Secured Aggregation for Privacy and Efficiency in Energy in WSN

N Sunil nag, P Raghuveer Kumar, Vaddi Naveen
U.G Scholar, Departmentof ECE, SRM University, Chennai,
Ms S. Sudarvizhi
Assistant Professor, Department of ECE, SRM University, Chennai,
Tamil Nadu-603203

Abstract:The proposed system in WSN’s have many applications in critical secured areas, mostly in military applications, since it hides data using many nodes from third parties. The existing techniques uses hop by hop based protocols which does not provide efficiency in energy, due to which it may reveals large amount of data to the adversaries. There by loses its confidentiality of data. The proposed technique is best suited to overcome the constraints of the existing system. This uses end to end encryption which aggregates the encrypted data and sends to the base station, which provide a complete security, data freshness, confidentiality. Because of the aggregation of the encrypted data it reduces the energy consumption.

Keywords*:WSN, Data aggregation, privacy homomorphism, confidentiality, end to end encryption.*

*****

1. INTRODUCTION

The WSN’s has many nodes which will forward data to the base station by aggregating the encrypted data from the other sensor nodes.

WSN has some constraints regarding reliability energy efficiency. Because of these constraints efficient routing of the data is delayed and decreased, which results in loss of data privacy as this is the major issue. Different routing protocols are designed for efficient routing .We use privacy homomorphism for confidentiality of the data. Energy efficiency can be achieved by aggregating the encrypted data at each node. Aggregation is the process of sending the data which are appended with the node identityto the base station.

In this proposed system we send the data from base station and same act as a sink. The data is aggregated and appended with the encrypted data, which decreases the process of decryption, saving much of its energy and increasing the privacy much better than existing system.

2. EXISTED SYSTEM

The energy efficiency and privacy aggregated solutions is very much certain in power constrained wireless networks. This can’t be achieved by hop by hop encrypted protocols. In existed system we use a small network switch which doesn’t provide any access to the large topologies. This [PEPPDA][1] uses Privacy Preserving and Integrity Assured data aggregation, which addresses integrity assured data encryption with efficiency and privacy as a different objectives.

3. OBJECTIVES OF THE PROPOSED SYSTEM

3.1 Privacy of the Data: Generally data privacy is the most constrained issue in WSN. The data privacy should be preserved during the transmission of the data. This system ensures that the data at each node reaches the sink node irrespective of the number of nodes.

3.2 Data Freshness: The aggregation is done at each node which creates new data by encrypting the data with the session keys.

3.3 Energy Efficiency: The encryption at each node and decrypting at next node utilises more energy. This SEPPE is used to reduce the consumption of energy by encrypting the aggregated data without decrypting it.

4. NODES STRUCTURE

Generally it consists of three layers[3]

- Aggregator node
- Intermediate nodes
- Leaf nodes

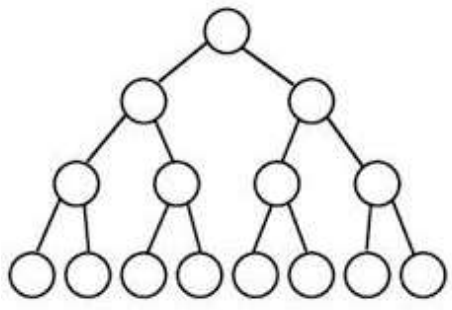


Figure 1. Tree structure

5. STAGES OF THE SAPEE

5.1. Tree construction[1]: The tree is constructed using TAG(Tiny Aggregation) protocol. The tree is formed from the nodes through random structure which are aligned at different points.

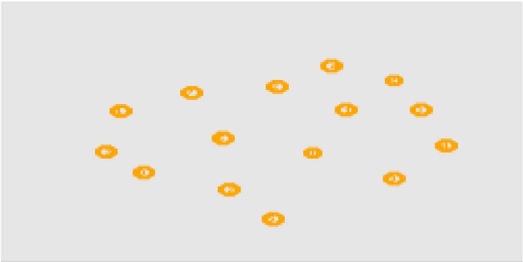


Figure 2.Random structure

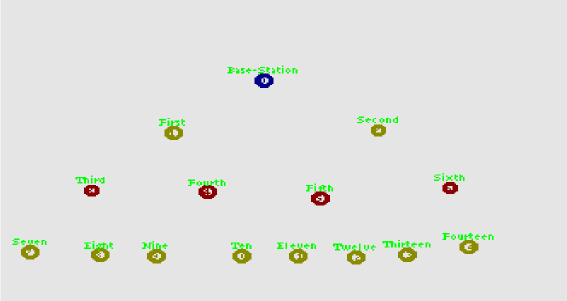


Figure 3.Tree construction

5.2. Key Generation: Base station contains one source node ki, and the other nodes contains their session keys ks.

The base station send the source key to all the nodes and each node receives the key. At leaf nodes the data is encrypted using XOR gate of both session key and source key.

