AggreLEACH: Enhance Privacy Preserving In Wireless Sensor Network

Jaydeep M Patel¹ Umang D Shukla² Mayank P Devani³
¹M.Tech Student ²,³Assistant Professor
¹,²,³Department of Information Technology
¹Ganpat University, Kherva, Mahesana, Gujarat, ²,³Sal College of Engineering, Ahmedabad, Gujarat, India

Abstract—Privacy preservation is an important issue in today's context of extreme penetration of internet and mobile technology. It is more important in the case of wireless sensor network where collected data often requires in network processing and collaborative computing. Security is always booming in wireless sensor network. Privacy preserving data aggregation emerged as an important concern in designing data aggregation algorithm. Encryption schemes that support operation over cipher text are of utmost for wireless sensor networks & especially in LEACH protocol. The salient limit of LEACH is energy. Due to this limitation, it seems important to design Confidentiality scheme for WSN so that sensing data can be transmitted to the receiver securely and efficiently and the energy consumed must be minimum hence we proposed AggreLEACH in which confidentiality scheme i.e. holomorphic encryption is added to LEACH protocol. In holomorphic encryption data can be aggregated without decryption and hence less energy consumption. The objective is to provide secure data transmission between sensor node and aggregator. Simulation result are obtain in terms of two metrics- total energy Consumed of node, lifetime of node. It is observed that the performance of AggreLEACH compare to LEACH. We have performed theoretical analysis as well as simulation to check the performance in terms of accuracy, complexity and security. Key Words: wireless sensor network, LEACH protocol, AggreLEACH.

I. INTRODUCTION

Wireless sensor network consists of spatially distributed autonomous sensors deployed randomly in a large scale. Usually these node have limited power, storage, communication and processing capabilities. WSN are ad-hoc network involve of tiny sensing devices. These devices are called sensor or mote. These devices are severely resource constrained with a typical sensor mote consisting of only 4-8MHz processor, 4-8 KB RAM, 128 KB flash memory and ideally 916MHz of radio frequency and 2 x AA batteries[1]. These sensor node deployed in physical and environment condition. The potential application of wireless sensor network typically range from those in defense military, environmental monitoring, health monitoring, home appliances, civilian societal surveillance application etc.[2]

A. Wireless Sensor Network Model

Unlike their ancestor ad-hoc networks, WSNs are resource limited they are deployed densely, they are prone to failures the number of nodes in WSNs is several orders higher than that of ad hoc networks. The major components of a typical sensor network are:

1) Sensor Field:
A sensor field can be considered as the area in which the nodes are placed.

   Sensor Nodes:
Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink.

2) Sink:
A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes[3]. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. Sinks are also known as data aggregation points.

3) Task Manager:
The task manager also known as base station is a centralized point of control within the network which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, A powerful data processing storage center and an access point for a human interface. The base station is either a laptop or a workstation. Data is streamed to these workstations either via the internet, wireless channels, satellite etc. Nodes can use wireless communication media such as infrared, radio, optical media or Bluetooth for their communications. The transmission range of the nodes varies according to the communication protocol is used.

Fig. 1: Illustration of WSN[2].

B. Routing Protocol of Wireless Sensor Network
Routing protocol is an important factor of affecting the energy consumption of sensor nodes. There are three routing protocol of wireless sensor network[5].

1) Flat Based Routing Protocol
In this routing protocol nodes play the same role and have similar functionality in transmitting and receiving data. In many application of WSNs due to lack of global identification along with random deployment of sensor nodes. It is hard to select 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[6]. This approach is called data centric routing.
2) Location-based protocols
In most cases location information is needed in order to calculate the distance between two particular nodes so that energy consumption can be estimated. Generally two techniques are used to find location one is to find the coordinate of the neighboring node and other is to use GPS

3) Hierarchical routing protocol
In this nodes will be assigned different roles in the network like cluster heads, members of cluster 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. Hierarchical-based routing protocols also known as cluster based routing protocols. In order to avoid redundancy hierarchical routing protocols are best. 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

C. LEACH
LEACH [7] is one of the most popular cluster-based routing protocols for WSNs. LEACH minimizes energy dissipation by dividing. WSNs into clusters to reduce the number of messages and restrict direct communication between micro-sensor nodes and the BS [7,9]. The data aggregation can exclude a lot of redundant data to decrease the communication load on the CH node. The CH node’s energy is rapidly exhausted because it has to process more work than other nodes. In order to overcome this problem, after being the cluster head for a certain time the CH node passes this role to another node to balance energy consumption between all nodes in the WSN. The member nodes in a cluster communicate with their CH node by single-hop and only the CH can forward aggregative data to the BS directly[4]. In order to avoid internal communication collisions. CH nodes use a time division multiple access (TDMA) schedule for members and the BS categorizes the CHs with a code division multiple access (CDMA) schedule [7].

