Secure Data Aggregation Scheme for Wireless Sensor Networks Using Homomorphic Encryption Algorithm

S Sathya¹
¹Anna University Regional Campus Coimbatore, Information Technology, sathyasmpc@gmail.com

J Jayavel²
²Anna University Regional Campus Coimbatore, Information Technology, jaya.jana@gmail.co

Abstract - In recent years, secure in-data aggregation in wireless sensor networks becomes a challenge issues, there is a large in amount research on this area due to the many applications where the sensors are deployed and the security needs. In the past years, aggregation of encrypted data has been proposed in order to maintain the secure information between the sensors and the base station, so the end-to-end data confidentiality is Provied. There are various security attacks in WSN, such as selective forwarding, cipher text analysis, and pocket forgery and so on. Many existing approaches discuss about the security protocols. In order to improve security and to minimize the computational and communication overhead, SPEED protocol is used. It is maintaining the desired speed, when its packets delivered to the base station. The proposed algorithm achieves security by aggregating the encrypted data and send to the base station. The base station decrypts and retrieves the original information using homomorphic algorithm and thus enhancing the performance of WSN.

Index Terms - Cryptography, Data aggregation, Data Security, Homomorphic encryption, Wireless Sensor Networks.

1 INTRODUCTION

Wireless sensor networks (WSNs) are composed of a more number of sensor nodes, which actually have a wide range of real time applications such as military Surveillance, environmental monitoring and wildfire tracking [1, 2]. In sensor networks, sensor nodes are collectively monitoring an area. These large sensor networks generate a strongly large amount of data, yet the sensor nodes often have limited resources, such as computation power, memory, storage, communication, and most importantly, battery energy [9]. For better power utilization, a cluster-based WSN has been used in network topology, sensor nodes are grouped into multiple clusters. Each cluster contains several sensor nodes and one cluster head. When sensor nodes send their data to the cluster head, the cluster head would aggregate multiple data’s into one, and then send the aggregated data to the base station [1, 10]. The purpose of the above method is saving energy by reducing the transmission cost and data redundancy. This technique is named as data aggregation [10].

In general, data aggregation can be done in cluster head and base station [1, 7, and 10]. Aggregated data can be algebraic operations on numeric data and statistical operations on numeric data, such as median, minimum, maximum, and mean of a data set [7, 10]. Data aggregation is one of the solutions of increasing the sensor node life time [3, 8]. In-network processing is done at cluster Head(CH) or intermediate node in the case of multi-hop network, it aggregates the data coming from its child nodes or clusters by performing the aggregation function such as min, max sum etc. and results send to the upper level node or sink [12]. However, in hostile or unattended environments, the aggregated data should be prevented from various types of attacks that can be send by unauthorized or compromised nodes, and hence, security services such as end-to-end data confidentiality and data integrity are widely used for providing security [1, 12].

The main problem of data aggregation is when we aim to provide data security to aggregation and reduce the number of packet transmission. These both problems are opposite goals [1, 13]. To cope with the security risks, several security studies have been described, secure data aggregation can be classified into two types: hop-by-hop security and end-to-end data security. Hop by hop encryption scheme, in which sensor nodes encrypt the collected data and send the ciphertext to the Cluster Head, the Cluster Head node decrypts, gathering the data and then send the encryption of the resultant data to the upper aggregator node this process not only prevents the secrecy of data, but also, results in an necessary of computation overhead and delays [4-7]. In order to give data secrecy, end-to-end security schemes have been projected in that the data is hid end-to-end nodes and decrypted solely base station. In these schemes, the intermediate nodes perform the aggregation operation over encrypted data while not decrypting that results in lesser computation overhead and provides the end-to-end data confidentiality. However, in these solutions, the homomorphic encryption is used and it is known that this kind of encryption suffers from malleability, in other word, given a ciphertext, an attacker will simply generate a ciphertext so as to deceive the base station by accepted the corresponding m’ that's associated with the first plaintext m, and while not essentially proverbial to the attacker. Therefore, it is of in the beginning of time necessary to develop security in aggregation schemes that provide both end-to-end data confidentiality and data integrity [1].

