Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Confidentiality Scheme for Energy Efficient LEACH Protocol Using Homomorphic Encryption

**Alisha Gupta***
*CSE & Kurukshetra University*
*Haryana, India.*

**Vivek Sharma**
*CSE & Kurukshetra University*
*Haryana, India.*

***Abstract— Wireless Sensor Network (WSN) has been an active research area over the past few years. However, the salient limit is energy. Due to this limitation, it seems important to design a routing protocol for WSN so that sensing data can be transmitted to the receiver securely and efficiently and at the same time energy consumed must be minimum. Hence there is a need to develop a confidentiality scheme for energy efficient Leach protocol (hierarchical clustering protocol) using homomorphic encryption. In homomorphic encryption data can be aggregated algebrically without decryption and hence less energy consumption.***

***Keywords— Wireless sensor network (WSN); Clustering; Leach protocol; Energy Efficient;Homomorphic Encryption***

## I. INTRODUCTION

Recent advances in wireless communications have enabled the development of low-cost, low-powered multifunctional sensor nodes that are small in size and jointly communicate in short distances .These sensor nodes consist of data sensing, data processing, and communication units. A wireless sensor network are special kinds of adhoc network system usually includes sensor nodes, sink nodes and cluster heads [1]. Fig 1 below shows a large number of sensor nodes deployed in the monitored area, constituting a network through the way of self organization. The data monitored by sensor nodes is transmitted along the other nodes hop by hop that will reach the sink node after a multi-hop routing [2].

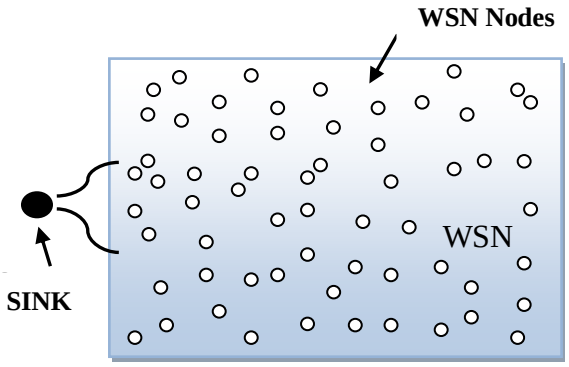


**Fig.1 Illustration of data flow in a clustered Network[3]**

One major application of WSN is to monitor environmental data and to transmit it to a central point called sink node. The sink node analyzes the data which is then used to initiate some specific action. The data analysis carried out by sink node is to compute minimum or maximum, or computation of average. This data analysis can occur either at the sink node or in the network. If analysis is carried out at sink node every sensed data is to be transmitted to sink node. Upon receiving the data from all the nodes, sink node computes the required aggregate. Wireless sensor network have some advantages, such as reliability, self-organization, dynamic, easy to expand and easy deployment, but due to the sensor nodes are generally dispersed in a hostile environment, it costs high or is impossible for people to replace or charge the battery. However, the numbers of such nodes are considerably high and monitoring these nodes is quite difficult, especially in the cases when the nodes are distributed in the regions far away from a city or town. The network once established, keeps on sensing the data and the energy of the nodes keep on dissipating whenever, they receive some information and send it further to other nodes or BS.

Routing protocol is an important factor affecting the energy consumption of sensor nodes. There are two routing protocols of wireless sensor network[1]:

1) *Flat based routing protocol*: In flat routing protocols nodes play the same role and have similar functionality in transmitting and receiving data. In this type of network it is not possible to assign a global identifier to each node

 

due to large number of nodes. Therefore, base station send queries to different part of the field and waits for the data from sensors in selected parts of the field. This approach is called data centric routing.

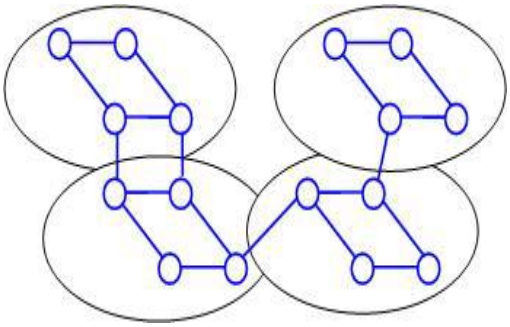

**Fig. 2 Flat Networks**

2) *Hierarchical routing protocol***:** In this nodes will be assigned different roles in the network like cluster heads, members of clusters, etc[1]**.** The hierarchical network is shown in fig. 3 below.Some of the nodes are responsible for processing and communication, while other nodes can be used for sensing the target area. Hierarchical routing is mainly considered as two layer architecture where one layer is engaged in cluster head selection and the other layer is responsible for routing.

