Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 5; April-June, 2015 pp. 416-424
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Analysis of Routing Protocols in Wireless Sensor Networks

Pramod Nath[1] and Pragya Rajput[2]

[1]Department of Computer Science and Engineering, Jaypee Institute of Information Technology (JIIT), Student, Noida, U.P, India
[2]Department of Computer Science and Engineering, SRM University, Student, NCR Campus, India
E-mail: [1]er.pramodnath@gmail.com, [2]rajputpragya91@gmail.com

Abstract—*Wireless Sensor Networks (WSNs) is the combination of many independent and coordinated set of sensor nodes that are deployed in the hectic unattended environment conditions. These sensor nodes are not limited to one specific application instead used in many real world applications such as in military, industries, environment sensing and so on. During their lifetime, these sensor nodes face many issues related to energy degradation, resource constraint and quality of service. This issue affects the performance for sensor nodes. Efficient routing protocols usage has great importance in increasing the lifetime of sensor nodes. Routing protocols provide efficient and reliable path to destination, thus reducing the energy consumptions. In this paper, we have discussed about different issues or challenges for routing in WSNs and also described routing protocols classification and their detailed comparison as well stating strengths and weakness of the routing protocols.*

Index Terms*: Wireless sensor network (WSN), Routing protocols, flat, Hierarchical, Geographical, QoS routing protocols.*

1. INTRODUCTION

A Wireless Sensor Networks (WSNs) is the combination of many independent and coordinated set of sensor nodes that are deployed in the hectic unattended environment conditions. These sensor nodes have different capabilities ranging from sensing, monitoring, processing, computations of data captured from the surrounding. A sensor node has following components namely, memory, transceiver, microcontroller, power source, and some external interfaces. All these components have limited capabilities. A given sensor node has defined coverage area for sensing but it can extent on demand as the topology may change on time.

A routing protocol gives the sensor nodes the desired and efficient route for information exchange. By this, a given sensor node may get the complete topology structure of the networks and can perform the operations more easily.

Routing process can be static or dynamic. In static routing, all the routes are static and predetermined. Static routing is not fault-tolerant and any change to the topology will require manual intervention. Pros of static routing are: minimal processing overhead, no bandwidth overhead and granular control. Cons of static routing are: not scalable for large networks, no dynamic recovery from fault and manual configuration changes.

In dynamic routing, a series of periodic messages containing routing information are exchanged by the routers for the best route that exists. Dynamic routing is fault-tolerant and can quickly adapt changes in network topology. Pros of dynamic routing are: fault tolerance, scalable, load balancing between multiple links, and easy to configure in large networks. Cons of dynamic routing are: some protocols results in additional load on processing unit of router, updates shared between routers consume high bandwidth, and less control over selected paths.

The structure of wireless sensor network (WSN) is shown below:

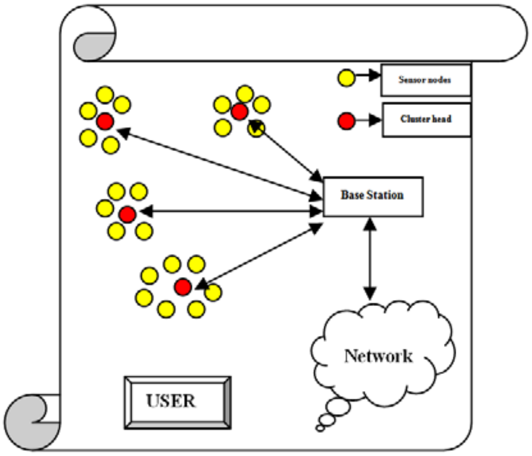


Fig. 1: A Wireless Sensor Network Structure

2. CHALLENGES FOR ROUTING IN WSNS

Routing is one of the major research issues in WSN that attracts many research scholars. Considering following aspects, we can have more effective and efficient routing protocols. We have identified different challenges for routing listed below:

1.1 *Energy Consumption:* Due to limited energy constraint, a sensor node needs to optimize energy as well as reliable communication between two given nodes. There is need for careful analysis of reasons for energy consumption in WSN. The factors can be: neighborhood discovery or communication and computation. Most of the routing protocols require each sensor nodes to exchange information between its neighbors, thus consuming more energy while information exchange through wireless medium and increasing protocols overhead. Sometimes it happen that information from multiple nodes needs to send in one single packet, thus reducing traffic and redundancy. So computation plays an important role as compared to communication.

1.2 *Scalability:* WSN is robust in nature. Deployment of more number of nodes depends on network topology. In WSN, many protocols that operate with limited knowledge of topology define scalability of sensor nodes coverage, thus there is need to design such protocols that can have scalability with minimal overhead.

1.3 *Addressing:* With the large number of sensor nodes in the network, assigning unique address to each sensor nodes is not feasible to facilitate communication with its neighbors. Information from multiple sensors is used instead of information from individual sensor. Developing new addressing mechanism in routing protocols that does not require unique IDs is a challenging issue in WSN.

