Study of LEACH Routing Protocol for Wireless Sensor Networks

Reenkamal Kaur Gill[1], Priya Chawla[2] and Monika Sachdeva[3]
[1,2,3]Department of Computer Science and Engineering,
Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India
E-mail: [1]reenkamalgill@gmail.com, [2]piyachawla12@gmail.com,
[3]monika.sal@rediffmail.com

***Abstract*—Wireless Sensor Network are in great demand from the recent years, as nowadays we have seen a wide growth of wireless devices including cellular phones, laptops, mobiles, PDA's etc. Wireless Sensor Networks consists of thousands of tiny sensor nodes. In a wireless sensor network a node is no longer useful when its battery dies, so to avoid this problem many protocols were introduced, but most of the rank is given to hierarchical routing protocols. In this paper, we analyze LEACH protocol, its phases, advantages and disadvantages and also various kinds of attacks on this routing protocol.**

Keywords: Wireless Sensor Networks, LEACH Protocol, Cluster, Cluster Head, Attacks

I. Introduction

A wireless sensor networks consist of tiny sensor nodes to monitor physical or environmental conditions such as temperature, pressure, sound, humidity etc. The network must possess self configuration capabilities as the positions of the individual sensor nodes are not pre-determined.

Routing strategies and security issues are a great research challenge now days in WSN but in this paper we will emphasize on the routing protocol. A number of routing protocols have been proposed for WSN but the most well known are hierarchical protocols like LEACH [1] and PEGASIS [2].

Hierarchical protocols are defined to reduce energy consumption by aggregating data and to reduce the transmissions to the Base Station. LEACH is considered as the most popular routing protocol that use cluster based routing in order to minimize energy consumption.

In this paper firstly we analyze LEACH protocol and then in the third section we will discuss the phases of LEACH protocol. In the fourth section we define various possible attacks on it and in the fifth section there are the advantages and disadvantages of LEACH. In the last section we compare LEACH with other protocols.

II. LEACH

Low Energy Adaptive Clustering Hierarchy (LEACH) protocol is a TDMA based MAC protocol. The principal aim of this protocol is to improve the lifespan of wireless sensor networks by lowering the energy consumption required to create and maintain Cluster Heads. The operation of LEACH protocol consists of several rounds with two phases in each [3] [4]: Set-up Phase and Steady Phase.

In the Set-up phase the main goal is to make cluster and select the cluster head for each of the cluster by choosing the sensor node with maximum energy. or by randmization Steady Phase which is comparatively longer in duration than the set-up deals mainly with the aggregation of data at the cluster heads and transmission of aggregated data to the Base station.

III. Phases of LEACH

As described earlier the operation of LEACH consists of several rounds with two phases in each round. Working of LEACH starts with the formation of clusters based on the received signal strength.

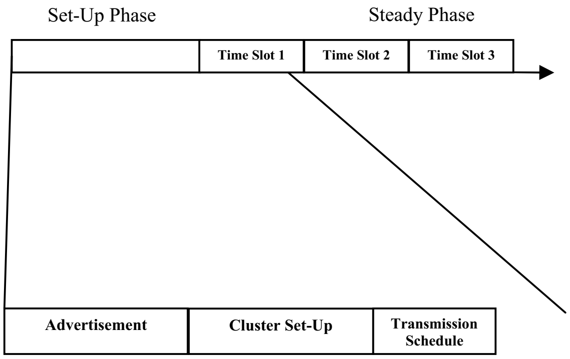

Fig. 1 Time Line Operation of LEACH

The algorithm for LEACH protocol is as follows:

The first phase of LEACH is Set-up phase and it has three fundamental steps.

1. Cluster Head advertisement
2. Cluster setup
3. Creation of Transmission Schedule

During the first step cluster head sends the advertisement packet to inform the cluster nodes that they have become a cluster head on the basis of the following formula [5]:

Let x be any random number between 0 and 1.

Where n is the given node, p is the probability, r is the current round, G is the set of nodes that were not cluster heads in the previous round, T(n) is the Threshold.

$$T(n) = \begin{cases} \dfrac{P}{1 - P[r * \mathrm{mod}(1/P)]} & if \quad n \in G \\ 0 & otherwise, \end{cases}$$

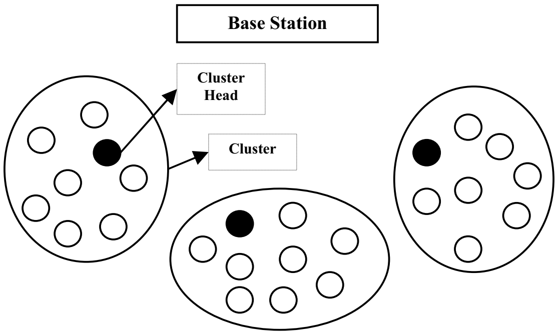

Fig. 2 Cluster Formation in LEACH.

The node becomes cluster head for the current round if the number is less than threshold T(n). Once the node is elected as a cluster head it cannot become cluster head again until all the nodes of the cluster have become cluster head once. This helps in balancing the energy consumption.

In the second step, the non cluster head nodes receive the cluster head advertisement and then send join request to the cluster head informing that they are the members of the cluster under that cluster head as shown in Fig. 2 [6].

These non cluster head nodes saves a lot of energy by turning off their transmitter all the time and turn it ON only when they have something to transmit to the cluster head.