Kie = Ks ⊕ Ki[1]

Kie : Encrypted key

Ks : Session key

Ki : Source key.

The base station holds the pair of all the encrypted keys from all the nodes. So, whenever sink has the aggregated encrypted data from aggregator, it determines Ki of sender node using the identities of aggregator and sender.

5.3. Slicing

Slicing[1] is done at the leaf nodes. Whenever the leaf nodes receives the data, it slices the data into m number of slices. It holds one of the encrypted slice on the node itself and the remaining m-1 slices are sent to the neighbouring nodes.

The neighbouring nodes receives the data with an appended identity of the previous node.

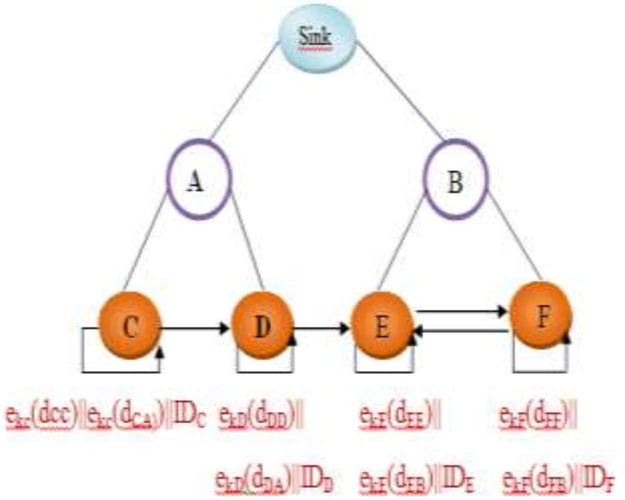


Figure 4. Slicing

5.4.Mixing[1][2]: After slicing is done, each node ensures that all the slices received by the particular node without loss.

During this process each leaf node sum up the encrypted slices from neighbour nodes with one encrypted slice left on the node during slicing.

The main disadvantage of Privacy Homomorphism is that it can be used only for SUM aggregation function.

From figure 4 we can see the mixing process is done by appending the identity of the lea nodes and sending it to the parent nodes or intermediate nodes.

If there are seven leaf nodes the slicing nodes identity will be appended with the data of the each node.

For example at node 3 and 4.

d3A = ek3(d33)|| ek3(d31)|| ID3.

d4A=ek4(d44)+ek3(d34)+ek5(d54)||ID3||ID5||ek4(d41||ID4.[1][3]

We used 15 nodes so for node 8 and 9 (leag nodes in proposed system)

d8A=Eke8 (d88) || Eke8 (d84) || ID8

d9A=Eke9 (d99) + Eke8 (d89)+ Eke10(d109) ||ID8||ID10|| Eke9(d94) || ID9.

5.5. Aggregation[1,4]: After the intermediate nodes receives the data from leaf nodes, it sends the aggregated encrypted slice to the aggregator node or base station. Aggregator node verify the data whether the data is from valid nodes or not.

Each node in a sensor has its common secret key, node specific key, and a unique id (ID). If any changes occur in the data at BS, the leaf nodes will sense the changed data and follow the same procedure.

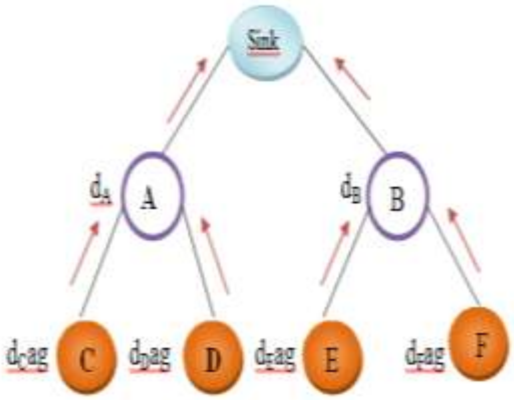
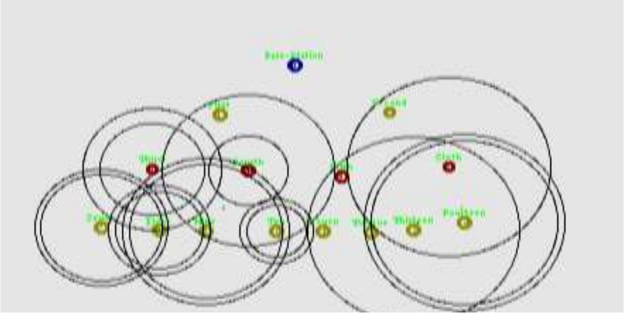