1.4 *Robustness:* Routing protocols in WSN must rely on sensor nodes as they have low-cost component. These components sometimes may result in unexpected failure. The routing protocols should provide robustness in such failure by fetching information even if sensor node dies.

1.5 *Topology:* The topology in WSN may be predetermined or randomness. At initial stage, individual nodes may not be aware of network topology. It is the task of routing protocols to provide topology structure so that each node know about its neighbors, thus best communication route is made. With the time, the network topology may change dynamically. If a node is inactive, then it should be set into sleep mode so that energy consumption is achieved. So the routing protocols should be adaptive to dynamic network topology.

1.6 *Application:* The design of routing protocols should be compatible with the type of application. For monitoring application, there is a periodic communication between sensor node and sink. So static routes is used for information exchange by choosing the efficient route. But in case of event-based applications, most of the sensor nodes are in sleep mode and for any prompt request the route are generated accordingly. Thus the challenge for design of routing protocols with different techniques is to develop such application based protocols that can perform on application requirement basis.

3. ROUTING PROTOCOLS CLASSIFICATION

In WSN, routing protocols are used for exchange of information between sensor nodes and the base station. Various routing protocols have been proposed and classified based on different parameters. The routing protocols are classified as below:

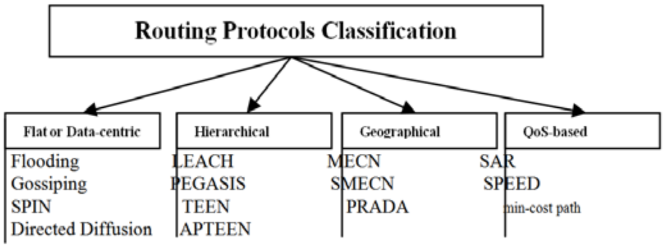


Fig. 2: Classification of Routing protocols in WSN.

3.1 Flat or Data-centric routing protocols

The most important difference between WSN and ad-hoc network is that because of large number of sensor nodes in WSN, it becomes difficult to assign specific IDs to each sensor nodes, thus address-based routing protocols are not used in WSN. To overcome this issue, flat or data-centric routing protocols are used. In data-centric routing, the protocol provides routes based on the content of query, and thus nodes sending the information may change depending upon each query and also for each data-centric query multiple nodes can be addressed.

3.1.1 Flooding

Flooding is the simplest routing protocol that is developed for multi-hop networks.

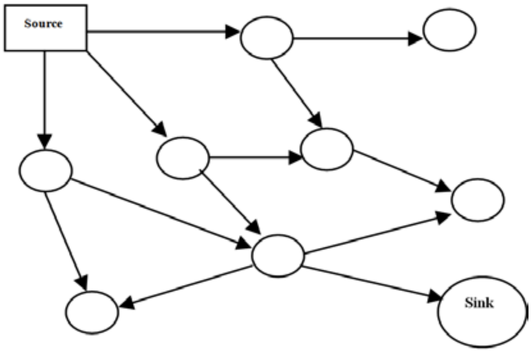


Fig. 3: Flooding Protocol

In flooding, whenever a node receives a packet and the node broadcast the packet to all the neighbors. This process is repeated until all the nodes in the network receive the packet, thus a packet can be flooded through the whole network. For flooding, all nodes have same functionality and sensor nodes are homogenous with respect to hardware or software. Steps involved in flooding are as follows: (1) Send packets to all neighbors. (2) Never send data back to the immediate sender or originator. The advantages of flooding protocols are: (1) its simplicity since a node does not require neighbourhood information, (2) flooding doesn't require costly topology maintenance and complex route discovery algorithms. The disadvantages of flooding protocol are: (1) Too-much wastage of bandwidth. (2) Multiple copies of same data might reach to some nodes causing *data implosion.* (3) No privacy of data. (4) Network gets heavily congested. (5) Overlap sensing area leading to duplicates packet receiving at sensor nodes.

3.1.2 Gossiping

The gossiping protocol is used to avoid the data implosion problem where multiple of same data traverse the network.

The gossiping avoids data implosion problem by selecting only one node at a time for packet transfer. Once a node receive a packet, it does not broadcast the packet instead it will select a random path from its neighbor and send accordingly. The same procedure is followed by its neighbor also.

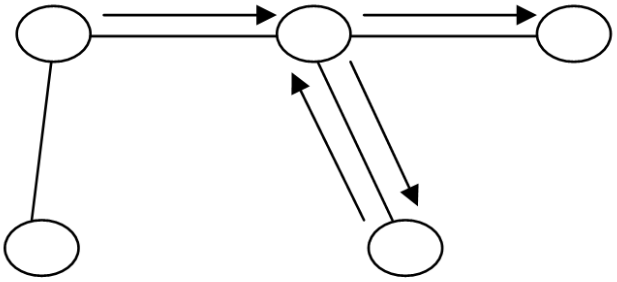


Fig. 4: gossiping protocol

In gossiping, data disseminates at slower rate as compared to flooding. Gossiping is a time consuming process than flooding. Exception in case of gossiping are: (1) Data can be send back to the originator. (2) A neighbor once chosen will not be chosen again. Advantages of Gossiping are: (1) No multiple copies of a packet, thus the energy consumption of gossiping is lower than that of flooding. (2) Avoid data implosion. Disadvantage of Gossiping are: (1) increases latency in propagating the message to all sensor nodes. (2) Since a single node at a time is informed about the packet, the information is distributed slowly.

