

# Clustering Algorithm for Energy Efficient Routing using LEACH Protocol in Wireless Sensor Networks

Varsha Tiwari<sup>1</sup> Vivek Sharma<sup>2</sup> Akhilesh A. Waoo<sup>3</sup>

<sup>1</sup>Research Scholar <sup>2</sup>Head of Department <sup>3</sup>Head  
<sup>1,2,3</sup>Department of Computer Science & Engineering  
<sup>1,2</sup>TIT College Bhopal, India, <sup>3</sup>AKS University, India

**Abstract**— WSN (Wireless Sensor Network) is a network consists of a large no. of low power sensor nodes. Here LEACH is a Less Energy Adaptive Clustering Hierarchy Protocol. These cluster-based sensor networks main goal is to decrease system delay and reduce energy consumption. And leach is a cluster-based protocol for micro sensor networks which achieves energy efficient, scalable routing and fair media access for sensor nodes. Security is very compulsory in wireless sensor network. Therefore, its security purpose many improvements are done in wireless sensor network. In this paper mainly describes LEACH Protocol, Their phases and various attacks with different techniques and also these advantages and disadvantages etc.  
**Key words:** Wireless Sensor Networks, Sensor Nodes, Leach Protocol, Clustering System, Attacks

## I. INTRODUCTION

Here LEACH Protocol is a Cluster based-routing protocol for WSN (Wireless Sensor Networks). A WSN consist no. of tiny sensor nodes to monitor or environmental conditions such as temperature, humidity, sound, pressure etc. Wireless sensor networks are designed to use the energy efficiently. While the network must possess self-configuration capabilities as the positions of the individual sensor nodes are not predetermined, for these conditions controlled by routing protocol cluster-based LEACH Protocol. 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 second section we will discuss the phases of LEACH protocol with various possible attacks. In the third section we define its different techniques and in the fourth section there are proposed model and simulation model and in last section discuss the advantages and disadvantages of LEACH.

## II. CLUSTER BASED ROUTING PROTOCOLS IN WSNS

In Wireless Sensor Network LEACH (Low Energy Adaptive Clustering Hierarchy) is a typical cluster-based routing protocol using a distributed clustering formation algorithm? The large number of sensor nodes will be divided into several clusters, in LEACH. In this method for each cluster, a sensor node is selected as a cluster head. Where the selection of cluster head nodes is based on a pre-determined probability of sensor. And other non-cluster head nodes choose these nearest cluster to join by receiving the strength of the advertisement message from the cluster head nodes. A non-cluster head node can only monitor the environment and send data to its cluster head node.

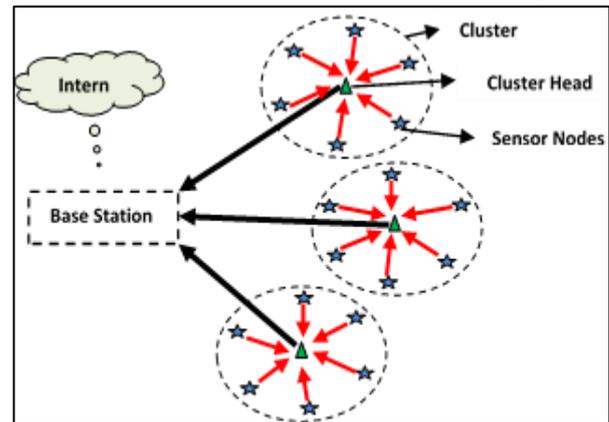


Fig. 1: Cluster Based Wireless Sensor Network

The cluster head node is responsible for collecting the information of non-cluster head nodes in the cluster. Then, it processes data and sends data to the BS. As a non-cluster head node cannot send data directly to the BS, the data transmission distance of the sensor node is shrunk. Therefore, the energy consumption is reduced in the wireless sensor networks. However, the random selection of the cluster head node may obtain a poor clustering setup, and clusterhead nodes may be redundant for some rounds of operation. The distribution of cluster head nodes is not uniform; thus, some sensor nodes have to transfer data through a longer distance and the reasonable energy saving is not obtained in wireless sensor networks.

## III. LEACH PROTOCOL

LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is a TDMA (Time-Division Multiple Access) based MAC (Medium Access Control) protocol. The principal aim of LEACH protocol is to improve the average length life 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: Set-up Phase and Steady Phase.

### A. Phases of LEACH

Phases of leach protocol are as follows:

#### 1) The Set-Up Phase

main goal of first set-up phase is to make cluster and select the cluster head for each cluster by choosing the sensor node with maximum energy. There are three phases of Set-up phase has fundamental steps:

- Cluster head advertisement
- Cluster set up
- 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:

$$T(n) = \frac{P}{1 - P \times (r \bmod P^{-1})} \text{ if } n \in G$$

$$T(n) = 0$$

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.

