



Secure and Reliable Data Transmission Using Homomorphic Encryption in WSN

Priyanka Vasan*, Manjit Behniwal

CSE & Kurukshetra University
Haryana, India

Abstract— *The aim of this research is to achieve reliable data transmission in Leach protocol using fully homomorphic encryption in Wireless sensor network and show comparison of Leach without encryption, Leach with Reliable Scheme using Homomorphic Encryption and Leach with homomorphic encryption. In Wireless Sensor Network Energy, security and reliable data transmission is the main issue. The objective is to maintain integrity of data by providing reliable data transmission and maintain confidentiality of data using Homomorphic encryption.*

Keywords— *Wireless sensor network (WSN); Leach protocol; Reliable data Transmission; Confidentiality.*

I. INTRODUCTION

A Wireless sensor network is composed of tens to thousands of sensor nodes which are densely deployed in a sensor field and have the capability to collect data and route data back to base station. Wireless Sensor Network is used in many application now a days, such as detecting and tracking troops, tanks on a battlefield, measuring traffic flow on roads, measuring humidity and other factors in fields, tracking personnel in buildings. Sensor nodes consist of sensing unit, processing unit, and power unit.

II. ROUTING

Routing in WSN is a challenging task as it is very different from wireless ad hoc network and cellular network as:

1. Sensor nodes are densely deployed.
2. Sensor nodes have limited memory and power resources.
3. The topology changes due to failures or mobility.

Routing protocols in wireless sensor network are divided in to 3 main groups:-

1. Flat-based routing protocol
2. Hierarchical routing protocol
3. Location based routing protocol.

In Flat-based routing, all nodes are assigned equal roles or functionality. In Hierarchical-based routing, nodes will play different roles in the network like cluster members, cluster heads. In location-based routing, sensor nodes positions are estimated to route data in the network.

A. HIERARCHICAL ROUTING PROTOCOL

A Wireless sensor network is composed of tens to thousands of sensor nodes which are densely deployed in a sensor field and have the capability to collect data and route data back to base station. Wireless Sensor Network is used in many application now a days, such as detecting and tracking troops, tanks on a battlefield, measuring traffic flow on roads, measuring humidity and other factors in fields, tracking personnel in buildings. Sensor nodes consist of sensing unit, processing unit, and power unit.

III. LEACH

LEACH stand for Low-Energy Adaptive Clustering Hierarchy and LEACH was one of the first hierarchical protocols. In this the sensor nodes will be organizing themselves into clusters, with one of the nodes acting as the cluster head. Leach uses rotation of cluster heads to evenly distribute the energy load among the sensors in the network. The node chooses a the number is less than the following

$$T(n) = \begin{cases} \frac{P}{1 - P^{*(r \bmod \frac{1}{P})}} & \text{if } n \in G \\ 0 & \text{Otherwise} \end{cases}$$

Here, not only the cluster heads have the responsibility of collecting data from their clusters, but also to aggregate the collected data for reducing the amount of messages to be sent to the BS, which results in less energy dissipation, to enhance the network life time. The operation of LEACH is done into two phases.

1. Setup phase.
2. Steady State phase

In setup phase the clusters are organized and CHs are selected. Cluster heads change randomly over time in order to balance the energy dissipation of nodes. This decision is made by the node choosing a random number between 0 and 1. In steady state phase data transmission begins Nodes send their data during their allocated TDMA slot to the CH. This transmission uses a minimal amount of energy. The radio of each non-CH node can be turned off until the nodes allocated TDMA slot, thus minimizing energy dissipation in these nodes.

IV. HOMOMORPHIC ENCRYPTION

A Homomorphic encryption scheme allows arithmetic operations on ciphertexts, multiplicatively homomorphic scheme, where the decryption of the efficient manipulation of two ciphertexts yields the multiplication of the two corresponding plaintexts. Homomorphic encryption schemes are especially useful whenever some party not having the decryption key(s) needs to perform arithmetic operations on a set of ciphertexts. In cluster head mode, a node gathers data from the other nodes within its cluster, performs data fusion, and routes the data to the base station through other cluster head nodes.

V. PROBLEM STATEMENT

Like most routing protocols for WSNs, LEACH is vulnerable to a number of security attacks, including jamming, spoofing, replay, etc. 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 an intruder manages to become a CH, it can stage attacks such as sinkhole and selective forwarding, thus disrupting the workings of the network. Of course, the intruder may leave the routing alone, and try to inject bogus sensor data into the network, one way or another.