3.1.3 SPIN

SPIN stands for **S**ensor **P**rotocols for **I**nformation via **N**egotiation. SPIN protocol is used to overcome the drawback of flooding by negotiation and information exchange. In this protocol, three types of packets are send: Request packet (size 8 bytes), Advertisement or meta-data packet (size 16 bytes) and data packet (size 500 bytes).

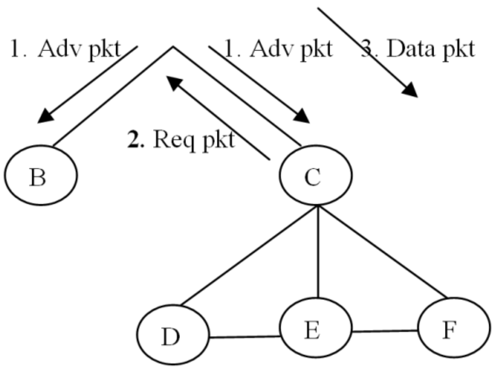


Fig. 5: SPIN protocol

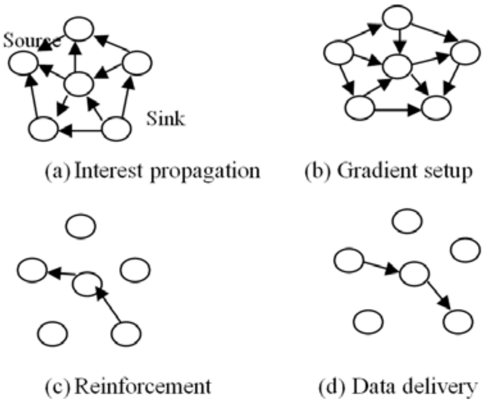
In this protocol, before sending the DATA packet, a node firstly advertises the information by broadcasting the ADV packet. This ADV packet contains the description of DATA packet with it. If a neighbor is interested for the data, it relies back with the REQ packet. Finally the DATA packet has to be send to the requested node. This protocol is also known as point-to-point SPIN protocol (SPIN-PP)

Thus information exchange is done based on the negotiation of the three types of packets. Each node must ensure that sufficient energy available with them for further communication. The advantages of SPIN protocol are: (1) Compared to flooding this protocol reduces the energy consumption with the help of energy-aware steps. (2) Since local interactions are required for routing, SPIN is scalable. The main disadvantages of SPIN protocol are: (1) latency rate in data transmission is much higher as compared to flooding, thus increase in overhead by handshaking mechanism. (2) resource-blindness problem is not addressed. (3) This protocol does not provide any mechanism to prevent collisions when multiple REQ packets are send.

3.1.4 Directed Diffusion

Directed diffusion is a data-centric routing protocol that eliminates redundancy, minimizes number of transmission, save bandwidth and sensor energy. Compared to SPIN, the communication starts firstly from sink node and propagates to neighbor nodes. The four stages in directed diffusion are: (1) Interest propagation, (2) gradient setup (3) Reinforcement and (4) Data delivery.

In interest propagation phase, the sink node broadcast the information request message to all its neighbor sensor nodes. Once the node receives the message, each sensor node stores it in an interest cache. The interest cache contains following fields: timestamp, gradient, interval and duration. The timestamp field indicates the time when the message is received. The gradient field indicates the node from which the message is received. This field is used as a reverse path for the next phase. The interval and duration fields indicate the message storage time at the cache.



(a) Interest propagation (b) Gradient setup

(c) Reinforcement (d) Data delivery

Fig. 6: Directed diffusion mechanism

The main drawback of directed diffusion protocol is the flooding operation at the interest propagation phase. An improvement to directed diffusion developed is Push diffusion where interest propagation phase is removed, thus initiation of data request is done by sensor node instead of sink node.

3.2 Hierarchical Routing Protocols

In case of flat or data-centric routing protocols, most of the information is generated at the sensor node nears to the sink node. This result in the data overload at the sink node and sometimes node becomes heavily congested leading to the node failure and link breakdown between WSN and sink node. To overcome this issue, we have the hierarchical routing protocols. In this protocol, sensor nodes are grouped into clusters and one node in each cluster is chosen as cluster head. It is the responsibility of cluster head to communicate sink node information to the sensor node and vice versa.

Many protocols have been developed based on hierarchical routing.

3.2.1 LEACH

LEACH protocol stands for **L**ow-**E**nergy **A**daptive **C**lustering **H**ierarchy. This protocol minimizes node energy in WSN by applying clustering operation at each node.

