Study of Routing protocols in Wireless Sensor Networks: A Review

Promila[1], Sandeep Dalal[2]

[1]M.tech Scholar, Department of Computer Science and Applications,
M. D. University, Rohtak-124001, Haryana, India

[2]Assistant Professor, Department of Computer Science and Applications, M. D. University,
Rohtak-124001, Haryana, India

ABSTRACT

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power which enable us to deploy a large-scale sensor network. Such sensor networks are expected to be widely deployed in a vast variety of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering. In this paper, we focus on study of routing protocols and compare two most important protocols of wireless sensor networks i.e. Zigbee and Leach.

Keywords: networks, wireless sensor networks, Zigbee, leach

1. INTRODUCTION

The advances in the Wireless technology are also one of the major stimuli for the growth of mobile computing. But here in this ubiquitous computing environment we can't follow the normal architecture and protocols which have been used in the fixed network due to its battery powered devices involved in the computing and transmission of the data. The sensor networks can also be used in Disaster Relief, Emergency Rescue operation, Military, Habitat Monitoring, Health Care, Environmental monitoring, Home networks, detecting chemical, biological, radiological, nuclear, and explosive material etc. [1], [2], [3].

The sensor nodes not only collect useful information such as sound, temperature, light etc., they also play a role of the router by communicating through wireless channels under battery-constraints [1].Since the entire sensor nodes are battery powered devices, energy consumption of nodes during transmission or reception of packets affects the life-time of the entire network. To make routing, an energy efficient, number of protocols like LEACH was developed [4]. Though they have achieved efficiency by more than 8 times than the previous protocols, still these are used for only static sensor nodes.

2. ROUTING STRATEGIES IN WSN

Routing is a process of determining a path between source and destination upon request of data transmission. In WSNs, the layer that is mainly used to implement the routing of the incoming data is called as network layer. A number of routing protocols have been developed for the WSN till today. Due to its constraints in the processing power and limited battery power, the routing protocols for the wired networks cannot be used here. All the proposed protocols will fall under any of the three categories:

1) Direct approach
2) Location based routing
3) Attribute based routing.

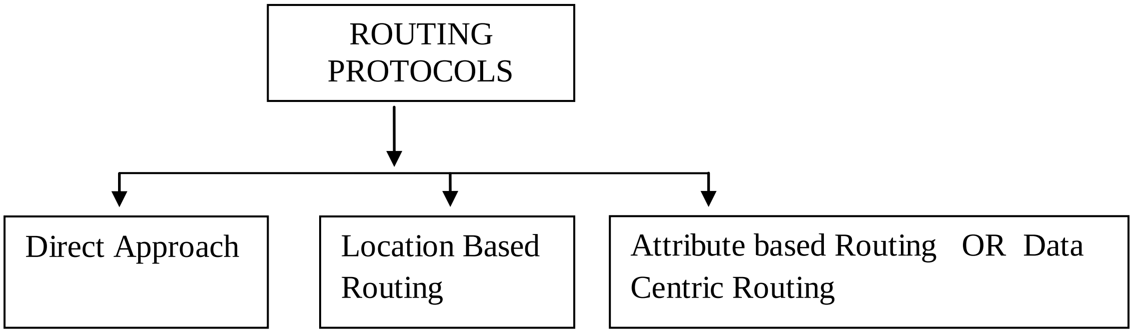

Figure 1. Hierarchical classification of routing strategies

The simple flooding type routing protocols falls under the direct approach. Though it is simple in its implementation, it is not an energy efficient protocol for the sensor networks.