### 2) Steady Phase

In 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 Figure 2. After the certain predefined time, which is decided beforehand, the network again goes back to the Set-up phase.

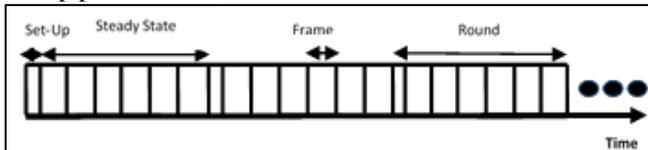


Fig. 2: Time Line Operation of LEACH

## B. Attacks on LEACH

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

### 1) Sybil Attack

The most peer to peer networks face of security threats due to Sybil attack. In this attack is the most difficult attack to detect. In this attack, malicious node uses the identity of many other legal nodes to gain the data exchanged between the legal 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.

### 2) Selective Forwarding

LEACH protocol is also perceptive to selective forwarding attack. In this kind of attack a malicious node places itself in the path where data is exchanged between the two legal 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.

### 3) 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.

## IV. MULTIPLE HOPPING TECHNIQUES

To describe the cluster-based routing protocol of LEACH Protocol different multiple techniques, Comparison of different variants of LEACH protocol as follows:

### – LEACH-B

It introduced a new adaptive strategy to choose cluster heads and to vary their elections. It used the engaged energy to improve the network lifetime. Still it had the problem of extra overhead for electing cluster head.

### – LEACH-C

In this each node used to send information about their current location and the residual energy level to the base stations. Cluster heads were selected on the basis of residual energy. It achieved higher number of rounds in small area network.

### – LEACH-P

The networks are distributed randomly in remote areas. This contained homogenous, static nodes and the location of the node was unknown.

### – LEACH-M

All the nodes are homogenous in the sense of antenna gain; all nodes had their location information using GPS and the base stations were considered fixed in this network. It supported nodes mobility by membership declaration to the existing LEACH protocol.

### – LEACH-V

In this network the base station is fixed, all the nodes are homogenous and had same energy level. In the cluster head selection is done on random basis. It also had a sub-cluster head that took the role of cluster head if it dies.

### – LEACH-S

This is the first modified secure version of LEACH called SLEACH. SLEACH provides protection in LEACH by using the structure block of SPINS (Security Protocol for Sensor Network), symmetric-key methods and MAC (Message Authentication Code). SLEACH protects beside selective forwarding, sinkhole and HELLO flooding attacks. It prevents intruder to send factitious sensor data to the CH and CH to forward phony message.

### – LEACH-R

Secure solution for LEACH has been introduced called RLEACH in which cluster are formed dynamically and periodically. In RLEACH the orphan node problem is higher due to random pair-wise key scheme so they have applied improved random pair-wise key scheme to stunted. RLEACH has been used the one-way hash chain, symmetric and asymmetric cryptography to endow protection in the LEACH Hierarchical routing protocol. RLEACH protest many attacks like spoofed, alter and replayed information, sinkhole, worm- hole, selective furthering, HELLO flooding and Sybil attack.

### – LEACH-DD

Protocol It is a combination of LEACH, a hierarchical based protocol and directed diffusion, a data-centric dissemination protocol. It supports two levels. At the first level, LEACH model is used and at the second level, directed diffusion model adopted. As in LEACH protocol, cluster formation is

done, CH is particular over a cluster and TDMA schedule is distributed among nodes by CH. After undergoing setup and steady state phases, the BS transmits the query to the nearby CHs and those CHs in turn pass the query to other CHs.

### V. PROPOSED MODEL

In order to increase energy efficiency and extend the lifetime of the sensor nodes in wireless sensor networks, efficient power saving algorithm must be developed and designed. Based on the centralized clustering architecture, here proposed a clustering algorithm to provide efficient energy consumption and better network lifetime in the wireless sensor networks named CAFEE (Clustering Algorithm for Energy Efficient). In the proposed scheme, assume that the BS receives the information of location and residual energy for each sensor node and the average residual energy can be calculated. In this algorithm, the operation includes two models: set up model and Steady state model.

#### A. REER Algorithm Details

The operation of REER is broken upon in to some steps, where initial step is cluster building stage, after building of clusters second step is election of cluster head based on cost value calculations which is calculated by some random node chosen as supervisor node outside the cluster followed by third step which is data transmission phase in which data is transmitted from that supervisor node to the base station and alteration of cluster is done based on packet loss ratio calculated by supervisor node itself. In order to minimize overhead, the data transmission and cluster size alteration phase is long compared to the cluster building phase.

#### B. Factors for Expense Value

The expense value (EV) is determined based on following factors:

- Residual energy (E) The residual energy of a node preferably is greater than the approximate energy dissipated in previous round by the cluster head.
- Distance to coordinator node (D) we know that energy consumption is directly proportional to the square of distance.
- Expense value depends upon what is the residual energy of a node how much distance from the supervisor node.
- The cost is greater when the residual energy is more and the less distance to the supervisor node. Formula for EV is given by

$$EV = (a \times E) + (b \times (1/D))$$

Where, a and b are taken as normalization constants.