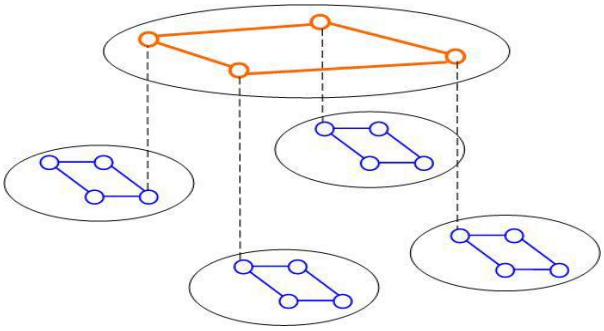

**Fig. 3 Hierarchical Networks**

Hierarchical-based routing protocols also known as cluster based routing protocols. In order to avoid redundancy hierarchical routing protocols are best. This type of protocols enforces a structure on the network to use the energy efficiently, enhance the lifetime and scalability. In this protocol, nodes are grouped into the clusters in which higher energy nodes (e.g. act as cluster head) can be used to process and forward the data, while other nodes can be used to sense the target. Cluster heads do data aggregation and fusion in order to reduce the size of transmitted messages to the base station.

## II. HOMOMORPHIC ENCRYPTION

A homomorphic encryption scheme allows arithmetic operations on cipher texts. Homomorphic encryption schemes allow aggregation on cipher text. One example is a multiplicative homomorphic scheme, where the decryption of the efficient manipulation of two cipher texts yields the multiplication of the two corresponding plaintexts [4].
In additive homomorphic encryption, we encrypt by adding a key to the data value, and we decrypt by subtracting a key from the aggregated value. An important property of the encryption and decryption functions is that they are commutative. Homomorphic encryption schemes are especially useful whenever some party not having the decryption key(s) needs to perform arithmetic operations on a set of cipher texts.

### *A. Advantages of Homomorphic Encryption*

1) *Trapdoor Encryption:* Homomorphic Encryption makes it possible to give user a way to perform some operation on encrypted data without decryption key. So we are using the same property in this paper, the cluster head is doing aggregation operation on encrypted data.
2) *Secret Sharing:* It means that a secret is shared between several parties in such a way that no single party can retrieve the secret.

## III. LEACH PROTOCOL

LEACH (Low Energy Adaptive Clustering Hierarchy) is first proposed by Wendi B. Heinzelman of MIT[6]. LEACH is a clustering-based protocol that randomly rotates cluster head (CH) to evenly distribute the energy load among the sensor nodes in the network [5]. LEACH incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to base station. LEACH rearranges the network periodically and dynamically, making it difficult

 

for us to rely on long lasting node-to-node trust relationship to make protocol secure [5]. The Leach protocol routing topology is shown in fig. 4 below:

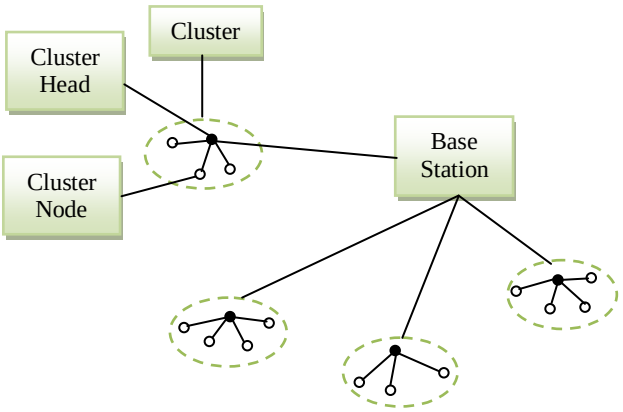


**Fig 4. LEACH routing topology**

LEACH protocol works in various rounds. Each round contains two phases:
1. Setup phase
2. Steady phase

**1. Setup phase**

Each node decides whether or not to become a cluster head for current round. It depends on decision made by the node by choosing a random number between 0 and 1[6]. The node whose number is bigger than the threshold will become the cluster-head. The threshold is set as:

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

Where,

P is the probability of the node being selected as a cluster-head node
r is the number of rounds passed
G is the set of nodes that have not been cluster-heads in the last 1/p rounds mod denotes modulo operator.

Nodes that are cluster heads in round r shall not be selected in the next 1/p rounds.