In the Location based routing the base station communicates with sensor nodes based on its location identity [14] . Here all the nodes are aware of its location through GPS (Global Positioning System) receivers in the network. The location information of the individual nodes is obtained by the low power GPS receivers embedded in the nodes. Some of the most important protocols coming under the Location based routing strategy are:

- Greedy approach
- Compass routing
- DREAM
- GPSR
- GEAR

In WSN, instead of collecting information from all the nodes the application needs the data only from the nodes which satisfies its interest and this information gathering technique is widely called as the data centric approach or attribute based routing. Some of the protocols which follow the data centric routing are:

- Directed diffusion
- SPIN
- Rumor routing

3.ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

Routing protocols have a large scope of research work when implemented in a WSN, because the functioning of these protocols depends upon the type of network structure designed for the application or the network operations carried out using these protocols for a specific application model. Figure 2 shows the protocol classification or routing taxonomy for routing protocols which are further sub-divided into subcategories. A brief introduction of each category is given below.

3.1 Structure Based Routing Protocols

Routing protocols are divided into structure-based routing protocols, which are in turn classified as flat routing, hierarchical routing and location-based routing[13]. The protocols which falls under these categories work with respect to the design constraints given for the network structure or area.

3.1.1 Flat network Routing (FNR)

This is a routing technique in which all the sensor nodes play the same roles, such as collecting data and communicating with the sink, i.e. all the data collected in the remote area can be same or duplicated as all the sensor nodes work in the same way .

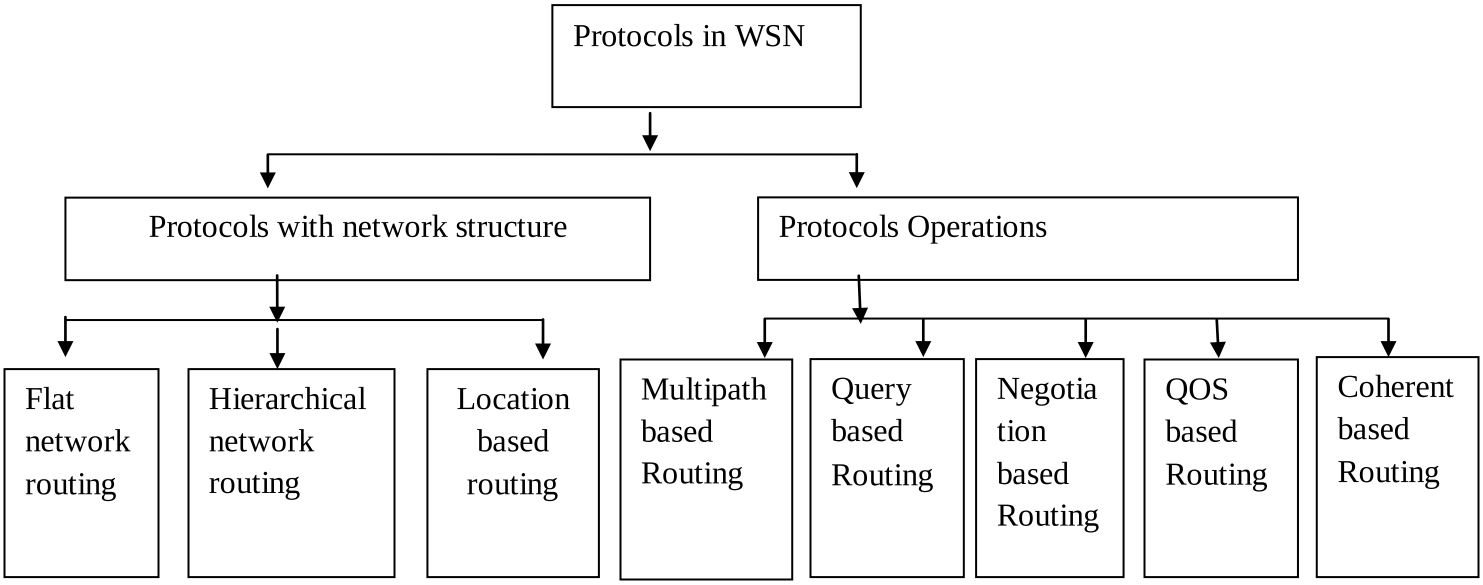

Figure 2. Routing Protocols in Wireless Sensor Networks: Taxonomy

3.1.2 Hierarchical Network Routing

In this routing technique all the routing sensors in the network are clustered and a cluster head collects and aggregates the data and checks for redundancy of the data that is collected before it is sent to the sink. This saves communication and processing work and also saves energy .

