Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 5, May -2015

Reduce Energy Consumption in Data Aggregation Using Homomorphic Technique in Wireless Sensor Network

Deviyani N. Patel, Prof. Parimal Patel

Student, Computer Science & Engineering Department, S.P.B Patel Engineering collage, Mehsana, India
Prof; Department of Computer Science & Engineering,S.P.B Patel Engineering collage, Mehsana, India

Abstract—*In the wireless sensor network data aggregation is used for solve the energy constrain Problem of sensor node. The main aim of this paper is reduce the energy consumption and provide the Security from the malicious node in the WSN. In the proposed scheme we will use data aggregation and homomorphic technique with paillier cryptosystem using this technique there is no need to encryption operation at the aggregator node so that privacy is provided and also energy consumption is decrease.*

Keywords— *Wireless sensor network; LEACH; Data aggregation; Homomorphic encryption technique; paillier cryptosystem.*

I. INTRODUCTION

The Wireless Sensor Network is Adhoc Network, Which is consisting of Small Sensor Node. In the Wireless Sensor Network multiple sensor nodes is Deployed Randomly. This sensor node is also called Mote. A typical Sensor Node Processor is of 4-8 MHz, having 4-8 KB RAM , 128 KB Flash Memory and Ideally 916 MHz of radio Frequency And 2 x AA Batteries [6]. The application of wireless sensor network is Health Monitoring, military survival, Building Monitoring etc. Wireless Sensor Network is special kind of Adhoc Network which includes a Sink, cluster head Node and the Sensor Node [5, 7]

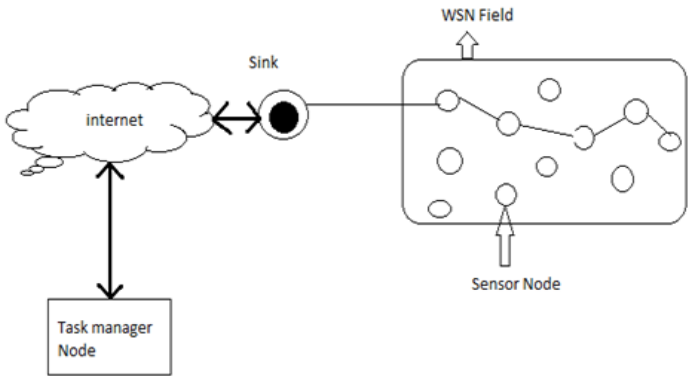


Figure 1. Illustration of WSN [12]

II. DATA AGGREGRATION IN WSN:

In wireless sensor network data aggregation is used for enhance the lifetime of network [8]. Aggregation approach can be applied along the path from sensor to sink [7]. So that carried information contain confidential data. Data aggregation is happened by four approaches [8].

- Tree based.
- Cluster Based
- Multipath approach
- Hybrid

Figure 2: Interaction between WSN security and data aggregation process [9].

III. HOMOMORPHIC TECHNIQUE:

In WSN, data is sense by various nodes and data can be transmitted to receiver securely and efficiently and at the same time energy consumed must be minimum. So that homomorphic technique is used. In the homomorphic technique encryption data can be aggregated algebraically without decryption so that less energy is consumption [1]. Homomorphic encryption makes it possible to give user a way to perform some operation on encrypted data without decryption Key [6]. Homomorphic Encryption scheme allow aggregation on cipher text. One of the example is a multiplicative homomorphic scheme, where the decryption of the efficient manipulation of two cipher text yield the multiplication of the two corresponding plaintext.

IV. LEACH PROTOCOL:

Low energy adaptive clustering hierarchy (LEACH) is a clustering based routing protocol in which it is decrease the energy consumption and enhances the network's lifetime. For the Sensor network, Main objective of LEACH is to provide a data aggregation operation which is used for the reduce the data transmission. LEACH is divide into round and each round is divide into two phase[10].

The Set up phase

The set up phase divide into three steps.

Step 1: cluster-head selection

In this step, each sensor node select a one random number between the [0, 1] interval. After choosing the random number compare it with a threshold value p(t)n. if that random number is less than threshold value p(t)n then that Member Node will Become a Cluster head node for the current round.