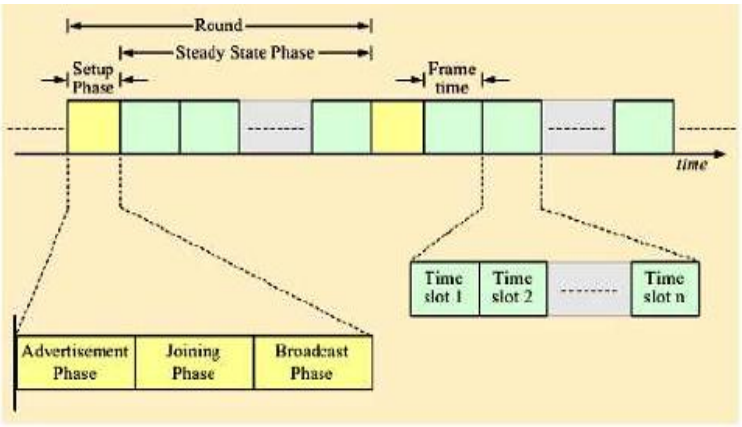


**Fig 5. Timeline diagram for LEACH protocol[2]**

Then the CH will broadcast an advertisement message to inform all others that it is the new cluster-head. The nodes send the join-request message containing their IDs by using CSMA (carrier sensing multiple access) to join a cluster. The node joins that cluster from which they received strongest strength signal. After that, each CH knows its own cluster

 

members information.Based on the message, the CH creates TDMA schedule table and broadcasts it to the cluster members. So all the member nodes know their idle slots, and then the steady-state phase begins.

**2. Steady state phase**

During the Steady-state phase, each node turns on its radio only when it senses necessary data. The member nodes can send their data to CH during their allocated schedule table created during the set-up phase. When the CH receives all the data sent by their members, it will aggregate them and then send the aggregating data packets to BS. Aggregation of data saves energy and hence reduces the consumption of energy in Leach protocol.

Sensor networks are often deployed in hostile a environment, which makes them targets for malicious attacker. However, several features of sensor networks make it very challenging to provide security in sensor networks:

- Sensor nodes are typically resource constrained due to the need to lower the cost. As a result, it is usually undesirable to use expensive mechanisms such as public key cryptography on such nodes.
- Sensor networks are often deployed in an unattended fashion, possibly exposed to physical attacks. Sensor nodes may be captured, and any secret information on a captured node can potentially be disclosed to attackers.
- WSNs have special security requirements, for example, data confidentiality, data integrity, data authentication, freshness, self-organization and secure localization.

In a sensor mote a small amount of resources are left for security to be implemented. This is insufficient to even hold the variables for asymmetric public key based cryptographic algorithms like RSA and Diffie-Hellman. Thus public key based systems do not work for sensor networks. Because of the resource constraints another solution is to use global keys. This is feasible but a global key based system does not provide the desired level of security. On the contrary, complete pair-wise keying between nodes provides the best possible security, but it is not a choice for sensor network because of the resource constraints.

*A. An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks*

Lan Tien Nguyen et al. proposed M-Leach with reduced network energy consumption as compared to LEACH. The features that are not supported are: LEACH assumes a homogeneous distribution of sensor nodes in the given area which is not very realistic; LEACH does not really support movement of nodes.The proposed algorithm put some features that LEACH does not support such as:

- Mobility of cluster head and member node during one round
- Currently remaining battery power and the number of nodes per cluster are also considered[7]

*B. Improved LEACH Routing Communication Protocol for a Wireless Sensor Network*

Fuzhe Zhao et al. proposed improved clustering protocol that performs better than the LEACH and the LEACH-C by reducing the consumption of energy. LEACH and LEACH-C suffers from many drawbacks like:

- CHs' selection is random and periodic, which does not take into account the residual energy of every node.
- Reclustering of network wastes a certain amount of energy.
- It cannot cover a large area.
- CHs are not distributed uniformly.

Fuzhe Zhao et al developed improved formula to select appropriate cluster heads (CHs). They also 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. 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 further extend the lifetime of the whole network[8].

*C. The Improvement of Leach Protocol in WSN*

Luwei Ding, et al. proposed Leach-N that performs better than LEACH in the following three aspects, the number of live nodes, energy consumption and data transmission. They added a factor taking into account the current residual energy during calculating the threshold of node, which is

$$T(n) = \begin{cases} \dfrac{P}{1-P(r \bmod (1/P))} * \dfrac{E_{init} - E_{current}}{E_{init}} & ,\text{if } n \in G \\ 0 & ,\text{other} \end{cases}$$

Where,

P is the expected proportion of cluster head nodes
r is the current number of rounds
G is nodes set which has not been selected as cluster head nodes in the last 1/P rounds.
$E_{init}$ is the initial energy of the node, and
$E_{current}$ represents the node's current residual energy.

 

The new protocol LEACH-N will increase calculation time of the node's threshold, but the overhead of calculation is smaller than that of the cluster head election which does not take into account the residual energy of nodes. Therefore, the set of residual energy factor is reasonable and can reduce the energy cost of network nodes to a certain extent[9].

