LEACH PROTOCOL IN WIRELESS SENSOR NETWORK: A SURVEY

Ramya C M[1], Vinutha K M[2], Thejas R J[3] ,Vikas B K [4] , Impana Appaji[5]

[1234] BE Students, Computer Science & Engineering, Academy for Technical and Management Excellence college of Engineering, Mysore, Karnataka, India, cmr.mallik@gmail.com, vinukm2014@gmail.com, thejas350@gmail.com, ,vikasgowda227@gmail.com

[5]Assistant Professor, Computer Science & Engineering, Academy for Technical and Management Excellence college of Engineering, Mysore, Karnataka, India, impana.appaji@gmail.com.

Abstract: A wireless sensor network consists of hundreds to thousands of low-power multi functioning sensor nodes, operating in an unattended environment with sensing and computational capabilities. Out of many routing protocols in the wireless sensor network routing protocols are divided as flat and hierarchical routing protocols due to several limited resources like CPU, memory size, battery etc. LEACH is a hierarchical routing protocol and which makes use of clustering scheme and provides better performance than flat routing protocol. If the LEACH routing protocol is applied to the large wireless sensor network sensor nodes in the specific area cannot communicate with the base station. Hence it will cause serious communication problem. Clusterhead chaining scheme is used to solve the communication problem. But if the clusterhead gets failed the whole data present in that particular head will get lost. Hence we can make use of a secondary clusterhead which contains the maximum amount of data as that of first clusterhead.If the first clusterhead gets failed we can make use of second one while forming chain so that the information will not be lost while forming chain.

KEYWORDS*: Clusterhead Chaining; LEACH Protocol; Secondary Clusterhead*

I. Introduction

A wireless sensor network consists of many small sensor nodes with sensing, processing and wireless communication capabilities. Many routing protocols are proposed for wireless sensor networks because the sensor nodes have limited resources such as CPU, memory and battery. The proposed routing protocols can be divided into flat and hierarchical routing protocols. In flat routing protocols, a data aggregation process is essential to reduce its energy consumption which results from the duplicate transmission of similar information among the adjacent nodes. The hierarchical routing protocols are proposed to solve this problem. It divides sensor network into several clusters and clusterheads are selected in the every cluster. The clusterhead is responsible for the gathering and aggregation of the information in its cluster[1]. In general, they have better performance than flat routing protocols on the energy consumption. However, the hierarchical routing protocol has an assumption that a clusterhead can communicate with the base station which is located outside of the wireless sensor networks by a one-hop routing. Especially, if the network size become larger, this protocol is unsuitable for the vast sensor networks because of a long distance can cause serious communication problems[2]. Therefore, considering restricted resources of the sensor node, this assumption is inappropriate for applications in massive sensor networks. In general, the hierarchical routing protocols have this assumption. The LEACH(low energy adaptive clustering hierarchy) routing protocol is a representative hierarchical routing protocol. It also has this assumption. This paper proposes the clusterhead chaining scheme to overcome this problem. It is suitable for massive sensor networks and the proposed scheme shows better performance than the LEACH routing protocol in addition. But if the clusterhead gets failed whole data present in that particular head will get lost. Hence we can make use of a secondary clusterhead. If the first clusterhead gets failed the second one can be used in the formation of chain and information can be transferred to its neighbour and finally the information will be received by the base station, so that the information will not be lost here. The reminder of this paper is divided into five sections. Section 2 discusses the hierarchical routing protocols and the possible problems in the massive sensor networks. Section 3 discusses the proposed scheme using the clusterhead chaining technique. Section 4 evaluates the proposed scheme and section 5 concludes the paper.

II. Literature Review

A. Cryptography-based approaches

1) F-LEACH

L. B. Oliveria et al. proposed FLEACH, a protocol for securing node to node communication in LEACH-based network. It used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH. FLEACH provides authenticity, integrity, confidentiality and freshness to node-to-node communication. But it is vulnerable to node capturing attack [4].