Figure 5. Aggregation

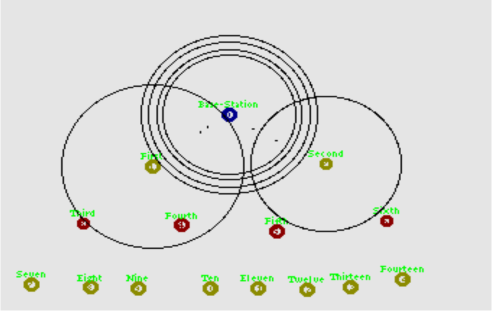
6. SIMULATION STUDY

The proposed system is implemented in ns2. We considered with 15 nodes randomly deployed over an area of 800nm×800nm. One of the node is taken as a sink or BS, and the remaining nodes form a tree structure, with intermediate nodes and leaf nodes.

Parameters of simulation are transmission power = 0.660W, receiving power = 0.395W, Idle power = 0.395W. and energy of 100J.



Slicing.



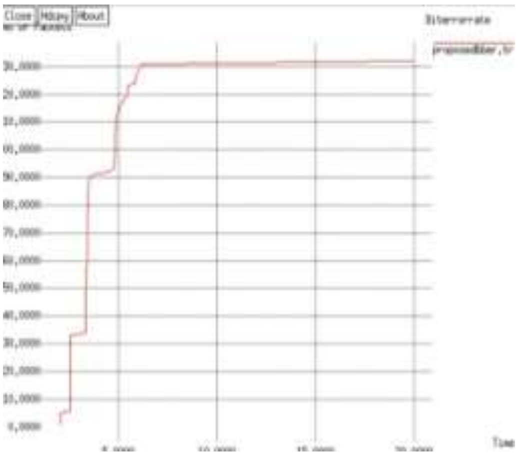
Aggregation.

Simulated Graphs:

The output of this system can be determined by using the network simulator 2 and plotting the graphs of few parameters.

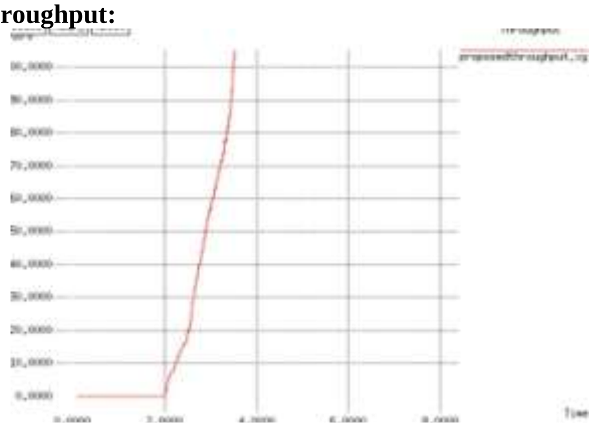
1. Bit error rate
2. Throughput
3. Control overhead packets
4. Packet delivery ratio

Bit error rate:



Bit error rate is the no of error packets delivered per unit time.The graphs defines as the no of error packets increases at the beginning i.e.; for very less packets and then it is maintained constant, where as in existed system it increases gradually.

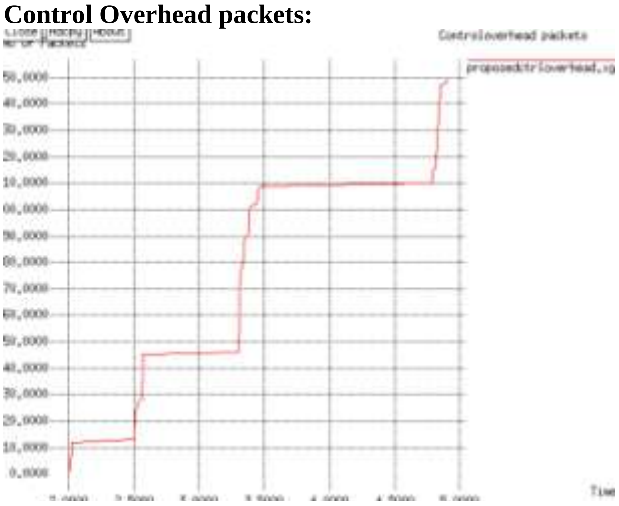
Throughput:



In the proposed system, the throughput is the how fast the data aggregation is performed at the agggregator node and how fast the aggregated data is sent to sink node.