An attacker can carry out a more variety of attacks. For example, once the assaulter compromised the base station or the aggregators, the assaulter might perform a denial-of-service attack and stop responding to any queries. In the time after we assume that the attacker is fully controlling the compromised node, there is nothing to prevent the attacker from more intense...
such denial-of-service attacks. However, we focus on another variety of attack that is stealthy attack. In a lurking attack, the attacker’s goal is to form the user settle for false aggregation results, that square measure considerably completely different from verity results determined by the measured values, whereas not being detected by the user. In particular, we want to guarantee that if the user accepts a reported aggregation result from the aggregators, then the reported result is “close” to the true aggregation value with high probability; otherwise, if the reported worth is considerably completely different from actuality worth attributable to the misconduct of the compromised aggregators, the user can observe the corruption and reject the reported aggregation result with high likelihood. We stress that within the thought about model the corrupted sensors and aggregators may deviate from the protocol in an arbitrarily malicious way, and our goal is to stop the user from accepted incorrect results [6].

During data aggregation, data packets may be lost from collision, congestion, noise, or other network difficulties. It is called insider packetdrop attacks refer to a set of attacks where compromised nodes intentionally drop packets. Such attackers disguise their malicious behavior behind the aforesaid natural packet loss development. This kind of attack has become a significant security threat in WSNs. A well-positioned malicious corporative executive are on the routing path of several detector nodes and so receive many data packets [7].

Normally selective forwarding attack, an associate degree assailant seeks to realize one among the subsequent two goals. First, degrade the performance of the network in terms of packet loss rate. Second, prevent data collected by certain sensor nodes from reaching the BS. In the second case, the victim node won’t be able seek advice to the BS, and that we name this attack selective forwarding-based denial-of-service (DoS) attack [11].

In this paper Section (2), deals with the various other methods used for security. Section (3), focuses on the proposed method for data security and Section (4), explains the Analysis and Results of the proposed model that is been developed in Matlab wherever the encryption and decryption is finished and conclusion of the paper.

2 RELATED WORKS

O. Rafik, S. Mohammed Senouci, Mohammed Feham use Stateful public key cryptography algorithm and digital signatures, aggregate MAC it is provides end to end data confidentiality and end to end data integrity. It is implemented on TelosB as well as MicaZ sensor network platforms and measures the execution time of our various cryptographic functions [1].

J.Gubbi, R. Buyya, S. Marusic, M. Palaniswami uses IOT, Here cloud centric vision for worldwide implementation of Internet of Things. Cloud implementation victimization Aneka that is predicted on interaction of private and public cloud is given finally concluded IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological investigation community [2].

Xiangqian Chen, Kia Makkii, Kang Yen, and Niki Pissinou dividing the security problems in seven classes, cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion. And Chen summarizes the techniques and methods used in these categories, and point out the open research issues and directions in each area. Security in sensor networks could be a new area of research, with a restricted, however space growing set of analysis results. X Chen explained the feasible to apply public key cryptography to WSNs by choosing appropriate algorithms, parameters, etc., [4].

K. Akkaya, M. Demirbas, R.S. Aygun explains the First, comparison of the prevailing data aggregation techniques with relevancy totally different networking metrics. Second, declaring each the necessity for collaboration between data management and networking investigation communities functioning on data aggregation in WSNs [3].

Hung-Min Sun, Yue Hsun Lin, Ying-Chu Hsiao, and Chien Ming Chen they combines Boneh et al.’s aggregate signature scheme and Mykleton et al.’s concealed data aggregation scheme to overcome the compromising secret in captured sensor nodes problems [10].

3 SYSTEM MODEL

Large number of sensor nodes are deployed in the region of interest, the nodes will collect the information further physical Environment. The sensed data will be Encrypted (cipher text), using homomorphic encryption. Then sensor nodes are grouped to form the clusters, the nodes with higher residual energy will be act as a cluster head the main role of cluster head is to aggregate all the collected data from the nodes and remove the redundant data. The aggregated data is form of cipher text is send to the base station. The base station will decrypt and retrieve the original sensed information, to improve the security in Wireless sensor network. The speed protocol is used, if will reduce the communicational and computational overhead.

3.1. System Architectural Design

Figure 1 shows the architectural diagram, the collected data from sensor node will be encrypted. Cluster head will aggregate thedata and send to the base station. The base station will decrypt and verify the individual data. Encryption and decryption are performed by using homomorphic encryption algorithm.

3.2. Homomorphic Encryption Algorithms

Homomorphic encryption could be a style of encryption that enables computation to be done out on ciphertext, so generating
an encrypted result that, once decrypted, matches the results of operations performed on the plaintext. HE is would allow the chaining together of different techniques without exposing the result of data. Homomorphic property of various cryptosystem can be used to create many other secure system, if treated carefully homomorphism can used to perform computation securely.