3.1.3 Location-based Routing

In location-based routing, all the sensor nodes are addressed by using their locations. Depending upon the strength of the incoming signals, it is possible to calculate the nearest neighboring node's distance. Due to obstacles in the network often the signal strength becomes weaker and nodes find it difficulty in finding the nearest neighbor nodes, Small minimum energy consumption network performs well in such situations also by creating a sparse graph of the network nodes before transmitting to the next node. All the nodes in the network exchange this data in order to know about neighboring nodes. This is useful for communicating and transferring information. As energy is the major factor of concern in routing protocols, location-based schemes demand that nodes should change their state from active to sleep mode when there is no activity. The more nodes in sleep mode, the more energy is saved. There are many location-based schemes of which GAF (Geographic Adaptive Fidelity) and GEAR (Geographic and Energy aware Routing) are two examples[19].

3.2 Protocol Operation Based Routing Protocols

Routing protocols taxonomy has another basic and important classification, namely operation-based routing protocols, which is in turn divided into multi-path based, query-based, Negotiation-based, quality-of-service (QoS) based and coherent-based routing protocols[13]. The protocols which come under this classification work according to the network-structure operation, or the way the structure needs the protocols to work depending upon the sudden changes it undergoes.

3.2.1 Multi path-based Routing

These protocols are efficient in handling multiple paths. Nodes send the collected data on multiple paths rather than using a single path. The reliability and fault tolerance of the network increases as there is, as long as it is possible, an alternative path when the primary path fails.

3.2.2 Query-based Routing

Query-based routing propagates the use of queries issued by the base station. The base station sends queries requesting for certain information from the nodes in the network. A node, which is responsible for sensing and collecting data, reads these queries and if there is a match with the data requested in the query it starts sending the data to the requested node or the base station (here). This process is known as Directed Diffusion where the base station sends interest messages on to the network [17]. These interest messages, which move in the network, create a path while passing through all the sensor nodes. Any sensor node, which has the data suitable to the interest message, sends collected data along with the interest message towards the base station. Thus, less energy is consumed and data aggregation is performed on a route.

3.2.3 Negotiation-based Routing

These protocols use high-level descriptors coded in high level so as to eliminate the redundant data transmissions. Flooding is used to disseminate data, due to the fact that flooding data are overlapped and collisions occur during transmissions [13]. Nodes receive duplicate copies of data during transmission. The same data content is sent or exchanged again and again between the same set of nodes, and a lot of energy is utilized during this process. Negotiation protocols like SPIN are used to suppress duplicate information and prevent redundant data from being sent to the next neighboring nodes or towards the base station by performing several negotiation messages on the real data that has to be transmitted .

3.2.4 Quality of Service (QoS)-based Routing

In this type of routing protocol, both quality and energy have to be maintained within the network. Whenever a sink requests for data from the sensed nodes in the network, the transmission has to satisfy certain quality-of-service parameters, such as, for example, bounded latency (data has to be sent as soon as it is sensed without delaying any further) and bandwidth consumed. Sequential Assignment Routing (SAR) is one of the first routing protocols that use the notion of QoS in routing decisions. Routing decision in SAR depends on three factors: energy consumption within the network by the sink and the nodes, QoS of each path in the network, and priority level of each packet sent.

3.2.5 Coherent-based Routing

In a WSN, the sensor nodes collect data and send it to the nearest neighbors or the sink within the network. In this process, the processing of the collected data is the most important event. There are two types of data-processing techniques followed within the network structure: coherent and non-coherent data processing based routing. All the nodes within the network collect the data and process it before sending to the next nearest node for further processing. This technique is called non-coherent data process routing and the nodes that perform further processing on the data are called aggregators. In coherent routing, after minimum processing, the data is forwarded to the aggregators. This minimum processing includes functions like time stamping or duplicate suppression. This technique is energy efficient as all the processing is done by the nodes, which reduces the total time and energy consumption .

