Review for Secure Data Aggregation In Wireless Sensor Networks

Shweta Rana, Prof. Arundhati Dudhgoankar

[1]*Department of MCA , Jawaharlal Nehru Engineering college*
[2]*Professor, Department of MCA & Jawaharlal Nehru Engineering college, Maharashtra, India*

---***---

Abstract - *Now a day data aggregation is widely used technique in **WSN.** Security is important issue in data aggregation. In many application ,the data collected from particular node is aggregate at a base station. Data aggregation is a technique to process and analysis the collected data from surrounding environment. In this paper we express or represent achieving security in wsn for data aggregation using Hop-by-Hop and End-to-End data aggregation encryption model research have focus on avoiding forgery using above techniques.*

***Key Words*: Wireless Sensor Network, Data Aggregation, Security Requirement.**

1. INTRODUCTION

Wireless sensor network can be define infrastructure less wireless network to observe surrounding environmental condition such as temperature, motion, vibration, sound etc. In wsn have been successfully applied in various application domain like military application, area monitoring, health application, environmental sensing etc. The sensor have rigid component in term of storage, cpu, battery power, network bandwidth. Data aggregation is a technique to remove unnecessary transmission from collected data and provide information to base station. The main function of data aggregation subdue the redundancy, so that lifetime network is improve. Usually, two method can be used for secure data aggregation in wsn: Hop-by-Hop and End-to-End encrypted data aggregation. In Hop-by-Hop sensing node generate data encrypt it and send it to the aggregator, this encrypt data decrypted at the aggregator encrypted back after aggregation. This is repeated at every node. In End-to-End the sensing node encrypt the data but only base station has to decrypt. Data encryption and decryption done only at the end[6].

2. DATA AGGREGATION IN WSN

Data aggregation is an efficient way to minimize energy consumption. On sensor data aggregation is defined as the process of aggregation of data from the multiple sensor to eliminate unnecessary or redundant transmission and provide combined information to the base station. Base station send queries to the network instead of sending each sensor node data to the base station, one of the sensor node data aggregator. It collects the information from its neighboring nodes, aggregate them and send the base station over a multi hop path. The data collected from sensor needs to be processed in order to extract meaningful information from it may time this processing is done by means of aggregation function like SUM, AVERAGE, MEAN, MEDIAN, etc. Data aggregation in sensor network portion to the processing of sensor data, with in the network in a distributed manner. In fig[1] if each sensor has to send its reading back to the base station, without aggregation each of the leaf node sensor generates a reading of sends it to its parent.

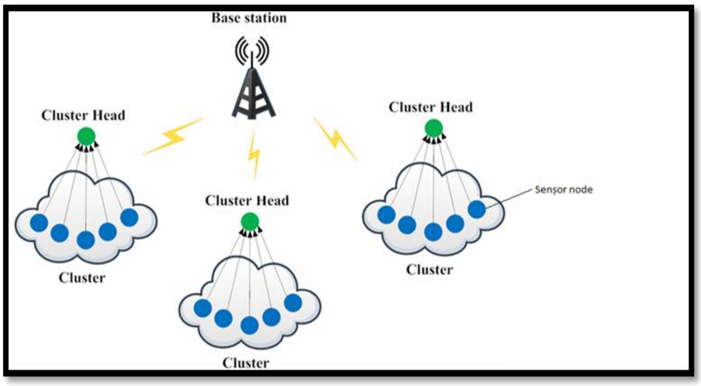

fig.[1] data aggregation in wsn

In network data aggregation also enable the network to directly. Provide service rather than raw data, when we enable the nodes to do computation and processing of data rather than just sensing and forwarding message, sensor process processed information instead of just raw data.

3. SECURITY REQUIREMENT OF DATA AGGREGATION

Data aggregation is an efficient way to minimize energy consumption on sensor but it also create new security challenges. Security is the important issue in wsn it is related with data aggregation process[3][8].

I)Data Confidentiality:

Data confidentiality is a fundamental issue in every aspect of security. Confidentiality is equivalent to privacy. The data confidentiality is protecting the data from unauthorized access. It can be divided into Hop-by-Hop basis and End-to-End basis.

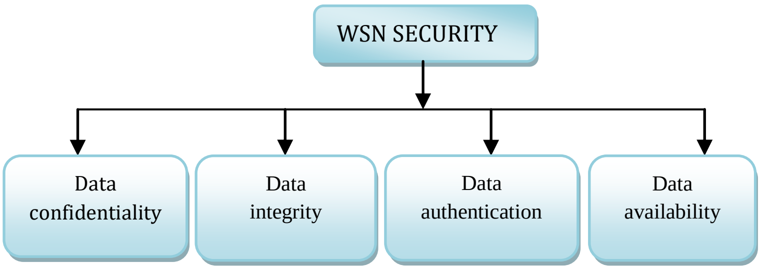

fig.[2] wireless sensor network security issue

II)Data Integrity:

Data integrity assured that a message being transferred is never computed. Data integrity deals with insuring that the received data has not been tempered with in the path between in receiver and sender. Integrity engage maintain the truth and honesty of data in the entire network.

III)Data Authentication:

Data authentication permits a sensor node to ensure the identity of the peer node. Data authentication guarantee that the reported data is the same as the original one. Sender and receiver share a secret key to calculate the message authentication code for all transmitted data.

