isrjournals

International Journal of Advanced Research in Electronics, Communication & Instrumentation Engineering and Development

Volume: 3 Issue: 2 Dec,2016,ISSN_NO: 2347 -7210

PRIVACY PRESERVING DATA SHARING NETWORKS USING ELLIPTICAL CURVE CRYPTOGRAPHY IN SIDECHANNEL ATTACKS

K.Iswarya, V.N.Arumbu,
Student, Assistant Professor, Department of ECE,
IFET College of engineering
Villupuram – 605108.
ishwaryaece66@gmail.com, arumbu.ece@gmail.com

Abstract- In, multihop wireless sensor network data transmitted between sender and receiver through intermediate nodes. However sensor networks are deployed various no of real time applications where data aggregation is performed to collect the entire data from various no of sources. While performing data aggregation in sensor networks trustworthiness important keyfactor to achieve in network. In senor network there maybe presence of adversary nodes which leads untrustworthiness of data and makes the network subjects to various attacks and form packet drop. The scope of this paper is to provide source sharing information over the network for different attacks prevention methods which gives more secure environment and to transmit the data without packet drop. This paper we proposes a **"elliptical curve cryptographic" technique to transfer the data in secure manner. Elliptical curve scalar technique shows resistance to side channel attacks in sensor network and verify the data correctness in the cryptographic system.**

Keywords – privacy, elliptical curve cryptographic, secure, intruder, aggregate, network.

INTRODUCTION

Data trustworthiness is the important key factor to achieve multihop sensor network. Sensor networks are collaboratively used to monitor physical and environmental conditions which are applied to real world application in field of healthcaring, military applications, cybercrimes applications..etc. The sensor network which are deployed in the network sometimes may lead to vulnerable attacks. The presence of malicious node in the network which leads to untrusthworthiness of data. Security solutions are considered to transfer data in secure manner. Privacy, verification ,non-repudiation, reliability are protected solutions for the secure data transfer. So, our goal to achieve these security solutions and to provide the secure environment for the users . This paper framework is split up into two task .first we provide cryptographic method for secure transmission using elliptical curve cryptographic method for secure transmission using elliptical curve cryptographic technique .second part is performance analysis parameters are analysed.

Elliptical curve cryptography is a public key cryptography system in which both the public and private keys are utilized. And hence data is encrypted at the sender side by cryptographic technique and decrypted ,data verification performed at the reciver side.And this proposed technique shows resistance to the side channel attacks but the present system fails to overcome such attacks.

The rest of this paper is organized as follows, section 2 related work , section 3 comprises design system module, section 4 contains reports based on experimental results.

RELATED WORK

Hyo-sang lim was the first to briefly discuss about the trustworthiness management in sensor networks [2]. S.sultana, et al proposed idea about to find packet drop in wireless sensor networks due to malicious node [3]. Further analysed the paper [4] to know the causes and factor that create side channel attacks in sensor networks. In paper [5], studied how to achieve privacy among sensor network .

In the paper [1] “in packet bloom filter technique is suggested for the data transmission however, the present system fails to show resistance to the side channel attacks that occur in sensor networks and they posses certain limitations they are bloom filter technique requires more space, difficult to find the attacker, cost of error detection method is high, provides no solution to avoid packet drop in sensor networks. In[6], studied about the types of cryptographic system. In order to know about brief description of elliptical curve cryptographic system revised [7] this was given by Nicola contantinescu.

In[8],which was given by S Sathish Kumar et al how the secure transmission was performed using elliptical curve cryptography in a data aggregation. And to know the ecc performs and shows the resistance to the fault attacks in sensor networks [9] revised given by R.Lercirer .And to find error detection mechanism in low cost LOEDAR scheme is used in combination with ecc.

SYSTEM DESIGN

The proposed system should be in the way of overcome such limitations of the existing system. The wireless network explodes and in need of secure transmit of data over the network .Both for secure(authenticated ,private) web transaction of data the efficient public key technique is needed.