Adding security to LEACH-like protocols is challenging, as its dynamic and periodic rearranging of the network's clustering (and changing links) makes Key distribution solutions that provide long-lasting node-to-node trust relationships (to be sure, provided by most existing solutions) inadequate. There are a number of KD schemes in the security literature, most of which are ill-suited to WSNs: public key based distribution, because of its processing requirements; global keying, because of its security vulnerabilities; complete pair wise keying, because of its memory requirements; and those based on a key distribution centre, because of its inefficiency and energy consumption.

In previous work done no reliable data transmission was provided and integrity of data was not maintained in Leach .We need to add security to Leach without increasing the energy consumption and provide confidentiality of data.

VI. PROPOSED WORK

In this we introduce a reliable Data Transmission Scheme using homomorphic encryption known as Leach_RS in which Integrity of data is maintained. Leach_RS is compared with other protocols known as simple Leach and Leach with homomorphic encryption (Leach_HE). Data transmission by individual nodes is also studied which was not studied in the previous work.

VII. SIMULATION RESULTS

In this we examine the performance of Leach_RS through NS2 simulations. The main parameters of simulation are described in Table1.

TABLE I
PARAMETERS USED IN SIMULATION EXPERIMENT

Parameter	Value
Simulation Time	500 Sec
No. of Nodes	100
BS location	(50, 175)
Numbers of CH	5
Maximum X-coordinate value	1000 M
Maximum Y-Coordinate value	1000 M
Initial node power	2 J
Traffic Type	CBR
MAC Protocol	802.11
Mobility Model	Random Waypoint
Routing Protocol	LEACH

Performance metrics are used to compare the results of Leach_RS with other two protocols known as simple Leach and Leach with homomorphic encryption. Along with this performance metric for data transmitted by individual nodes for simulation time 100 sec for Leach_RS is also shown.

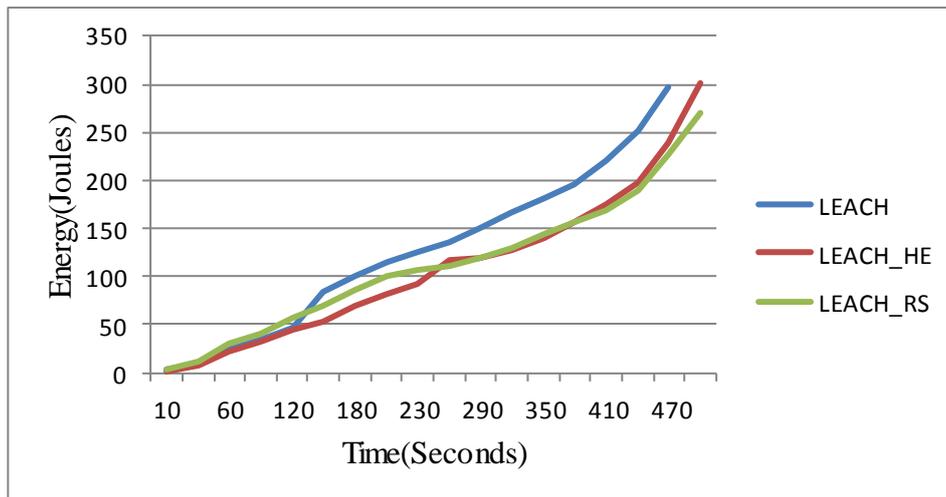


Fig.1 Energy consumed vs. Time

The graph above shows that energy consumed by Leach_RS is almost equal to energy consumed by simple Leach, in simple Leach no encryption and decryption is done but in Leach_RS homomorphic encryption is done which reduces the task of decryption at CHs hence no extra energy is consumed and hence LEACH_RS consumes almost equal energy as consumed by simple LEACH.