4. INTRODUCTION TO ZIGBEE AND LEACH PROTOCOLS

4.1 Zigbee Protocol

ZigBee is a standard protocol for Low-Rate Wireless Personal Area Networks (LR-WPAN). Its main features are network flexibility, low data rate, low cost and very low power consumption, which make it suitable for an ad-hoc network between inexpensive fixed, portable and moving devices [15],[18]. The IEEE 802.15.4 protocol includes a PHY layer and MAC sub-layer for the LR-WPAN [18]. The PHY layer offers three operational frequency bands; there are 27 channels allocated in the 802.15.4 range, with 16 channels in the 2.4 GHz band, 10 channels in the 915 MHz band, and 1 channel in 868 MHz band .
The MAC sub-layer handles all access to the physical radio channel. It provides an interface between the service specific convergence sub-layer (SSCS) and the PHY layer.

4.2 ZigBee specifications

Table 1 presents the basic specifications of the ZigBee 802.15.4 standard.

Parameters	**Zigbee values**
Transmission Range(meters)	1-100
Battery life(days)	100– 1,000
Network size	>64,000
Throughput (kb/s)	20-250

Table 1. Basic ZigBee specifications

4.2.1 Network components

IEEE 802.15.4 protocol generally defines three types of nodes:

1) **PAN (Personal Area Network) coordinator**: The main network coordinator identifies its PAN and can be connected to other nodes. In addition, it proposes global synchronization services to other nodes in the network through transmission of beacon frames that contained the identification of PAN and other relevant information.

2**) Coordinator**: It has the same functionality as PAN coordinator, except that it does not create its PAN. Coordinator is connected to the PAN coordinator and provides services for local synchronization of the nodes in its range with significant transfer beacon frames containing the identification of the PAN, which is connected.

3) **Simple (secondary) node**: It is a node with no coordinated functionalities. To be able to synchronize with the other nodes in the network, it is connected as a secondary node with the PAN Coordinator (or with the coordinator). In the IEEE 802.15.4 2003 standard, the first two types of nodes are defined as Full Function Devices – FFD, which means that they implement all the functionalities of the IEEE 802.15.4 protocol.

4.2.2 ZigBee topologies

IEEE 802.15.4 supports three types of topologies: Star, Mesh and Tree that can be considered as a special case of Mesh topology[15].

4.2.2.1 Star topology

In this simple topology, a coordinator is surrounded by a group of either end devices or routers. This type of topology is attractive because of its simplicity, but at the same time presents some key disadvantages. In the moment when the coordinator stops functioning, the entire network is functionless because all traffic must travel through the center of the star. For the same reason, the coordinator could easily be a bottleneck to traffic within the network, especially since a Zigbee network can have more than 60000 nodes [15].

