in a wireless sensor network setting. The wireless sensor network routing exhibits unique characteristics. These are the main reasons why protocols designed for traditional networks and wireless ad-hoc networks are directly not applicable in wireless sensor networks. These characteristics are enlisted below [79][70]:

i) Sensor nodes should be self-organizing. The operation of WSN is unattended; therefore, network organization and configuration are to be performed automatically.

ii) Sensor networks are application specific in the sense that design requirement of a sensor network changes with the kind of application.

iii) Data gathered by many sensor nodes are normally based on common phenomena and, therefore, there remains a high probability that these data contain redundancy. In-network data aggregation is a mechanism utilized to remove this redundancy and helps in energy efficient data delivery in the intended destination.

iv) WSNs are data-centric networks. In traditional networks, data are transmitted from specific node but in WSNs data are requested to send based on certain attributes. Sensor nodes may transmit data only when some event of interest is sensed and then the network should be able to configure accordingly in order to collect and transmit the interesting data.

v) Normally the number of sensor nodes deployed in the field is very high and the size of a sensor field may be in the order of thousands of nodes. The maintenance of unique ID of each sensor node in the system may be an expensive overhead in the memory constrained sensor nodes. Moreover, in data-centric WSNs data is more important than which node is sending those data.

vi) Attribute based routing is used in WSNs. Attribute based addresses are used in WSNs and such addresses are actually composed of sets of attribute-value pair [2].

vii) Knowing the location of the sensor nodes is an important aspect in WSN. Methods based on triangulation [122] allow sensor nodes to approximate their position. For this purpose radio strength from few known points may be used as reference. It is always favorable to use GPS free solutions [121] for determining the locations of the sensor nodes.

c) Routing Challenges

There are several challenges that must be overcome by the routing protocols designed for wireless sensor network in order to achieve effective and efficient operation of the network. Some of those challenges are enlisted below [79]:

Ad-hoc and random deployment: Sensor nodes are deployed in ad-hoc manner and most of the time they are randomly deployed. The nodes are to be self organized and form a
network without any human intervention and without any aid of network infrastructure. Therefore, the system needs to cope up with any pattern of resultant node distribution and establish connections among the sensor nodes. Moreover, the system needs to be adaptive to any topological changes due to node and link failure.

*Communication range of the sensor nodes:* The communication or transmission range of the sensor nodes is less. So routes generally consist of multiple hops and so the intermediate nodes in any route from a particular source node to the Base Station are to be identified cleverly.

*Connectivity among the nodes:* High node density in the sensor field may prevent complete isolation of some nodes from the others. This may produce highly connected network topology. But it does not prevent the change in the network topology and network size which may result from failure of some nodes due to many other reasons.

*Computation capability and memory space of the sensor nodes:* Since the availability of memory space and computing power of the sensor nodes are limited the network routing protocols are to be simple enough and lightweight.

*Scalability of the network:* Generally the sensor networks consist of hundreds or even thousands of sensor nodes. Though, specially for wireless sensor networks, it is not possible to have a single general solution for all kinds of situation but still any mechanism like routing should be able to cope up with large and increasing number of sensor nodes in the system. Therefore, the routing protocols should be adaptive to the changes in network size, density and topology.

*Network partition and rejoin:* Due to node and link failure the network partition may occur. Or even due to sudden availability or mobility of the sensor nodes the partitioned network may get joined. Under such circumstances rerouting or reorganization of the network may become necessary.

*Energy expenditure and rerouting of packets:* The sensor nodes expend their energy in sensing, processing and transmitting data. The sensor nodes may have to act as router as well in a multi-hop wireless sensor network setup. The life of a sensor node is heavily dependent on the available battery power in it. And death of a sensor node due to power failure may cause significant changes in the topology of the network and this fact can instigate rerouting of packets or even reorganization of the network.

*Hardware constraints:* The sensor network hardware is very simple and small in size. This is followed mainly in order to keep the cost of the node low. Still the tiny nodes should be able to cope up with the environment of deployment and function correctly.

*Transmission media:* In wireless sensor network the communication medium is radio. The sensor nodes are interlinked by the wireless medium radio. The general problems associated with the wireless channels are fading, high error rate etc, and they may cause trouble during the operation of the wireless sensor networks.
Control overhead: Whenever the retransmissions occur due to collision, packet loss or latency the energy consumption in the system also increases. Moreover, with the growth in node density the control overhead increases linearly. Therefore, energy consumption level, latency and throughput level may pose contradicting requirements.

Quality of service: The users may have different quality of service requirements. For example, in some time critical applications, data may be needed to deliver before deadline otherwise data may become useless. Under such circumstances, the network may not be able to tolerate latency. The network protocols need to take care of this quality of service requirement.

Fault tolerance requirements: Some of the sensor nodes may become useless after deployment for different reasons. The reasons might be power failure caused by energy depletion, physical damage to the sensor nodes or some environmental interference. Such failures in the sensor nodes should not influence the task to be done by the sensor network and the overall performance of the network should not degrade. Therefore, network protocols are to be designed to achieve a fault tolerant wireless sensor network.

