A Novella Framework for Secure Data Aggregation in Wireless Sensor Networks using Symmetric Homomorphic Encryption Scheme (SHES)

Md Sirajul Huque[1], Arun Singh Kaurav[2]

[1, 2] Assistant Professor, Department of CSE, GINTC, Hyderabad-India

Abstract: ***Wireless Sensor Networks becoming emerging Technology which consist of a variety of sensor nodes that monitor and record conditions at diverse locations. Wireless Networks are restricted with energy constraint. Data Aggregation is a method of efficient delivery of summarized results by ensuring privacy& Security. With Data Aggregation we can eliminate redundant data transmission there by reducing energy consumption & performance of the wireless sensor networks is increased. The aim of secure data Aggregation is to achieve two critical objectives namely Security & Aggregation. Here we proposed an End to End Privacy and Aggregation using Symmetric homomorphic encryption. Homomorphic Encryption is a form of encryption that allows computations to be carried out on the cipher text, thus generating an encrypted result which when decrypted matches result of operation performed on plain text. This symmetric key based homomorphic encryption significantly reduces energy consumption there by increases life time of sensor nodes.***

Keywords: Diverse, Constraint, Data aggregation, Privacy, Symmetric key

1. Introduction

A Wireless Sensor Network (WSN) is a large collection of sensor nodes called Motes. These Motes have Sensing, Processing and Communicating capability. The Wireless Sensor network is the collection of motes which will monitor and record conditions at diverse locations. The Sensor motes can sense the physical parameters like temperature, pressure, light, intensity and soon. WSN’s becoming more promising area which includes the applications like habitat monitoring, military applications, environmental, medical, Target tracking and many more. Sensor motes have the following constraints.

Constraints of Sensor motes:

- Low power processor usually 8 or 16 bit micro controller
- Limited storage space
- Low power Transmitter usually ISM Bands

Model of Wireless Sensor Network

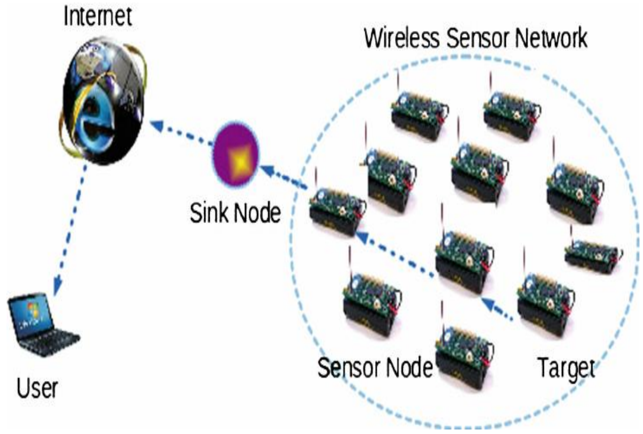

Figure 1: Wireless sensor network Architecture

Wireless Sensor networks are restricted with energy (power) constraint. Hence life time of WSN depends on Mote energy. Wireless sensor networks are differing from other wireless networks with unique characteristics such as

- Limited Power
- Cope with node failures
- Node fails fault tolerant
- Dynamic network topology
- Communication failures

2. Need for Data Aggregation

As Given in Fig.1 WSN consist the components like Sensor Filed (network), Sensor motes (nodes), the sink (Aggregator) and the base station. The sensor field is a network which observes various events. The sensor motes are the key players here which sense various physical parameters. The sensors depart this collected information to the aggregator (sink). As Sensor motes are deployed near to each other they can sense common parameters hence there is a possibility of redundant information is being sent to the sink.

In WSN with data aggregation we can eliminate duplicate data transmission thereby reduce the energy consumption. Therefore data aggregation aims at efficient delivery of a summarized result reported to a base station.

Sometimes these sensors networks are compromised and hence intruders will inject false data into the network. So data aggregation must be aimed at achieving Data aggregation by considering security issues.