*D. SEEDA: Secure End-to-End Data Aggregation in Wireless Sensor Networks*

A.S.Poornima et al. proposed a secure data aggregation scheme which provides end-to-end data privacy. Wireless Sensor Network (WSN) consists of a large number of nodes with limited resources. In such network consisting of resource constrained nodes, data transmission is a energy-consuming operation. Hence to extend the lifetime of the network it is necessary to reduce the number of bits transmitted. One widely used method for reducing the data bits is data aggregation. The security issues such as data integrity, confidentiality and freshness in data aggregation become crucial when the WSN is deployed in a remote or hostile environment where sensors are prone to node failures. Secure data aggregation schemes are suitable to achieve security in data aggregation. The data encrypted at SN-nodes is decrypted by the sink node. At aggregator nodes the cipher texts are added. The protocol uses additive homomorphic encryption method to encrypt the data. The additive homomorphic encryption allows addition of cipher texts which when decrypted results in addition of the plain text[10].

*E. Research and Improvement of LEACH Protocol for Wireless Sensor Network*

Baiping Li and Xiaoqin Zhang proposed LEACH-CC in which a chain routing between clusters is established to reduce the amount of nodes which communicate with the base station. It not only extends the lifetime of the network, but also improves the energy efficiency.

Using a central control algorithm to form the clusters may produce better clusters by dispersing the cluster-head nodes throughout the network. Then a chain routing between cluster-heads is established to reduce the amount of nodes which communicate with the base station. Further improvement in energy cost for data gathering can be achieved if only one cluster-head transmits to base station and if each cluster-head transmits only to local neighbour cluster-heads in the data fusion phase. This is the basis for LEACH-CC (LEACH Centralized with Chain)[11].

## IV. CONCLUSIONS

It is found that the main limiting factor in LEACH protocol is energy. Data gathering and forwarding is one of the important operations in WSNs and is main cause of energy consumption. Secure transmission of data in LEACH protocol is another area on which focus is needed. Since all nodes send their data to their CHs, hence CH can be the target for intruder. In case of public key methods data from nodes are to be decrypted at CH since CH needs original data on which it can perform aggregation. Hence there is need to develop new LEACH protocol in which data is transmitted in confidential way with least energy consumption and no need to decrypt data at CH. Homomorphic encryption is the solution to the problem.

## REFERENCES

[1] Nazia Majadi , "U-LEACH: A Routing Protocol for Prolonging Lifetime of Wireless Sensor Networks," (IJERA) Vol. 2, Issue4, July-August 2012

[2] Vikas Nandal and Deepak Nandal , "Maximizing Lifetime of Cluster-based WSN through Energy-Efficient Clustering Method," IJCSMS Vol. 12, Issue 03, September 2012

[3] Lianshan Yan and Wei Pan, " Modified Energy-Efficient Protocol for Wireless Sensor Networks in the Presence of Distributed Optical Fiber Senor Link,"*IEEE SENSORS JOURNAL*, VOL. 11, NO. 9, SEPTEMBER 2011

[4] A.S.Poornima and B.B.Amberker, "SEEDA : Secure End-to-End Data Aggregation in Wireless Sensor Networks," IEEE 2010

[5] Mona El_Saadawy,et al, " Enhancing S-LEACH Security for Wireless Sensor Networks," IEEE 2012

[6] Jia Xu,et al, "Improvement of LEACH protocol for WSN," 2012 IEEE

[7] Meenakshi Diwakar and Sushil Kumar, "An Energy Efficient Level Based Clustering Routing Protocol For Wireless Sensor Networks," IJASSN, Vol 2, No.2, April 2012

[8] Fuzhe Zhao, You Xu, and Ru Li , "Improved LEACH Routing Communication Protocol for a Wireless Sensor Network," *Hindawi Publishing Corporation* International Journal of Distributed Sensor Networks Volume 2012

[9] Yuling Li, Luwei Ding ,FengLiu, "The Improvement of LEACH Protocol in WSN," *IEEE International Conference on Computer Science and Network Technology* 2011

[10] Baiping Li1 and Xiaoqin Zhang, "Research and Improvement of LEACH Protocol for Wireless Sensor Network," 2012 International Conference on Information Engineering, Vol.25

[11] Abderrahim Beni Hssane, Moulay Lahcen, "Position-Based Clustering: An Energy-Efficient Clustering Hierarchy for Heterogeneous Wireless Sensor Networks," (IJCSE) Vol. 02, No. 09, 201

[12] Lan Tien Nguyen , Xavier Defago, Razvan Beuran , Yoichi Shinoda, " An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks," *IEEE ISWCS* 2008

[13] Kun Zhang, Cong Wang, Cuirong Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," 2008 IEEE

Yi Liu, Shan Zhong, Licai You, Bu Lv, Lin Du, "A Low Energy Uneven Cluster Protocol Design for Wireless Sensor Network," Int. J. Communications, Network and System Sciences, 2012, 5, 86-89.

 