2.3 Routing Protocols for Wireless Sensor Networks

There are several routing protocols proposed for wireless sensor networks [19] [20]. In this thesis the routing protocols for wireless sensor networks are broadly classified into two categories and these are General (Non Secure) Routing Protocol and Secure Routing Protocol. Again General (Non Secure) Routing Protocols are further classified into three sub-categories based on network structure. These are Flat Networks Routing, Hierarchical Networks Routing and Location based Routing. The taxonomy of the routing protocols is given in the Figure 2.1 drawn below:

![Figure 2.1 Taxonomy of WSN Routing Protocols](image)

Various representative protocols of the above mentioned categories are discussed in this section in detail.
2.3.1 General Routing (Non-Secure) Protocol

This category of routing protocol does not consider the security issues that are present in the network layer. The main objective of the routing protocols under this category is to discover a route from the source node to the Base Station or sink by optimizing certain parameters such as energy efficiency, reliability, throughput etc. In this section the state-of-the-art general routing protocols for WSN are surveyed.

2.3.1.1 Flat Networks Routing Protocol

This category of general routing protocols considers the network as a flat one in the sense that each node in the field typically plays the same role. The sensor nodes collaborate together to perform the sensing task and the data forwarding task. Different routing protocols under this category are discussed below.

a) Directed Diffusion (DD)

DD [131] is a very popular data aggregation protocol for wireless sensor networks. It is a data centric attribute based and application aware paradigm in which data generated by sensor nodes are named by attribute-value pairs. Directed Diffusion can route data coming from various sources towards the Sink and in an energy efficient manner by eliminating redundancy in sensory data and minimizing the number of transmissions. Figure 2.2 redrawn from [19] shows the functioning of Directed Diffusion. The protocol operates as mentioned below:

The Base Station requests data by broadcasting interests. Interest describes a required task to be implemented by the network. The Base Station defines the interest using a list of attribute-value pairs e.g., name of object, interval, duration, and geographical area.

(a) Propagate Interest
(b) Set up Gradients

(c) Send data and path Reinforcement

Figure 2.2 An example of interest diffusion in WSN [working of Directed Diffusion]

The interest is broadcasted through the network and it propagates through the network hop-by-hop. Each node receiving the interest can cache it which may be useful at a latter stage. At the intermediate hops gradients are set up towards the requesting node. A gradient is nothing but a reply link to the neighbor from which the interest was received.

Each sensor node receiving the interest, sets up a gradient towards the sensor nodes from which it received the interest. This process of setting up of gradient continues until gradients are set up from various sources of data towards the Base Station. It is the reverse direction of the propagation of interests. In this manner several paths are established and one suitable path out of those can be selected by reinforcement.

The advantages of Directed Diffusion are: Directed Diffusion is data centric and so there is no need of node addressing mechanism. Each node in the network can sense, process data and also they cache. Caching is an advantage in terms of energy efficiency, delay, robustness and scalability. The nodes are able to perform data aggregation which further reduces the data traffic and energy expenditure. However, the Directed Diffusion protocol may not be applicable to those applications of wireless sensor networks in which it is necessary to have continuous data delivery at the Base Station e.g., environment monitoring.
b) Sensor Protocols for Information via Negotiation (SPIN)

SPIN [132] is a family of adaptive protocols which can efficiently disseminate information in wireless sensor network systems. Under SPIN framework, a node assigns high-level names to their data, called metadata. A node performs metadata negotiations before any data transmission takes place. These negotiations are useful for restricting redundant data transmissions in the network. SPIN has access to the current energy level of the nodes and a suitable protocol is adapted to run on the basis of the remaining energy level of the nodes. Due to the metadata negotiation, energy is saved significantly, as it helps in avoiding redundant data transmission. This solves the classic problem of redundancy in data transmission associated with conventional data dissemination approaches, flooding and gossiping [2][58]. Figure 2.3 redrawn from [132] shows the functioning of SPIN.

![Figure 2.3 Working of SPIN Protocol](image)

(a) A starts by advertising its data to node B, (b) B responds by sending a request to node A, (c) Receiving the requested data, (d) B sends out advertisements to its neighbours, (e-f) Neighbours send requests back to B

Simulation studies reported in [132] show that SPIN is more energy efficient than flooding and gossiping. Under SPIN, each node negotiates with its single-hop neighbors only and therefore, topological changes are localized only.
c) Rumor Routing Protocol (RR)

The objective of Rumor Routing Protocol designed for wireless sensor network is to carry out routing at lower energy expenditure [133]. The protocol avoids flooding the whole network with queries. Instead, it spreads information of an event to other nodes in the network and then the queries discover paths to the events.