In the third step, each of the chosen cluster head creates a transmission schedule for the member nodes of their cluster. TDMA schedule is created according to the number of nodes in the cluster. Each node then transmits its data in the allocated time schedule.

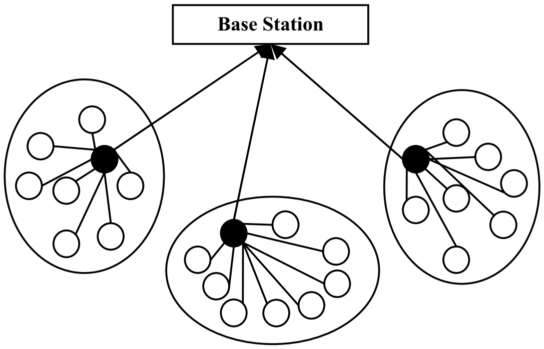

Fig. 3 Steady Phase in LEACH.

The second phase of LEACH is the Steady phase during which the cluster nodes send their data to the cluster head. The member sensors in each cluster communicate only with the cluster head via a single hop transmission. The cluster head then aggregates all the collected data and forwards this data to the base station either directly or via other cluster head along with the static route defined in the source code as shown in Fig. 3[7]. After the certain predefined time, which is decided beforehand, the network again goes back to the Set-up phase.

IV. Attacks on LEACH

LEACH protocol is threatened by the following types of attacks which degrade the performance of LEACH by dropping, altering, spoofing or replying the packets.

A. Sybil Attack

Most of the peer to peer networks face security threats due to Sybil attack [8], [9]. This attack is the most difficult attack to detect. In this attack, malicious node uses the identity of many other legitimate nodes to gain the data exchanged between the legitimate nodes. It affects the network by dropping vital packets, increasing traffic, lowering network lifetime etc. Encryption and authentication techniques can be used to prevent wireless sensor network from the Sybil attack.

B. Selective Forwarding

LEACH protocol is also susceptible to selective forwarding attack. In this kind of attack a malicious node places itself in the path where data is exchanged between the two legitimate nodes. It collects the data and instead of forwarding this node drops all the data. It is the case where the malicious node can easily be detected. The worst scenario of this attack is that when malicious node does not discard the entire data, but selectively forwards some of the non vital information. In this case it is very difficult detect the malicious node.

C. HELLO Flooding Attack

In many protocols sometimes it is required for node to transmit HELLO packets to advertise itself to its neighboring nodes. The nodes receiving these packets assume that it is within the range of the sender. But in case of malicious node, it continuously keeps on sending the HELLO packets and thus increases the network traffic and causes collisions. It also consumes the energy of the sensor nodes when these nodes receive large amount of HELLO packets continuously and thus lowering the lifetime of the wireless sensor networks. This type of attack is known as HELLO Flood attack [10].

V. Advantages and Disadvantages of LEACH

The various advantages [11] of LEACH protocol are:

1. The Cluster Heads aggregates the whole data which lead to reduce the traffic in the entire network.
2. As there is a single hop routing from nodes to cluster head it results in saving energy.
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.

Besides the advantages of LEACH it also has some demerits [11], [12] 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. Conclusion

Wireless Sensor Networks would be of great use in future mission applications. If we analyze the previous research, we could observe that a lot of work is being carried out on routing i.e. what is the best optimal path for the nodes to communicate with each other. In this paper, we have also discussed LEACH routing protocol. Basically how does it works has been explained above with its advantages and disadvantages. LEACH protocol is also vulnerable to various kinds of attacks which have been described above.

References

[1] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "*Energy-efficient communication protocol for wireless sensor networks*", in: Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[2] S. Lindsey, C.S. Raghavendra, "*PEGASIS: power efficient gathering in sensor information systems*", in: Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.

[3] Rajesh Patel, Sunil Pariyani, Vijay Ukani," *Energy and hroughput Analysis of Hierarchical Routing Protocol(LEACH) for Wireless Sensor Networks"*, International Journal of Computer Applications Volume 20- No. 4 (April 2011).

[4] Yuh Ren Tsai, *"Coverage Preserving Routing Protocols for Randomly Distributed Wireless Sensor Networks"*, IEEE Transactions on Wireless Communications, Volume 6- No. 4 (April 2007).

[5] Amrinder Kaur, Sunil Saini," *Simulation of Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Network*," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue7, July 2013.

[6] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci: "*A Survey on Sensor Networks"*, IEEE Communication Magazine, pp. 102-114(August 2002).

[7] Rajesh Patel, Sunil Pariyani, Vijay Ukani," *Energy and Throughput Analysis of Hierarchical Routing Protocol(LEACH) for Wireless Sensor Networks"*, International Journal of Computer Applications Volume 20- No. 4 (April 2011).

[8] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[9] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[10] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[11] Parul Kansal, Deepali KAnsal, Arun Balodi,*"Compression of Various Routing Protocol in Wireless Sensor Networks"*, International Journal of Computer Applications Volume 5-No. 11(August 2010) .

[12] M. Bani Yassein, A. AL-zou'bi, Y. Khamayseh, W. Mardini, *"Improvement on LEACH Protocol of Wireless Sensor Networks"*, International Journal of Digital Content Technology and its Applications Volume 3- No. 2 (June 2009).