2) SLEACH

This is the first modified secure version of LEACH called SLEACH, which investigated the problem of adding security to cluster-based communication protocol for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources. SLEACH provides security in LEACH by using the building block of SPINS (Security Protocol for Sensor Network), symmetric-key methods and MAC (Message Authentication Code). SLEACH protects against selective forwarding, sinkhole and HELLO flooding attacks. It prevents intruder to send bogus sensor data to the CH and CH to forward bogus message. But SLEACH cannot prevent to crowd the time slot schedule of a cluster, causing DOS attack or simply lowering the throughput of the CH and does not guarantee data confidentiality. The solution is meant to protect only outsider attack.

3) SHEER

J.Ibriq et al. proposed a secure hierarchical energy efficient routing protocol (SHEER) which provides secure communication at the network layer. It uses the probabilistic broadcast mechanism and three-level hierarchical clustering architecture to improve the network energy performance and increase its lifetime. To secure the routing SHEER implements HIKES a secure key transmission protocol and symmetric key cryptography. They have compared the performance with the secure LEACH using HIKES. *4) R. Srinath et al.* This protocol is based on LEACH protocol; named Authentication Confidentiality cluster based secure routing protocol. It uses both public key (in digital signature) and private key cryptography. This protocol deals with interior adversary or compromised node. Because of the high computational requirement (use of public key cryptography), it is not efficient for the WSNs.

5) Sec-LEACH

Sec-LEACH provides an efficient solution for securing communications in LEACH. It used random-key pre distribution and TESLA for secure hierarchical WSN with dynamic cluster formation. Sec-LEACH applied random key distribution to LEACH, and introduced symmetric key and one way hash chain to provide confidentiality and freshness. Sec-LEACH provides authenticity, integrity, confidentiality and freshness to communications.

6) SS-LEACH

Di Wu et al. introduced a secure hierarchical protocol called SS-LEACH, which is the secure version of LEACH. SS- LEACH improves the method of electing cluster heads and forms dynamic stochastic multi-paths cluster heads chains to communicate to the base station, In this way it improve the energy-efficiency and hence prolong the lifetime of the network. It used the key pre-distribution and self-localization technique to secure the basic LEACH protocol [4]. It prevent compromised node to take part in the network and preserve the secrecy of the packet. It avoids selective forwarding, HELLO flooding and Sybil attack.

7) RLEACH

Secure solution for LEACH has been introduced called RLEACH [4] in which cluster are formed dynamically and periodically. In RLEACH the orphan node problem is raised due to random pair-wise key scheme so they have used improved random pair-wise key scheme to overcome. RLEACH has been used the one way hash chain, symmetric and asymmetric cryptography to provide security in the LEACH Hierarchical routing protocol. RLEACH resists many attack like spoofed, alter and replayed information, sinkhole, worm- hole, selective forwarding, HELLO flooding and Sybil attack.

B. Non-cryptography based Approaches

1) Signal strength based detection approach

Virendra Pal Singh et al. proposed a technique in the paper Signal Strength based HELLO Flood Attack Detection and Prevention in Wireless Sensor Networks using AODV protocol [4]. In this paper, they have used a threshold for RSS i.e. fixed signal strength for sensor nodes, and the RSS of the each received HELLO packet is compared to this threshold. Signal strength = Fixed signal strength in radio, node = ‘friend’ Signal strength > Fixed signal strength in radio, node = ’stranger’ Nodes which are significantly far from adversary will wrongly categorise the adversary as ‘Friend’. As RSS is inversely proportional to the distance. The HELLO message receiving node sends simple test packet to HELLO sending node, if the reply comes in allotted time threshold then HELLO sending node is considered as a friend, if not
then it is classified as a stranger.