The main idea in Rumor Routing Protocol is to create route to each event as the event happens and at a latter stage route the queries along these routes. The protocol uses agents to create route towards each of the events when the events occur. The agents are nothing but long-lived messages traversing in the network. In order to find out a route, initially the queries are sent on a random walk in the network and this random walk continues till the query finds the event route. This random walk is applied instead of flooding the queries in the network. Each node in the network maintains a list of its neighbors and event table (information about different events in the network) along with forwarding information to all known events. The agent also maintains its event table and travels through the network. The agent can combine its event table with the event table of each node the agent come across in its path while it is traveling and finally the queries are routed through the agent generated routes.

Rumor Routing is an energy efficient protocol than flooding based protocols. This is useful especially when the geographic information of the nodes is not available. Simulation results show that the protocol handles node failures. The protocol performs well when the number of events in the network is small. This is because the cost of maintaining the agents and event tables in the nodes increases along with the growth in the number of events.

d) GRAdient Broadcast (GRAB)

GRAdient Broadcast (GRAB) [134] is a routing protocol designed for wireless sensor network and it is built on Directed Diffusion [131]. The basic idea in this protocol is to deliver the data packets at the Base Station which are generated from a source node through a route with decreasing cost. The route is selected along the direction of the Base Station but with decreasing cost.

GRAB first computes a cost field and is maintained at each sensor node. This attribute provides each sensor node the direction to forward the data packets. The cost at a node indicates the minimum energy overhead to forward a packet from itself to the Base Station along a particular route. The cost attribute implicitly indicates the global direction towards the Base Station. The important characteristic of the cost field is that the sensor nodes closer to the Base Station will have smaller values for energy overhead costs which are stored in the cost field associated with each sensor node. When a node forwards a packet, the node simply includes its own energy cost in the packet. After receiving this packet by the neighbors, they will participate in the packet forwarding process only when their own cost is smaller than the cost of the just previous sender of the packet.
GRAB requires the cost value associated with each sensor node to be periodically refreshed by the Base Station. This causes the problem of excessive message overhead just like flooding. Moreover GRAB does not work well in a dynamic network topology environment where the Base Station may move.

e) Gradient Based Routing (GBR)

Emphasis in GBR is on distribution of data traffic evenly throughout the network in order to increase the lifetime of the network [135]. GBR is another version of Directed Diffusion (DD) in which key idea is to memorize the number of hops during the diffusion of the interest through the whole network. Each node in the network computes a parameter called height of the node. Height of a node can be defined as the minimum number of hops required to travel in order to reach the Base Station. The gradient of a link is defined as the difference between a node’s height and that of its neighbor connected by the link under consideration. A packet is forwarded towards the Base Station through a link having the largest gradient.

Three different data dissemination techniques have been discussed in GBR. Those are stochastic scheme, energy-based scheme, and stream-based scheme. Under stochastic scheme, whenever there are two or more next hops having the same gradient a node picks up one gradient at random for data forwarding. Under energy-based scheme, a node increases its height whenever its remaining energy drops below a certain threshold. This helps in diverting data towards those nodes which have high amount of remaining energy. Under stream-based scheme, new streams are not routed to those nodes which are currently present on the route of other streams.

GBR increases overall life of the network by balancing the distribution of traffic in the network. It can avoid those parts of the network which are energy depleted and thus prolongs the overall lifetime of the network. Simulation studies of GBR reported in [135] exhibits the better performance of GBR against DD in terms of total energy used for communication.

f) Minimum Cost Forwarding Algorithm (MCFA)

Minimum Cost Forwarding Algorithm (MCFA) [136] is another routing protocol for Wireless Sensor Network that exploits the fact that the direction of routing is always known and it is towards the fixed external Base Station. The sensor nodes need not have a unique ID or they do not need to maintain routing tables. Each sensor node maintains the least cost estimate from itself in order to reach the Base Station. Whenever a sensor node has packets to forward to the Base Station, it broadcasts to its neighbors. After a node receives the packet, it checks if it is on the least cost route between the source sensor node and the Base Station. If it is so, the receiving node rebroadcasts the packet to its neighbors. This process is repeated until the Base Station is reached. Here each node should know the least cost route estimate from itself to the Base Station.
2.3.1.2 Hierarchical Routing Protocol

In hierarchical structure of the network, the higher energy nodes can be used for data processing and long distance data transmission whether the low energy nodes can be used to perform the sensing in the proximity of the target and also for short distance communication. Hierarchical routing protocols have special advantages related to scalability and efficient communication. Hierarchical routing protocols exhibit energy efficiency in data routing. Different routing protocols under this category are discussed below

a) Low-Energy Adaptive Clustering Hierarchy (LEACH)

LEACH [22] is one of the first hierarchical cluster based routing approach for wireless sensor network with static sensor nodes and static Base Station. The entire sensor field is logically divided into clusters and approximately 5% of the total deployed sensor nodes act as the cluster head. The cluster head nodes are elected with a probability based on the amount of energy left in the nodes.

