International Journal of Electrical and Electronics Engineering (IJEEE)
ISSN 2278-9944
Vol. 2, Issue 4, Sep 2013, 63-74

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

IMPLEMENTATION OF LEACH PROTOCOL USING HOMOMORPHIC ENCRYPTION

ALISHA GUPTA[1] & VIVEK SHARMA[2]

[1]Research Scholar, JMIT, Radaur, Haryana, India

[2]Assistant Professor & H.O.D, JMIT, Radaur, Haryana, India

ABSTRACT

Encryption schemes that support operations over ciphertext are of utmost importance for wireless sensor networks & especially in LEACH protocol. The salient limit of LEACH is energy. Due to this limitation, it seems important to design a confidentiality scheme 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 we proposed LEACH_HE in which confidentiality scheme i.e. homomorphic encryption is added to LEACH protocol. In homomorphic encryption data can be aggregated algebraically without decryption and hence less energy consumption. Simulation results are obtained in terms of three metrics- total energy consumed, amount of data transmitted and number of nodes alive. It is observed that the performance of LEACH_HE is somewhat similar to LEACH.

KEYWORDS: Clustering, Homomorphic Encryption, LEACHl, LEACH_HE, Wireless Sensor Network (WSN)

INTRODUCTION

Wireless sensor networks consist of many spatially distributed sensors, which are used to monitor various kinds of ambient conditions like temperature, humidity, etc and then transform them into electric signal. These sensor nodes consist of data sensing, communication and data processing units. Wireless sensor networks are special kinds of clustered adhoc network that usually includes sensor nodes, sink nodes and cluster heads [1,2]. The data sensed by sensor nodes is transmitted along the other nodes hop by hop that will reach the sink node after a multi-hop routing [2].

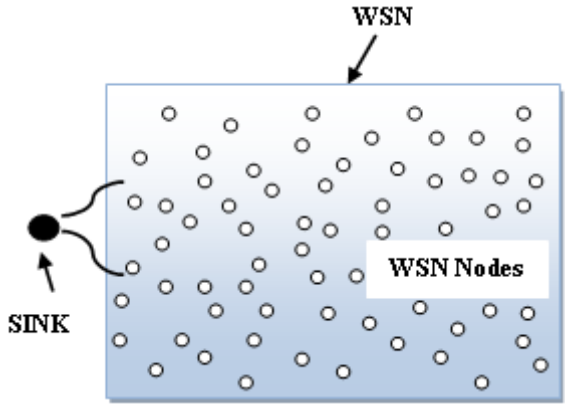

Figure 1: Illustration of WSN Network [3]

WSN has many advantages, such as wide coverage, high precision monitoring, self-organization, fault tolerance, and so on. At present, it shows a great charm in disaster salvage, target tracking, security monitoring, industrial control and monitoring, home automation and defence and other areas. The sensor nodes are generally deployed in a hostile environment, its cost is high or is impossible for people to replace or charge the battery. However, the number of such nodes is 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.

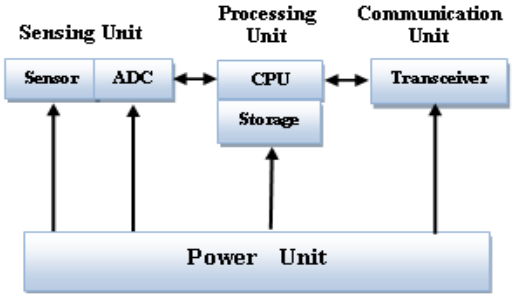

Figure 2: Architecture of Sensor Node

The sensor nodes act as both data generator and data router. The architecture of sensor node is shown in figure 1.2. Typically, data collected from same cluster members are highly correlated. Data aggregation process is done at CHs thus reducing the consumption of energy. The sink node analyzes the data which is then used to initiate some specific event or action. The network keeps on sensing the data and the energy of the nodes keep on dissipating. Whenever they receive some data, they send it further to other nodes or BS.

Routing protocol is an important factor of affecting the energy consumption of sensor nodes. There are three routing protocols of wireless sensor network [1,2]:

Flat Based Routing Protocol: In this nodes play the same role and have similar functionality in transmitting and receiving data. In many applications of wireless sensor networks, due to lack of global identification along with random deployment of sensor nodes, it is hard to select a specific set of sensor nodes to be queried. 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.

