ANALYSIS OF ROUTING PROTOCOL TO MAXIMIZE THE LIFETIME OF WIRELESS SENSOR NETWORK

Diksha, Neha Thakur

1,2Department of Computer Science & Engineering
Career Point University Hamirpur(H.P)

Abstract- A wireless sensor network is type of wireless network. Wireless sensor network is a group of small sensor nodes which communicate through radio interface. WSN is made up of tiny sensor nodes which senses the data and communicate to the base station via other nodes. In WSN, the sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are also limited. Sensor nodes have some constraints due to their limited energy, storage capacity and computing power. The communication of gathered data in the network from the node to base station is a prominent activity and this consumes the maximum amount of energy. Thus affect the lifetime of the wireless sensor network. Data are route from one node to another using different routing protocol. There are number of routing protocol for wireless sensor network. These energy efficient routing protocols select a best path for data transmission and consume less energy. In this paper the LEACH and PEGASIS and TEEN protocol is analyzed through simulation with sink mobility to maximize the lifetime of WSN.

Keywords: Wireless sensor network, Design issues, Routing protocol, LEACH, PEGASIS and TEEN.

1. INTRODUCTION

Wireless sensor networks (WSNs) have been used in a wide range of applications. Wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc.

A WSN can be defined as a network of devices, denoted as nodes, which can sense the environment and communicate the information gathered from the monitored field (e.g., an area or volume) through wireless links. The data is forwarded, possibly via multiple hops, to a sink (sometimes denoted as controller or monitor) that can use it locally or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving. They can be aware of their location or not. They can be homogeneous or not.

Sensing is a technique used to gather information about a physical object or process, including the occurrence of events. An object performing such a sensing task is called a sensor. If the sensor require external power, they are referred to as active sensor. WSN collects data from target area and then forwards towards an infrastructure processing node or base station (BS). A base station and/or sensor nodes may be a fixed or mobile. WSNs may consist of up to thousands of nodes, which can be deployed in very high density, in homes, highways, buildings, cities, and infrastructures for monitoring and/or controlling purposes.

Routing in WSN is very challenging due to the resource constraint characteristics that distinguish these networks from other wireless networks like mobile ad hoc networks or cellular networks. In WSN, the routing protocols [5] are application specific, data centric, capable of aggregating data and capable of optimizing energy consumption. The important characteristics of a good routing protocol for WSN are simplicity, energy awareness, adaptability and scalability due to limited energy supply, limited computation power, limited memory and limited bandwidth of WSN [4]. The main design goal of WSNs is to carry out data communication while trying to prolong the lifetime of the network.

A. Design Issues Of Routing Protocol

Initially WSNs was mainly motivated by military applications. Later on the civilian application domain of wireless sensor network have been considered, such as environmental and species monitoring, production and healthcare, smart home etc. These WSNs may consist of heterogeneous and mobile sensor nodes, the network topology may be as simple as a star topology; the scale and density of a network varies depending on the application. To meet this general trend towards diversification, the following important design issues [8] of the sensor network have to be considered.

- Fault Tolerance
  Some sensor nodes may fail or be blocked due to lack of power, have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures.
Scalability
The number of sensor nodes deployed in the sensing area may be in the order of hundreds, thousands or more and routing schemes must be scalable enough to respond to events.

Production Costs
Since the sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the networks and hence the cost of each sensor node has to be kept low.

Operating Environment
We can set up sensor network in the interior of large machinery, at the bottom of an ocean, in a biologically or chemically contaminated field, in a battle field beyond the enemy lines, in a home or a large building, in a large warehouse, attached to animals, attached to fast moving vehicles, in forest area for habitat monitoring etc.

Power Consumption
Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multi-hop routing will consume less energy than direct communication. However, multi-hop routing introduces significant overhead for topology management [11] and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink. Sensor nodes are equipped with limited power source. Node lifetime is strongly dependent on its battery lifetime.