After Select a CH node, CH node broadcast a HEAD adv_MSG to other member node.

Step 2: Cluster Formation

After receive the HEAD adv_MSG from the CH, each member node send the Join_clu_msg to CH node which Contain Node's id and CH's id.

Step 3: Schedule CDMA and TDMA

After two Steps, Network is organized into the cluster. After this each CH node create a TDMA time slot for each member node into the cluster. Each CH also selects CDMA Code which is used for sending the data to the BS.

The Steady phase

In this phase, each member Node send Data to the CH during their time slots. After receive the data from the member sensor node, CH aggregate the Data and send to the base station.

V. LITRETURE SURVEY ON RELATED RESEARCH PAPER

Paper 1: "Implementation of LEACH Protocol using Homomorphic Encryption"[1]
Protocol: **LEACH-HE**

Summary: In this, the proposed algorithm based on confidential scheme in which added the homomorphic encryption scheme in the LEACH protocol. Homomorphic encryption scheme allow property of mathematical function for aggregate the data without encryption so that less energy consumed.

Paper 2: "Energy Efficiency in the Wireless Sensor Network using Cluster Allocation and Routing Algorithm"[2]
Protocol: **M-LEACH (Multi hop-LEACH)**

Summary: In this proposed algorithm based on cluster allocation and routing algorithm with different LEACH algorithms. It is uses multi hop in the LEACH for transmission and deploys the denser nodes near to the BS. In this each CH will be transmitting the collected data to its nearest neighbor CH and then CH send data to BS. so efficiency of energy is improved.

Paper 3: "A Novel approach for secure data aggregation in Wireless sensor network"[3]
Protocol: **ECDSA-OU**

Summary: In this Scheme Elliptic curve cryptographic and digital signature to provide integrity first to implemented on the sensor node and other one to be implemented to the BS. Proposed system use homomorphic encryption EC- OU(Elliptic Curve Okamoto Uchiyama) algorithm to achieve data confidentiality.

Paper 4: "An Energy Efficient scheme for Mobile Wireless sensor network"[4]
Protocol: **M-LEACH**

Summary: In this the proposed protocol improves the network energy consumption compare to the LEACH. Using this it is support the movements of the nodes without degrade the performance.

Paper 5: "A Routing protocol for prolonging lifetime of
Wireless Sensor network"[4]
Protocol: **U-LEACH**

Summary: In this the proposed algorithm use uniform distribution technique(UDT) for selecting CH and their corresponding cluster. By using this protocol all node will remain inside the transmission range of CHs. so lifetime is prolonged compare to the LEACH protocol.

VI. PROPOSED DESIGN

In proposed scheme there are two phase: data aggregation which is providing a method for eliminate the redundant data at aggregator and other is data encryption phase which is providing lightweight algorithm which support data aggregation property, data privacy for data transmission.

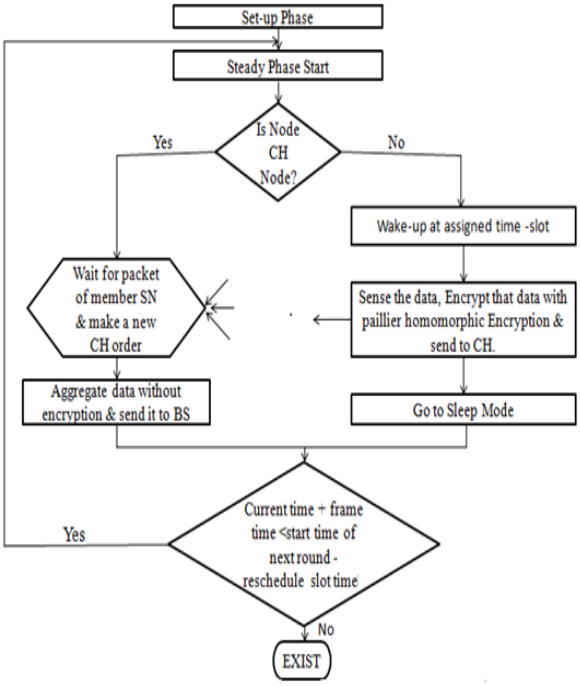


Figure 3: Framework of proposed scheme.