Hierarchical Routing Protocol: In this nodes will be assigned different roles in the network like cluster heads, members of clusters, etc. 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.

Location Based Routing Protocol: Sensor nodes are addressed by means of their locations. The distance between nodes can be estimated on the basis of incoming signal strengths. To save energy, some location-based schemes demand that nodes should go to sleep if there is no activity. [1]

Hierarchical-based routing protocols are also known as cluster based routing protocols. In order to avoid redundancy hierarchical routing protocols are the 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 classified 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 data. Cluster heads do data aggregation and fusion in order to reduce the size of transmitted messages to the base station.

LEACH PROTOCOL

LEACH (Low Energy Adaptive Clustering Hierarchy) an energy conserving routing protocol was proposed by Wendi B. Heinzelman of MIT [6]. The idea is to form cluster of sensor nodes based on signal strength and use the cluster-head as a router to forward data of other nodes in cluster to the base station. The data processing is performed at cluster-heads. [5] In this protocol, nodes are classified into two categories: CHs and SNs. The nodes are organised into local clusters and the communication process is divided into rounds. A dedicated node selected as CH is responsible for creating and manipulating a TDMA slots and aggregating the data coming from different nodes and sending it to the BS.

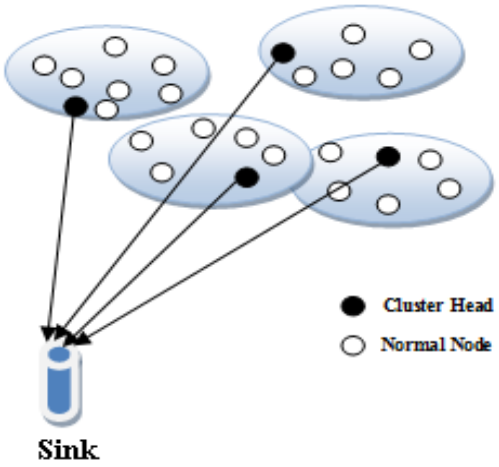

Figure 3: LEACH Routing Topology [6]

LEACH protocol works in rounds. Each round is divided into two phases:

- Setup phase
- Steady phase

Setup Phase

At the beginning of the round, each node decides independently of other nodes whether or not to become a cluster head for current round. Each sensor node generates a random number such that 0< random < 1 and compares it to a pre-defined threshold T (n). If random < T(n), the sensor node becomes cluster-head in that round, otherwise it is cluster member [6]. The threshold is given T(n) below:

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

Where,

P is the probability of the node being selected as a cluster-head node

r is the number of rounds of selection

G is the set of nodes that haven't 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. After CH selection, the CH will broadcast an advertisement message using CSMA MAC protocol to its neighbours that it is the new cluster-head. The nodes will send the join-request message containing their IDs by using CSMA (carrier sensing multiple access) to join a cluster from which they receive strongest strength signal. After that, each CH knows its own cluster members information. The CH node sets up a TDMA schedule for data transmission coordination within cluster and broadcast it to its cluster members. The TDMA schedule prevents collision among data messages and conserves energy among non-cluster head nodes. So all the member nodes know their TDMA slots, and then the steady-state phase begins. [15]

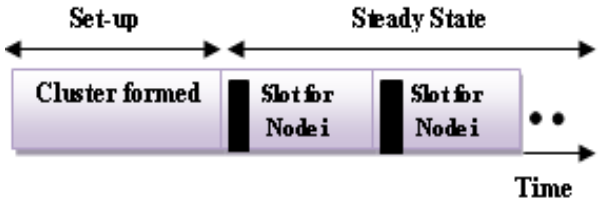

Figure 4: Period of LEACH [15]

Steady State Phase

In the steady-state phase, cluster members sense the surroundings and transmit the sensed data to their CH depending on the TDMA schedule received at the setup phase. SNs go into sleep mode to save energy for other slots. When the CH receives all the data sent by its cluster members, it will aggregate them and then send the aggregated data to BS. After a certain time, the network goes back into the setup phase again and enters another round of selecting new CH.