Fig. 2: LEACH Routing Topology [6]

D. Homomorphic Encryption
- Partially Homomorphic Encryption: Homomorphism over a limited set of functions only
- Somewhat Homomorphic Encryption: Allow many operations at a time but only a limited number of times. Each has predefined error term and if it exceeds a certain tolerance, the result will be of no use
- Full Homomorphic Encryption: It allows any number of operations any number of times

II. RELATED WORK
A. Data Aggregation
Proposed data aggregation approaches based on routing protocols data aggregation is very crucial technique in wireless sensor network because with the help of data aggregation they reduce the energy consumption by eliminating redundancy and also enhance the lifetime of the network[2]. Aggregation process enhance the robustness and accuracy of information but this approach cluster head or aggregator node may be attacked by malicious attacker if cluster head is compromised then the base station cannot be ensure the correctness of the aggregate data that has been send to it. It reduce the compromised sensor source nodes or aggregator nodes from significantly altering the final aggregation value. Sensor node in a sensor network is easily to compromised. Compromised nodes have a capability to modify or discard messages. Method for securing data is hop by hop encryption. This method follows some step
  - Encryption process has to be done by sensing nodes in wireless sensor network
  - Decryption process has to be done by aggregator nodes
  - After that aggregator nodes aggregates the result and then encrypt the result again.
  - The sink nodes gets final aggregated result and decrypt it. This method is very time consuming and energy consuming technique because this type of method sensor node encrypt the data and send the aggregator. Aggregator decrypt the data and aggregate the all the sensor node data and after encrypt the aggregate data and send the data to sink node

B. LEACH_HE
Proposed algorithm in which confidentiality scheme. Homomorphic encryption is added to LEACH protocol[6]. In homomorphic encryption data can be aggregated algebraically without decryption and hence less energy consumption. 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.

C. ECDSA
Proposed elliptic Curve cryptography and digital signatures (ECDSA)[8] to provide integrity proposed two algorithms first to be implemented on sensor node and other one to be implemented to the base station. Proposed approach use homomorphic encryption ECOU(Elliptic Curve Okamoto Uchiyama) algorithm to achieve data confidentiality. This proposed algorithm would combine preeminent features of PKC based OU and ECDSA to give more efficient result. but this approach is very time consuming and energy consuming because this security technique take more time to decrypt the data

D. HCDA
Proposed Hierarchical Concealed Data Aggregation (HCDA) protocol which allows concealed aggregation of data that are encrypted with different keys[13]. HCDA protocol virtually
partitions the network into several regions and employs a different public key in each region. Due to the privacy homomorphic encryption scheme of HCDA. The data collected in a region can be encrypted using the public key of the region and the encrypted data of several regions can be hierarchically aggregated into a single piece of data without violating data confidentiality. Moreover during the decryption of aggregated data the base station is able to determine the origin of the data based on the encryption key. Particularly useful when the base station needs data from a certain region of the network. In order to use multiple keys in the network area HCDA protocol employs a group based network deployment scheme where sensor nodes in a group use the same public key. In addition as HCDA protocol is based on elliptic curve cryptography, it is not affected by node compromise attacks whereas symmetric key based concealed data aggregation protocols are significantly affected from these attacks.

E. M-LEACH
Proposed M-Leach with reduced network energy consumption as compared to LEACH[11]. 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

F. CPDA
Proposed cluster based private data aggregation algorithm to applying data mining technique to preserve the privacy content of data[9]. A scheme to provide privacy preservation in much simpler way with the help of secure key management scheme[10] and random data perturbation technique. In this scenario two or more parties owning confidential data need to share only for aggregation purpose to a third party without revealing the content of the data. In this approach they have k number of keys. Which is stored in every source node? Of that Kk keys are shared with the server/aggregator for source to aggregator secure communication and k number of keys are kept for source to source communication in this approaches secure key distribution method has two parts
- Aggregator to source key exchange
- Source to Source key exchange

In this approach outperforms of other protocols in terms of energy consumption, network lifetime and network throughput and normalized routing load.

III. PROBLEM IDENTIFICATION
Main problems are energy of sensor node, strategy for selection of cluster head, efficient cluster hand over mechanism, security of sensitive data, processing overhead at aggregator. LEACH provides lower energy consumption which is required to create and maintain cluster in order to improve the life time of Wireless sensor networks. But, there is no trustworthy environment in LEACH, for malicious nodes, the aggregated data and aggregation operation. Malicious sensors are close to legitimate sensors, so malicious sensors collect all readings from all sensors to calculate aggregated values to know their routing paths. LEACH consumes more energy to aggregate the wrong data which is send by malicious node. So, privacy is an issue.