III. RELATED WORK

3.1 The LEACH routing protocol

The energy consumption of sensor nodes which is located in near the base station becomes larger because their size of data transmission from them to the base station becomes bigger than the other nodes. Therefore, the LEACH routing protocol uses a clustering scheme in order to distribute the energy consumption evenly and to maximize the survival time of sensor nodes in wireless sensor networks[3]. Several clusterheads are selected and clusters are formed with a clusterhead as the centre. All nodes perform on the role of a clusterhead in turns. Therefore, they can cost the energy evenly.

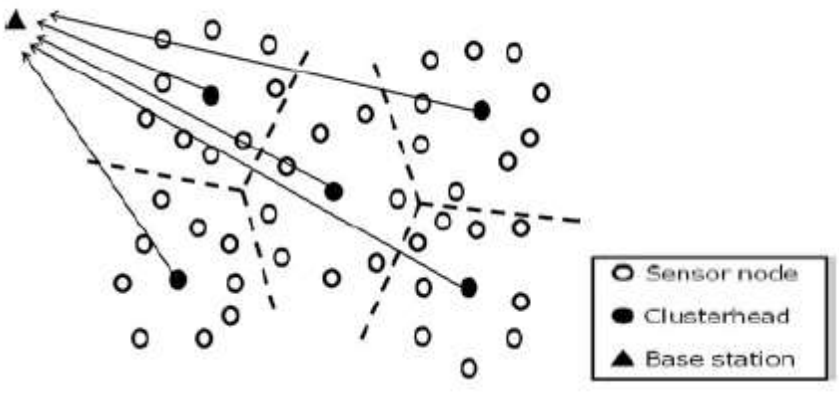

Fig 1: LEACH Protocol

LEACH [7] is one of the first energy-efficient clustering approaches proposed for WSNs. It assumes that sensor nodes communicate with each by single-hop. Its operation is divided into rounds and each round is composed of two phases, as shown in Fig. 2. In the setup phase, the clusters are organized and CHs are selected. Initially a node decides to be a CH with a probability and broadcasts its decision. Each non-CH node chooses the proper cluster to join according to the signal strength from the CHs. Once the clusters are formed, the CH node create TDMA schedule and assigns each node a timeslot when it can transmit. In the steady state phase, the sensor nodes can begin sensing and transmitting data to the CHs. The CH node, after receiving all the data, aggregates it before sending it to the BS. After a certain time, which is determined a priori, the network goes back into the setup phase again and enters another round of selecting new CHs. LEACH [4] divides the whole WSN into some clusters each containing some cluster members and a cluster head which regulates channel access among the cluster members using TDMA. The cluster members wake up from sleep state during their respective TDMA slot during which they transmit data to the cluster head which then aggregates, fuses and finally transmits the data directly to the sink. So that the cluster head doesn't die out quickly, at a fixed interval a new cluster head is dynamically elected from the not-yet chosen cluster members based on their residual energy. LEACH reduces energy consumption by a factor of 7 compared to direct communication and a factor of 4-8 compared to minimum energy transmission routing protocols by limiting the data transmission to long distance sink to only a few cluster heads. Moreover, each cluster head also performs local computation on the gathered data to reduce its volume. But, due to broadcast required during the cluster head selection process, good amount of energy is wasted.

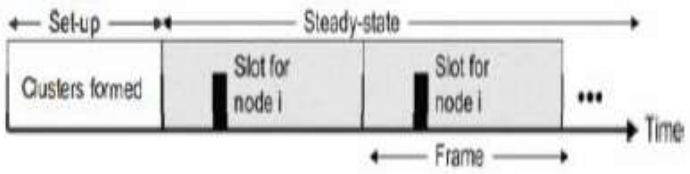

Fig 2: LEACH Operations

3.2 Communication Problem in LEACH Protocol

There is an assumption that all nodes have sufficient energy to perform the clusterhead in the hierarchical routing protocol[7]. Also, it is assumed that all nodes can communicate with the base station by one-hop routing regardless of the distance between them[1][2]. The LEACH routing protocol is the typical hierarchical routing protocol. It uses the clustering scheme and has this assumption. Therefore, if the LEACH routing protocol is applied to the massive sensor networks, then sensor nodes in the specific area cannot communicate with the base station. It can cause serious problem because there is no consideration about distance from sensor nodes to the base station in LEACH routing protocol.

