The Family of LEACH –Review

Joshua Reginald Pullagura, Rashmi V.V. Rao, Venkata Rao D

Abstract: Life time and Energy are major issues in the sensor networks, in order to enhance this Low energy adaptive Clustering Hierarchy (LEACH) routing protocol has been developed. However, this protocol has some drawbacks, to overcome these drawbacks, considering LEACH routing protocol as a basic algorithm many improvisations has been done based on different applications. In this review, we compare and discuss about some of the improvised methods in extended LEACH routing protocol.

Keywords: Cluster Formation, Energy, Extended Leach Routing Protocols and TDMA.

I. INTRODUCTION

Low Energy Adaptive Clustering Hierarchy (LEACH) is a cluster based TDMA protocol .The goal here is to minimize energy utilization which is required to generate and keep in existence the clusters for a long time. LEACH randomly distributes the energy load to sensors in the network evenly as it is self-organized. Nodes form themselves into clusters, cluster head (CH) is chosen among them based on their energy levels in the probabilistic method and the remaining nodes act as the cluster members. The CH has many responsibilities and performs the data aggregation process and transmits the data to the base station (BS). Cluster members communicate with the CH in TDMA method, according to the schedule created by the CH.

In sensor networks, there are many types of routing techniques but Cluster based techniques improve Life time [1]

LEACH can also use the CDMA technique as each cluster can use a various set of CDMA codes, to reduce the interference between the clusters [6].

The remaining paper is organized as section II describes the working of the LEACH routing protocol. Section III depicts issues LEACH protocol and various attacks on the LEACH protocol. Section IV reviews various methods of extended LEACH protocols. Finally section V gives the conclusion of the review .
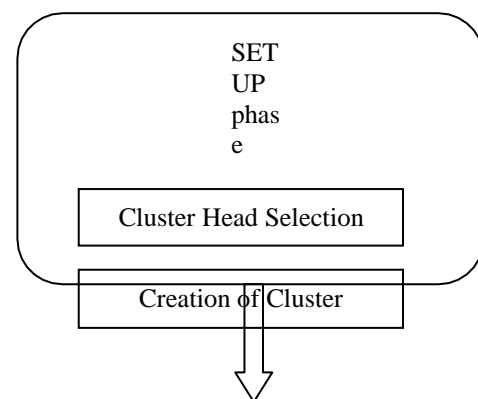
Membership in Cluster is versatile

➢ CH Performs data aggregation

➢ Communication of data is based on the TDMA technique

➢ Threshold value is important in selection CH

B. Phases of LEACH protocol

LEACH protocol has two phases

1. SETUP phase

2. STEADY phase

STEADY phase

II. WORKING OF LEACH ROUTING PROTOCOL

A. Properties of Algorithm

➢ It is based on clustering technique

- Cluster head selection is carried by probabilistic method considering nodes energy LEACH routing protocol is self-adaptive, which contains number of rounds with two phases in each.

- It is a self-organized protocol

- It observes each round as a unit and try to decrease the energy utilization.

1. Setup Phase

The main aim of this phase is cluster formation and CH selection. Following are the basic steps involved in this phase

a. Cluster head advertisement

b. Formation of cluster

c. Transmission schedule creation

During the setup phase CH sends metadata packet i.e., the advertisement to the remaining members of the cluster in order to inform that they have become the cluster head for this round on the basis of below equation.

$$(\square) = \cfrac{P}{1 - P * (r \bmod P^{-1})} \qquad \forall\ \square \in \square \quad (1)$$

$$(\square) = 0 \qquad\qquad \forall\ \square \notin \square$$

(2) Where n = random number between 0 to 1
P = cluster head probability
S = set of non-cluster head nodes in the Previous rounds

If the number of the node is less than the threshold value T (n), then the node will become the CH for the present round and that node cannot be made as the CH until each and every node in the cluster becomes the CH i.e., each and every node in the cluster will get a chance to become the CH. Through this method energy can be conserved

In the next step cluster members will receive the advertisement and send the joining request to the cluster head stating that they are the members of that cluster.

Finally CH creates a transmission schedule for the remaining nodes of the cluster through TDMA technique. Usually CBR traffic is considered in simulation [5]

2. Steady Phase

In this phase, the remaining nodes of the cluster send their data to the CH through single hop transmission. Then CH collects data and transmits it to the BS directly. After the completion of the allotted time, the network again goes back to the Setup phase and the procedure is continued.