IV. PROPOSED WORK
The goal of LEACH is provide lower energy consumption which is requiring creating and maintaining cluster in order to improve the life time of WSNs. There are two phase in our proposed scheme: data encryption phase and data aggregation phase. The encryption phase provides a lightweight encryption algorithm that supports data aggregation property, data secrecy and privacy for data transmission. The data aggregation phase provides a method to eliminate redundant reading from sensor mote without decrypting them. An aggregator cannot know anything about the plaintext so more power can be saved. Thus, we propose a protocol AggreLEACH based on LEACH protocol to save the energy consumption while providing confidentiality. The AggreLEACH 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 need much more energy than common nodes. Hence the amount of data to be transmitted to BS must be limited. So, aggregation function is needed to apply on data at CH before sending to BS. But in case of public key cryptography scheme, CH has all the decrypt data and then apply all aggregation function to remove redundant data and it again encrypt the data before sending to BS. Hence a lot of energy is wasted to encrypt and decrypt data at CHs. Hence we implement Paillier Cryptosystem scheme. This scheme is an additive homomorphic as well as multiplicative for constant values using LEACH protocol to reduce energy consumption. Here, I have mentioned Pseudo code and flowchart of my proposed scheme:

A. Pseudo code

a) if id = sender id
   i) call encryption() // asymmetric algorithm for public key cryptography
   ii) send (Encrypted_packet)

b) else if id = intermediate node
   i) call forward()

c) else if id = aggregator_id
   i) call decryption() /store packet in to database at regular interval do
      aggregation send into Base station

As per mentioned above Psuedocode and flowchart, Paillier homomorphic encryption allows mathematical functions on data without decryption in aggregator. With this encryption scheme, CH need not to decrypt data before applying aggregation function and, so there is no wastage of energy. AggreLEACH follows same set-up phase as the simple LEACH. The only difference lies in steady state phase of AggreLEACH. In steady phase the nodes send the encrypted data to its respective CH. CH doesn’t need to decrypt the data before applying aggregation function because the homomorphic property already allows arithmetic operations on encrypted data.
The proposed algorithm steps are depicted in figure 1. Paillier Cryptosystem developed by Pascal Paillier in 1999. This scheme is an additive homomorphic as well as multiplicative only for constant values. The Paillier Cryptosystem is a modular, public key encryption scheme. Paillier's work [12][13], shows that how to encrypt and decrypt messages using this cryptosystem. The concept of converting an alphanumeric message into a purely numeric message is to be broken into block in such that for each i, 0 < i < n, for a predetermined value, n. Also the term plaintext is be used to refer a message that is numeric but is not encrypted while the term cipher text will be used to refer to plaintexts.

B. Step of proposed AggreLEACH algorithm:

1) Set-Up Phase
- CH ==> N: id, , crc, adv
- \( n_i \) \( \rightarrow \) CH:id, , id, , crc, join_req
- CH ==>N: (...,( id, , T, )...), crc, sched

2) Steady State Phase
- \( n_i \) \( \rightarrow \) id, , C, , crc, where,
- \( C_i \equiv g^{m_i}i \times r_i^n \mod n^2 \)
- (... , ) = KG(3)
- CH \( \rightarrow \) BS: id, , id, , PE(......, , ...), ), crc, where,
- PE= \( g^{m_1} \times r_1^n \mod n^2 \times g^{m_2} \times r_2^n \mod n^2 \)
or
- PE= \( g^{k_1} \times k^n \)
- At base station after receiving data from all the cluster heads, base station decrypt Data to obtain the original data
- Dec(C, )= m, + m, mod n or
- Dec(C, )= m, k mod n where C= C, + C, ,

C. The following terms have used in proposed algorithm:
- CH , ni , BS : Cluster Head , ordinary node , Base Station
- N : Set of all nodes in network
- adv , join_req , sched : String identifier for message types
- Crc : Cyclic redundancy check
- plain Text ,cipher Text
- \( \mathcal{I} \) : Security Parameter.
- Nodes , CH , BS id's respectively
- \(<Y> : A node id y & its active slot in clusters

1) TDMA Schedule
---\( \rightarrow \): Unicast transmission
\( \Longrightarrow \): Broadcast transmission