3.2.1. Functions of Homomorphic Encryption

Homomorphic (public-key) Encryption H is a set of four functions,

\[ H = (\text{HE.Keygen}, \text{HE.Enc}, \text{HE.Dec}, \text{HE.Eval}) \]

1. Key generation

The algorithm \((pk, evk, sk) \leftarrow \text{HE.Keygen}(t^k)\)

Takes a single illustration of the security parameter and outputs a public cryptography key \(pk\), a public evaluation key \(evk\) and a secret decipherment key \(sk\).

Client will generate pair of keys public key \(pk\) and secret key \(sk\) for Encryption of plaintext.

2. Encryption

The algorithm is

\[ C \leftarrow \text{HE.Enc}_{pk}(\mu) \]

Takes the public key \(pk\) and a one bit message \(\mu \in \{0, 1\}\) and outputs a ciphertext \(c\).

Using secret key \(sk\) client encrypt the plain text \(PT\) and generate \(E_{sk}(PT)\) and along with public key \(pk\) this cipher text \(CT\) will be sent to the server.

3. Decryption

The algorithm

\[ \mu^* \leftarrow \text{HE.Dec}_{sk}(c) \]

Takes the secret key \(sk\) and a ciphertext \(c\) and outputs a message \(\mu^* \in \{0, 1\}\). Generated \(\text{Eval}(f(PT))\) will be decrypted by client using its \(sk\) and it gets the original result.

4. Homomorphic Evaluation

The algorithm

\[ c_f \leftarrow \text{HE.Eval}_{evk}(f, c_1, \ldots, c_l) \]

Takes the evaluation key \(evk\), a function \(f \{0, 1\}^i \rightarrow \{0, 1\}\) and a set of \(l\) ciphertexts \(c_1, \ldots, c_l\), and outputs a ciphertext \(c_f\).

Server has a function \(f\) for doing evaluation of cipher text \(CT\) and performed this as per the required function using \(pk\).

3.2.2. Properties of Homomorphic Encryption

Homomorphic Encryption has mainly two properties,

1. Additive homomorphic encryption

A Homomorphic encryption is additive,

\[ \text{Ek}(PT_1 \oplus PT_2) = \text{Ek}(PT_1) \oplus \text{Ek}(PT_2) \]

As the cryptography function is additively homomorphic, the subsequent identities are often represented,

The product of two cipher texts can decode to the adding of their corresponding plaintexts,

\[ D(E(m_1, r_1) \cdot E(m_2, r_2) \mod n_2) = m_1 + m_2 \mod n \]

2. Multiplicative homomorphic encryption

Homomorphic encryption is multiplicative,

\[ \text{Ek}(PT_1 \otimes PT_2) = \text{Ek}(PT_1) \otimes \text{Ek}(PT_2) \]

Where, \(Ek\) is the Encryption key and \(PT\) is plain Text.

3.3. SPEED Protocol

SPEED Protocol could be an unsettled protocol for Real time communication in WSNs. This protocol provides real time communication services, namely, unicast, real time region multi-cast and real time any cast. It is achieves the with minimum control overhead. End to End soft real time communication is achieved by maintaining a desired speed. This protocol could be a extremely economical and scalable protocol for device networks wherever the resources of each node scare [14].

4 PERFORMANCE EVALUATIONS

Our scheme reduces the computation and communication overhead and discuss about the energy consumption. In the following section, we analyze the performance:

4.1. Communication Overhead and Energy Consumption Analysis

Fig 2 shows this variation indicates the different type of cryptography methods. As our scheme is achieves minimum computation and communication overhead compare than ECDSA and SHA encryption schemes.
4.2. Conclusion

The important challenges of wireless sensor Network, security is the major issue of data aggregation. This project focuses on ensuring data confidentiality and integrity during data aggregation. It is a way of using speed protocol giving security with minimum computational overhead and communicational overhead. The simulation is done using the MATLAB and the results are analyzed.

REFERENCES


AUTHOR PROFILE:

- Sathyas is currently pursuing master’s degree program in mobile and pervasive computing in Anna University Regional Campus Coimbatore, India, E-mail: sathyasmpc@gmail.com
- Jayavel J is currently working as a Professor in the Department of Information Technology at Anna University Regional Campus, Coimbatore, India, E-mail: jaya.jana@gmail.com