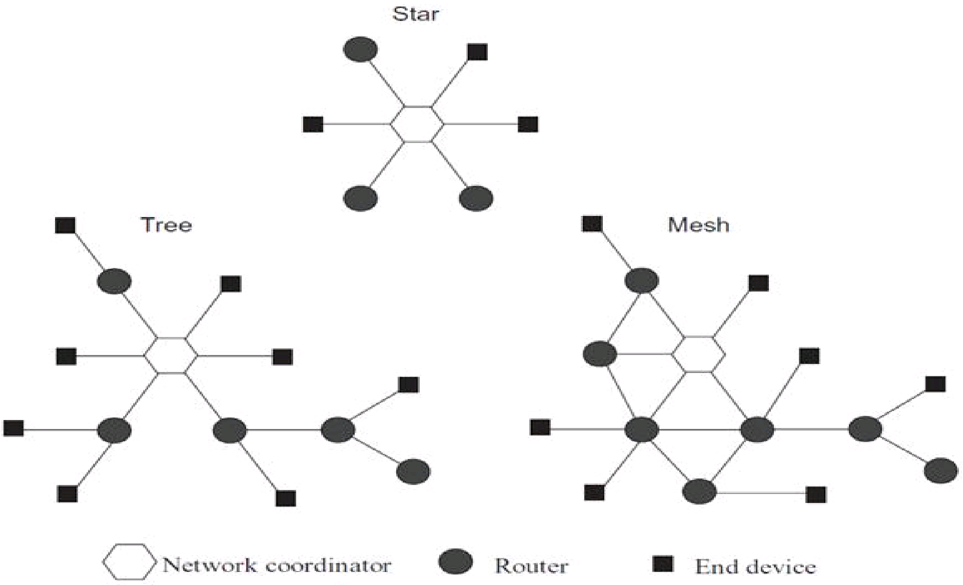

Figure 3. Network topologies

4.2.2.2 Tree topology

In a Tree network, a coordinator initializes the network, and is the top (root) of the tree. The coordinator can now have either routers or end devices connected to it. For every router connected, there is a possibility for connection of more child nodes to each router. Child nodes cannot connect to end devices because it does not have the ability to relay messages.

This topology allows different levels of nodes, with the coordinator being at the highest level. In order the messages to be passed to other nodes in the same network, the source node must pass the messages to its parent, which is the node higher up by one level of the source node, and the message is continually relayed higher up in the tree until it is passed back down to the destination node. Because the number of potential paths a message can take is only one, this type of topology is not the most reliable topology. If a router fails, then all of that router’s children are cut off from communicating with the rest of the network.

4.2.2.3 Mesh topology

Mesh topology is the most flexible topology of the three [15]. Flexibility is present because a message can take multiple paths from source to destination. If a particular router fails, then Zigbee self-healing mechanism will allow the network to search for an alternate path for the message to be passed .

4.2.3 ZigBee layers

ZigBee consists of four layers. The top two (Application and Network) layers specifications are provided by the ZigBee Alliance to provide manufacturing standards. The bottom two (MAC and PHY) layers specifications are provided by the IEEE 802.15.4-2006 standard to ensure coexistence without interference with other wireless protocols, such as Wi-Fi [18].

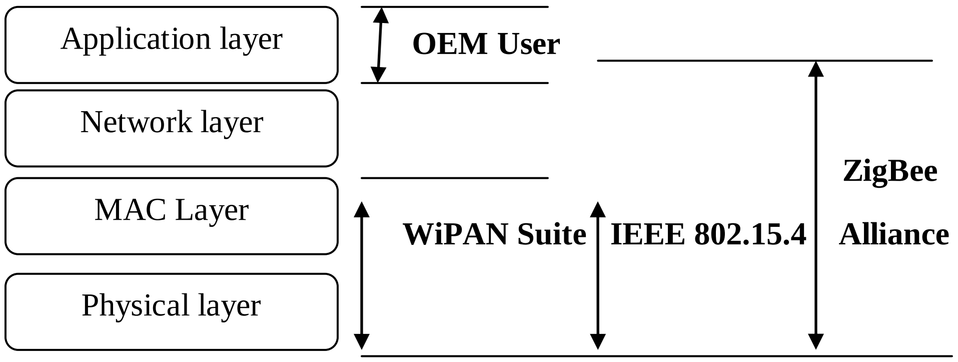

Figure 4. ZigBee layers

4.2.3.1 Application Layer

Application layer is the top layer defined in the specifications and it is an effective interface of ZigBee system to its end users. This layer makes the device useful to the user. It contains most of the components added by the ZigBee specification: an integral part of this layer is also both ZDO (ZigBee Device Object) and its management procedures, along with application objects defined by the manufacturer .

4.2.3.2 Network Layer

A feature of ZigBee such as the self-healing mechanism is acquired through this layer. This layer provides network management, routing management, network message broker, and network security management. The ZigBee Alliance defines this layer, which is an association of companies working together to enable reliable, cost-effective, and low-power wirelessly networked monitoring and control products based on an open global standard .