The operational time of LEACH is divided into two phases, namely, set-up phase and steady phase. During the set-up phase each node decides whether it becomes a cluster-head node or not for the current round. During the set-up phase a node \( n \) chooses a random number between 0 and 1. The node becomes a cluster head if the chosen random number is less than a threshold \( T(n) \) which is calculated as:

\[
T(n) = \begin{cases} 
\frac{p}{1-p} \cdot r \mod \left( \frac{1}{p} \right) & \text{if } n \in G \\
0 & \text{otherwise}
\end{cases}
\]  

(2.1)

where \( p \) is the desired percentage of the cluster-heads, \( r \) is the current round and \( G \) is the set of nodes that have not become cluster-heads in the last \( 1/p \) rounds. In this approach every node gets a chance to become cluster head once in \( 1/p \) rounds. Once the cluster head nodes are elected, they advertise their status to all other nodes. A non-cluster head node selects a cluster to join which requires minimum communication energy for communicating with the respective cluster head. Each cluster head node distributes a TDMA based Medium Access Control (MAC) schedule to its cluster members for interference free data communication. This schedule is used for communication in the steady phase.

The cluster head does data aggregation upon collection of data from its cluster members and removes redundancy in the sensed data and finally forwards the aggregated data towards the Base Station. This saves lot of energy by minimizing the volume of data to be transmitted. In LEACH the cluster headship is rotated among the sensor nodes in order to evenly spread the load among the sensor nodes. In LEACH, a non-cluster head node can go into sleep mode depending on the schedule, if the node is not expected to transmit. Thus, LEACH achieves energy optimization by shutting down the radio in some nodes and again balancing load among the sensor nodes. However, the single cluster head inside each cluster leads to single point of failure.
b) Power-Efficient GAthering in Sensor Information Systems (PEGASIS)

PEGASIS [28] is based on the philosophy of LEACH. In this protocol the key idea is to form a chain among the sensor nodes instead of cluster formation. Here, each node communicates with a close neighbor. The sensed data move from node to node and finally a designated node transmits the gathered data to the Base Station. The nodes rotate the responsibility of transmitting data to the Base Station and thus the network lifetime is prolonged. Simulation results show that PEGASIS extends network lifetime to twice of that possible through the use of LEACH protocol. This improvement in energy efficiency is due to the decrease in the number of transmissions by using data aggregation and also due to the elimination of overhead caused by cluster formation in LEACH protocol. PEGASIS suffers from excessive delay with respect to the transmissions to the distant nodes in the chain. PEGASIS is not suitable for large networks because it requires global network knowledge at each node. Acquiring global network knowledge at each node is difficult and also it demands huge memory space at each node. PEGASIS assumes that each node can communicate with the Base Station directly. In practical situations, it may not be feasible. Moreover, PEGASIS does not have any mechanism for handling topology changes due to node failure.

Hierarchical-PEGASIS [137] is an extension of PEGASIS in which the delay involved during the transmission from the designated node to the Base Station is reduced. In Hierarchical-PEGASIS, the packet delay is reduced significantly in comparison to original PEGASIS and LEACH protocol. Through simulation it has been shown that Hierarchical-PEGASIS performs better than original PEGASIS by a factor of 60 with respect to the energy × delay metric. But Hierarchical-PEGASIS does not address the other limitations of PEGASIS.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DD [131], SPIN [132], RR [133], GRAB [134], GBR [135], MCFA [136]</td>
<td>LEACH [22], PEGASIS [28], TEEN [29], APTEN [30], TTDD [138], SMECN [139], VGA [140], HPAR [141], SONS [72]</td>
<td>GAF [142], GEAR [143], GOAAR [144], Getraf [145], BeamStar [69]</td>
<td>SPINS [88], LEAP [115], TinySec [116], SEEM [78]</td>
</tr>
</tbody>
</table>

Table: 2.1 Routing Protocols for Wireless Sensor Networks
c) **Threshold-sensitive Energy Efficient sensor Network protocol (TEEN)**

TEEN [29] is a hierarchical routing protocol proposed for handling time-critical applications in wireless sensor networks. TEEN also uses data-centric mechanism. The sensor network architecture is hierarchical and the closer nodes in the sensor field form clusters. The clusters are formed at two levels until the Base Station is reached. Figure 2.4 redrawn from [29] shows hierarchical clustering present in TEEN.

![Hierarchical clustering (TEEN)](image)

**Figure 2.4 Hierarchical clustering [TEEN]**

After forming the clusters, the cluster head node broadcasts two thresholds namely hard and soft, to the nodes inside the respective clusters. The hard threshold is the minimum possible value taken by an attribute to trigger a sensor node to transmit data to the cluster head node. This approach significantly reduces the number of transmissions because a sensor node transmits only when the sensed attribute is in the range of interest. Once data values are transmitted, a node transmits only when the value of that attribute changes over the soft threshold. The use of soft threshold further reduces the number of transmissions. The two threshold values soft and hard can be tuned by the user. They control the trade-off between energy efficiency and data accuracy. The main drawback of this scheme is that this protocol cannot handle those applications properly in which periodic reports are needed. Moreover, the data transmissions by the nodes are completely dependent on the availability of threshold values at the sensor nodes. Therefore, if the sensor nodes do not receive the threshold values or the transmitted threshold values do not reach the sensor nodes then the nodes will never transmit data and the Base Station will not receive any data from the network at all.
d) Adaptive Threshold sensitive Energy Efficient sensor Network protocol (APTEEN)