HOMOMORPHIC ENCRYPTION

Homomorphic Encryption scheme was proposed by Rivest et al. in 1978. Homomorphic Encryption allows one to compute arbitrary functions over encrypted data without the decryption key i.e., given encryptions E(m1),……,E(m_t) of m_1,……,m_t, one can efficiently compute a compact ciphertext that encrypts f(m_1,……,m_t) for any efficiently computable function f.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]. 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.

Fully homomorphic encryption has numerous applications. For example, it enables private queries to a search engine- the user submits an encrypted query and the search engine computes a succinct encrypted answer without ever looking at the query in the clear. It also enables searching on encrypted data - a user stores encrypted files on a remote file server and can later have the server retrieve only files that (when decrypted) satisfy some boolean constraint, even though the server cannot decrypt the files on its own. More broadly, fully homomorphic encryption improves the efficiency of secure multiparty computation.

LITERATURE SURVEY

Vikas Nandal and Deepak Nandal [2] proposed a progressive algorithm for the cluster head selection. The proposed algorithm for cluster head selection is based on residual energy, distance & reliability. The cluster head generation algorithm with the original LEACH clustering protocol can cause unbalanced distribution of cluster heads, which often leads to redundant cluster heads in a small region and thus cause the significant loss of energy.The improved algorithm is as follows:

- The first round will be same as normal leach round.
- In the 2nd round, each node would send residual energy along with the sending time stamp T-S and the remaining lifetime of battery.
- When the base station receives the packet, it will calculate T-R - T-S (the difference between receiving timestamp and current time stamp)
- If difference > = remaining lifetime of node, the node will become non-cluster head else If remaining lifetime = max among all nodes of the cluster, choose the node as cluster head.

Lianshan Yan, Wei Pan, Bin Luo, et al. [3] investigated an improved energy-efficient communication protocol for wireless sensor networks (WSNs) in the presence of distributed optical fiber sensor (DFS) links located at the center of WSN fields based on the protocol—low-energy adaptive clustering hierarchy (LEACH). They investigated a modified energy-efficient communication protocol, called O-LEACH, for wireless sensor networks that consist of DFS links and

randomly scattered wireless sensor nodes. Survival round numbers of WSN nodes are simulated for various cases using different parameters. Network performances in terms of lifetime of nodes are simulated for the cases that two WSNs can or cannot communicate with each other. The lifetime of such sensor network with rectangular topology is further investigated. The lifetime of the situation that two WSNs are isolated is more than 20% better than that of the case where nodes inside two WSN fields are reachable to any live nodes within the whole sensor field. This can be a deployment guideline for such hybrid sensor networks.

A. S. Poornima and B.B.Amberker [4] 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. 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. 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.

Mona El_Saadawy and Eman Shaaban [5] proposed MS-LEACH to enhance the security of S-LEACH by providing data confidentiality and node to cluster head (CH) authentication using pairwise keys shared between CHs and their cluster members. The security analysis of proposed MS-LEACH showed that it had efficient security properties and achieved all WSN security goals compared to the LEACH protocol. A simulation based performance evaluation of MS-LEACH demonstrated the effectiveness of proposed MS-LEACH protocol and showed that the protocol achieves the desired security goals and outperforms other protocols in terms of energy consumption, network lifetime, and network throughput and normalized routing load.

Jia Xu, Ning Jin, Xizhong, et al. [6] proposed a revised cluster routing algorithm named E-LEACH to enhance the hierarchical routing protocol LEACH. In the E-LEACH algorithm, the original way of the selection of the cluster heads was random and the round time for the selection was fixed. In the E-LEACH algorithm, the remnant power of the sensor nodes was considered in order to balance network load. In the E-LEACH they used the minimum spanning tree between cluster heads, the cluster head which has largest residual energy was chosen as the root node. The main idea of the improved cluster head selection algorithm was to avoid the lower residual energy nodes and higher consumed energy nodes to be cluster-head. The simulation results showed that the proposed protocol increases network lifetime at least by 40% when compared with the LEACH algorithm.

Lan Tien Nguyen et al. [7] 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

PROPOSED WORK

In this paper we propose a protocol LEACH_HE based on LEACH protocol to balance the energy consumption while providing confidentiality. The LEACH_HE is based on same round concept as the original LEACH. In hierarchical routing protocols, energy consumption is a key factor that affects the performance of routing protocols. As the

communication between CHs and the BS needs much more energy than common nodes, hence the amount of data to be transmitted to BS must be limited hence aggregation function is applied to data at CH before sending to BS. But in case of public key cryptography scheme, CH has to first of all decrypt all the data and then apply aggregation function to remove redundant data and it again encrypt the data before sending to BS. Hence a lot of energy is wasted in encrypting and decrypting data at CHs.