E and is defined as residual energy and distance to coordinator node respectively.

### VI. SIMULATION MODEL

Simulations are conducted with MAT LAB (R2018b) to get specific plots.

| Network Parameters                                      | Value                                |
|---|--------------------------------------|
| Network Size  | 100X100m <sup>2</sup>                |
| Initial Energy of Sensor Nodes                          | 0.5 J                                |
| Packet Size   | 4000 bits                            |
| Transceiver idle state energy consumption               | 50 nJ/bit                            |
| Data Aggregation/ Fusion Energy consumption             | 5 nJ/bit/report                      |
| Amplification Energy (Cluster to BS) $d \geq d_o$       | $Efs$                                |
| Amplification Energy (Cluster to BS) $d \leq d_o$       | $Emp$                                |
| Amplification Energy (Intra Cluster Comm.) $d \geq d_1$ | $0.0013pJ/bit/m^2$                   |
| Amplification Energy (Intra Cluster Comm.) $d \leq d_1$ | $Efs/10 = Efs_1$<br>$Emp/10 = Emp_1$ |

### VII. ADVANTAGES & DISADVANTAGES OF LEACH

The various advantages of LEACH protocol are:

- In the entire network the whole data which lead to reduce the traffic of the cluster heads aggregates.
- There is a single hop routing from nodes to cluster head it results in saving the energy.
- It increases the lifespan of the sensor network.
- The nodes to create the cluster is not required of this location information.
- Here, 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 which are as follows:

- In Demerits, LEACH does not give any idea about the number of cluster heads in the network.
- One of the biggest disadvantages 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.
- Clusters are divided randomly, which results in uneven distribution of Clusters. For e.g. some clusters have more nodes and some have lesser nodes.

### VIII. CONCLUSION

In this paper briefly discussed in cluster based- routing protocol for WSN (Wireless sensor networks) is LEACH protocol. Wireless Sensor Networks would be of great use in future mission applications. Here, introduces the LEACH with cluster based WSN and these different hopping techniques. LEACH is a MAC protocol, it contains many advantages like it does not need any control information, it saves energy and reduce power consumptions. Basically, how does it work 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] Swati Gupta and Gaurav Banga', "Energy Efficient Leach Protocol in WSN", ', GMT, KKR, India, GMT, KKR, India 2016.
- [2] Vikas Upadhyay, Abhishek Swaroop, "A survey of LEACH based routing protocols for WSN" School of Computing Science and Engineering, Galgotias University, Greater Noida, India 2016.

- [3] Reshma I. Tandel Shri S'ad, "LEACH Protocol in Wireless Sensor Network: A Survey" Vidya Mandal Institute of Technology Bharuch 392-001, Gujarat, India 2016.
- [4] D. Suresh1, K. Selvakuma, "Improving Network Lifetime and Reducing Energy Consumption in Wireless Sensor Networks" Annamalai University, Annamalai Nagar, Tamilnadu, India 2014.
- [5] 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.
- [6] 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.
- [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] Yuh Ren Tsai, "Coverage Preserving Routing Protocols for Randomly Distributed Wireless Sensor Networks" IEEE Transactions on Wireless Communications, Volume 6- No. 4 (April 2007).
- [9] 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.
- [10] Ian F. Akyildiz, Weilian Su, Yogesh Sankara subramaniam, Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, pp. 102-114(August 2002).
- [11] Douceur, "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).
- [12] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the 3<sup>rd</sup> international symposium on Information processing in sensor networks, ACM, 2004,
- [13] 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.
- [14] Parul Kansal, Deepali KAnsai, Arun Balodi, "Compression of Various Routing Protocol in Wireless Sensor Networks", International Journal of Computer Applications Volume 5-No. 11(2010).
- [15] "Detection of HELLO flood Attack on LEACH Protocol", Shikha Magotra, Krishan Kumar, International Advance Computing Conference (IACC), IEEE, 2014.
- [16] Reen kamal Kaur Gill, Priya Chawla and Monika Sachdeva, "Study of LEACH Routing Protocol for Wireless Sensor Networks", International Conference on Communication, Computing & Systems (ICCCS), 2014.
- [17] Akhilesh A. Wao\*, Shivani Patnaha and Sanjay Sharma, "Clustering Methods for Improved Wireless Sensor Network", <http://www.jjar.in>, 2017.
- [18] Lalita Yadav, Ch., "Low Energy Adaptive Clustering Hierarchy in Wireless Sensor Network (LEACH)", Sunitha International Journal of Computer Science & Information Technologies, Vol. 5 (3), 2014.