APTEEN [30] is an extension of TEEN. APTEEN can handle both time critical applications and applications having periodic data collection requirements. After formation of the clusters, the cluster head node sends a transmission schedule to all the member nodes of the respective cluster. This is in addition to the attributes and threshold values (soft and hard). If a particular node does not transmit data for a time period equal to the count time, the node is forced to sense and transmit data towards the Base Station.

Simulation results show that TEEN and APTEEN perform better than LEACH [22]. It is also shown through experiments that APTEEN performs even better than LEACH and TEEN with respect to energy expenditure. The main disadvantage of TEEN and APTEEN is that these two protocols involve significant overhead in forming and maintaining clusters at two levels. The implementation of threshold based functions is also complex. Moreover, attribute based naming of queries is somewhat difficult.

e) Two-Tier Data Dissemination (TTDD)

TTDD [138] is hierarchical routing protocol for wireless sensor network which considers multiple mobile Sink and it is based on a decentralized architecture. The protocol assumes the sensor nodes to be homogeneous, location aware and static. TTDD uses a two-tier data dissemination model to deal with the Sink mobility problem and to reduce energy consumption in the network. In the network model, it is considered that there are multiple sources and mobile Sinks, which query the network to collect sensory data.

Under TTDD, each data source divides the topology of the network into cells. Only those sensor nodes located at the cell boundary will forward the data. The data Sink proactively creates the two-tier grid structure spread over the entire sensor field. It also sets up data forwarding points known as dissemination nodes which are the sensor nodes closest to the grid boundary. As the name of the protocol suggests there exists two tiers in the system, the lower tier is the cell at the Sink’s current location and the higher tier consists of the dissemination nodes located at the cell boundaries. The data Sink is the node which generates query and floods it within its own cell. The nearest dissemination node in the cell receives the query and forwards it to the adjacent dissemination node located in another cell. This process of forwarding the query is repeated until the query reaches the data source. A dissemination node located in a different cell even may have the corresponding data. At the time of query propagation, the network establishes the reverse path towards the Sink. This reverse path is used to send the desired data to the Sink node and thus the data travels through the same route as the query propagated. Figure 2.5 redrawn from [138] shows the grid structure in TTDD.
Simulation results show that the lifetime of the network elongates under the influence of TTDD and TTDD shows better performance than Directed Diffusion in this regard. The limitations of TTDD are as mentioned below: the overhead associated with maintaining and recalculating the grids with changes in the network topology is high, maintaining two-tier grid structure is expensive when mobility of the Sink increases, determining accurate location information for each sensor node is too expensive.

f) **Small Minimum Energy Communication Network (SMECN)**

SMECN is a routing protocol for wireless sensor network proposed in [139] that uses low power GPS to compute an energy efficient sub-network called minimum energy communication network (MECN). MECN determines a relay region for every node and this relay region consists of nodes in the surrounding area. The characteristic of those nodes in the relay region is that the transmission through those nodes is less costly than direct transmission. However, this algorithm is local because it does not actually find the minimum-energy path. The algorithm just constructs a sub-network in which the path is guaranteed to exist.

g) **Virtual Grid Architecture Routing (VGA)**

VGA routing [140] is an energy efficient routing protocol proposed for wireless sensor networks that utilizes data aggregation and in-network processing in order to maximize
the network lifetime. The nodes are assumed to be stationary or they have extremely low mobility. It uses a GPS free approach [23] to create clusters which are fixed, equal, adjacent and non-overlapping with symmetric shapes. In this protocol data aggregation is carried out at two levels first local and then global. The set of cluster head nodes, also known as Local Aggregators (LAs) perform the first level of aggregation i.e., local aggregation. Then a subset of these LAs is used to perform global aggregation. However, the determination of optimal global aggregation points (known as Master Aggregators, MAs) is NP-hard problem. The suitable number of MAs out of the LAs is to be selected in such a way so that the network lifetime is maximized.

h) Hierarchical Power Aware Routing (HPAR)

HPAR proposed in [141] is another routing protocol designed for wireless sensor networks. In this protocol the network is divided into several groups of sensors. The groups of sensor nodes in a geographic proximity are clustered to form a zone. Each zone is then treated as an entity. The routing is carried out hierarchically across the zones. Each zone is allowed to decide how a message will be routed towards the Base Station across other zones. The objective behind such routing is to maximize the battery lives of the sensor nodes in the network system. The protocol uses an approximation algorithm called the \( \text{max-min } zP_{\text{min}} \) algorithm to select the suitable routes. The algorithm tries to minimize the total power consumption and maximize the minimal residual power of the network. In this algorithm the messages are routed along the path which offers the maximum over all the minimum of the remaining power and such a path is called the \( \text{max-min path} \). The objective in such approach is that using those nodes which have high residual power for routing may be expensive as compared to the path with minimal power consumption.

