

LEACH: IMPLEMENTATION OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

¹Satish Beniwal, ²Nitya Chaudhary, ³Vidhi Sen

¹ M. Tech. Scholar Global Institute of Technology, Jaipur, Rajasthan, India.

² M. Tech. Scholar Global Institute of Technology, Jaipur, Rajasthan, India.

³ M. Tech. Scholar Global Institute of Technology, Jaipur, Rajasthan, India.

Received 10 December 2013; Revised 22 December 2013; Accepted 26 December 2013

ABSTRACT

Wireless Sensor Networks is an active research area in today's computer science & Engineering and telecommunication field. The Wireless Sensor Networks consists of a number of tiny sensor nodes to watch corporeal or physical and ecological situation, such as temperature, vibration, pressure, sound or motion, and then collectively send this information to a central computing system, called the base station or sink. Different routing protocols govern the movement of this information. Broadly the routing protocols can be classified as at-based routing, hierarchical-based routing, and location based routing. LEACH (Low Energy Adaptive Clustering Hierarchy) is a hierarchical-based routing protocol which uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network.

Key Words: WSN, LEACH, CH, TDMA, CDMA, Protocol

INTRODUCTION:

Sensor networks refers to a heterogeneous system consisting of multiple detection stations called sensor nodes with a communications infrastructure intended to monitor and record conditions at diverse locations. Sensor nodes, also known as mote are small, lightweight and portable devices equipped with a transducer, microcomputer, transceiver, and power source.

Wireless Sensor Networks (WSN) offers a rich, multi-disciplinary area of research, in which a number of tools and concepts can be applied to address a whole diverse set of applications. Sensor networks may consist of many different types of sensors such as magnetic, thermal, visual, seismic, and infrared and radar, which are able to monitor a wide variety of conditions.

A hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH arranges the nodes in the network into small

clusters and chooses one of them as the cluster-head [1]. Node first senses its target and then sends the relevant information to its cluster-head. Then the cluster head aggregates and compresses the information received from all the nodes and sends it to the base station. The nodes chosen as the cluster head drain out more energy as compared to the other nodes as it is required to send data to the base station which may be far located. Hence LEACH uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network. After a number of simulations by the author, it was found that only 5% of the total number of nodes needs to act as the cluster-heads. TDMA/CDMA MAC is used to reduce inter-cluster and intra-cluster collisions. This protocol is used were a constant monitoring by the sensor nodes are required as data collection is centralized (at the base station) and is performed periodically.

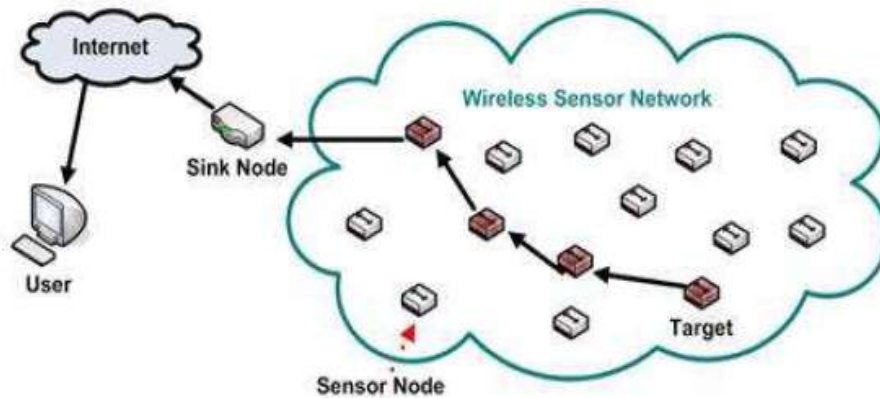


Figure 1: Wireless sensor network architecture

1. LEACH PROTOCOL:

Based on the LEACH, LEACH-C also organizes the sensor nodes into clusters with each cluster a cluster head and divides a round into set-up and steady-state phases. It differs from LEACH only in that it uses a high-energy base station to finish the choice of cluster heads. In the set-up phase of each round, every sensor node sends its information about energy to remote BS. Then the BS selects the cluster heads based on the energy information and broadcasts the IDs of cluster heads to other member nodes. This method can make the nodes with more energy and more chance to become the cluster head in the current round. But in this phase, every sensor node needs to send its ID and energy information to remote BS to compete for the role of cluster heads, which causes energy consumption on the long distance transition. Equation (2) has a good description of transition distance influence on the consumption of energy [2]

$$E_{\text{trans}}(k, d) = \begin{cases} kE_{\text{elec}} + k\epsilon_{fs}d^2 & (d < d_0), \\ kE_{\text{elec}} + k\epsilon_{mp}d^4 & (d \geq d_0). \end{cases} \quad \dots(2)$$

The transmission energy of transmitting a k-bit message over a distance 'd' will cost 'E Trans' ϵ_{fs} and ϵ_{mp} are the power consumption of transferring 1 bit of data in different condition. We can obtain that there will be a certain amount of energy needed to be spent on the transition of energy information for each sensor node in every round, which cannot be neglected in communication; especially the BS locates far away from the monitor field and the network has a lot of sensor nodes.