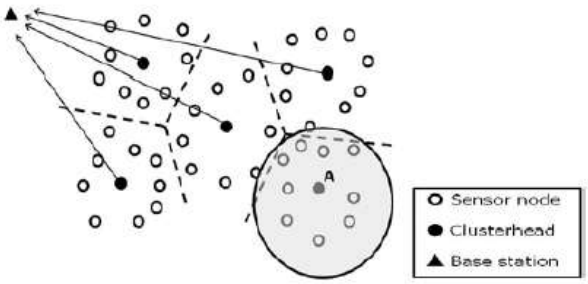

Fig 3: Communication Problem

For example, as shown Fig.3, the clusterhead of the cluster A cannot communicate with the base station since the distance between the clusterhead and the base station is too far. Most of hierarchical routing protocols in general have this problem. Previously proposed CCRS scheme used to overcome this problem. A wireless sensor network field is divided into several clusters which are shaped a concentric circle. These clusters are called levels. In each level, all sensor nodes are formed a chain and one of the sensor nodes is selected as a head node in each round. After the head node collects the data from all sensor nodes in its level, it delivers the data to the head node in upper level. It seems to be suitable to vast sensor network. However, there is a problem which is imbalance of the energy consumption among the sensor nodes because the number of sensor nodes in each level is different. Also, there is no thought of the number of levels compared with the size of the sensor network or the number of all sensor nodes in the network. Therefore there is a need of an enhanced scheme to support massive sensor networks to avoid communication problem

IV. PROPOSED SCHEME.

The proposed scheme consists of four phases which are the clusterhead selection, cluster formation, clusterhead chaining, and data transmission. This proposed scheme is based on the LEACH routing protocol and trying to improve it by using the clusterhead chaining scheme. The performance of LEACH protocol is improved here. The energy consumption of sensor nodes which is located in near the base station becomes larger because their size of data transmission from them to the base station becomes bigger than the other nodes. Therefore, the LEACH routing protocol uses a clustering scheme in order to distribute the energy consumption evenly and to maximize the survival time of sensor nodes in wireless sensor networks[3]. Several clusterheads are selected and clusters are formed with a clusterhead as the center. All nodes perform on the role of a clusterhead in turns. Therefore, they can cost the energy evenly. The four phases are

- **Clusterhead selection**

At this Phase base station sends threshold signal to the network. In the network sensor nodes communicates with each other and it calculates the number of nodes one particular node communicates. If it is greater than or equal to the threshold it is selected as the clusterhead or else it is a normal sensor node

- **Cluster formation**

The node reports that they are member of the cluster to its clusterhead by analyzing the distance between this node and the clusterhead.

- **Clusterhead chaining**

At this phase, every clusterhead realizes neighbouring clusterheads. All clusterheads are formed a chain by using a chaining scheme. The clusterhead can always send its data only to neighbouring clusterhead, even though the size of a sensor network becomes a very larger. If any clusterhead gets failed it makes use of secondary clusterhead to form chain.

- **Data transmission.**

Each sensor node sends a message by its TDMA schedule. Then a clusterhead receives the information of all nodes and performs a data aggregation. After that, a clusterhead sends a processed data to a neighbouring clusterhead.

