Abstract— Encryption schemes that support operations over ciphertext are of utmost importance for wireless sensor networks & especially in LEACH protocol. Energy is salient limit of LEACH. 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_HMH in which confidentiality scheme i.e. homomorphic encryption and max-heap i.e. load balancing is added to LEACH protocol. In max-heap cluster head with maximum nodes is selected so that some of the nodes can be shifted to other cluster head’s to achieve load balancing and in homomorphic encryption data can be aggregated algebraically without decryption and hence energy consumption get reduced. Simulation results are obtained in terms of three metrics- amount of data transmitted, total energy consumed and number of nodes alive. It is observed that the performance of LEACH_HMH is somewhat better to LEACH_HE.

Keywords: Clustering, Homomorphic Encryption, maxheap, loadbalancing, LEACH_HMH, LEACH_HE, Wireless Sensor Network (WSN)

I. 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].

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.
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]:

1) 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.

2) 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.

3) 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.

A. 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.

LEACH protocol works in rounds. Each round is divided into two phases:
- Setup phase
- Steady phase

1) 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:

\[ T(n) = \frac{P}{1 - P(r \mod(1/p))} \quad n \in G \]

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
2) **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 (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]

**B. 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 $E(m_1),...,E(m_t)$ 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.

**C. Max Heap**

A max binary heap is an almost complete binary tree with keys and objects stored at the nodes, such that a node’s key is less than or equal to its parent’s. The name “heap” is appropriate: it is described a sort of spreading mound of objects. When the base station receives the packet, it will calculate $T-R-S$ (the difference between receiving timestamp and current time stamp). When the base station receives the packet, it will calculate $T-R-S$ (the difference between receiving timestamp and current time stamp).

If $\text{difference} \geq \text{remaining lifetime}$ of node, the node will become non-cluster head else If remaining lifetime $= \text{max}$ among all nodes of the cluster, choose the node as cluster head.

**II. 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 $\geq$ remaining lifetime of node**, the node will become non-cluster head else If remaining lifetime $= \text{max}$ 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 Nguyet 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

Alisha gupta & vivek sharma 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.

A.Babu Karuppiah, P.Suresh proposed an Energy Efficient Load Balanced Clustering Technique which is used to find energy efficiency as well as load balancing. Energy Efficient Load Balanced Clustering Technique is a min heap based Clustering algorithm. Efficiency of WSNs is measured by the total distance between nodes to the base station and data amount that has been transferred. Cluster–Head which is totally responsible for the creating cluster and cluster nodes may affect the performance of the cluster. The result show that the proposed algorithm is efficient in terms of load balancing, energy efficiency, and the number of sensor nodes that die during the network period.

III. PROPOSED WORK

In this paper we propose a protocol LEACH_HMH based on LEACH_HE protocol to balance the energy consumption as well as load balancing while providing confidentiality. The LEACH_HMH 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. Hence we implement homomorphic encryption and max-heap 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. Max-heap allows better cluster head management to achieve load balancing. LEACH_HMH follows same Set-up phase as the simple LEACH.

The only difference lies in steady state phase of LEACH_HMH.

1. 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.
2. Load balancing and energy efficient clustering, for the sensor networks with unpredictable loads of the sensor nodes by max heap

The proposed algorithm
Set-Up Phase

© 2014, IJARCSSE All Rights Reserved
1. CH $\rightarrow$ N: id$_{CH}$, crc, adv
2. n$_i$ $\rightarrow$ CH: id$_{ni}$, id$_{CH}$, crc, join_req
3. CH $\rightarrow$ N: id$_{CH}$, ($\ldots$, (id$_{ni}$, T$_{ni}$)$\ldots$), crc, sched

Steady State Phase

4. Call Max-Heap
   n$_i$ $\rightarrow$ CH : id$_{CH}$, c$_i$, crc
   Where,
   
   $c_i = E(m_i, P_k)$
   
   (S_k, P_k) = KeyGen(γ)

5. CH $\rightarrow$ BS : id$_{CH}$, id$_{BS}$, FHE(($\ldots$,c$_i$, $\ldots$), P_k), crc
   Where,
   
   FHE= Add(c$_i$, c$_{i+1}$, P_k) or
   FHE= Mult(c$_i$, c$_{i+1}$, P_k)

6. 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$_i$ $\diamondsuit$ m$_{i+1}$
   Where,
   
   C=c$_i$ + c$_{i+1}$ or C= c$_i$ $\ast$ c$_{i+1}$

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

$\leftarrow$, $\rightarrow$: Unicast, broadcast transmissions, respectively

IV. SIMULATION RESULTS

In this section we examine the performance of LEACH_HMH 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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>550 sec</td>
</tr>
<tr>
<td>BS location</td>
<td>(50,175)</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100</td>
</tr>
<tr>
<td>Numbers of CH</td>
<td>5</td>
</tr>
<tr>
<td>Maximum X-coordinate value</td>
<td>100M</td>
</tr>
<tr>
<td>Maximum Y-coordinate value</td>
<td>100M</td>
</tr>
<tr>
<td>Initial node power</td>
<td>2J</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>CBR</td>
</tr>
<tr>
<td>MAC protocol</td>
<td>802.11</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Waypoint</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>LEACH</td>
</tr>
</tbody>
</table>

In order to compare LEACH_HMH protocol with LEACH_HE, 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.

Fig. 6 Energy Consumed vs. Time
Observed from the figure 6, LEACH_HMH consumes less energy as compared to LEACH_HE. Since max-heap provides better load balancing so no extra energy is consumed and hence LEACH_HMH consumes less energy as consumed by LEACH_HE.

The figure 7 shows that data transmitted in LEACH_HMH is less as compared to LEACH_HE initially but after some time it increases rapidly. This clearly depicts that addition of max-heap in LEACH_HE increases its performance.

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

V. CONCLUSIONS & FUTURE WORK

In this paper, we have presented LEACH protocol with homomorphic encryption and max-heap for providing confidentiality and proper load balancing scheme to energy efficient LEACH protocol. Many times repeated research in the area of public key cryptography is done and it shows that it is very energy consuming. We have analyzed the behavior and different performance metrics for LEACH_HMH and LEACH_HE. Graphs of performance comparison in figure 6-7 shows that LEACH_HMH consumes less energy as consumed by LEACH_HE. LEACH_HMH transmits more number of bits as compared to LEACH_HE. Adding max-heap to LEACH_HE does not reduce the network lifetime nor does it consume extra energy. Hence these performance parameters depicts that adding max-heap to LEACH_HE increases the performance. Research in the area of LEACH protocol in WSN is still actively done. Due to the time constraint and code limitations the present work i.e. simulation of LEACH protocol with homomorphic encryption and max-heap was only focused on evaluating some selected performance metrics. The evaluation of LEACH_HMH discussed in this paper with some more performance metrics like average energy consumed, throughput etc will be considered as future research work.

REFERENCES

16. Alisha gupta & vivek sharma: implementation of leach protocol using homomorphic encryption (ijece) issn 2278-9944 vol. 2, issue 4, sep 2013, 63-74 © iaset