i) Self Organizing Network Survivability routing protocol (SONS)

SONS [72] is designed to cope with large area of deployment and also link or node failure under forest fire like situations. This is a hierarchical cluster based routing protocol and its operation is divided into three parts: the start-up phase, the setup phase and the process phase. During the start-up phase different clusters are formed, cluster head nodes are selected and a tree is created from the sink as the root up to the leaves considering only the cluster head nodes. During the setup phase the cluster head node assigns communication time slot to each cluster member. During the process phase the sensor nodes transmit the sensed data to the sink via cluster head nodes. The process phase is a longer period of time with respect to start-up phase and setup phase.

2.3.1.3 Location based Routing Protocol

This class of routing protocols exploits the geographical location information of the sensor nodes to find a relatively optimal route towards the Base Station. This class of routing protocols avoids flooding. These protocols improve network scalability by reducing the total routing overhead. The location information is used to reduce propagation of control messages, control packet flooding and simplified decisions are
made regarding packet forwarding process. The most well known approach for discovering the geographical location of the sensor nodes is the use of Global Positioning System (GPS). However, integration of GPS unit with the sensor nodes involves expenditure and it becomes an expensive approach for low-cost wireless sensor networks. There are some alternate ways of computing the locations of the sensor nodes which are GPS free. For example, information such as connectivity, incoming signal strength, angle of arrival etc. are successfully used in order to determine the location or position of the sensor nodes with only localized computations. Following are some location based routing protocols designed for wireless sensor networks.

a) Geographic Adaptive Fidelity (GAF)

In the GAF protocol [142] the redundant nodes are kept in small groups. Based on the locations of the sensor nodes, some sensor nodes are identified as redundant nodes since they belong to the same closely located area. Then, based on the geographic locations of the sensor nodes, localized and distributed algorithms are used to control node duty cycle which in turn extends network operational lifetime. In GAF, the whole sensor field is divided into some small virtual grids. The nodes belonging to the same virtual grid are equivalent for routing. Such equivalence is used to keep some of the redundant nodes present inside the same virtual grid area in inactive state in order to save energy. Therefore, some nodes inside the virtual grid are scheduled for sleep state which is an inactive state. The nodes inside the virtual grid coordinate with each other to determine the sleep schedule. The nodes periodically wake up. GAF tries to rotate the role of active node inside each virtual grid periodically. In this way GAF achieves load balancing among the sensor nodes and uses the load balancing strategy to extend the network lifetime. Figure 2.6 redrawn from [142] shows how the whole area where nodes are distributed is divided into small virtual grids as per GAF protocol.

![Figure 2.6 Virtual Grids and Active Nodes in GAF](image)
Simulation results show the energy efficiency of GAF. It extends network lifetime in proportion to the node density. With respect to the packet loss and latency, GAF performs as good as normal ad hoc routing protocols. However, GAF assumes that the sensor nodes discover their geographical locations through GPS unit integrated with each sensor node and this increases the expenditure of the wireless sensor network setup.

b) Geographic and Energy Aware Routing (GEAR)

GEAR [143] is an energy aware routing protocol for wireless sensor network which prolongs the lifetime of the network. It uses geographic information to send a query to only certain region of the network instead of flooding the query interest in the whole network. This approach limits the query flooding in Directed Diffusion [131].

Each node stores an estimated cost, which is a combination of the residual energy of the node and the distance to the destination node through its neighbors. Each node also maintains a learned cost, and this cost accounts for the real network topology, especially the routing holes. The learned cost is the propagation cost of a packet. A node encounters a routing hole when no other neighbor nodes are closer to the destination than itself. In the presence of a routing hole, learned cost is larger than the estimated cost.

At the time of data forwarding from the source node to the destination node, the GEAR protocol uses two phases. In the first phase, the packets are forwarded towards the target region. The forwarding sensor node chooses one of the neighbors closest to the target region as the next hop. In the presence of a routing hole, one of the neighbors is picked in order to forward the packet based on the learning cost function. In the second phase, after the data packets reach the target region, the packets can be diffused towards the destination node by any one of the two approaches namely recursive geographic forwarding or restricted flooding. Recursive geographic forwarding (flooding) can be used when the target region node density is high. In this approach the target region is divided into sub-regions and a copy of the packet is sent to each of the regions. This splitting and forwarding process continues until the destination is arrived. This approach saves energy. On the other hand, restricted flooding can be used as the mechanism when the target region node density is low.