4.2.3.3 MAC sub-layer

The MAC layer is responsible for the data addressing in order to determine either where the frame is going, or coming from. This layer also provides multiple access control such as CSMA/CA allowing for reliable data transfer. Beaconing is another feature implemented through this layer [15]. Finally, the MAC sub-layer can be exploited by higher layers to achieve secure communication .

4.2.3.4 Physical Layer

The physical layer is provided by the IEEE 802.15.4 standard. This standard manages the physical transmission of radio waves in different unlicensed frequency bands around the world to provide communication between devices within a WPAN. Operates on 2.4 GHz frequency band with 250 kbps data rate and 16 available channels. This layer allows channel selection to avoid radio interference .

4.3 Leach Protocol

Low Energy Adaptive Clustering Hierarchy (LEACH) is the first hierarchical cluster-based routing protocol for wireless sensor network which partitions the nodes into clusters[13],[20]. In each cluster a dedicated node with extra privileges called Cluster Head (CH) is responsible for creating and manipulating a TDMA (Time division multiple access) schedule and sending aggregated data from nodes to the BS where these data is needed using CDMA (Code division multiple access). Remaining nodes are cluster members as shown in figure 5.

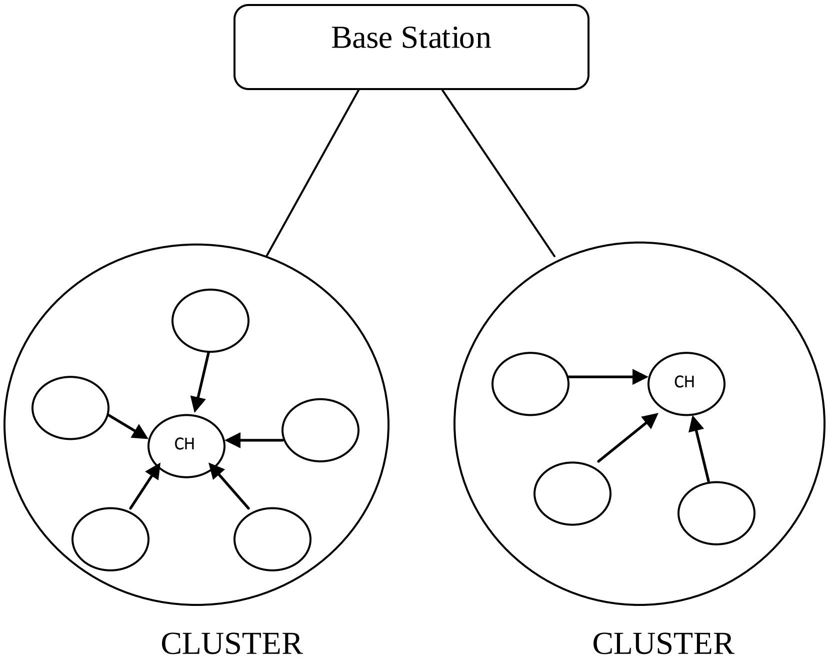

Figure 5: Leach Protocol

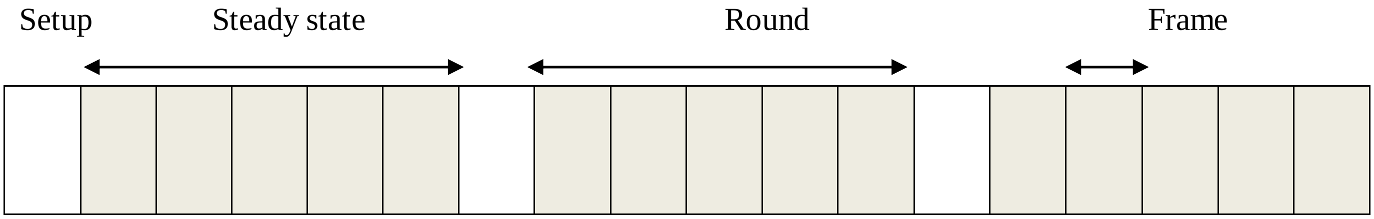

Figure 6 . LEACH protocol phases

This protocol is divided into rounds, each round consists of two phases as shown in figure 6.