Data Delivery Models
Data delivery models determine when the data collected by the node has to be delivered. Depending on the application of the sensor network, the data delivery model to the sink can be Continuous, Event-driven, Query-driven and Hybrid [9]. In the continuous delivery model, each sensor sends data periodically. In event-driven models, the transmission of data is triggered when an event occurs.

Data Aggregation/Fusion
Data aggregation is the combination of data from different sources by using functions such as suppression (eliminating duplicates), min, max and average. This technique has been used to achieve energy efficiency and traffic optimization in a number of routing protocols.

Quality Of Service (QoS)
The quality of service means the quality service required by the application, it could be the length of life time, the data reliable, energy efficiency, location-awareness, collaborative-processing. These factors will affect the selection of routing protocols for a particular application. In some applications (e.g., some military applications) the data should be delivered within a certain period of time from the moment it is sensed.

Node Deployment
Node deployment is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data is routed through pre-determined paths.

B. Routing Protocols in WSN:
Routing is a process of determining a path from a source node to its destination node for data transmission. Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements [5]. Many routing algorithms were developed for wireless networks in general.

i) LEACH:
LEACH (Low Energy Adaptive Clustering Hierarchy) is one of the first hierarchical routing approaches for sensors networks. LEACH is a self-organizing, adaptive clustering protocol. It uses randomization for distributing the energy load among the sensors in the network. Low energy adaptive clustering hierarchy LEACH is one of the most popular routing algorithm for sensor network. The idea is to form cluster of the sensor node based on received signal strength and use local cluster head as router to the sink. This will save energy since the transmission will only be done by such cluster head rather than all sensor node[10].
In LEACH operation is divided into rounds, during each round a different set of nodes are cluster head (CH). Nodes that have been cluster head cannot becomes cluster head again for P rounds. At the end of each round, each node that is not a cluster head select the closest cluster head and joins that cluster to transmit data. The cluster head aggregate and compress the data and forward it to the base station. For the network, we use a model where nodes always have data to send to the end user and nodes located close to each other have correlated data. Although LEACH is optimized for this situation, it will continue to work if it were not true.
LEACH Operation
The operation of leach can be executed by number of iterations. Each iteration contain two phase:1) setup phase and 2) steady phase.

- Setup phase
  In the set-up phase, clusters are formed and a CH is selected for each cluster. The CH is selected from the sensor nodes at a time with a certain probability. The job of the cluster head is to collect data from their surrounding nodes and pass it on to the base station. LEACH is dynamic because the job of cluster head rotates.

- Steady phase
  During the steady phase operation is divided into frames where each node in the cluster sends data to the CH at most once per frame. From the cluster head finally data is sent to the base station. If the same node would remain as the cluster head throughout the working of the network, it would die quickly because of the extensive load so cluster head are re-elected when their energy reduced to certain threshold level.

ii) PEGASIS:
PEGASIS (Power-Efficient Gathering in Sensor Information Systems), which is near optimal for this data gathering application in sensor networks. The key idea in PEGASIS is to form a chain among the sensor nodes so that each node will receive from and transmit to a close neighbour. The data from one node to another makes data aggregation and send by leader to BS. [11] Gathered data moves from node to node, get fused, and eventually a designated node transmits to the BS. Nodes take turns transmitting to the BS so that the average energy spent by each node per round is reduced.

Inexpensive sensors capable of significant computation and wireless communications are becoming available. A web of sensor nodes can be deployed to collect useful information from the field, for example, in harsh physical environments. Since wireless communications consume significant amounts of battery power, sensor nodes should spend as little energy as possible receiving and transmitting data. It is necessary for communication protocols to maximize nodes lifetimes, reduce bandwidth.