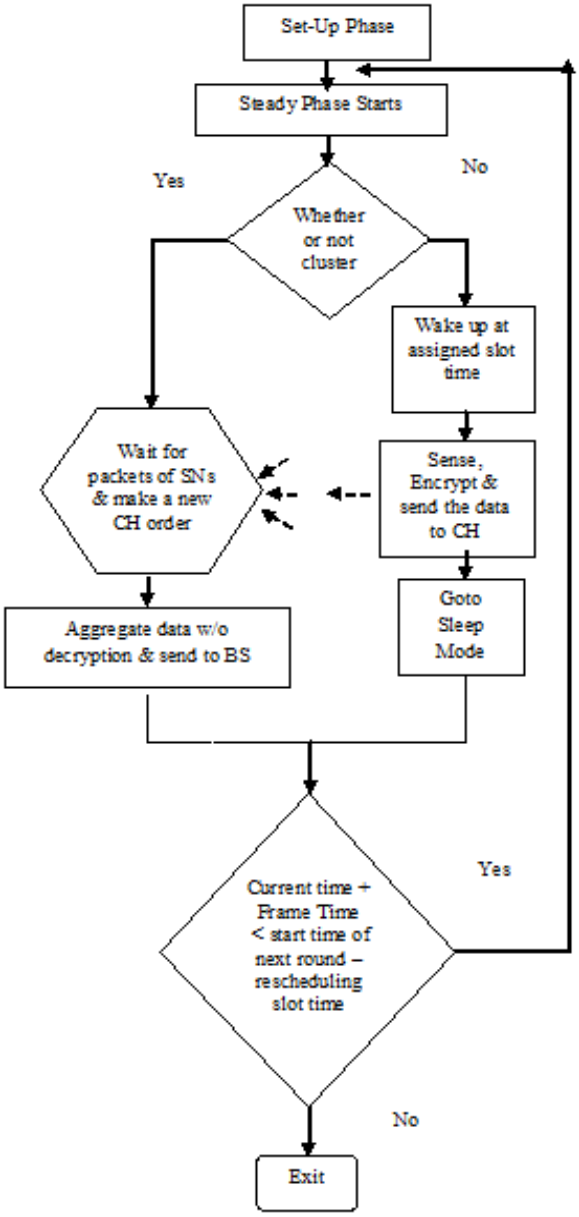

Figure 5: Flowchart Depicting Proposed Algorithm

Hence we implement homomorphic encryption in LEACH protocol to reduce energy consumption. Homomorphic encryption allows mathematical functions to be applied on data without the need to decrypt it. Hence with this encryption scheme CH will not need to decrypt data before applying aggregation function and hence no wastage of energy. LEACH_HE follows same Set-up phase as the simple LEACH.

The only difference lies in steady state phase of LEACH_HE. The nodes send the encrypted data to its respective CH. CH doesn't need to decrypt the data before applying aggregation function because of the homomorphic property to allow arithmetic operations on encrypted data. The proposed algorithm steps are depicted in figure 5.

A homomorphic encryption scheme consists of five algorithms:

- **Key Generation (KG):** The algorithm takes as an input a security parameter k and outputs a public and private key pair (P_k, S_k), where P_k is public, while S_k is kept secret.
- **Encryption(E):** The algorithm takes as input a plaintext m {0,1} and the public key P_k and output a ciphertext c, denoted as

  $c=E(m,P_k)$
- **Decryption (D):** The algorithm takes as input a ciphertext c and the private key S_k, and outputs a plaintext m ε {0,1}, denoted as

  $m=D(C, S_k)$
- **Homomorphic Addition (Add):** The algorithm takes as input two ciphertexts $c_1=E(m_1, P_k)$, $c_2=E(m_2, P_k)$, and the public key P_k, and outputs a ciphertext c, denoted as $C= Add(c_1,c_2,P_k)= c_1 \boxplus c_2$ such that