The key features of LEACH protocol are: (1) Localized coordination and control for cluster set-up and execution. (2) The base station or cluster head and the corresponding cluster rotation and. (3) Local comparison to reduce global variant communication. In LEACH protocol, assumptions are: (1) homogenous sensor nodes. (2) Same initial energy for each node. (3) All the sensor nodes are unclustered. (4) Let *p* be desired percentage for selection of cluster head and is taken as the pre-determined network parameter. The phases of LEACH protocol are as follows: (1) startup phase (2) set-up phase (3) communication phase.

Start-up phase: The start-up phase consists of two sub phases namely, cluster head (CH) nomination phase and Advertisement phase. In this phase, each node decides whether to become CH or not on the basis of parameter *p* and number of time it has become CH for 1/*p* rounds.

A Threshold T(n) is calculated as:

$$T(n) = \left\{ \begin{matrix} \dfrac{p}{1 - p*(r \bmod 1/p)} \\ 0 \end{matrix} \right\} \text{if n is in G else 0}$$

Where r = current round and
G = nodes that are not CH in last 1/*p* rounds.
The node uses a random number generator RNG$_i$ to choose a number between 0 and 1.

```
NG$_i$ (n) $\psi$ ($i^{th}$ round)
if $\psi < T(n)$ then
N becomes CH for r = $i$.
G G – {n}
endif
```

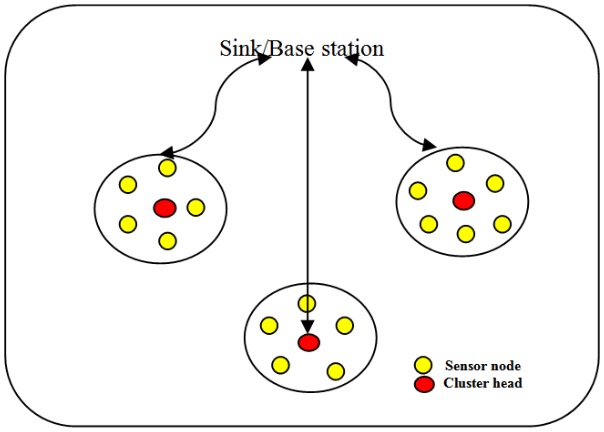


Fig. 7: LEACH protocol

Once a node is chosen as CH, it advertises or flood ADV$_{ch}$ packet to all nodes. On the basis of RSS (Received Signal Strength), each non CH node decides to which cluster it should rightfully belong. Here each non CH node, have its own RSS value depending upon its neighbor nodes. Nodes closer to each other have more RSS value than the other nodes.

Set-up phase: This phase is also known as cluster set-up phase. After the non-CH node decide the cluster it would eventually belong to, each node sends an approval packet APR$_{non-ch}$ to its respective CH node.

Communication phase: In this phase, CH periodically generates a query and the sensor node report the monitored data due to event-based having the shortest path to the cluster head. These cluster head nodes send the received data to the sink node.

Sleep scheduling algorithm can be applied to certain nodes that do not possess the data for any round in order to save energy of the sensor nodes.

In this protocol, cluster head selection is dynamically distributed to each sensor node in the cluster so that energy consumption is evenly distributed.

3.2.2 PEGASIS

The PEGASIS protocol stands for **P**ower-**E**fficient **GA**thering in **S**ensor **I**nformation **S**ystems. This protocol is used to overcome the drawback of LEACH protocol i.e. it does not form cluster of nodes instead chain of nodes are formed to reduce the overhead issue. Assumptions of PEGASIS protocol are: (1) the sensor nodes have complete knowledge of the network (2) chain formation of nodes begins from the nodes that are far away from the sink node.

In this protocol, instead of maintaining the cluster information of different nodes only the previous and next sensor node information is taken into consideration. Similar to LEACH, here also we have chain leader that controls the chain of nodes for information propagation. The communication is done sequentially from one node to another node until all the data is not aggregated at the chain leader.

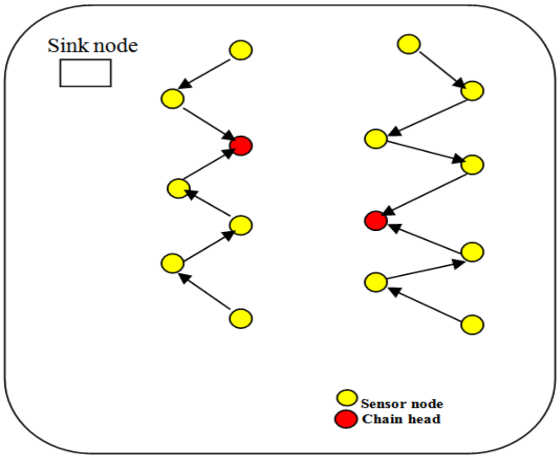


Fig. 8: PEGASIS protocol

An advantage of PEGASIS is the higher rate of energy consumption than LEACH protocol. This is due to chain formation strategy rather than the cluster formation.