4.1 Methodology

4.1.1 Clusterhead selection phase

At this phase, clusterheads are selected [8]. Each sensor node selects random number from 0 to 1. If the random number is smaller than a threshold, the sensor node is selected as a clusterhead. As shown in Fig. 4, the clusterheads notice that they are selected as a clusterhead to neighbouring nodes. The nodes which are received this message compare the strength of the signal from clusterheads and choose the clusterhead which sends the strongest signal as its clusterhead. Two clusterheads are selected per cluster. Because in case any clusterhead gets failed it can make use of the second one The size of the cluster is an important parameter. If the cluster size is decreased, the power consumption within each cluster is smaller. Yet the number of CHs will then be increased, so that the resulting backbone network formed by these CHs will become more complicated. A smaller number of CHs will form a simpler backbone network. Yet that would require larger cluster size, so that the RF power in each cluster becomes higher. There is then a trade-off between the cluster size and the number of CHs. Currently, most clustering protocols assume the network is organized into clusters of equal size, but such clustering results in an unequal load on the cluster head nodes. In multi-hop WSNs, when CHs cooperate with each other to forward their data to the BS, the CHs closer to the BS are burdened with heavy relay traffic and tend to die early, leaving areas of the network uncovered and causing network partition.

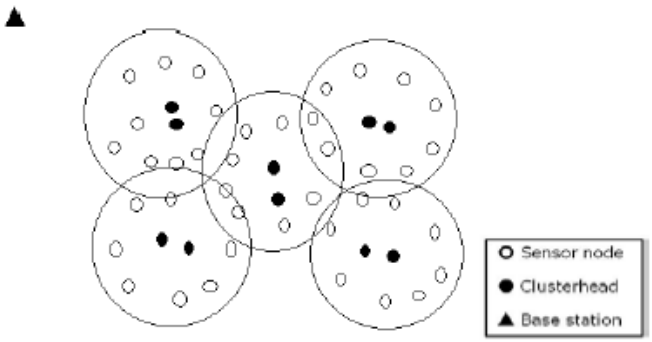

Fig 4: Clusters Heads

4.1.2 Cluster Formation Phase

The node reports that they are member of the cluster to its clusterhead. After that, the clusters are formed. Also, clusterheads and the member of clusters are fixed as shown Fig. 5.

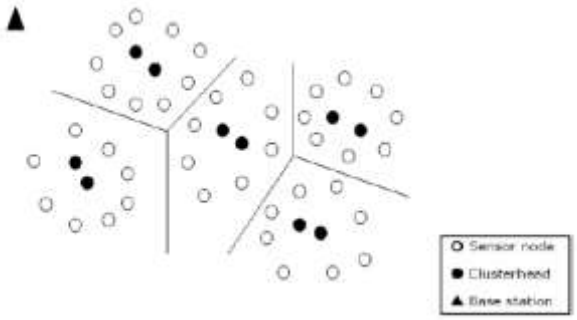

Fig 5: Formation of Clusters

4.1.3 Clusterhead Chaining Phase

At this phase, every clusterhead realizes neighbouring clusterheads. A clusterhead in a cluster involves in the formation of chain using chaining technique. If any clusterhead gets failed it makes use of secondary clusterhead which is present in the cluster as shown in the Fig.6.Secondary clusterhead also involved in large number of communications with the sensor nodes. The clusterhead can always send its data only to neighbouring clusterhead, even though the size of a sensor network becomes a very larger.

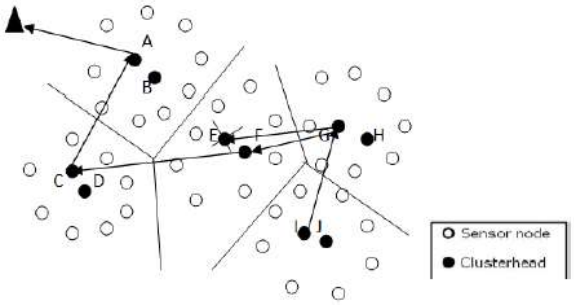

Fig 6 : Chain of Clusters

4.1.4 Data Transmission Phase

As shown in Fig. 7, each sensor node sends a message by its TDMA schedule. Then a clusterhead receives the information of all nodes and performs a data aggregation. After that, a clusterhead sends a processed data to a neighbouring clusterhead.