C. ASSETS OF LEACH PROTOCOL

- ➢ CH collects the data which reduces the congestion in the network
- ➢ CH broadcast the data to the BS through single hop transmission by which energy can be conserved
- ➢ Network lifetime is enhanced.
- ➢ Location information of the nodes is not required to the BS
- ➢ It does not need any control information from the BS

III.ISSUES IN LEACH PROTOCOL

Following are the major issues in the LEACH protocol

- ➢ Cluster heads are selected through probabilistic methods
- ➢ Irregular and random cluster formation
- ➢ Continuous monitoring
- ➢ Communication from CH to BS

- ➢ Predefined number of CH
- ➢ Variable cluster size

A. Attacks on LEACH Protocol

1. HELLO Flooding Attack

In some routing protocols, sometimes it is necessary to send the HELLO packets for the purpose of advertisements, in order to inform the neighboring nodes. But some malicious nodes with stronger transmission power broadcast the HELLO packets continuously [12]. The neighboring nodes will be misguided and transmit all its data to the HELLO sending nodes and draining their energies due to this process. The BS will also broadcasts the same type of message but only some of the nodes will be same type of message but only some of the nodes will be responding to it. Congestion is increased in the network through this attack [9].

2. Selective Forwarding Attack

In this attack the malicious node place itself in the routing path where the packets are transmitted and it acts like a black hole. The malicious node will refuse to forward some of the packets and prevents them from passing through the route. The malicious node can be easily detected in some cases but in worst case in which the malicious node selectively forwards some packets which are not essential, it is very difficult to identify the malicious node [12] [3].

3. Sybil Attack

It is attack in which, the malicious node poses the multiple identities to obtain the data transmitted between two legitimate nodes. It is difficult to identify this node. The network is affected as this malicious node will drop the important packets. Congestion is increased and the lifetime of the network is decreased [6] [12].

4. Denial of Service (DoS)

This attack causes the radio jamming, restraining from the network protocol and due to the battery exhaustion [7]. DoS attacks make the resources unavailable to the users, for example if node 'x' wants to communicate with node 'y', and send 'REQ', node 'y' sends the 'ACK' in return, but node 'x' keep on sending 'REQ' continuously to node 'y' and thus 'y' is unable to communicate with other nodes and becomes unavailable to them[3][12].
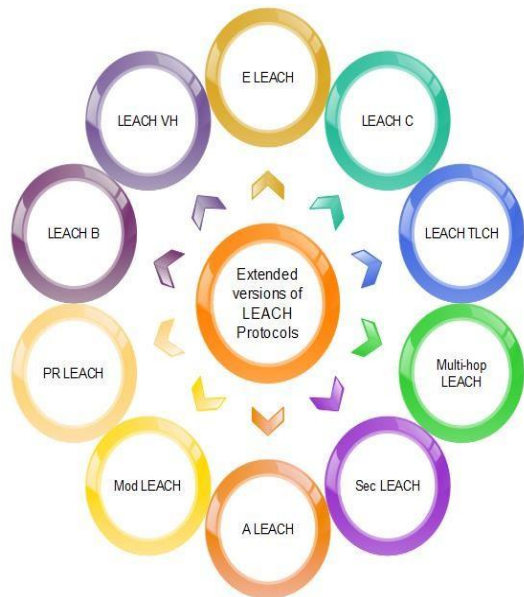
IV.REVIEW OF IMPROVISED LEACH PROTOCOL

Fig1. Extended versions of LEACH Protocols

1. Centralized LEACH (LEACH C)

LEACH protocol, it does not guarantee about the number of CH nodes and their positioning. Improper clustering is one of the major issues. However, to overcome this problem LEACH C is developed. It uses the centralized algorithm to form the clusters which produce consistent clusters by dispersing the CH nodes in the network.

Initially, during the Setup phase of LEACH C, each node in the cluster sends the information to the BS about its current location and power level. For example the information can be sent through the GPS or any other location sensing technique. After receiving the information the BS must ensure whether the energy is evenly distributed among the nodes in the cluster. In this process the BS calculates the average node energy and takes appropriate decision whether to participate in data transfer or not [5].

Once the CH and associated cluster are found, the BS broadcast the message which contains the CH ID for each node. If the CH ID matches with its own ID, the node is considered as the CH, else it goes for TDMA slot for data transmission and goes to sleep mode. This phase is identical to LEACH protocol [7].

2. Two level cluster head LEACH (LEACH TLCH)

LEACH protocol addresses the problem of uneven energy distribution which is caused by the random CH formation. To overcome this problem LEACH TLCH has been introduced to balance the energy consumption.