Disadvantages of PEGASIS are: (1) since data have to be sequentially transferred, there may a delay issue at the chain head for data aggregation. (2) Chain head have to wait until all the data is not aggregated. (3) Chain head send the aggregated data into one single packet to the sink node, thus can have loss or inaccuracy of data at the sink node.

3.2.3 TEEN and APTEEN

The TEEN protocol stands for **T**hreshold-sensitive **E**nergy-**E**fficient sensor **N**etworks. Aggregation technique is applied in LEACH and PEGASIS protocol for information exchange between sensor node and sink node. For event-based applications, these protocols are not applied instead TEEN protocol is used. In this protocol, sensor nodes cluster hierarchy is formed.

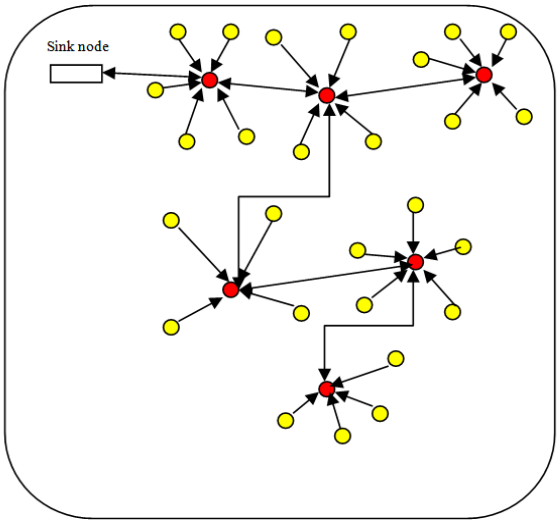


Fig. 9: TEEN protocol

In this protocol, firstly data are transmitted by sensor nodes to the respective cluster head, the CH node then send the data to the next level in the hierarchy and by this way data reaches the destination node or base station. Further the probability of becoming a cluster head in evenly distributed so that energy can be saved at the sensor end.

TEEN protocol uses two types of threshold namely, hard-threshold and soft-threshold for event based applications. The nodes frequently sense the hard-threshold value of concerned environment and if this value exceeds then the sensor node sends the monitored data to the cluster head. This happens only when some event has been occurred. The use of soft-threshold comes when the event occurs for long time and the redundancy of transmission time has to be reduced. So whenever hard-threshold value is exceeded, the sensor nodes also check the soft-threshold value also and if the difference for consecutive read data does not exceed the soft-threshold value, the respective sensor node does not send the data to the cluster head. This indicates to the cluster node that same data is obtained again. New reading values are only transmitted in case the soft-threshold value is exceeded. Thus with the use of both threshold, transmission limit can be optimized at the cluster head and overhead is reduced as well.

An extension to TEEN protocol, we have APTEEN protocol.

APTEEN protocol stands for Adaptive Threshold-sensitive Energy-Efficient sensor networks.

Some application requires periodic updates of the observed data at the cluster head. This is not performed by TEEN protocol because TEEN protocol is based on the limited value of threshold parameters.

In APTEEN protocol, for the transmission of observed information TDMA mechanism is used. As a result each sensor node now can send the periodic updates of sensed data to the cluster head. Here also threshold values are used for when to send the data or how to send the data to the cluster head.

The advantages of Hierarchical routing protocols can be: (1) high scalability factor in the network. (2) Less traffic generation. (3) Better energy consumption than flat routing protocols. (4) CH takes decision for the sensor nodes. (5) Enhance lifetime of network as well.

The main disadvantages of Hierarchical routing protocols are: (1) sometimes there can be threat attack at cluster head and fails to do the task. (2) Increase in cluster formation results increased overhead. (3) Not suitable for single-hop inter cluster communication. (4) Not applicable for large-scale networks where single hop communication with the sink is infeasible.

3.3 Geographical Routing Protocols

In WSN, the routing protocols provide the best route available for information exchange between the sensor nodes and the base station. Sometimes it becomes necessary to have the location of sensor node as well. When it comes to the application of WSN, the concept of Location Information is used. In order to get the location of sensor node, a GPS device can be enabled in the processing component of the node. Thus routing when combined with location results into Geographical routing protocols. Geographical routing protocols are also known as Location-based protocols where efficient and reliable routing is done to exploit the location information exchange. Several protocols have been developed based on the concept of geographical routing protocols.

3.3.1 MECN and SMECN

The MECN protocol stands for Minimum Energy Communication Network.

In this protocol, given a communication network an energy-efficient sub network is created, so to have more energy with the node in the network.

The purpose of MECN is to draw a graph from the given network where the vertices represent the sensor node and the edges represent the link between the nodes. A sub graph is then derived with the same number of vertices but fewer edges.

Since in the sub graph, links have been reduced, the energy required to transmit the data from one node to another node is much less than the energy transmission in the given graph.