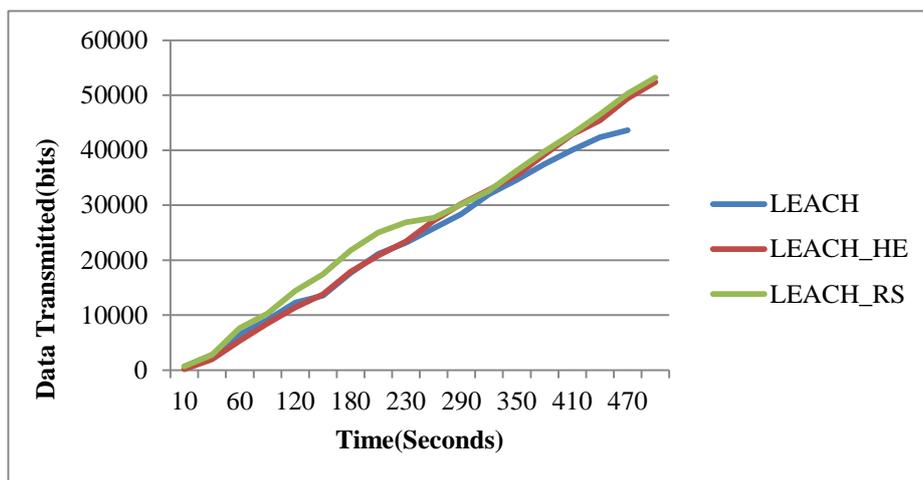


Fig. 2 Data Transmitted (bits) vs Time

The results shown above shows that the data transmitted by Leach_RS is almost equal to Leach_HE , and better than simple Leach , Leach_RS donot degrade the performance as Homomorphic encryption was introduced in it.

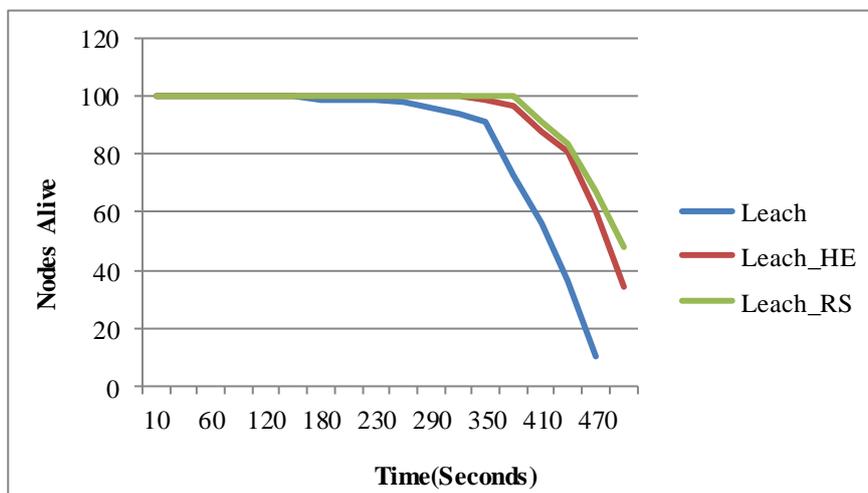


Fig. 3 Nodes Alive vs. Time

The graph above shows that greater the nodes alive better is the network lifetime, in the starting simulation time Leach_HE and Leach_RS have more nodes alive as the simulation time increases nodes alive of Leach_RS are more as compared to other two Leach Protocols.

The Graph below shows data transmitted by individual nodes which is beneficial in maintaining the data integrity and providing reliable data transmission. Similarly for all other 99 nodes the data transmitted can be plotted and any loss of data can be detected.