2. LOW ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH) PROCESSING:

LEACH is the most popular hierarchical cluster based routing protocol for a wireless sensor network [3]. In

LEACH, the nodes in the deployed area are organized into local clusters and the communication process is divided into rounds with each round including set-up and steady-state phases. During the communication process, each cluster has a cluster head (CH) which is responsible for creating and manipulating a TDMA (time division multiple access) schedule table used by its member nodes to get when to transmit data packets. Once some emergency affairs happen in the monitor area, the sensor nodes are triggered to send data to their own cluster head instead of the remote BS by themselves. The cluster head mainly collects the data coming from different member nodes and does some aggregation to diminish the redundancy firstly and then transmits them to BS. In the whole process, the cluster head just works as a relay node to help member nodes shorten the transmission distance so as to save energy.

LEACH processing can be divided into two categories processes:

- A. Association process
- B. Stable Process

In Association process, the clusters are formed and a cluster-head (CH) is chosen for each cluster. While in the steady phase, data is sensed and sent to the central base station. The steady phase is longer than the setup phase. This is done in order to minimize the overhead cost.

A. Association Process: - During the setup phase, a predetermined fraction of nodes, p, choose themselves as cluster-heads. This is done according to a threshold value, T (n). The threshold value depends upon the desired percentage to become a cluster-head- p, the current round r, and the set of nodes that have not become the cluster-head in the last 1/p rounds, which is denoted by G. The equation: 1 formula is as follows:

$$T(n) = \frac{p}{1 - p \times (r \times \text{mod} \frac{1}{p})} \quad \forall n \in G \quad \dots (1)$$

Every node wanting to be the cluster-head chooses a value, between 0 and 1. If this random number is less than the threshold value, $T(n)$, then the node becomes the cluster-head for the current round. Then each elected CH broadcasts an advertisement message to the rest of the nodes in the network to invite them to join their clusters. Based upon the strength of the advertisement signal, the non-cluster head nodes decide to join the clusters. The non-cluster head nodes then informs their respective cluster-heads that they will be under their cluster by sending an acknowledgement message. After receiving the acknowledgement message, depending upon the number of nodes under their cluster and the type of information required by the system (in which the WSN is setup), the cluster-heads creates a TDMA schedule and assigns each node a time slot in which it can transmit the sensed data. The TDMA schedule is broadcasted to all the cluster-members.

If the size of any cluster becomes too large, the cluster-head may choose another cluster head for its cluster. The cluster-head chosen for the current round cannot again become the cluster-head until all the other nodes in the network haven't become the cluster head.

B. Stable Process :- During the steady phase, the sensor nodes i.e. the non-cluster head nodes starts sensing data and sends it to their cluster-head according to the TDMA schedule. The cluster-head node, after receiving data from all the member nodes, aggregates it and then sends it to the base-station.

After a certain time, which is determined a priori, the network again goes back into the setup phase and new cluster-heads are chosen. Each cluster communicates using different CDMA codes in order to reduce interference from nodes belonging to other clusters.

3. IMPLEMENTATION TO THE CLUSTER-BASED LEACH PROTOCOL:

Motivated by the original LEACH, LEACH-C and other improvement protocols [4], we propose a modification to the cluster head selection process to reduce energy consumption. For a micro sensor network, we first make the following assumptions.

- A.** The base station (BS) is located far from the sensors and is immobile.
- B.** All nodes in the network are homogenous and have limited energy with an indentify ID.

C. All nodes are able to reach BS and can communicate with each other.

D. Cluster heads perform data compression and aggregation.

In the improvement, we also make use of the clustering ideology in hierarchical and divide a round into a set-up phase and steady-state phase. The set-up phase will use improved formula to select appropriate cluster heads (CHs) which are responsible for collecting data from their member nodes and transmitting them to BS. As CHs will consume more energy than member nodes because of the heavy tasks. In order to avoid making the CHs die early, LEACH and LEACH-C take the measure of beginning a new round and rebuilding the clusters. However, in this paper, we will make use of the member nodes' information dynamically achieved by cluster heads in the steady phase to choose the vice cluster heads (VCHs) which take over the role of cluster heads in the later period of steady phase. Comparing with the traditional LEACH and LEACH-C, the VCHs proposed will diminish the frequency of reclustering in the same interval and prolong the time of being in steady-state phase, which will prolong the lifecycle of the whole network.

4. LEACH PROTOCOL ATTACKING:

LEACH protocol is difficult to attack as compared to the more conventional multi-hop protocols. In the conventional multi-hop protocols, the nodes around the base station are more attractive to compromise. Whereas in LEACH, the CHs are the only node that directly communicate with the base station[8]. The location of these CHs can be anywhere in the network irrespective of the base station. And more over the CHs are periodically randomly changed. So spotting these CHs is very difficult for the adversary.