V. RESULT AND ANALYSIS
We have examined the performance of AggreLEACH through Castalia simulations. We deployed different no of nodes in WSNs. WSNs nodes are deployed in area of 60m * 60m for the sink node no.55. The main parameters of the simulation experiments are describe table 1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time Limit</td>
<td>200 Sec</td>
</tr>
<tr>
<td>Sink Node</td>
<td>55</td>
</tr>
<tr>
<td>Maximum Sample Interval</td>
<td>2000</td>
</tr>
<tr>
<td>Minimum Sample Interval</td>
<td>200</td>
</tr>
<tr>
<td>Number of CH in percentage</td>
<td>5</td>
</tr>
<tr>
<td>Maximum X-coordinate value</td>
<td>60</td>
</tr>
<tr>
<td>Maximum Y-coordinate value</td>
<td>60</td>
</tr>
<tr>
<td>MAC protocol</td>
<td>Tunable MAC</td>
</tr>
<tr>
<td>Initial Energy</td>
<td>18720J</td>
</tr>
</tbody>
</table>

Table. 1: Parameter Used in the Simulation Experiment

In order to compare AggreLEACH protocol with LEACH, we have used four performance metrics for the comparison. Metrics are consumed energy, estimated network lifetime, estimated per node lifetime, remaining energy of nodes.

We have discussed about the performance of proposed AggreLEACH and LEACH algorithm. The results are shown in table 2.

<table>
<thead>
<tr>
<th>NODE</th>
<th>AggreLEACH Routing</th>
<th>LEACH Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>13.6421</td>
<td>13.9381</td>
</tr>
<tr>
<td>150</td>
<td>13.6626</td>
<td>13.9356</td>
</tr>
<tr>
<td>200</td>
<td>13.6799</td>
<td>13.9942</td>
</tr>
<tr>
<td>250</td>
<td>13.6602</td>
<td>13.9755</td>
</tr>
<tr>
<td>300</td>
<td>13.6904</td>
<td>13.9594</td>
</tr>
<tr>
<td>350</td>
<td>13.7044</td>
<td>13.9792</td>
</tr>
<tr>
<td>400</td>
<td>13.7244</td>
<td>13.9551</td>
</tr>
<tr>
<td>450</td>
<td>13.7062</td>
<td>13.9594</td>
</tr>
<tr>
<td>500</td>
<td>13.7562</td>
<td>13.9551</td>
</tr>
<tr>
<td>550</td>
<td>13.7162</td>
<td>13.9551</td>
</tr>
<tr>
<td>600</td>
<td>13.7424</td>
<td>13.9952</td>
</tr>
<tr>
<td>1000</td>
<td>13.8053</td>
<td>13.9381</td>
</tr>
</tbody>
</table>

Table. 2: Consumed Energy

Nodes in AggreLEACH have consumed less energy as compare to LEACH. In LEACH, there is no trustworthy environment in LEACH, for malicious nodes, the aggregated data and aggregation operation. Malicious sensors are close to legitimate sensors, so malicious sensors collect all readings from all sensors to calculate aggregated values to know their routing paths. LEACH consumes more energy to aggregate the wrong data which is send by malicious node and this wrong aggregated value send to base station so node consumed more energy in LEACH.
algorithm. So AggreLEACH provide better result compare to LEACH shown in figure 2.

Figure 4. Consumed Energy

In figure 4, the Y axis indicates the energy in joule and X axis represents the number of nodes. When we use paillier homomorphic encryption technique in LEACH, node consumed less energy and also provide confidentiality in WSNs. Shown in figure 4, AggreLEACH provide better result.

Now we discuss about the network life time of proposed AggreLEACH and LEACH algorithm. The results are shown in table 3.

Table 3: Estimated Network Lifetime

AggreLEACH routing protocol consumed less energy compare to LEACH routing protocol. So the network life time of AggreLEACH routing protocol is increase compare to LEACH routing protocol.

Table 4: Estimated Per node Lifetime

AggreLEACH routing protocol consume less energy. So, AggreLEACH is routing protocol that saves more energy. Compare to LEACH routing protocol. We compare LEACH protocol and AggreLEACH protocol for remaining energy shown in table 5.
AggreLEACH routing protocol have more remaining energy. Because they consume less energy and provide better result compare to LEACH.

VI. CONCLUSION & FUTURE WORK

We proposed a secure encrypted-data aggregation scheme for wireless sensor network. Our scheme has the following enhancements: (1) the aggregator does not need to decrypt it's received encrypted-data. Aggregator direct aggregate the encrypted data and send this aggregate data to BS. No power are wasted in data decryption, (2) the aggregator does not have decryption keys and therefore aggregator cannot know anything about data, and (3) use of random keys to encrypt data. We used homomorphic encryption in our proposed algorithm named AggreLEACH which increases the node & network lifetime and save energy. Thus, AggreLEACH give the better performance compare to LEACH.

Simulation of LEACH protocol with homomorphic encryption was only focus on some selected performance metrics. The AggreLEACH can enhance with some more performance metrics like throughput, data transmission rate.

REFERENCES