  $D(C, S_k) =m_1 \boxplus m_2$
- **Homomorphic Multiplication (Mult):** The algorithm takes as input two ciphertexts $c_1=E(m_1,P_k)$, $c_2=E(m_2, P_k)$, and the public key P_k, and outputs a ciphertext c, denoted as $C= Mult(c_1,c_2,P_k)= c_1 \oplus c_2$ such that

  $D(C, S_k) =m_1 \oplus m_2$

The steps of proposed algorithm:

Set-Up Phase

- CH ⟹ N: id_{CH} ,crc ,adv
- n_i ⟶ CH: id_{ni} , id_{CH} ,crc, join_req
- CH ⟹ N: id_{CH} ,(… ,(id_{ni} , T_{ni})…) , crc ,sched

Steady State Phase

- n_i ⟶ CH : id_{CH} ,c_i , crc

  Where,

  $c_i = E(m_i , P_k)$

  $(S_k , P_k) = KeyGen(\gamma)$
- CH ⟶ BS: id_{CH} , id_{BS}, FHE((…,c_i,….) , P_k), crc

  Where,

  FHE= Add (c_1, c2, Pk) or

  FHE= Mult(c_1,c_2,P_k)
- At Base Station after receiving data from all the cluster heads, base station decrypt the data to obtain the original data.

  $Dec(C, S_k) = m_i \lozenge m_{i+1}$

Where,

$C=c_i + c_{i+1}$ or $C= c_i * c_{i+1}$

$\lozenge$= + or *

The symbol used in proposed algorithm denotes:

CH, n_i, BS: Cluster Head, ordinary node, base station

N: Set of all nodes in the network

Adv,join_req,sched : String identifiers for message types

Crc : Cyclic redundancy check

m_i, c_i: plaintext , cipher text

γ : Security Parameter

id_{ni} , id_{CH} , id_{BS} : Nodes n_i ,CH, BS id's respectively

<y, T_y> : A node id y & its active slot T_y in the clusters TDMA schedule

⟶: Unicast transmission

⟹: Broadcast transmission

SIMULATION RESULTS

In this section we examine the performance of LEACH_HE through NS2 simulations. A network of 100 nodes is deployed in an area of 100m*100m with BS at (50,175). The main parameters of the simulation experiments are described in Table 1.

Table 1: Parameters Used in the Simulation Experiment

Parameter	Value
Simulation Time	500 Sec
No. of Nodes	100
BS location	(50, 175)
Numbers of CH	5
Maximum X-coordinate value	100 M
Maximum Y-Coordinate value	100 M
Initial node power	2 *J*
Traffic Type	CBR
MAC Protocol	802.11
Mobility Model	Random Waypoint
Routing Protocol	LEACH

In order to compare LEACH_HE protocol with LEACH, we use three performance metrics for the comparison: numbers of nodes alive, the consumption of the network's energy & the data amounts transmitted by the two different protocols. The simulation results are depicted in figure 6-8.

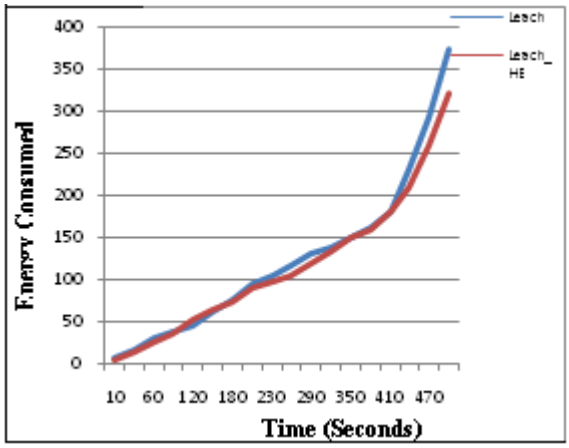

Figure 6: Energy Consumed vs. Time

Observed from the figure 6, LEACH_HE consumes somewhat equal energy as compared to LEACH. Since homomorphic encryption reduces the task of decryption at CHs hence no extra energy consumption and hence LEACH_HE consumes almost equal energy as consumed by LEACH.