The simulation results show GEAR improves energy efficiency during route setup and performs better in terms of successful packet delivery. GEAR is sensitive to location errors. It also increases the average path length for each packet. Moreover the location discovery process for the sensor nodes is considered to be expensive for wireless sensor networks.

c) Greedy Other Adaptive Face Routing (GOAFR)

GOAFR [144] is a geometric ad-hoc routing protocol. It combines greedy and other adaptive face routing techniques. GOAFR is asymptotically optimal and also efficient on average case graphs.
In the GOAFR, during the process of selecting the next node, the closest-to-destination method is used. This is the greedy mode of GOAFR. However, this phase may easily get stuck at a routing hole. A routing hole is a condition when there is no neighbor node closer to a destination node than itself. When the greedy mode gets stuck, a face routing algorithm is used to bypass the routing hole. Face routing is a technique that uses a planar graph to route the packets. Under this technique, first of all a planar graph is computed considering the underlying wireless connectivity graph. Then the face routing algorithm routes exclusively along the paths of the planar graph. The face routing algorithm defines a consistent forwarding mechanism for routing in the presence of routing holes.

GOAFR is a worst-case optimal and average-case efficient algorithm and it is the first of its kind. Simulation shows the algorithms behaves well in dense networks. The algorithm needs to improve average case performance.

d) Geographic Random Forwarding (GeRaF)

GeRaF [145] is another routing protocol for wireless sensor network which is based on the principles of Geographic Routing. Here the packets are relayed on a best-effort basis. The sender node does not know in advance about the actual node which is going to act as a relay. It is decided after the transmission has taken place from the sender node. GeRaF assumes that each sensor node has knowledge about its own location and the location of the Base Station. Whenever a node has a packet to send, it transmits using some types of broadcast address. The sender node specifies its own location and the location of the intended destination. Then all the active nodes in the coverage area of the sender node will receive this message (since broadcast) and then they assess their priority for becoming a relay node for this transmission. This assessment is based on their respective distances to the intended destination. Priority is assessed based on how close they are to the destination.

Simulation results show that GeRaF has significantly fewer hops than GAF [142]. GeRaF incurs smaller energy consumption for delivery of a packet to the destination. The limitation of GeRaF is that it needs knowledge about the location of the Base Station (destination) which may be expensive to collect. Moreover, it may be even more complex problem while the Base Station moves. The protocol is designed for a dense network and it may fail in the case of a sparse network.

e) BeamStar

BeamStar [69] is an edge-based routing protocol for wireless sensor network in which the Base Station (edge) exploits the properties associated with directional antenna and power control at the Base Station. Under this protocol each sensor node can determine its location information with minimum control overhead. Most of the computing burdens are shifted to the Base Station and sensor nodes are relieved of the activities linked with control and routing. Therefore, the sensor nodes can be much simpler with respect to their hardware and software implemented on them. The intermediate sensor nodes do not need
to store any routing table and each node can act in a purely stateless manner. Thus the requirement of large memory in the sensor nodes is also avoided.

### 2.3.2 Secure Routing Protocol

This class of routing protocols addresses the issue of security in the network layer of the protocol stack. There are different security threats present in the network layer [85]. A secure routing protocol strives to put defense against those security threats apart from general routing task. The major objective of this class of routing protocols is to route data from the source node to the Base Station or Sink in a secure manner. Different routing protocols under this category are discussed below.

**a) Security Protocols for Sensor Networks (SPINS)**

SPINS is a suite consisting of two security building blocks proposed in [88]. The two building blocks of SPINS are SNEP (Secure Network Encryption Protocol) and µTESLA (“micro” version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol). SNEP provides data confidentiality, two-party data authentication, and data freshness. On the other hand µTESLA provides authenticated broadcast for severely resource-constrained environment such as wireless sensor networks. µTESLA is an improvement over TESLA [147] in order to cope up with resource constrained environment. Under the SPINS framework, all the cryptographic primitives for example, encryption, Message Authentication Code (MAC), hash, and random number generator are constructed out of a single block cipher. This helps in code reuse. SPINS also uses symmetric cryptographic approach. Therefore, code reuse scheme along with symmetric cryptographic approach reduces overhead in the resource constrained environment. Though it is difficult to achieve data authentication through a symmetric key cryptographic approach specially in broadcast medium such as radio, the µTESLA security block achieves authenticated broadcast through symmetric key cryptographic approach only. µTESLA achieves this in broadcast medium such as radio by introducing asymmetry through delayed key disclosure and use of one way function key chains.

**SNEP:** SNEP achieves confidentiality through the use of encryption. It uses Message Authentication Code (MAC) to achieve two-party authentication and data integrity. SNEP also achieves semantic security in order to ensure nondisclosure of any information about the plaintext to the eavesdroppers even if the eavesdroppers see multiple encryptions of the same plaintext. SNEP offers the following properties: Semantic Security, Data Authentication, Replay Protection, Data Freshness, and Low Communication Overhead.