4.3.1 Set-up Phase

Each node decides independent of other nodes if it will become a CH or not. This decision takes into account when the node served as a CH for the last time (the node that hasn't been a CH for long time is more likely to elect itself than nodes that have been a CH recently).

In the following advertisement phase, the CHs inform their neighborhood with an advertisement packet that they become CHs. Non-CH nodes pick the advertisement packet with the strongest received signal strength.

In the next cluster setup phase, the member nodes inform the CH that they become a member to that cluster with "join packet" contains their IDs using CSMA [19]. After the cluster-setup sub phase, the CH knows the number of member nodes and their IDs. Based on all messages received within the cluster, the CH creates a TDMA schedule, pick a CSMA code randomly, and broadcast the TDMA table to cluster members. After that steady-state phase begins.

4.3.2 Steady-state phase:

Data transmission begins; Nodes send their data during their allocated TDMA slot to the CH. This transmission uses a minimal amount of energy (chosen based on the received strength of the CH advertisement). The radio of each non-CH node can be turned off until the nodes allocated TDMA slot, thus minimizing energy dissipation in these nodes [20]. When all the data has been received, the CH aggregate these data and send it to the BS. LEACH is able to perform local aggregation of data in each cluster to reduce the amount of data that transmitted to the base station [14]. Although LEACH protocol acts in a good manner, it suffers from many drawbacks such like:

- CH selection is randomly, that does not take into account energy consumption.
- It can't cover a large area.
- CHs are not uniformly distributed.

Where CHs can be located at the edges of the cluster.
Since LEACH has many drawbacks, many researchers have been done to make this protocol perform better.

5.COMPARISON OF ZIGBEE AND LEACH PROTOCOL : A REVIEW

In a WSN environment, where nodes can be deployed at random and in large quantities and the network topology may vary due to sensor failures or energy efficiency decisions, assigning and maintaining hierarchical structures is impractical. The message overhead to maintain the routing tables and the memory space required to store them is not affordable for the energy and resource constrained WSNs.
Reactive protocols such as ZIGBEE and LEACH alleviate some of these problems but questionably scale to very large networks since they depend on flooding for route discovery[13]. Furthermore, LEACH requires the management of large route caches and large packet headers to store the path.

Routing protocols for WSNs should be lightweight in both processing power and memory footprint and should require minimal message overhead. Ideally they should be able to route packets based on information exchanged with its neighborhood and should be resilient to node failures and frequent topology changes. For these reasons most of the research on routing in sensor networks has focused on localized protocols which are tree-based or geography-based.

Routing Tree: Simple data gathering applications where readings collected by sensors are sent to the sink, possibly with some aggregation along the path, need trivial routing. As the query propagates through network, each node just remembers its parent toward the sink and later forwards it any messages it receives/originates.. Routing trees are very easy to construct and maintain but this approach is not suitable for more complex applications that require end-to-end communication.

Especially, broadcast-based routing schemes such as ZIGBEE, LEACH and directed diffusion have a weakness of highly power assumption due to massive broadcast message which cause to deliver duplicated messages [19]. Also, these duplicated messages reduce the efficient bandwidth over network, and frequent collisions of messages due to reduced bandwidth occur. As a consequence, a series of these events reduce the network lifetime overall. Considering above problems, our contribution is find a proper routing method that as well as maintains reasonable efficient bandwidth.