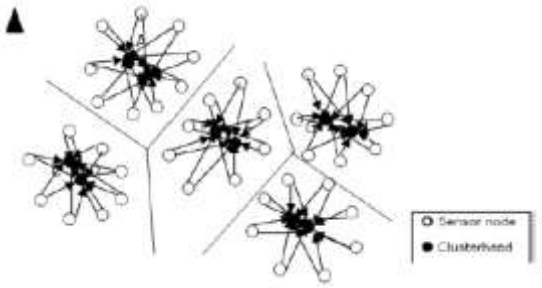

Fig 7: Delivery of Data to cluster Heads

As shown figure 8, each clusterhead transmits its data not to the base station but to the closest neighbouring clusterhead. Therefore, this scheme brings us the scalability of a sensor networks. After all clusterheads perform the process of the chain construction, each clusterhead delivers its sensing data to its neighboring clusterhead. Then the neighbouring clusterhead aggregates them with its data and transmits these data to its neighbouring clusterhead. Finally, the nearest clusterhead from the base station sends whole data to the base station.

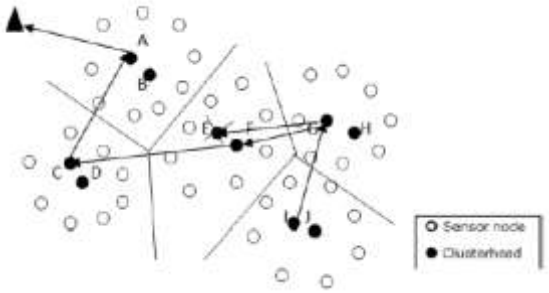

Fig 8 : Delivery of Data to Neighboring Clusterhead

As mentioned above, sensor nodes have several limited resources such as a CPU, memory, and battery. So, if the distance between the base station and clusterhead is too far, then a clusterhead may not communicate with the base station. Therefore if the network size becomes larger, to apply the existing routing protocols which use clustering scheme may cause a communication problem. In this paper, we proposed improved scheme by using a clusterhead chaining. It is adaptable to vast wireless sensor networks and energy efficient.

V. ADVANTAGES AND DISADVANTAGES

The various advantages of LEACH protocol are:

1. The Cluster Heads aggregates the whole data which lead to reduce the traffic in the entire network [8].
2. As there is a single hop routing from nodes to cluster head it results in saving energy [5].
3. It increases the lifetime of the sensor network.
4. In this, location information of the nodes to create the cluster is not required.
5. LEACH is completely distributed as it does not need any control information from the base station as well as no global knowledge of the network is required [5]. Besides the advantages of LEACH [9] it also has some

Demerits which are as follows:

1. LEACH does not give any idea about the number of cluster heads in the network.
2. One of the biggest disadvantage of LEACH is that when due to any reason Cluster head dies, the cluster will become useless because the data gathered by the cluster nodes would never reach its destination i.e. Base Station.
3. Clusters are divided randomly, which results in uneven distribution of Clusters. For e.g. some clusters have more nodes and some have lesser nodes. Some cluster heads at the center of the cluster and some cluster heads may be in the edge of the cluster this phenomenon can cause an increase in energy consumption and have great impact on the performance of the entire network.

VI. Experimental Results

An initial energy of each sensor node is 1 joule. Consider an environment of 200 sensor nodes. Therefore, the total initial energy of all sensor nodes in the field is 200 joules in the simulation environment. After comparing residual energy of all sensor nodes between the LEACH routing protocol and the proposed scheme, the graphical result can be given as shown in the Fig.9. By using the above formulas, we compute the total residual energy in all sensor nodes from 1 round to 200 rounds. It is also possible to compare the total residual energy of the LEACH routing protocol and the proposed scheme.