In LEACH protocol CH are responsible for not only receiving data from the BS but also collecting the data from the cluster members. In this process the energy consumption for the transmission of data is more than the collecting the data from the nodes. If the energy of the CH is less or the CH is far from the BS the CH will expire due to the heavy energy burden [7].

In LEACH TLCH if the CH energy is less than the average energy or the CH distance is less than the average distance then secondary head is elected .This technique can improve the lifetime of the clusters.

3. Vice cluster head LEACH (LEACH VH)

LEACH VH introduces the concept of vice cluster head (VH) selection in addition to the CH into the cluster. After the cluster formation, the CH receives the information about the residual energy from the cluster member. Node with the highest energy is selected as VH and thus VH get into the sleep mode as soon as it is selected by the CH and it does not perform any operations such as transmitting, storing, sensing, idle listening etc. [14]. Through this process the network lifetime can be enhanced and it prevents the CH from the early death.

4. Energy LEACH (E LEACH)

It considers the residual energy as the main criteria for CH selection. In LEACH, the CH selection is based on the probabilistic method and in the first round. Every node has the equal chance to become the CH as every node consists of some amount of energy imprecisely. In the second round the node with highest residual energy is set as the CH. The procedure will continue until all the nodes are dead in the considered clusters [13].

5. MULTI-HOP LEACH

Multi-hop LEACH the CH selects the ideal path and follows the Multi-hop communication. The CH transmits the data to another CH which is nearer to the BS and thus the data is transmitted [6].

The major difference between LEACH and Multi-hop LEACH is that LEACH follows single hop communication and the Multi-hop LEACH follows the multi-hop communication. We can improve the network lifetime through this method. Below table tabulated the comparison protocol

Table1.Comparison of various LEACH Protocols

Types of LEACH Protocol	Data Transmission	Network Type	Delay	Deployment Strategy	Energy Efficiency	Scalability
LEACH C	Single Hop	Homogeneous	Low	Random	Good	Low
LEACH TLCH	Single Hop	Homogeneous	Medium	Random	Good	Medium
LEACH VH	Single Hop	Homogeneous	Medium	Random	Good	High
E LEACH	Single Hop	Homogeneous	Low	Random	Good	Medium
Multi-hop LEACH	Multi Hop	Homogeneous	High	Random	Good	Medium
Sec LEACH	Single Hop	Homogeneous	Low	Random	Poor	Medium
LEACH B	Single Hop	Homogeneous	Medium	Random	Very Good	Medium
PR LEACH	Multi Hop	Heterogeneous	Medium	Random	Good	Medium
MOD LEACH	Single Hop	Homogeneous	High	Random	Good	High
A LEACH	Single Hop	Heterogeneous	High	Random	Good	Medium

6. Secure LEACH (Sec LEACH)

Sec LEACH is the secure version of LEACH protocol. It uses key (RD) pre-distribution Algorithm for selection of the CH. Generally in LEACH the CH is selected by the probabilistic method. This results in the various drawbacks. To overcome this issue, RD key method is introduced; this method undergoes three phases [11].

I Phase is the key pre-distribution phase

II Phase is the shared key discovery phases. In this phase all the nodes advertise their ID's on their key rings and determines with which of the neighbor node they can share their key.

III Phase is the path key establishment phase in which the pair of nodes which did not shared their keys can setup their own keys.

7. Balanced LEACH (LEACH B)

Considering the drawbacks of the LEACH extended version of LEACH has been proposed called LEACH B [3]. In this method second CH selection is done in order to modify the CH in setup phase based on the nodes residual energy.This protocol makes sure the cluster partition is based to achieve this concept, the CH numbers are dominated and optimal amount of channels are required in the network [4].

8. Percentage LEACH (PR LEACH)

PR LEACH is the Percentage LEACH in which the setup phase is similar to the core LEACH. But in the Steady phase the energy of the nodes are varied due to the transmission. Cluster nodes transmit the information about their energy levels to the CHs which are forwarded to the BS through different CHs. BS receives the information about all the nodes and calculate the range by these energies and broadcast this information to all the CHs based on the multi-hop technique. CHs forward this range to the members. Each member of the cluster uses this range to calculate the threshold for itself, if the energy is superior when compared to threshold then the node can become the CH, otherwise the node does not participate in the CH election [10].