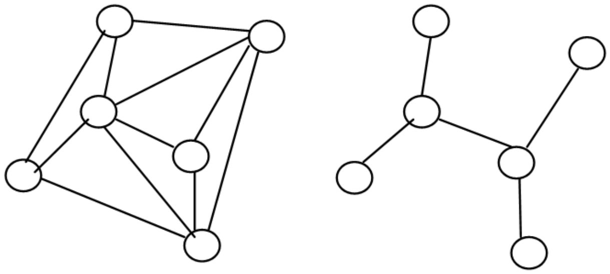


Fig. 10: Graph and sub graph in MECN

The power required to transmit the data from one node to another node is given by:

$p(node1,node2)= t*d(node1,node2)^n$

Where t is a constant,

$d(node1,node2)$ is the distance between node1 and node2,

n is path-loss component ($n \geq 2$).

We have c be received power rate. Let r be the path from node A (i.e. A_0) to node B (i.e. A_k), where r = (A_0, A_1.... ,A_k) is in the sub graph which contains nodes in some order such that the pair $(A_i, A_{i+1}) \in E$.

The total power consumption between A_0 to A_k is given by

$$C(r) = \sum_{i=0}^{k-1} (p(Ai, Ai+1)+c)$$

Where $p(A_i, A_{i+1})$ is the power required to transmit data between node A_i and A_{i+1}, and c is the power required the data. Thus a path r is called minimum energy path if $C(r) \leq C(r^*)$ for all r* between node A_0 to A_k in G*.

MECN protocol uses the concept of relay region. A relay region is the region consisting of nodes from the surrounding area where transmitting through the nodes is more energy efficient than the direct data transmission. Suppose if a node1 is trying to have communication with node2, which is in the relay region of node3, then the node3 can be used as an intermediate node for energy efficiency. The SMECN protocol stands for Small MECN. This protocol is developed to improve the channel modelling concept in MECN. In SMECN protocol, a graph with even fewer edges than that of MECN is derived by considering the obstacles between the sensor nodes. The same minimum energy path is followed by SMECN to achieve the network lifetime.

3.3.2 PRADA

The Geographical routing protocols aim to select one of the feasible nodes as the next hop to advance the packet toward the destination. As a result, routing loops are prevented. The selection of the next hop inside the feasible region depends on the forwarding algorithm such as greedy forwarding, distance-based blacklisting, best reception neighbour forwarding, and best PRR (packet reception rate) distance algorithms. So collecting this information is very costly. It is assumed that if a node has complete knowledge of the network, then the desired and optimum path to the destination node can be found on the basis of next hop count. But the complete network knowledge is not possible in WSNs due to the high density and associated high cost. Hence, geographical routing protocols aim to provide decision-making mechanisms using a limited view of the network, i.e., information about neighbours of a node. PRADA protocol is a probe-based distributed protocol that used the forwarding decision and techniques of knowledge range adjustment concept. The PRADA protocol solves the problem of the cost associated with the larger topology knowledge and the accuracy of forwarding decision. Thus for a node to have larger topology knowledge, the node must have more transmitting power and increase its transmission range. This leads to increase cost of topology knowledge. With the increased topology knowledge, optimum routes can be created and subsequently node energy can be reduced.

The PRADA protocol is based on a centralized forwarding scheme called partial topology knowledge forwarding (PTKF), which aims to minimize the energy consumption and the cost of topology. Here in the network each node constructs a route based on weighted shortest path algorithm with the link cost given as the energy consumption. Based on this route, the next hop is selected and then this hop then calculates the route according to its topology knowledge. In order to minimize the overall energy consumption, PTKF scheme gives the best range of knowledge set. It minimizes the total sum of topology information and communication cost for any given node i.

In PRADA, each node adjusts its knowledge range according to the feedback mechanism it receives from its neighbour nodes. Advantages of Geographical routing protocol are: (1) low complexity as next hop is selected based on local information. (2) Scalable routing protocols. (3) Based on location of node, the neighbor node information is easily constructed. Disadvantages of Geographical routing protocol are: (1) the error in location detection can cause error in routing. (2) Monetary cost for GPS may be expensive for some applications. (3) Since nodes are more in number and being operated by batteries, thus power consumption and size of GPS may not be appropriate.

3.4 QoS-Based Protocols

All the routing protocols discussed above mainly focus on the energy consumption and accordingly route are generated. Along with the energy efficiency issue, the quality of service (QoS) requirements are also taken into consideration.

Following are the QoS Based protocols:

3.4.1 SAR

The SAR protocol stands for Sequential Assignment Routing. The objective of SAR algorithm is to have minimum average weighted quality of service QoS metric throughout the network lifetime.
Assumption: Multiple paths to the sink node.

For the path selection, the entire sensor nodes follows SAR algorithm. It considers parameters namely QoS factor and energy on every path and also packet's priority level. SAR algorithm computes weighted QoS value for each and every packet routed through the network.