3. Motivation for Secure Data Aggregation

Data Aggregation is needed when motes directly cannot reach a base station. Here sensor nodes are data centric (no IP address concept). Secure data aggregation aims at efficient delivery of summarized information to be reported to a base station thereby maintaining privacy and security.

Requirements of Data aggregation security:

Secured Data Aggregation is achieved by the following security measures.

1) **Data Confidentiality**
   In data Aggregation summarized information cannot provided to any unauthorized users. The aggregation is done in two ways.
   - Hop by hop(plain sensor data)
   - End-to-End(Encrypted sensor data)
2) **Data Integrity**
   The summarized information sent to base station must be accurate without any changes done by intruders. It ensures integrity of information collected.
3) **Data Freshness**
   The data must be recent one without any old data being used.
4) **Data Availability**
   Data Availability ensures availability of network at all times.
5) **Authentication of data**
   Proper authentication measures should be taken to ensure correct recipient and correct data.
6) **Non repudiation**
   The summarized information once deployed to a base station by the sink(aggregator) could not be deny then back.

Security Attacks in Wireless Sensor network aggregation:
Various security attacks includes

1) DoS (Denial of Service) Attacks
2) Spoofing
3) Sinkhole attack
4) Wormhole attack
5) Hello flood attack
6) Sybil attack

4. Existing Work in Secure Data Aggregation

- Karthikeyan vaidyanathan [1] proposed three data aggregation techniques: in-network,grid-based and hybrid schemes to perform data aggregation.
- Ameya S.bhatlavande [2] proposed in-network aggregation (temporal coherency-aware-in network aggregation), tree based approach and cluster based approach of aggregation.
- Parmar, k [3] proposed an integrity and privacy preserving secure data aggregation protocol.
- Vivaksha J. Jariwala [4] proposed an additively digital signature algorithm based on Elliptic Curve Digital Signature Algorithm (ECDSA) to achieve integrity of the aggregate
- Vimal Pambhar [5] proposed an adversarial model for security on Data Aggregation its help us to give batter performance compare to existing scheme.
- Vivaksha Jariwala [6] proposed a novel approach using homomorphic encryption and additive digital signatures to achieve confidentiality, integrity and availability for secure data aggregation in wireless sensor networks
- Xing Li proposes FESA, secure data aggregation with fully homomorphic encryption in large-scale wireless sensor networks. FESA can effectively reduce the network overhead while satisfying the above requirements. Compared to the existing technologies, our scheme can ensure the data confidentiality and integrity during data aggregation process and forwarding process, and also detect the false data as early as possible, leading to reduction of communication overhead and hence less energy consumption

5. Proposed Work of Secure Data Aggregation Using SHES

Here we are proposing a symmetric key based Homomrphic encryption for end-to-end secure data aggregation.

Symmetric key Encryption Scheme
Symmetric key based encryption uses a Single shared key to encrypt the information and uses the same key to decrypt the information. Symmetric key encryption is very fast to use. With symmetric key encryption a secret key is used for encryption and decryption so it must be kept secret.

Homomorphic encryption
Homomorphic encryption is a form of encryption that allows computations to be performed on cipher text thus generating an encrypted result which when decrypted matches the result of operations performed on plain text.
Homomorphic encryption schemes are malleable.

Symmetric key based homomorphic encryption (SHES):

Additively homomorphic encryption scheme:

1) Encryption: Considering m as integer.
   m €[0, M,-1] where M is a Large integer. Let k be a random generated key streams where k€[0,M,-1]
   Compute C=encryption (m,k,M)=m+k(mod M)
2) Decryption process:
   Decryption(c,k,m)=c-k(mod M)

Architecture of Secure Data Aggregation:

