Enhancement of Energy in Data Aggregation using Homomorphic Technique in Wireless Sensor Network

Deviyani N. Patel[1] Prof. Parimal Patel[2]
[1]Student [2]Professor
[1,2]Department of Computer Science & Engineering
[1,2]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.

Key words: 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 [4]. 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 [11, 5]

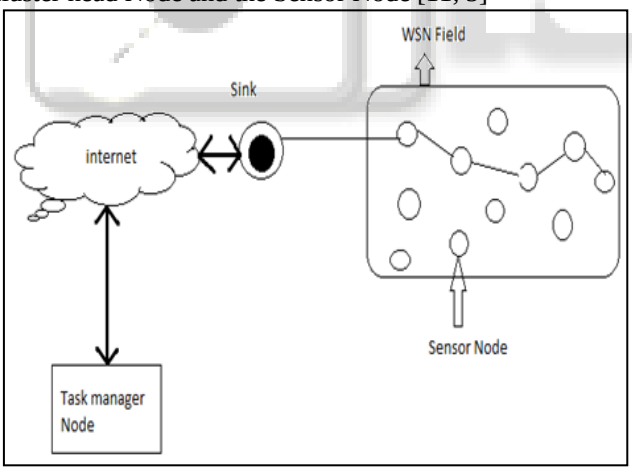

Fig. 1: Illustration of WSN [12]

II. DATA AGGREGRATION IN WSN

In wireless sensor network data aggregation is used for enhance the lifetime of network [12]. Aggregation approach can be applied along the path from sensor to sink [11]. So that carried information contain confidential data. Data aggregation is happened by four approaches [12].

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

Fig. 2: Interaction between WSN security and data aggregation process [13].

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 [10]. Homomorphic encryption makes it possible to give user a way to perform some operation on encrypted data without decryption Key [4]. 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 dividing into round and each round is dividing into two phase [8].

A. 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 Pt(n). if that

random number is less than threshold value Pt(n) then that Member Node will Become a Cluster head node for the current round.

$$P_t(n) = \begin{cases} \dfrac{k}{1 - k(r \bmod \frac{1}{k})} & ,if\ n \in G_t(n) \\ 0 & otherwise \end{cases}$$

Where, k is the probability value of candidate node who wants to Cluster head.
r indicate current round in the network
Gt(n) is a set of nodes
Pt(n) is a threshold probability Value
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.

B. 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. LITERATURE SURVEY ON RELATED RESEARCH PAPER

NO	DEFINATION	ALGORITHAM, TECHNIQUE, PROTOCOL	CONCLUSION
1	"A secure enhanced data aggregation based on ECC in WSNS"[1]	Approach: SEDA-ECC Technique: Homomorphic encryption	Result show that SEDA-ECC can achieve highest security level on the aggregated result comparing with other asymmetric schemes and it is efficient with respect to reasonable energy cost.
2	"Secure and Energy Efficient Data aggregation With Malicious aggregation Identification in WSN"[2]	Technique: Homomorphic Protocol: MAI	Ensure that BS does not accept the forged aggregation Result And none of the tried to find that node which inject the bogus aggregation result into the network
3	"Energy efficiency in WSNS using cluster allocation and routing algorithm." [3]	Technique: Clustering. Protocol: Multi-hop communication (M-LEACH).	In this paper result show that residual energy of WSNS is much improved by using multi-hop in LEACH compared to direct transmission hence by deploying sensor nodes near to the base station improved the energy efficiency much more than general multi hop LEACH.
4	"Secure & Energy Efficient Routing For Hierarchical WSNS"[4]	Protocol : LEACH - C Technique: Homomorphic Encryption	Protocol, which can have a significant impact on the over all Reliability & Energy Dissipation of their Network
5	"U-LEACH: A routing protocol for prolonging lifetime of WSNS."[5]	Technique: Clustering. Protocol: U-LEACH	LEACH Protocol is failed in some condition where high energetic nodes are concentrated and some node having high probable to remain outside of any CHS victiny will die with short term period so rotation of CH and metric of residual energy is not sufficient to balance energy consumption. This is solve by U-LEACH. Also increase nodes lifetime.
6	"Privacy Preserving data aggregation In WSNS" [6]	Protocol: CPDA	This scheme is basically part of SMC concept. It is focus on efficiency and compare with the existing scheme.
7	"Hierarchical Conceal data aggregation for WSNS"[7]	Protocol: HCDA	This scheme is allow the aggregation of data packet which are encrypted with different keys and therefore increase data aggregation efficiency without compromising security.
8	"An improved LEACH routing protocol for energy efficiency of WSNs" [8]	Protocol : LEACH - DE	Using this protocol, this considers the residual energy & geometric distance between Candidate Nodes & the BS to select CH nodes. CH is closer to the BS

			will Consume the less energy than other nodes because communication of data consumes the most energy in WSNS
9	"An energy efficient routing scheme for mobile wireless sensor networks." [9]	Technique: Clustering. Protocol: M-LEACH	This paper present an energy efficient sensor network clustering algorithm based on LEACH with mobility aware.
10	"Implementation of LEACH protocol using Homomorphic encryption." [10]	Technique: Clustering, Homomorphic Encryption. Protocol: LEACH_HE.	Using LEACH_HE which consumes almost same energy as consumed by LEACH. LEACH _HE transmit almost same no. Of bit as compared to LEACH. Hence, it is so that adding Homomorphic encryption to LEACH does not degrade the performance.

VI. 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 are privacy is needed. So that there are 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] Qiang Zhou, Geng Yang and Liwen He. "A secure enhanced data aggregation based on ECC in WSNS" ISSN 1424-8220, Issue 11 April 2014, pp.6701-6721.
[2] Hongjuan Li, Keqiu Li, Wenyu Qu, Ivan Stojmenovic."Secure and Energy Efficient Data aggregation With Malicious aggregation Identification in WSN" Science Direct 108-116, 2014.
[3] 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
[4] 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.
[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] Arjit Ukil "Privacy Preserving Data Aggregation In Wireless Sensor Network" IEEE ICW/CMC, 2010.
[7] 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.
[8] 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.
[9] Lan Tien Ngu yen, Xavier Defago, Razvan Beuran, and Yoichi Shinoda. "An Energy Efficient Scheme For Mobile Wireless Sensor Networks" IEEE ISWCCS, 2008.
[10] 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.
[11] 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.
[12] 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.
[13] Suat Ozdemir, and Yang Xiao. "Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview". Elsevier, Computer Networks 53,ISSN 1389-1286, 2009, pp.2022-2037.