Weighted QoS = (Additive QoS metric)*(weight coefficient associated with priority level of packet)

So whenever a node has to send a packet, it calculates the weighted QoS metric for the packet. Finally a path with higher QoS is used for the higher priority packets.

3.4.2 Minimum Cost Path Forwarding

The minimum cost path forwarding protocol combines the delay, throughput, and energy consumption characteristics to establish routes between nodes in the network. This is done by assigning a cost function to each link. So due to cost function, a new cost field is indicated at sensor node. Now the case is that packets flow through this field, containing the description of the next hop with the lowest cost.

Two phases of this protocol are: (1) cost field establishment (2) cost path forwarding.

The cost field establishment phase aims to determine the minimum cost between any node and the sink. The sink broadcasts an ADV advertisement message having cost zero. Here forwarding of ADV message is done by cost updates. Each node *j*, which receives an ADV message from node *i*, and calculates the cost as $S_{\mathrm{i}} + T_{\mathrm{j,i.}}$

Where S_i is the node *i* cost (for sink value is 0) and from node *j* to node *i* cost is $T_{j,i}$. Now a backoff timer is set at each node, proportional to its cost to node *i*, *Tj,i* , and the ADV message is broadcasted. The backoff time is used to make the node to update its cost to the base station or sink by selecting the minimum cost node to the base station or sink.

In the second phase, the source node broadcasts the data message to its neighbouring nodes. The message is now routed through cost field mentioned in sensor nodes. So, when a sensor node (source) broadcasts a message, it also sends the minimum cost of the source to the base station or sink.

Based on the cost field concept, the messages can be routes without specific route information, neighbourhood information, or node IDs. Each packet is broadcast without specifying the next hop and the next hop is selected as a result of the budget and sum of link cost and minimum cost. The message is dropped when it is assured that the cost is insufficient to reach the destination, otherwise, the message is forwarded until it reaches the sink. As a result, the minimum cost path forwarding mechanism delivers the messages according to the minimum costs at each node.

3.4.3 SPEED

The SPEED protocol exploits the fact that considering end-to-end performance requirement, distance between the source and destination is also important. Thus the protocol provides guaranteed packet arrival on time constraint..

Several components are used to provide speed guarantees to the packet in the network. The *neighbour beacon exchange* protocol is periodically run to exchange location information between neighbours. As a result, each node constructs a neighbour table and stores the information about its neighbours with the following fields: SendToDelay, NeighbourID, Position, and ExpireTime. The SendToDelay is the delay estimated at the neighbour node and ExpireTime controls the expiration time when the particular entry is deleted from the table if no updates are received.

In addition to the location, each node stores the estimated delay to its neighbours in its neighbour table. Delay estimation is performed at the sender node when any packet is sent to the particular neighbouring nodes. The sender saves the time of keeping the packet in its queue and receiving the ACK from its neighbours. Moreover, the receiver neighbour communicates the duration of processing for the ACK using the ACK packet, which is subtracted from the delay estimate. In case multiple packets are sent to the same neighbour, the moving average of the delay estimates is stored in the neighbour table. The SendToDelay value stored for each neighbour is used for forwarding using the stateless nondeterministic geographic forwarding (SNGF) algorithm of SPEED. SNGF aims to forward the packets to neighbours that can provide a minimum delivery speed of $S_{setpoint}$. SNGF chooses the next hop among the forwarding candidates with estimated speed higher than $S_{setpoin}t$. As a result, forwarded packets are guaranteed to reach a minimum speed. However, if no node is found to satisfy this requirement, the packet is randomly dropped according to the neighbourhood feedback loop (NFL). The NFL component of SPEED controls the packet drop procedure in case there is no neighbour satisfying the the condition of minimum speed. Therefore we have a miss ratio. The miss ratio of each neighbour is define as the rate at which the neighbour node does not satisfy the speed requirement, is calculated. Based on the miss ratio of the neighbour, the NFL determines either to drop or forward the packet.

In some cases, the packets can be routed toward *hot spots*, where there exists a high contention. To prevent further packets from being forwarded to the same region, SPEED also employs a backpressure mechanism. Nodes which experience high miss rates send backpressure beacons to the upstream nodes. The backpressure beacons are used to remove these neighbours from the neighbour list and, as a result, packets are rerouted around the hot spots to relieve congestion. Advantages of SPEED are: (1) Energy efficient because of the small overhead of establishing the route. (2) SPEED is enhanced to provide multiple speed guarantees for different traffic types through the MMSPEED protocol.

The main disadvantage of SPEED is that only a single speed guarantee can be supported in the network.

4. CONCLUSION

Wireless sensor networks (WSN) have many applications that demands energy consumption, optimum path selection and desirable quality of service. So designing such routing protocols that extend the lifetime of sensor node as well as the network lifetime is an emerging issue. In this paper, we have addressed different challenges in routing in WSN and also tried to explain different routing protocols stating their strength and weakness as well. Many authors have proposed different routing protocols but still some issues need to be addressed in the future.