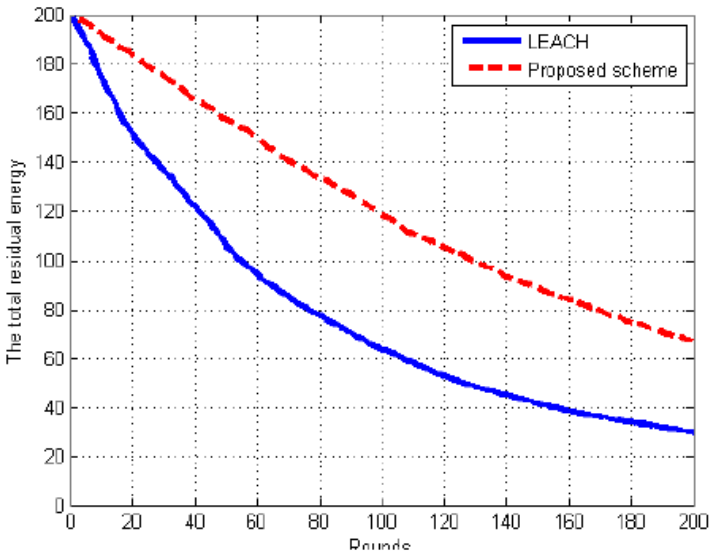

Fig 9: The Total Residual Energy

VII. CONCLUSION AND FUTURE ENHANCEMENT

In the case of LEACH routing protocol, sensor network is divided into several clusters and clusterheads are selected for each cluster. The clusterheads are responsible to gather and aggregate the data of the cluster. The clusterhead sends collected information to the base station. Hierarchical routing protocol is energy efficient because all sensor nodes take the role of a clusterhead in turns. However, most of the hierarchical routing protocols have the assumption that all sensor nodes can transmit the data to the base station by one hop routing. Therefore, if the network size becomes larger, serious communication problems may occur. If the distance between a clusterhead and the base station is too long, then the clusterhead cannot communicate with the base station and its data can be missing. To solve the above problem an enhanced scheme is proposed i.e. clusterhead chaining scheme. In this system clusterheads sends data not to the base station directly, instead it sends data to its neighbour and the process continues. Finally the clusterhead near to the base station sends collected information to the base station. Hence base station receives most of the information from using proposed chaining scheme. This scheme is suitable for the massive sensor networks and also energy efficient. In case if any clusterhead gets failed, the whole information will be lost. Hence secondary clusterhead is selected in every cluster. If any clusterhead gets failed secondary clusterhead can be used to transfer the information. Future enhancement is to evaluate the performance to various environments and to make the system as more energy efficient.

REFERENCES

1. Jamal N. Al-Karaki, Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks : A survey", *IEEE Wireless Communications*, Volume 11, Issue 6, Dec. 2004, pp.6-28.

2. Jamil Ibriq and Imad Mahgoub, "Cluster-Based Routing in Wireless Sensor Networks:Issue and Challenge", 2004.

3. W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-Specific Protocol Architecture for Wireless Microsensor Networks", *IEEE Transactions Wireless Communications*, Volume 1, Issue 4, Oct. 2002, pp. 660–670.

4. W. B. Heinzelman, A. P. Chandarkasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks" , *Proceedings of the 33rd Hawaii International Conference on System Sciences*, Maui, HI, Jan. 2000.

5. Jin-Young Choi, Sung-Min Jung, Young-Ju Han, Tai-Myoung Chung, "Advanced Concentric-Clustering Routing Scheme Adapted to Large –Scale Sensor Networks" ,The Second International Conference on Sensor Technologies and Applications, pp.440-746, Korea

6.Chunjuan Wei, Junjie Yang, Yanjie Gao, Zhimei Zang ,"Cluster Based Routing Protocols in Wireless Sensor Networks: A Survey" International Conference on Computer Science and Technology, Dec 24-26,2011

7. K. Ramesh and Dr. K. Somasundaram, "A Comparative study of Clusterhead Selection Algorithms in Wireless Sensor Network", International Journal of Computer Science And Engineering A Survey, Volume 2, No.4,Nov.2011