Secure Data Aggregation in Hierarchical based Protocol in Wireless Sensor Network

Nishant Inamdar¹ Swati Bendale²
1Department of Computer Engineering ²Department of Information Technology
1²SVIT, Vasad-388306, India

Abstract— securing data aggregation in wireless sensor network is very important. Here we have used homomorphic encryption scheme. Using this method we can achieve secure data aggregation in a energy efficient manner. But the current scheme uses Elgamal and EC-Elgamal algorithm for securing data. As Elgamal uses multiplicative homomorphism approach it is very time consuming process and it is complex and it consumes more energy of the nodes. Here to overcome these problems we have proposed another homomorphic encryption scheme it uses pallier algorithm for securing data. Pallier algorithm uses additive homomorphism approach. Its computation cost is lower than the elgamal algorithm and so it uses less energy of the nodes and it uses less time to compute the data. Here we will use leach protocol.

Keywords: Data Aggregation, Elgamal Algorithm, Homomorphic Method, Leach Protocol, Pallier Algorithm

I. INTRODUCTION

Wireless Sensor Network is a network made up of tiny nodes which are deployed over a geographical area. These nodes communicate with each other over the network. Here each node has power supply, computing capabilities and sensing, these nodes gather themselves and form a cluster to perform any task. These sensors are used to take measurement of the environment; they are used in military and for domestic use also. So WSN can thus be viewed as a smart distributed measurement technology sufficient for many different monitoring and control contexts. So in recent years the trend for wireless sensors have increased in day to day life for different purposes and it is expected to increase more in future.

Here different techniques are used to handle data among them the data aggregation is one which also help reduce the overhead to the network. The data aggregation does different function on the data to process it. The aggregator uses Average, Sum, Multiplication etc functions on the data. Data aggregation refers to using an aggregation function f such as SUM AVG, MIN/MAX, MULT, etc. on n data items, at intermediate nodes, to produce one aggregate value v = f(x1, x2, ..., xn). Thus aggregation process increases the efficiency of the network and reduces the energy consumption of the nodes and reduces the end to end delay. Data aggregation is done on the cluster head so cluster head is the single point for attack. So we have to secure the data on the cluster head by using some security mechanism. In current time Elgamal algorithm is used to secure data. How the elgamal algorithm works in securing data is shown in the next section.

II. EXISTING WORK ELGAMAL ALGORITHM

Elgamal algorithm is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange method. It was developed by Taher Elgamal in 1985. The algorithm consists of three components: key generator, encryption algorithm, and decryption algorithm. Here in this algorithm the method chooses a large prime no P, then the next step is to choose a primitive element αA modulo P, then a (possibly random) integer dA with 2 ≤ dA ≤ P – 2. Now we can calculate βA = αAdA mod P.

So the public key is (P, αA, βA). This algorithm works on privacy homomorphism.

1) Encryption:

To encrypt the message M:
- Choose a random integer K which should be kept secret.
- Compute r=αA^K (mod P, βA) and t=βA^K M(mod P, βA).
- Then discard K.
- Send encrypted message (r, t).

2) Decryption:

To decrypt the cipher text:
- Use the private key dA
- compute tr-dA = βA(KM(αA^K)-dA) (mod PA) =M(mod PA)

A. Privacy Homomorphism

It is an encryption technique that allows computation directly on the encrypted data. In other encryption technique if any function is to be applied on the encrypted data then it has to be decrypted. There are two types of PH, Additive PH and multiplicative PH.

The Additive homomorphism supports additive property. It does addition function on the data and it does not require decrypting the data to apply this function. The function states that E(x+y)=E(x)+E(y).

And multiplicative homomorphism supports multiplicative property. It does multiplication function on the data without decrypting it.

The Additive PH are more better then the multiplicative PH because of their less expensive operational cost.

The PH based cryptosystems are divided in two types 1).Symmetric PH and 2).Asymmetric PH.

I) Symmetric PH[3]

Here in symmetric PH the nodes encrypt there data using the shared key between the nodes and the base station. So in this system the end to end confidentiality is achieved.

But here the problem is the nodes keep the secret keys so if any node is attacked then data can be achieved or tempered.

2) Asymmetric PH[3]

In asymmetric PH the nodes encrypts data using the public key of the base station and the base station decrypts the data using its private key.
So here end to end data confidentiality is achieved and the nodes are also made secure. So if any attack happens on the node the data cannot be viewed as the private key is with the base station.

If an encryption is said to be asymmetric additive PH, then it must satisfy the condition $a+b=Dr(Eu(a)+Eu(b))$. Where $(r,u)$ are private and public key pair.

III. PROPOSED SCHEME

Paillier cryptosystem was invented by Pascal Paillier in 1999. This algorithm is a probabilistic asymmetric algorithm the problem of computing $n$th residue classes is believed to be computationally difficult. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based.

The algorithm works as follow there are three steps involved in this algorithm.