REFERENCES

[1] Dave, P. M., & Dalal, P. D. “Simulation and Performance Evaluation of Routing Protocols in Wireless Sensor Network.” *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(3), (2013).

[2] Singh, S. K., Singh, M. P., & Singh, D. K. “Routing protocols in wireless sensor networks–A survey.” *International Journal of Computer Science & Engineering Survey (IJCSES) Vol*, *1*, 63-83. (2010).

[3] Goyal, D., & Tripathy, M. R. “Routing protocols in wireless sensor networks: A survey.”In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 474-480), IEEE (2012, January).

[4] Patil, M., & Biradar, R. C. “A survey on routing protocols in Wireless Sensor Networks.” In *Networks (ICON), 2012 18th IEEE International Conference on* (pp. 86-91), IEEE (2012, December).

[5] Abdullah, M., & Ehsan, A. “Routing Protocols for Wireless Sensor Networks: Classifications and Challenges. “*Journal of Electronics and Communication Engineering Research*, *2*(2), 5-15. (2014).

[6] KalaiMagal R. and Revathy M. “A Survey On Wireless Sensor Network Protocols.” International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.

[7] Al-Karaki, J. N., & Kamal, A. E. “Routing techniques in wireless sensor networks: a survey.”*Wireless communications, IEEE*, *11*(6), 6-28, (2004).

[8] García Villalba, L. J., Sandoval Orozco, A. L., Triviño Cabrera, A., & Barenco Abbas, C. J. “Routing protocols in wireless sensor networks.” *Sensors*,*9*(11), 8399-8421, (2009).

[9] Frey, H., Rührup, S., & Stojmenović, I. “Routing in wireless sensor networks.” In *Guide to Wireless Sensor Networks* (pp. 81-111), Springer London, (2009).

[10] Li, C., Zhang, H., Hao, B., & Li, J. “A survey on routing protocols for large-scale wireless sensor networks.” *Sensors*, *11*(4), 3498-3526, (2011).

[11] Radi, M., Dezfouli, B., Bakar, K. A., & Lee, M. “Multipath routing in wireless sensor networks: survey and research challenges.” *Sensors*, *12*(1), 650-685, (2012).

[12] Liu, X. “A survey on clustering routing protocols in wireless sensor networks.” *Sensors*, *12*(8), 11113-11153, (2012).

[13] Tyagi, M. P., & Jain, M. S. “Comparative Study of Routing Protocols in Wireless Sensor Network.” *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(9), (2012).

[14] El-Bendary, N., Soliman, O. S., Ghali, N. I., Hassanien, A. E., Palade, V., & Liu, H. “A secure directed diffusion routing protocol for wireless sensor networks.” In *Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on* (pp. 149-152). IEEE, (2011, June).

[15] Beydoun, K., & Felea, V. “WSN hierarchical routing protocol taxonomy.” In *Telecommunications (ICT), 2012 19th International Conference on*(pp. 1-6), IEEE, (2012, April).

[16] Sharma, M. “Wireless sensor networks: Routing protocols and security issues.”In *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on* (pp. 1-5), IEEE, (2014, July).

[17] Kumar, P., Singh, M. P., & Triar, U. S. “A review of routing protocols in wireless sensor network.” In *International Journal of Engineering Research and Technology* (Vol. 1, No. 4 (June-2012)). ESRSA Publications, (2012, June).

[18] Raza, M., Ahmed, G., Khan, N. M., Awais, M., & Badar, Q. “A comparative analysis of energy-aware routing protocols in wireless sensor networks.” In *Information and Communication Technologies (ICICT), 2011 International Conference on* (pp. 1-5). IEEE, (2011, July).

[19] Wei, C., Yang, J., Gao, Y., & Zhang, Z. “Cluster-based routing protocols in wireless sensor networks: a survey.” In *Computer Science and Network Technology (ICCSNT), 2011 International Conference on* (Vol. 3, pp. 1659-1663), IEEE, (2011, December).

[20] Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. “Energy-efficient routing protocols in wireless sensor networks: A survey.” *Communications Surveys & Tutorials, IEEE*, *15*(2), 551-591, (2013).

[21] Latif, K., Jaffar, M., Javaid, N., Saqib, M. N., Qasim, U., & Khan, Z. A. “Performance Analysis of Hierarchical Routing Protocols in Wireless Sensor Networks.” *arXiv preprint arXiv:1208.2397*, (2012).

[22] Ghaffari, Z., Jafari, T., & Shahraki, H. E. “Comparison and Analysis Data-Centric Routing Protocols in Wireless Sensor Networks.” In*Communication Systems and Network Technologies (CSNT), 2013 International Conference on* (pp. 351-355), IEEE, (2013, April).

[23] Gnanasekaran, T., & Francis, S. A. J. “Comparative analysis on routing protocols in Wireless Sensor Networks.” In *Computer Communication and Informatics (ICCCI), 2014 International Conference on* (pp. 1-6), IEEE, (2014, January).