**µTESLA:** Most of the proposals for authenticated broadcast rely on asymmetric digital signatures for authentication purpose. And, therefore, these are impractical for wireless sensor networks. µTESLA uses symmetric cryptographic approach but still achieves authentication by introducing asymmetry through a delayed symmetric key disclosure mechanism. This results in an efficient broadcast authentication scheme. In µTESLA framework the Base Station and sensor nodes are to be loosely time
synchronized, and each node needs to know an upper bound on the maximum synchronization error.

b) Localized Encryption and Authentication Protocol (LEAP)

LEAP [115] is a key management protocol designed for wireless sensor networks. It supports in-network processing without compromising with the desired security in the sensor network setup. The design of this protocol is motivated by the fact that different types of messages to be exchanged among the sensor nodes have different security requirements. Therefore, single keying mechanism in which one key is shared by all the sensor nodes in the network system is not suitable for meeting these different security requirements. Under the influence of LEAP, four different types of security keys are established for each sensor node. These four keys are as mentioned below:

**Individual Key:** Each node in the network has a unique secret key and the node shares this individual key only with the Base Station.

**Group Key:** This group key is a globally shared key and it is used by the Base Station for encrypting the broadcast messages intended for all the legitimate sensor nodes present in the network. This group key is shared among all the sensor nodes in the network.

**Cluster Key:** The cluster key is a shared key for a node in the network and all its neighbors. Since the cluster key is shared by a node and all its neighbors, it is mainly used for encrypting the locally broadcast messages and securing those messages. Each node possesses a unique cluster key and it is used for encrypting the broadcast messages intended for its neighbors and the immediate neighbors use the same key for decrypting the received messages.

**Pairwise Shared Key:** Every node in the wireless sensor network shares a pairwise secret key with each of its immediate neighbors.

The protocol used in order to establish these secret keys and also updating these keys happens to be energy efficient. This approach also minimizes the Base Station involvement.

c) TinySec

TinySec [116] is a security package that is incorporated in the official release of TinyOS. It is a lightweight, generic security package. End-to-end security mechanisms are not ideal for wireless sensor networks. Since in-network processing such as data aggregation is an important aspect of wireless sensor networks, the end-to-end security mechanisms will not allow the intermediate nodes to access the data packets. In-network processing is used to avoid data redundancy and to reduce traffic which indirectly minimizes energy expenditure in the system. Therefore, link layer security is ideal for wireless sensor network setup [116]. A link layer security architecture can detect unauthorized packets if
these are injected into the network system. TinySec exhibits basic security properties such as message authentication, message integrity, message confidentiality, semantic security, and message replay protection. It achieves message authentication and message integrity using Message Authentication Code (MAC). Message confidentiality is achieved through encryption. And semantic security is achieved through an Initialization Vector. TinySec provides two different security options: authenticated encryption named as TinySec AE and authentication only known as TinySec-Auth. Under the authenticated encryption (i.e., TinySec AE) option the data payload is encrypted and the packet is authenticated with a MAC. The MAC is computed over the encrypted data and the header of the packet. On the other hand under the authentication only (TinySec-Auth) option, the entire packet is authenticated with a MAC but the data payload is not encrypted.

In TinySec framework, encryption is carried out using Cipher Block Chaining (CBC) [146]. Encryption is optional in TinySec framework but it always does message authentication.

TinySec uses a Cipher Block Chaining construction called CBC-MAC for computing and verifying the Message Authentication Codes. CBC-MAC is faster and also efficient. It relies on block cipher and also minimizes the number of cryptographic primitives to be implemented in limited memory space available with the sensor nodes.

TinySec uses separate secret key for each pair of sensor nodes who wishes to communicate with each other. The use of such pair wise keys restricts the attack propagation under node capture attacks [116].

d) Secure and Energy-Efficient Multi-path routing protocol (SEEM)

SEEM [78] is a routing protocol designed for wireless sensor network which uses multiple paths alternately for data transmission between two nodes. Thus the protocol saves energy in the sensor nodes and prolongs lifetime of the network. Moreover, SEEM can put resistance to some routing layer attacks which have character of pulling all traffic through the malicious nodes. SEEM has three phases namely topology construction, data transmission, and route maintenance. During the topology construction phase, the network topology is setup; during the data transmission phase, the sensor network starts its tasks; and during the route maintenance phase, the Base Station updates the available energy status at each node and finally re-selects new routes necessary for data transmission. SEEM is an energy efficient and also secure routing protocol for wireless sensor network which transfers most of the routing related task to the Base Station.
2.4 Conclusion

Routing is wireless sensor network is a challenging task. The unique characteristics of wireless sensor networks pose significant challenges in front of the designers of wireless sensor networks. It is extremely important to design efficient and suitable routing protocols for wireless sensor networks in order to have successful deployment and efficient operation of such networks. Moreover the protocols and algorithms for sensor networks are application specific. In this chapter author discusses the limitations of wireless sensor networks, characteristics of routing in wireless sensor networks and also different challenges to be faced during the design of routing protocols for such networks. Different routing protocols for wireless sensor networks are surveyed. The routing protocols are broadly classified with respect to their ability to defend routing layer attacks. Then representative protocols of each of the sub categories are discussed along with their strengths and weaknesses.