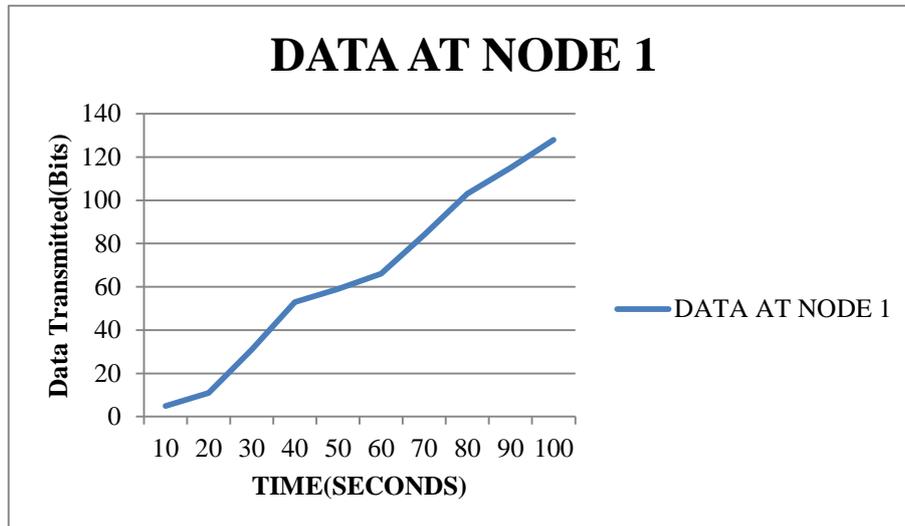


Fig. 4 Data Transmitted by Node 1

VIII. RELATED STUDY

Nazia Majadi[1] proposed an approach to describes a technique that is Uniform Distribution Technique (UDT) for selecting CHs and their corresponding clusters. The original Leach cannot select CHs uniformly Therefore there is the possibility that the elected CHs will be concentrated in certain area of the network. Hence, some nodes will not have any CHs in their vicinity. The proposed approach is in which each sensor node remains inside the transmission range of CHs and therefore, the lifetime of the network is prolonged.

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 the current time stamp).
- If difference \geq 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.

S. Poornima and B.B.Amberker [3] 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 [4] 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.

Alisha Gupta and Vivek Sharma [7] 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.

IX. CONCLUSION

In this paper Leach with homomorphic encryption is proposed. In Wireless sensor network it is found that energy, reliable data transmission and security are the main issues. In this paper reliable data transmission of individual nodes was checked and integrity of data was maintained and evaluation of proposed Leach is done on following metrics Energy consumed , Data transmitted and Number of alive nodes.

The graphs in figure 1-3 tell us about the energy consumed, data transmitted and number of alive nodes. Energy consumed by Leach_RS is almost same as Leach which means adding homomorphic encryption donot degrade the performance but maintains confidentiality of data. The graph in figure 4 tells us about individual data transmission of node 1 which is beneficial in maintaining the integrity of data similarly for all other nodes data transmission can be studied.

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] A. S. Poornima and B. B. Amberker. SEEDA: Secure End-to-End Data Aggregation in Wireless Sensor Networks: IEEE 2010
- [4] Mona El_Saadawy, et al.Enhancing S-LEACH Security for Wireless Sensor Networks: IEEE 2012.
- [5] Meenakshi Diwakar and Sushil Kumar. Energy Efficient Level Based Clustering Routing Protocol For Wireless Sensor Networks: IJASSN, Vol 2, No.2, April 2012.
- [6] Mr. Navneet Verma, Mr.S.C. Gupta and Ms. Pooja Sethi. Secure and Energy Efficient Routing for Hierarchical WSNs: IJETTCS, Vol 1, Issue 3, Sep-Oct 2012.
- [7] Alisha Gupta and Vivek Sharma. Implementation of Leach Protocol using homomorphic encryption: IJEEE, Vol.2, Issue 4 Sep 2013.
- [8] Fuzhe Zhao, You Xu and Ru Li. Improved LEACH Routing Communication Protocol for a Wireless Sensor Network: International Journal of Distributed Sensor Network, Vol 2012, Nov 2012.
- [9] 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.
- [10] Lianshan Yan and Wei Pan,. Modified Energy-Efficient Protocol for Wireless Sensor Networks in the Presence of Distributed Optical Fiber Sensor Link: IEEE SENSORS JOURNAL, VOL. 11, NO. 9, SEPTEMBER 2011.
- [11] Baiping Li1 and Xiaoqin Zhang, "Research and Improvement of LEACH Protocol for Wireless Sensor Network," 2012 International Conference on Information Engineering, Vol.25
- [12] Abderrahim Beni Hssane, Moulay Lahcen, "Position-Based Clustering: An Energy-Efficient Clustering Hierarchy for Heterogeneous Wireless Sensor Networks," (IJCSSE) Vol. 02, No. 09, 201
- [13] Mortaza Fahimi Khaton Abad , Mohammad Ali Jabraeil Jamali, "Modify LEACH Algorithm for Wireless Sensor Network," IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011
- [14] Wendi B. Heinzelman ,Anantha P. Chandrakasan and Hari Balakrishnan,"An Application-Specific Protocol Architecture for Wireless Microsensor Networks" IEEE Transactions On Wireless Communications, Vol. 1, No. 4, October 2002
- [15] Xiaohua (Edward) Li" Application of STBC-Encoded Cooperative Transmissions in Wireless Sensor Networks" IEEE SIGNAL PROCESSING LETTERS, VOL. 12, NO. 2, FEBRUARY 2005