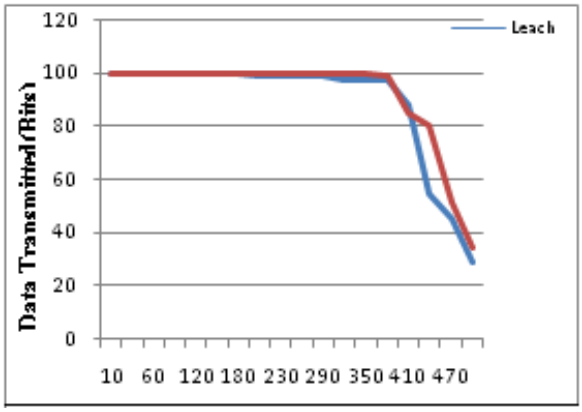

Figure 7: Data Transmitted (bits) vs. Time

The figure 7 shows that LEACH_HE transmits somewhat equal bits in each round as compared to LEACH. This clearly depicts that addition of homomorphic encryption in LEACH doesn't degrades its performance.

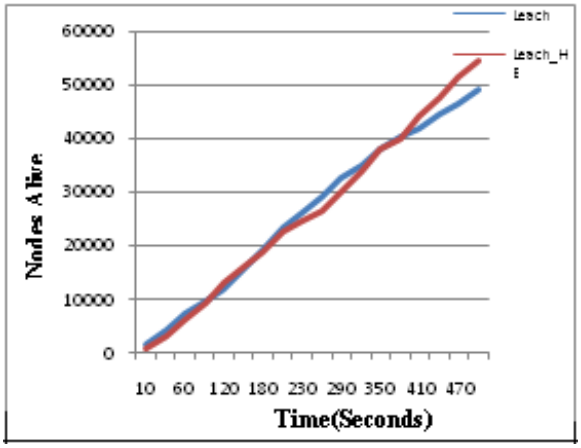

Figure 8: Nodes Alive vs. Time

The figure 8 shows that numbers of nodes alive in LEACH_HE are more as compared to LEACH initially but at the end of simulation time both have equal number of nodes alive. Hence it shows that LEACH_HE performance is similar to LEACH.

CONCLUSIONS & FUTURE WORK

In this paper, we have presented LEACH protocol with homomorphic encryption for providing confidentiality scheme to energy efficient LEACH protocol. Much of research in the area of public key cryptography is done and it shows that it is very energy consuming. This paper uses the power of homomorphic encryption to provide confidentiality to LEACH.

We have analyzed the behavior and different performance metrics for LEACH_HE and LEACH .Graphs of performance comparison in figure 5-7 shows that LEACH_HE consumes almost same energy as consumed by LEACH. Adding homomorphic encryption to LEACH does not reduce the network lifetime nor does it consume extra energy. LEACH_HE transmits almost same number of bits as compared to LEACH. Hence these performance parameters depicts that adding homomorphic encryption to LEACH donot degrades the performance.

Research in the area of LEACH protocol in WSN is still actively done. Due to the time constraint and code limitations the current work i.e. simulation of LEACH protocol with homomorphic encryption was only focused on evaluating some selected performance metrics. The evaluation of LEACH_HE discussed in this paper with some more performance metrics like throughput, average energy consumed, etc will be considered as future research work.

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. 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. 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
14. 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
15. Jafar Amiri, Masoud Sabaei, Bahman Soltaninasab: A New Energy Efficient Data Gathering Approach in Wireless Sensor Networks, Copyright © 2012 SciRes.

AUTHOR'S DETAILS

Er. Alisha Gupta (15 August 1989) received her B.TECH degree in Computer Science in 2011 with honours from Kurukshetra University, Kurukshetra, Haryana, India. She is currently pursuing M.TECH in Computer Science 2011-13 from Seth Jai Prakash Mukand Lal Institute of Technology, Kurukshetra University, Kurukshetra, Haryana India. She has published 1 research paper in International Journal. Her current research interest includes Wireless Sensor Networks, LEACH, NS2.

Er. Vivek Sharma (5 Jan 1981) received his B.Tech (CSE) & M.Tech (CSE) degrees from Kurukshetra University and achieved gold medal during his graduation. Presently he is working as Assistant Professor (HOD) in CSE department JMIT, Radaur, Yamunanagar India. He is a member of CSI (Computer Society of India). His area of interest is Mobile Networks. His publications include the field of Wi-Fi protocols, mobile sensor networks in health care.