6. CONCLUSION

From the existing study , we observed that Zigbee is more efficient in case of flooding for route discovery whereas Leach in the same requires special management. It is important to mention here that Zigbee and Leach have a weakness to deliver the duplicate messages due to massive broadcast messages which results unnecessary reduction of efficient bandwidth of the network.As a consequence, it reduces the lifetime of the network. The two protocols Zigbee and Leach should be compared using simulation, it would be interesting to note the behavior of these protocols on a real life test bed.

REFERENCES

[1] W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. A survey on sensor- networks. IEEE Communications Magazine, pages 102{114, 2002.

[2] Kumar.S.P. Chee-Yee Chong. Sensor networks: Evolution, opportunities, and challenges. Proc IEEE, August 2003.

[3] Ismail H. Kasimoglui Ian .F. Akyildiz. Wireless sensor and actor research challenges. (Elsevier) Journal, 2(38):351{367, 2004.

[4] Sarika Agarwal Leszek Lilien Maleq Khan, Bharat Bhargava and Pankaj. Self-configuring node clusters, data aggregation, and security in microsensor networks. Department of Management Information Systems Krannert Graduate School of Management Purdue University, West Lafayette, (IN 47907), 2007. pankaj@mgmt.purdue.edu.

[5] Sundeep Karthikeyan Vaidynathan, Sayantan sur and Sinha. Data aggregation techniques in sensor networks. Technical Report,OSU-CISRC-11/04- TR60, 2004.

[6] D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 239-249, 2004. ACM Press.

[7] Xiuli Ren and Haibin Yu1. Security mechanisms for wireless sensor networks. IJCSNS International Journal of Computer Science and Network Security, VOL.6(No.3):100{107, March 2006.

[8] . S. Setia S. Zhu and S. Jajodia. Leap: efficient security mechanisms for large scale distributed sensor networks. Proceedings of the 10th ACM conference on Computer and communications security, pages 62{72, 2003. ACM Press.

[9] J. Stankovic A. Perrig and D. Wagner. Security in wireless sensor networks.

[10] P.Nair H.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda: Energy- efficient and secure pattern based data aggregation for wireless sensor networks. Computer Communications IEEE Sensors, 29:446-455, 2006.

[11] Feng Zhao and Leonidas Guibas, “Wireless Sensor Networks, an information processing approach”, Morgan Kaufmann publishers, pp.294-300, 2004.

[12] Culler D., Estrin D., and Srivastava M., “Overview of Sensor Networks”, IEEE Computer, Vol.37, Iss.8, Aug., 2004.

[13]J. N. Al-Karaki and A. E. Kamal. “Routing techniques in wireless sensor networks: a survey”. In IEEE Wireless Communications, Volume 11, pp. 6-28, 2004

[14] Shamsad Parvin,and Muhammad Sajjadur Rahim. Routing Protocols for Wireless Sensor Networks: A Comparative Study.International Conference on Electronics, Computer and Communication (ICECC 2008)University of Rajshahi, Bangladesh

[15] Dr.S.S.Riaz Ahamed "The role of zigbee technology in future data communication system"Journal of Theoretical and Applied Information Technology2005 - 2009 JATIT.

[16] Kemal Akkaya, Mohamed Younis "A survey on routing protocols for wireless sensor networks", in: Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD 21250, USA, 1 September 2003.

[17] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva, "Directed Diffusion for Wireless Sensor Networking", in Proceedings IEEE/ACM, Vol. 11, No. 1, Fb 2003.

[18] J. Zheng and J. L. Myung, "Will IEEE 802.15.4 Make Ubiquitous Networking a Reality? A Discussion on a Potential Low Power, Low Bit Rate Standard", IEEE Communications Magazine, vol. 42, No. 6, pp. 140- 146, , 2004.

[19] W. Heinzelman, A. Chandrakasan and H. Balakarishnan, "Energy-Efficient Communication Protocols for Wireless Microsensor Networks," Proceedings of the Hawaaian InternationalConference on Systems Science, January 2000.

[20]Wendi Heinzelman, Joanna Kulik, and Hari Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks",Proc. 5th ACM/IEEE Mobicom Conference, Seattle, WA, August 1999.