ISSN:0975-9646

Leach Protocol in Wireless Sensor Network: A Survey

Reshma I. Tandel
Department of Information Technology
Shri S'ad Vidya Mandal Institute of Technology
Bharuch 392-001, Gujarat, India

***Abstract*— wireless sensor network (WSN) is a network consists of large number of low power sensor nodes. Leach is a less energy adaptive clustering hierarchy protocol. The main goal of cluster based sensor networks is to decrease system delay and reduce energy consumption. Leach is a cluster based protocol for micro sensor networks which achieves energy efficient, scalable routing and fair media access for sensor nodes. Many improvements are done in wireless sensor network. Security is very essential in wireless sensor network. This paper describes LEACH protocol, their advantages, disadvantages etc. The paper is organized as follows: In section I, contains introduction, section II contains description of LEACH protocol, and section III contains literature review.**

***Keywords*— wsn,sensor nodes, LEACH protocol, cluster, TDMA.**

I. INTRODUCTION

WSN form a subset of Ad-hoc networks. WSN consists of specially distributed autonomous sensors to cooperatively monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion etc. [1] LEACH protocol is the first protocol of hierarchical routing which proposed data fusion; it is of milestone significance in clustering routing protocol. Routing strategies and security issues are great research challenge. Nowadays in WSN, numbers of routing protocols have been proposed for WSN but most well-known protocols are hierarchical protocols like LEACH. Hierarchical protocols are defined to reduce energy consumption by aggregating data and to reduce the transmissions to the base station [2].

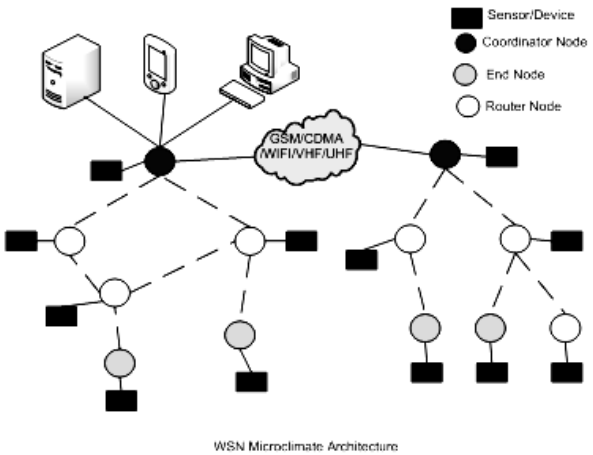

Fig 1.Wireless sensor network [1]

II. LEACH PROTOCOL

Leach protocol is a TDMA based MAC protocol. The main aim of this protocol is to improve the lifespan of wireless sensor networks by lowering the energy.

Leach protocol consists of two phases:

1) Set-up phase
2) Steady phase

Operation of leach protocol consists of several rounds with two phases in each round. Leach protocol is a typically representation of hierarchical routing protocol. It is self-adaptive and self-organized [2]. Leach protocol uses round as unit, each round is made up of cluster set-up stage and steady state storage for the purpose of reducing unnecessary energy costs.

Phases of leach protocol are as follows:

A. Set-up 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 [3].

Set-up phase has three fundamental steps:

1. Cluster head advertisement
2. Cluster set up
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:

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

$$T(n) = 0 \quad \forall n \notin G$$

Where n is a random number between 0 and 1
P is the cluster-head probability and
G is the set of nodes that weren't cluster-heads the previous rounds

Fig 2.cluster head selection [4]

T (n) is the threshold.

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

In the second step, non-cluster head nodes receive the cluster head advertisement and then send join request to the cluster head informing that they are members of the

cluster under that cluster head. All non-cluster head nodes save 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 [2].

In 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 [3].

B. Steady phase

In steady phase, cluster nodes send their data to the cluster head. The member sensors in each cluster can communicate only with the cluster head via a single hop transmission.

Cluster head aggregates all the collected data and forwards data to the base station either directly or via other cluster head along with the static route defined in the source code. After predefined time, the network again goes back to the set-up phase.

III. 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 predistribution 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.

IV. 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 [5].
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 [10]; this phenomenon can cause an increase in energy consumption and have great impact on the performance of the entire network [5].

V. ATTACKS ON LEACH

A. Sybil Attack

Most of the peer to peer networks face security threats due to Sybil attack [5]. 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 [6]. 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 [7]. In this kind of attack a malicious node places itself in the path where data is exchanged between the two legitimate nodes [5]. 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 neighbouring nodes [4]. 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 [8] of the sensor nodes when these nodes receive large amount of HELLO packets continuously and thus lowering the lifetime of the wireless sensor networks [9]. This type of attack is known as HELLO Flood attack [5].

VI. CONCLUSION

LEACH is a MAC protocol, it contains many advantages like it does not need any control information, it saves energy, it is completely distributed and also contain many disadvantages like if cluster head dies then cluster become useless, clusters are divided randomly etc. various improvements are done on LEACH protocol and so there are various version of LEACH protocol.

REFERENCES

[1] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energyefficient communication protocol for wireless sensor networks", in: Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.
[2] Bao Zhenshan, Xue Bo, Zhang Wenbo. "HT-LEACH: An Improved Energy Efficient Algorithm Based on LEACH", International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), 2013.
[3] Lalita Yadav, Ch. Sunitha, "Low Energy Adaptive Clustering Hierarchy in Wireless Sensor Network (LEACH)", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.
[4] Shikha Magotra, Krishan Kumar, "Detection of HELLO flood Attack on LEACH Protocol", International Advance Computing Conference (IACC),IEEE,2014.
[5] Reenkamal Kaur Gill, Priya Chawla and Monika Sachdeva, "Study of LEACH Routing Protocol for Wireless Sensor Networks", International Conference on Communication, Computing & Systems (ICCCS),2014.
[6] A. A. Abbasi, and M. Younis, ―A Survey on Clustering Algorithms for Wireless Sensor Network," Computer Communications 30, 2826-284 1, 2 1 June 2007.
[7] Mortaza Fahimi Khaton Abad, Mohammad Ali Jabreil Jamali, "Modify LEACH Algorithm for Wireless Sensor Networks," International Journal of Computer science Issues, Vol. 8, Issue 5, No. 1, September 2011.
[8] Yrjölä Juhana. Summary of Energy-Efficient Communication Protocol for Wireless Microsensor Networks, 13th March 2005
[9] Wang N B, Zhu H. "An energy efficient algorithm based on LEACH protocol" 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, Zhejiang, China. 2012: 339 – 342.
[10] O. Younis and S. Fahmy, ―HEED: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks,‖ IEEE Transactions on Mobile Computing, Vol. 3, No. 4, 2004, pp. 366–379.