However, because it is a cluster-based protocol, relying fundamentally on the CHs for data aggregation and routing, attacks involving CHs are the most damaging. If any adversary nodes become a CH, then it can facilitate attacks like Sybil attack, HELLO food attack and selective forwarding. The intruder can broadcast a powerful advertisement to all the nodes in the network and hence, every node is likely to choose the adversary as the cluster-head. The adversary can then selectively forward information to the base-station or modify or dump it.

Key management is an effective method to improve network security. These schemes typically assume that a node interacts with a quite static set of neighbors and that most of its neighborhood is discovered right after the deployment [9]. However, clusters in LEACH are formed dynamically (at random) and periodically, which

changes interactions among the nodes and requires that any node needs to be ready to join any CH at any time. There are a number of standard key distribution schemes but most of them are ill suited to WSNs *for example*, public key based distribution requires a lot of processing; global keying is quite vulnerable and complete pair wise keying requires a huge memory [5].

5. COMPARETIBLY BEHAVIOR OF LEACH PROTOCOL:

A LEACH protocol has number of sub Protocols which may create comparetibly behavior between each other in the real-time system.

A. F-LEACH:

F-LEACH, a protocol for securing node to node communication in LEACH-based network [9]. It used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH. FLEACH provides authenticity, integrity, condentiality and freshness to node-to-node communication. But it is vulnerable to node capturing attack.

B. S-LEACH:

This is the first modified secure version of LEACH called SLEACH [1], 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. S-LEACH 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 coding 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 condentiality.

C. NHRPA:

The proposed routing protocol can adopt suitable routing technology for the nodes according to the distance of node to the BS, density of the nodes distribution and residual energy of the nodes [6]. NHRPA compared with Directed Discussion (DD), LEACH and PEGASIS in terms of the energy usage, packet latency and security in the presence of node compromised attacks, results show that the proposed routing algorithm is more efficient for WSNs.

D. 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 condentiality and freshness. Sec-LEACH provides authenticity, integrity, condentiality and freshness to communications.

E. SS-LEACH:

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 [5]. In this way it improves the energy efficiency and hence prolongs the lifetime of the network. It used the key pre-distribution and self-localization technique to secure the basic LEACH protocol.

F. R-LEACH:

Secure solution for LEACH has been introduced called RLEACH [5] 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 Hi- hierarchical routing protocol.

6. CONCLUSION:

The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol and analyzed the protocol based on network lifetime, stability period and the network throughput. We have put light on the comparison of LEAH protocol with the effect of heterogeneity and selective forwarding attack. This method can make the nodes with more energy and more chance to become the cluster head in the current round. In LEACH, the nodes in the deployed area are organized into local clusters and the communication process is divided into rounds with each round including set-up and steady-state phases.

7. REFERENCES:

1. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd Annual Hawaii International Conference on System Siences (HICSS '00), January 2000.
2. M. Bern R. Dahab L. B. Oliveira, H. C. Wong and A. A. F. Loureiro. Secleach- a random key distribution solution for securing clustered sensor networks. In Fifth IEEE International Symposium on Network

- Computing and Applications, pages 145{ 154, Washington, DC, USA, 2006.
3. M. Bern R. Dahab L. B. Oliveira, H. C. Wong and A. A. F. Loureiro. Secleach- a random key distribution solution for securing clustered sensor networks. In Fifth IEEE International Symposium on Network Computing and Applications, pages 145{ 154, Washington, DC, USA, 2006.
 4. A. V. Reddy R. Srinath and R. Srinivasan. Ac: Cluster based secure routing protocol for WSN. In Third International Conference on Networking and Services, page 45, Washington, DC, USA, 2007.
 5. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS '00), January 2000.
 6. K. Khamforoosh and H. Khamforoush, "A new routing algorithm for energy reduction in wireless sensor networks," in Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT '09), pp. 505–509, August 2009.
 7. M. A. Vilaa H. C. Wong M. Bern R. Dahab L. B. Oliveira, A. Ferreira and A. A. F. Loureiro. Secleach-on the security of clustered sensor networks. (87(12)):2882{2895, December 2007.
 8. Vinh Tran-Quang, Takumi Miyoshi. A novel gossip based sensing coverage algorithm for dense wireless sensor networks Computer Networks 53 (2009) 2275–2287.
 9. M. Bani Yassein, A. Al-zou'bi, Y. Khamayseh, W.Mardini. Application-Specific Protocol Architectures for Wireless Networks. International Journal of Digital Content Technology and its Applications, Volume 3, Number 2, June 2009.
 10. Baiping Li1, Xiaoqin Zhang. Research & Improvement of LEACH Protocol for Wireless Sensor Network. International Conference on Information Engineering, 2012.