- key generation
- encryption
- decryption

A. Key Generation:

1) Choose two large prime numbers $p$ and $q$ randomly and independently of each other such that $\text{gcd}(pq,(p−1)(q−1))=1$.

2) Calculate RSA modulus $n=pq$ and, Carmichael’s function $\lambda=(p−1)(q−1)$ it can be computed using $\lambda=(p−1)(q−1)/\text{gcd}(p−1,q−1)$.

3) Select generator $g$ where $g \in Z^*_n$. There are two ways of selecting the $g$.
   a. Randomly select $g$ from a set $Z^*_n$.
   b. Select $a$ and $b$ randomly from a set $Z_n^*$ then calculate $g=(a^a \cdot b^b) \mod n$.

4) Calculate the following modular multiplicative inverse
   $\mu=(L_1(g^a \mod n^2))^{-1} \mod n$

   Where the function $L_1$ is defined as $(u)=u−1/n$

   This multiplicative inverse exists if and only if valid generator was selected in previous step.

   - The public (encryption) key is $(n,g)$.
   - The private (decryption) key is $(\lambda,\mu)$.

1) Encryption

   - Let $m$ be a message to be encrypted where $m \in Z_n$.
   - Select random $r$ where $r \in Z_n^*$.
   - Compute ciphertext as: $c=g^m \cdot r^d \mod n^2$.

2) Decryption

   - Cipher text $c \in Z_n^*$.
   - Compute message: $m=(c^\mu \mod n^2) \cdot \mu \mod n$.

3) Mathematical functions and notations

   - General common divisor (gcd) of two or more non zero integers is the largest positive integer that divides the numbers without a remainder. The greatest common divisor of $a$ and $b$ is written as $\text{gcd}(a, b)$, or sometimes simply as $(a, b)$.
   - Least common multiple (lcm) of two or more non zero integers is the smallest integer that is divisible by every member of a set of numbers without a remainder.

   - Euler’s totient function (phi function) The totient of a positive integer $n$ is defined to be the number of positive integers less than or equal to $n$ that are coprime to $n$.

   - Carmichael’s function (\lambda function) is given by the least common multiple (lcm) of all the factors of the totient function $\Phi(n)$. If $n$ can be factorized to prime number $p$ and $q(n)=\text{lcm}(p−1,q−1)$.

   - Modular multiplicative inverse of an integer $a$ modulo $m$ is an integer $x$ such that $a^x \equiv x \mod m$. This is equivalent to $ax=1 \mod m$. The multiplicative inverse of a modulo $m$ exists if and only if $a$ and $m$ are coprime (i.e., if $\text{gcd}(a,m) = 1$).

   - Converting a decimal Number to any base number The remainders that we get when we sequentially divide the decimal number by the base end up being the digits of the result, which are read from bottom to top. Example: convert 190 to base 3. $190 = 2 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^1 + 1 \cdot 3^0$.

   The following notations are used frequently in Paillier Cryptosystem explanation:
   - $Z_n^*$ - set of integers $n$
   - $Z_n^{\ast}$ - set of integers coprime to $n$ - this set consists of $\Phi(n)$ number of integers
   - $Z_n^{\ast}$ - set of integers coprime to $n^2$ - this set consists of $n(n)$ number of integers.

Now we will implement these algorithm in leach protocol in wireless sensor network using Castalia tool.

B. LEACH

The first network protocol which uses hierarchical routing for wireless sensor networks to increase the life of the network is leach protocol. In this protocol all the nodes form a cluster and one node is decided to be the cluster head. Here all the nodes send the data to the-cluster head the cluster head process the data and send it to the remote base station. Here the node which is selected as the cluster head has sufficient energy but as the cluster head is also a node at one point its energy also drains out. So if the cluster head is dead then all the nodes will lose the communication with the cluster head and each other. So to avoid this problem LEACH incorporates randomized rotation of the high energy cluster head position such that it rotates among the sensors in order to avoid draining the battery of any one sensor in the network.

IV. RESULTS

![Fig. 1: Results](Fig 1: Results)

All rights reserved by www.ijsrd.com
This is the result showing that why leach is used not any other protocol. Here the comparison is between LEACH and AODV PROTOCOL.

Fig. 2: Results
Here the energy consumption comparison is done between the two algorithms Elgamal and Paillier. Paillier have proved more energy efficient then the Elgamal algorithm.

Fig. 3: Results
Here the time efficiency comparison is done between the Elgamal and Paillier algorithm. Paillier is better then the Elgamal.

V. CONCLUSION
From the above results we have concluded that paillier is better then Elgamal due to is homomorphic additive property.

So paillier is a energy efficient, time efficient and computation cost efficient algorithm and can be used in wireless sensor network.

REFERENCES
[8] “Homomorphic Tallying with paillier cryptosystem”
[12]“Analysis of LEACH Protocol in Wireless Sensor Networks” by Meena Malik, Dr. Yudhvir Singh and Anshu Arora in 2013, IJARCSSE.