Algorithm:

- **Set-Up Phase**
  - CH ==> N: id_{ch}, crc ,adv
  - n_i ⟶ CH:id_{ni}, id_{ch} , crc, join_req
  - CH ==>N:(....,(id_{ni},T_{ni})....) , crc, sched

- **Steady State Phase**
  - n_i ⟶ id_{ch} , C_i , crc
    Where $C_i \equiv g^{m_i} * r_i^n \mod n^2$
    $(S_k , P_k) = KG(\exists)$
  - CH⟶BS: id_{ch},id_{BS},PE(.....,C_i,....) , P_k) , crc
    Where ,
    PE= $g^{m_1} * r_1^n \mod n^2 * g^{m_2} * r_2^n \mod n^2$ or
    PE= $(g^m * r^n)^k$
  - 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)= $m_i + m_{i+1} \mod n$ or
Dec(C, S_k)= m_i*k mod n
Where C= $C_i * C_{i+1}$
The following terms have used in proposed algorithm:

CH, n, 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
mi, ci: plain Text, cipher Text
∃: Security Parameter.
$idni$, $idCH$, $idBS$: Nodes n, CH , BS id's respectively
<Y, Ty>: A node id y & its active slot T in clusters TDMA Schedule
-->: Unicast transmission

==>: Broadcast transmission

VII. SIMULATION RESULTS

The main parameter of simulation experiment are describe table 1.

Parameter	Value
Simulation Time Limit	200 sec
Sink Node	55
Maximum Sample Interval	2000
Minimum Sample Interval	200
Number of CH in percentage	5
Maximum X-coordinate value	60
Maximum Y-coordinate Value	60
Mac protocol	Tunable MAC
Initial Energy	18720J

Table 1: Parameter used in simulation experiment

There are four parameter in my proposed scheme: consumed energy, estimated network lifetime, estimated node lifetime, remaining energy.