IV)Data Availability:

Once the attacker gets into the wsn by compromising a node, the attack will affect especially in those party of the network where the attack has been launched. Availability of data aggregation is more important than regular sensor node.

4. SECURE DATA AGGREGATION PHASE

Data aggregation schemes can be classified into 2 groups based on the type of encryption is used:

1) Hop-by-Hop
2) End-to-End

1) Hop-by-Hop Encryption:

In Hop-by-Hop encryption[6], the bootstrapping phase used, the keys are securely distributed to the sensor these keys are brought into used in the data aggregation phase. Sensing node generate data encrypt it and send it to the aggregator, this encrypted data is decrypted at the aggregator node and encrypted back after aggregation this is repeated at every node. The encryption can either be symmetric or asymmetric key. The parent decrypts the data using the shared pair wise key and aggregate all such data received from its children. This process continuous till the data reaches the base station which decrypts it in a similar fashion.

2) End-to-End Encryption:

In End-to-End Encryption[6] provide protection from this, as the data is not decrypted. Anywhere in the network, but the base station also, since encryption and decryption operations are computationally expensive and time consuming. End-to-End encryption help save resource data encryption and decryption done only at the end, to achieve End-to-End security. This can be done using homomorphism encryption algorithm. In that, the sensor use public key to encrypt the data and send it to their parent. The parent receives the encrypted data from all its children.

We also provide secure data aggregation by trust model:

- ❖ **Efficient Distributed Trust Model**

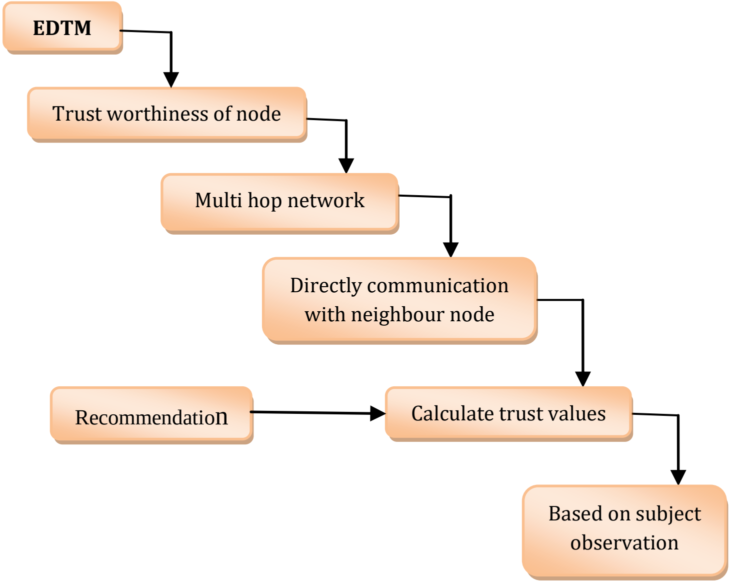

fig.[3] EDTM data flow diagram

In wireless sensor network efficient distributed trust model is used to compute the direct trust and recommendation trust while calculating the direct trust, the other trust like communication trust, energy trust, etc are consider. Recommendation trust is to improve accuracy for sensor node. The EDTM model[5][7] detects the harmful node based. EDTM provide more security and increase the packet delivery ratio. In WSN, EDTM provide trustworthiness for all the sensor node in the network node used for data aggregation may not be malevolent node therefore by using EDTM in wireless sensor network before data aggregation process can help in avoiding false data aggregation. There are 3 kinds of node in the network subject node, recommender and object node. If a sensor node A trust value another node B. The evaluating sensor node A is reference as subject node and the evaluated node B is the object node. The trust value is calculated from a third party. By using EDTM in WSN before data aggregation it can avoided forgery data.

5. CONCLUSIONS

In these paper is studied about data aggregation, security requirement or issues and secure data aggregation phase in wireless sensor network. In additional it reviewed about the efficient distributed trust model (EDTM) for data aggregation basically important requirement of WSN are excellent security with high energy efficiency. These paper have focus on avoiding data forgery or falsification data to reduces the energy consumption. It avoiding multiple redundant or unnecessary data transmission data from multiple sensor using above techniques during aggregation process.

REFERENCES

1) M. Suraj, B. Raja, T. Vengaltaraman “ Secure Data Aggregation In Wireless Sensor Network Using Trust Model” in IJEST April-2016

2) Yingpeng Sang, Hong Shen “Secure Data Aggregation In WSN: A survey”

3) N. Vidhya, Dr. P. Sengottuvelan “Secure Data Aggregation Technique In Wireless Sensor Network” in IJIRCCE Oct-2015

4) Vimal Kamal and Sanjay Madria “Secure Data Aggregation In Wireless Sensor Network”

5) Nefilda K. Joseph, Jathin Jos “A Secure EDTM For Wireless Sensor Network” in IJSER FEB-2016

6) Patel Swapnil “Secure data aggregation in Wireless Sensor Network :A survey ”

7) Dheeraj Vdayaravi Moorti, Shih Yu Chang “An Efficient Distributed Trust Model For Wireless Sensor Network” in IJMETMR

8) Hani Alzaid, Ernest Foo, Gunzales Nieto “Secure Data Aggregation In WSN: A survey ”

9) S. Shashank, R.Precila “An Efficient Distributed Trust Model for Secure Transmission In Wireless Sensor Network” in IJETCSE Mar-2016