From the graph we can say that initially the throughput of the system is less as the data transmission increases the throughput is increased.

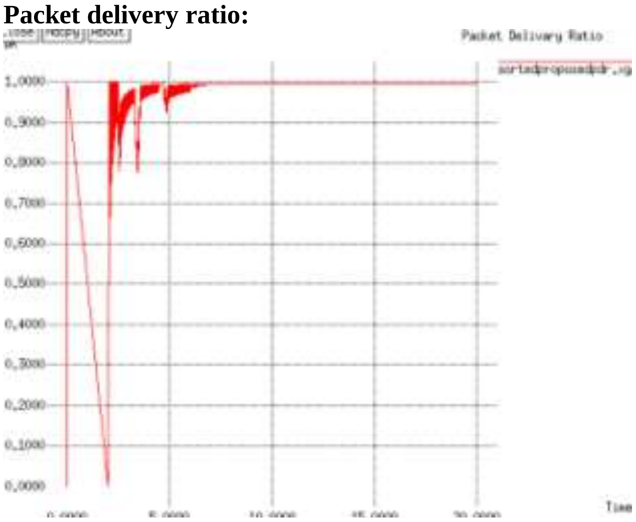
Control Overhead packets:



In the proposed system the encrypted slice is transmitted to the BS along with the transmission of aggregation result from the leaf node. So it reduces the number of transmissions.

The reduced number of transmission and non-delayed aggregation leads to improve the energy efficiency and thus the traffic is reduced as a result the control overhead is reduced.

Packet delivery ratio:



It is the number of packets successfully delivered per unit time.

It can be increased by avoiding the decrypting time at the aggregated node.

7. ANALYSIS

The existed system uses 7 nodes as the proposed system uses 15 nodes. The proposed approach is mainly based on end to end aggregation. As a result energy consumption is reduced. While forwarding the encrypted data from leaf nodes to the aggregated node a forwarding node will select a node which is higher level and hence minimises the cost of unnecessary excitation at the forwarding node. As the leaf nodes slices and sends the data to the neighbouring nodes at the same time the data is encrypted and send to the parent node.

8. CONCLUSION

This paper presents the privacy preserving aggregation and enhances the security constraints in the existing system. Third party access is restricted which ensures the data freshness and reliability of the system. Due to the reduced decryption steps it fortifies the energy efficiency in the system.

Throughput of the system proliferates due to non-delayed transmission. So, it can be used in time critical secured applications.

9. REFERENCES

[1] Joyce Jose, M.Princy, Josnajose,Post Graduate Scholar Dept. Information Technology, Karunya University, Coimbatore, India "Power Efficiency Privacy Preserving Data Aggregation", journal of International Conference on Emerging Trends in Computing, Communication and Nanotechnology(ICECCN 2013).

[2] Priyanka N, Y R Manjunath ”Performing data aggregation on encrypted data for preserving privacy in wsn”, Digital Electronics and Communication systems, SJCIT, Chickballapur India.

[3] Vaibhav Pandey, Amarjeet, Narottam Chand, "A review on data aggregation techniques in wireless sensor network", Journal of Elecronics& Electrical Engineering, ISSN: 0976-8106 & E-ISSN: 0976-8114,Vol.1, Issue 2,2010,pp-01-08.

[4] Nadini.S.Patil, Prof.P.R.Patil, "Data Aggregation in wireless sensor network", IEEE International Conference on Computational Intelligence andComputing Research, 2010, ISBN 97881 8371 3627.

[5] K. Akkaya and I. Ari. "In-network Data Aggregation in Wireless Sensor Networks", Handbook of Computer Networks, Ed. H. Bidgoli, John Wiley & Sons, Vol. 2, pp. 1131-1146, 2008.

[6] Hongjuan Li, Kai Lin, Kequi Li, "Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks", Computer Communication,34 (2011);591-597.

[7] Castelluccia, C.; Mykletun, E.; Tsudik, G. Efficient aggregation of encrypted data in wireless sensor networks. In Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous, San Diego, CA, USA, July 17–21, 2005; pp. 109–117.

[8] Chien -Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, Hung-Min Sun, "RCDA:Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks". IEEE TRANSACTIONS ON PARRALLEL AND DISTRIBUTED SYSTEMS, VOL 23, NO 4, APRIL 2012.

[9] Taban, G.; Gligor, V.D. Privacy-preserving integrity-assured data aggregation in sensor networks. In Proceeding of International Symposium on Secure Computing, SecureCom, Vancouver, Canada, August 29–31, 2009; pp. 168–175.