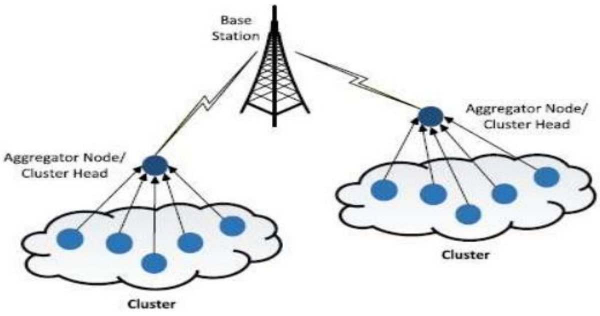

Figure 2

As Shown in figure 2. In wireless sensor networks motes are deployed near to each other. They can sense common parameters, hence there is possibility of redundant information is being sent to a sink. Hence by using data aggregation efficient delivery of a summarized result reported to a base station.

6. Conclusion

The most critical parameter in wireless sensor network during data aggregation is security. Because sensor motes are deployed and operated at various locations at harsh conditions. The Wireless sensor networks are limited with energy constraints. With data aggregation energy consumption is utilized. In this paper we have proposed an efficient method for secure data aggregation in Wireless sensor networks using Symmetric key based encryption scheme. With the literature review presented in this paper various existing methods for secure data aggregation is presented. Here we conclude by expecting many more research work towards secure data aggregation considering limited resources of wireless sensor networks.

References

[1] Karthikeyan vaidyanathan,sayatan sue, sundeep narravula,prasum.sinha,” Data Aggregation techniques in Sensor Networks” Semantic scholor.org.

[2] Ameya S Bhatlavande,Amol A.Phatahk,” Data Aggregation Techniques in Wireless sensor networks: Literature survey”,International Journal of Computer applications(0975-887_ Volume 112-no.10,April 2015.

[3] Parmar,K.and Jinwala ,D.(2015), “Symmetric key based homomrphic primitives for end to end secure data aggregation in wireless sensor networks,Journal of information security,6,38-50.doi:10.4236/jis.2015.61005.

[4] Vivaksha J. Jariwala, Sankita J. Patel “An Improved Approach for Secure Data Aggregation in Wireless Sensor Networks” , International Journal of Computer Applications (0975-8887) Volume 137– No.9 , March 2016.

[5] Vimal Pambhar, Bhoomi Bangoria and Bhavik Kataria' "A Framework: Secure Data Aggregation in Wireless Sensor Networks “International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN ONLINE (2278-8875) PRINT (2320-3765)

[6] Vivaksha Jariwala, Devesh Jinwala “A NOVEL APPROACHES FOR SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS “Department of Mathematics and Computer Applications, 10th National Workshop on Cryptology Department of Mathematics and Computer Applications September 2 – 4, 2010.

[7] Hani Alzaid, Ernest Foo and Juan Gonzalez Neito, DongGook Park,” Secure Data Aggregation in Wireless Sensor Networks”, Emerging Communications for Wireless Sensor Networks.

[8] Xing Li , Dexin Chen , Chunyan Li and Liangmin Wang,” Secure Data Aggregation with Fully Homomorphic Encryption in Large-Scale Wireless Sensor Networks” , *Sensors* 2015, *15*, 15952-15973; doi:10.3390/s150715952

[9] S. Gopikrishnan, P. Priakanth,” HSDA: hybrid communication for secure data aggregation in wireless sensor network” Gopikrishnan, S. & Priakanth, P. Wireless Netw (2016) 22: 1061. Doi: 10.1007/s11276-015-1122-x.

[10] Jyoti Rajput, Naveen Garg,” A Survey on Secure Data Aggregation in Wireless Sensor Network”, International Journal of Advanced Research in Computer Science and Software Engineering, Page | 407 Volume 4, Issue 5 May 2014

[11] **Priti Arora, Suman Sangwan,”** Secure Hierarchical Data Aggregation in Wireless Sensor Networks – General Framework”, **International Journal of Engineering Research & Technology, Vol. 3 - Issue 6 (June - 2014), e-ISSN: 2278-0181.**