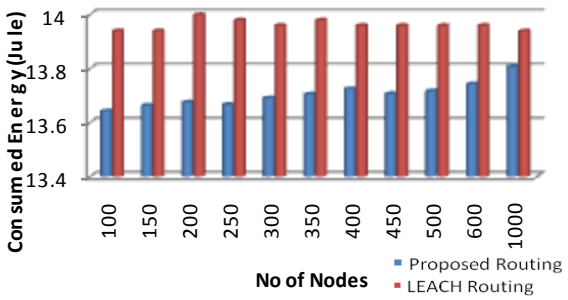


Figure 4: Consumed Energy

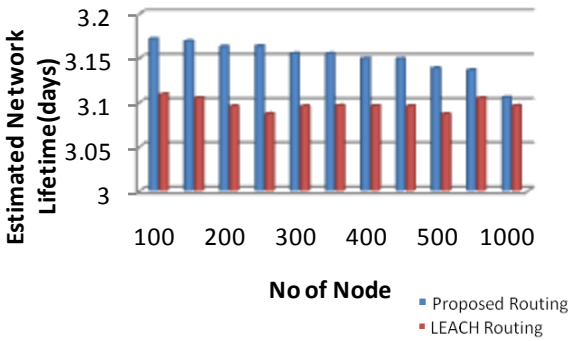


Figure 5: Estimated Network Lifetime

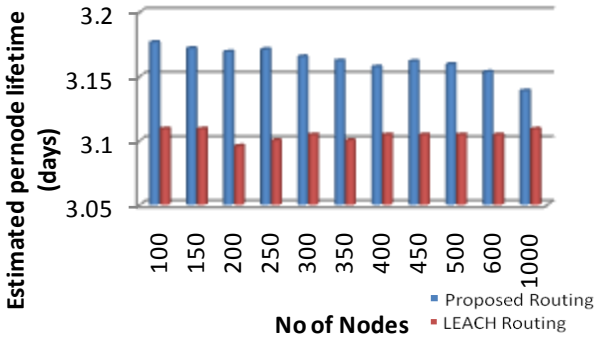
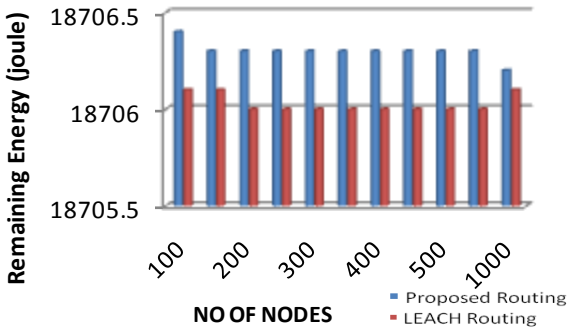


Figure 6: Estimated per node Lifetime



VIII. CONCLUSION

I have studied several related research paper and I found some problem in the Wireless sensor network. In the WSN, data collecting and Transmitting is most important Operation and is main cause of energy consumption. LEACH protocol is used for decrease the energy consumption but LEACH does not provide trustworthy environment for the malicious node, the aggregated operation and aggregated data. Also LEACH consumes more energy to aggregate the wrong data which is send by the malicious node. Hence there is privacy is needed. So that there is needed to develop new protocol in which data is forwarded in confidential way with minimum energy consumption and no need to encryption at CH node .so homomorphic encryption with paillier cryptosystem technique is solution for this problem.

REFERENCES

[1] Alisha Gupta and Vivek Sharma. "*Implementation Of LEACH Protocol Using Homomorphic Encryption*". IJEEE, ISSN 2278-9944, Vol.2, Issue 4, Sep 2013, pp.63-74.

[2] M.Vivek Kumar, R.Maheshwar, P. Jayarajan and f.Nathirulla Sheriff. "Energy efficiency in WSNS using cluster allocation and routing algorithm."ICIIIOSP-2013, pp.12-15.

[3] Vivaksha Jariwala and Devesh Jinvala. "A Novel Approach for Secure data aggregation in wireless Sensor Network". 10th National Workshop on Cryptology Department of Mathematics and Computer application. PSG College of technology, peelamedu, Coimbatore, September 2-4, 2010.

[4] Lan Tien Ngu yen, Xavier Defago, Razvan Beuran, and Yoichi Shinoda. "An Energy Efficient Scheme For Mobile Wireless Sensor Networks" IEEE ISWCCS, 2008.

[5] Nazia Majadi. "U-LEACH: A Routing Protocol for Prolonging Lifetime of Wireless Sensor Networks". IJERA, ISSN 2248-9622, Vol.2, Issue 4, July-August 2012, pp.1649-1652.

[6] Navneet Verma, S.C.Gupta, and Pooja Sethi." Secure and Energy Efficient Routing For Hierarchical WSNs". IJETTCS, ISSN 2278-6856, Vol.1, Issue 3, Sep-Oct 2012, pp.51-54.

[7] Jacques M.Bahi, Christophe Guyeux, and Abdallah Makhoul. "*Secure Data Aggregation in WSNs Homomorphism versus Watermarking Approach*". ADHOCNET, 2nd Int. Conf. on Ad-hoc Networks, Canada , 2010.
[8]Kiran Maraiya, Kamal Kant, and Nitin Gupta. "*Wireless Sensor Network: A Review on Data Aggregation"*. IJSCR, ISSN 2229-5518, Vol.2, Issue 4, April-2011.
[9] Suat Ozdemir, and Yan g Xiao. "Hierarchical Concealed Data Aggregation for Wireless Sensor Networks". In: Proceeding of the Embedded Systems an Communications Security Workshop in conjunction with IEEE SRDS, 2009.
[10] Nguyen Duy Tan, Longzhe Han, Nguyen Dinh Viet, and Minho Jo "An Improved LEACH Routing Protocol for Energy-Efficiency of Wireless Sensor Networks." smart Computing Review, Vol.2, Issue 5, October 2012, pp.360-369.