The improvement of LEACH protocol is PEGASIS (power efficient gathering in sensor information system). It makes the chain of nodes instead of making clusters of it. The farther node will transmit the data via its neighbour node and in this way chain is created. The last node in the chain is called the leader node which will transmit all the data to sink (base station).
Fig: PEGASIS Protocol

**PEGASIS operation**

The PEGASIS operation is divided into two steps: a) chain construction  b) gathering data

- **Chain construction**
  
  PEGASIS protocol forms a chain of the sensor node and the chain is formed using a greedy approach, starting from the node farthest to the sink node. The nearest node sends the data to the neighbour node. This procedure is continued until all the nodes are included in the chain.

- **Gathering data**
  
  For gathering data in each round, each node receives data from one neighbour, fuses with its own data, and transmit to the other neighbour on the chain. Note that node i will be in some random position j on the chain. Thus the leader in each round of communication will be at a random position on the chain which is important for node to die at random location. The idea in node dying at random places is to make the sensor network robust to failure. In a given round, we can use a simple control token passing approach initiated by the leader to start the data transmission from the ends of the chain. The cost is very small since the token size is very small. PEGASIS performs data fusion at every node except the end node in the chain. Each node will fuse its neighbour’s data with its own to generate a single packet of the same length and then transmit than to its other neighbour.

**iii) TEEN:**

It stands for Threshold Sensitive Energy Efficient Sensor Network Protocol. The first protocol developed for reactive networks is TEEN (Threshold sensitive Energy Efficient sensor Network protocol). TEEN is based on cluster based hierarchical approach and uses data centric method. TEEN is event-driven, reactive protocol which is best suited for time critical application. It transmits data based on hard threshold and soft threshold values as it uses data centric approach in which data is crucial and requested based on attribute value[14]. In TEEN protocol cluster head formation process is based on LEACH (Low Energy Adaptive clustering in Hierarchy). First the clusters are formed, and then CH broadcasts two thresholds to the all member nodes: hard threshold (HT), and soft threshold (ST). At every cluster change time this two attributes are also broadcast by CH[15].

The functioning of TEEN is:

- **Hard threshold (HT):** This is a threshold value for the sensed attribute. It is the absolute value of the attribute beyond which, the node sensing this value must switch on its transmitter and report to its cluster head.

- **Soft Threshold (ST):** This is a small change in the value of the sensed attribute which triggers the node to switch on its transmitter and transmit.

**III. SIMULATION AND ANALYSIS**

**A. LEACH:**

Leach graph shows that the number of dead nodes in the network increases in the successive round. This graph between the number of nodes and number of rounds shows that the last sensor node dies at less than 2000 rounds.
B. PEGASIS:
The graph between the number of nodes and number of rounds shows that the first sensor node dies at around 150 rounds and last node dies at around 1000 rounds for the given simulation for 1000 rounds.
C. TEEN:
In this protocol the graph between the number of nodes and number of rounds shows that the first sensor node dies at around 1500 rounds and the last node dies at around 4000 rounds for the given simulation for 5000 rounds.

![Graph between no. of nodes and no. of rounds](image)

**Fig 3: Graph between no. of nodes and no. of rounds**

**Protocol and lifetime of network**

**Comparison of LEACH, PEGASIS AND TEEN routing protocol:**

![Comparison of no. of nodes and no. of rounds](image)

**Fig 4: Comparison of no. of nodes and no. of rounds**

**IV. CONCLUSION**

Routing protocol is a very important area in wireless sensor network. In this paper we have discussed several protocol and design issues in the wireless sensor networks. We have several no. of routing protocols and these were used based upon the type of network and its application.

One of the main challenges in the design of routing protocols for WSNs is energy efficiency due to the scarce energy resources of sensors. The ultimate objective behind the routing protocol design is to keep the sensors operating for as long as possible, thus extending the network lifetime. The energy consumption of the sensors is dominated by data transmission and reception. Therefore, routing protocols designed for WSNs should be as energy efficient as possible to prolong the lifetime of individual sensors, and hence the network lifetime.
REFERENCES