9. Modified LEACH (MOD LEACH)

It is the modified LEACH protocol with two concepts introduced in its first is modifying the placement mechanism of the CH and the second is introducing the concept of soft threshold and hard threshold. The first concept uses the distribution mechanism for CH selection by removing the CH when their energy level is less than the remaining nodes.
The second concept is based on threshold. If the defined threshold is much more than the hard threshold value then the data is transmitted. If the threshold data is compared with the previous data and value is found to be different, then the data is transmitted.

10. Advanced LEACH (A LEACH)

A LEACH (Advanced LEACH) is the static clustering protocol where entire network is divided into static cluster and then each cluster is applied with separate a separate LEACH Protocol. It improves the scalability and reduces the amount of battery consumption [2]

V. CONCLUSION

This review paper gives the overview of the LEACH routing protocols. The different issues and drawbacks have been stated. Based on these drawbacks LEACH has been extended in different methods in order to enhance the lifetime and energy of the network. In this review it is observed that clustering and CH selection has been major criteria for improvement of the network lifetime and energy efficiency.

REFERENCES

1. Joshua Reginald Pullagura, Dr.D.Venkata Rao, "Simulation based performance evaluation of Energy efficient routing protocols in Ad hoc Networks" Journal of Advanced Research in Dynamical and Control Systems (JARDCS), 2017, Vol.9, pp.1141-1149.
2. Ali, M. S., Dey, T., & Biswas, R. (2008, December). ALEACH: Advanced LEACH routing protocol for wireless microsensor networks. In Electrical and Computer Engineering, 2008. ICECE 2008. International Conference (pp.909-914).IEEE.
3. Tong, M., & Tang, M. (2010, September). LEACH- B: associate improved LEACH protocol for wireless sensing element network. In Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on (pp1- 4).IEEE.
4. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on wireless communications, 1(4), 660-670.
5. Handy, M. J., Haase, M., & Timmermann, D. (2002). Low energy adjustive clump hierarchy with settled cluster-head choice.
6. In Mobile and Wireless Communications Network, 2002. 4th International Workshop on (pp. 368-372). IEEE.
7. [6] Al·Baz, A., & El·Sayed, A. (2018).A new formula for cluster head choice in LEACH protocol for wireless sensing element networks. International journal of communication systems, 31(1), e3407.
8. Xiangning, F., & Yulin, S. (2007, October). Improvement on LEACH protocol of wireless sensor network. In Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on (pp.260-264).IEEE.
9. Magotra, S., & Kumar, K. (2014, February). Detection of HELLO flood attack on LEACH protocol. In Advance Computing Conference (IACC), 2014 IEEE International(pp.193-198).IEEE.
10. Zia, T., & Zomaya, A. (2006, October). Security issues in wireless sensor networks. In null (p. 40). IEEE.
11. Khan, F. A., Ahmad, A., & Imran, M. (2018)
12. Energy optimisation of PR-LEACH Routing theme exploitation Distance Awareness in web of Things Networks.
13. International Journal of Parallel Programming, 1-20.
14. Oliveira, L. B., Wong, H. C., Bern, M., Dahab, R., & Loureiro, A. A. F. (2006, July).Sec LEACH-A random key distribution answer for securing clustered sensing element networks.Innull (pp.145-154).IEEE.
15. Joshua Reginald Pullagura , Dr.D.Venkata Rao, "Attacks on Mobile Ad hoc Networks A Survey", International Journal of Computer Applications (IJCA), 2016, ISSN: 0975-8887.
16. [13] Fu, C., Jiang, Z., Wei, W. E. I., & Wei, A. (2013). An energy balanced formula of LEACH protocol in WSN.
17. International Journal of computing problems (IJCSI), 10(1), 354.
18. Mehmood, A., Mauri, J. L., Noman, M., & Song, H. (2015).
19. Improvement of theWireless sensing element Network period of
20. time exploitation LEACHES

with Vice-Cluster Head. Ad Hoc & Sensor Wireless Networks, 28(1-2), 1-17.

AUTHORS PROFILE

Joshua Reginald Pullagura is Asst. Prof in Vignan's foundation for Science Technology and Research (Deemed to be university) Guntur. He has published more than 10 research papers in International and National Journals. His area of interest includes Wireless Networks and Data Communications.

M.Rashmi V.V.Rao has done M.Tech in Vignan foundation for science technology and research (Deemed to be University) Guntur. Her area of interest is wireless sensor networks.

Dr.Venkata Rao Dhulipalla is working as Principal QIS College of Engineering and Technology Ongole. He has published more than 35 research papers in International and National journals.