The proposed model is “elliptical curve cryptographic “system which is a public key cryptographic system based on the algebraic structure of elliptic curves. the proposed architecture retains the efficiency of Montgomery ladder algorithm to show strong resistance to the attacks in the environment.

LOEDAR scheme is used to counteract against the various power analysis attacks, fault attacks.

ECC OVERVIEW

Elliptic curves are suggested for cryptography by victor miller, Neal koblitz. Ecc is an public key cryptographic system. Elliptical curves are used in pseudo random generators, digital signatures.

However when compared to other cryptographic techniques such as RSA, ECC is very efficient. ECC first it will translates the message or data into affine point on the elliptic curve (EC).

In this cryptographic technique, most efficient part is data verification for that elliptical curve scalar multiplication technique (ECSM) is used the reason for using Montgomery ladder algorithm is to show resistance to side channel attacks during ECSM.

In ECC both encryption and decryption are the dominant operations in scalar multiplications where data loss occurs due to fault attacks in order to obtain efficiency and authentication Montgomery ladder algorithm technique is used.

ECC based on the discrete logarithmic problem. If A and B are the two points on the elliptic curve such that C is scalar with the help of know A and B it is difficult to compute C

$$\mathbf{cA=B}$$

Where “C” is the discrete logarithm of B to A. The main operation in ECC is point multiplication. Where the point multiplication is performed by point addition and point doubling .

The designed system is modelled or framed with three major steps they are,

- Broadcasting the public key
- Neighbour hood discovery process
- Elliptical curve scalar multiplication.

Hence in this process receiver mode and the sender mode is assigned dynamically. The data to be transmitted is mentioned during the simulation process and hence ECC technique is performed to encrypt and decrypt the data

Modules Operation

- Broadcasting message:

In this module, after initializing the sender and the receiver node data to be transmitted is mentioned and the topology for the network is designed.

By, continuing that public key for the cryptographic system is broadcasted to the all the nodes in the network.

- Neighbour hood discovery process:

After the public key allocation to the network neighbourhood discovery nodes are determined in the network. Neighbourhood request are send from the server to all the nodes in the network by sending neighbourhood request .if the nodes in the network accepts the request in addition to that both nodes shared their public key information and addition to that it will get acknowledgment from node, which sends the neighbourhood request.

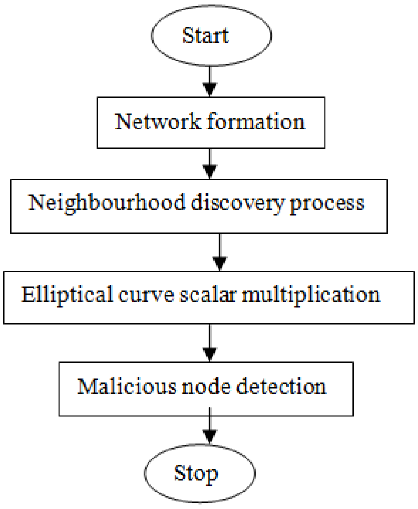

Start
Network formation
Neighbourhood discovery process
Elliptical curve scalar multiplication
Malicious node detection
Stop

Fig1 flowchart for system design

The above diagram is the flow chart for our proposed scheme

- Elliptical curve scalar multiplication.

This the technique where data encryption and decryption technique is performed where this is central operation in the elliptical curve scalar multiplication However sensor networks may contain adversary nodes which may leads to some attacks in order to show resistant to side channel attacks “ MONTGOMERY LADDER” algorithm is used.

This section performs “point multiplication “ technique.

By selecting sender and receiver node shortest path between sender and receiver is determined and data transmitted is encrypted using public key when it reaches at the receiver side data decrypted using private key of receiver .

- Malicious node detection:
  The sensor network may contain adversary node so to find malicious node LOEDAR scheme is used. And this algorithm is used to detect errors. This error detection will be carried periodically the point verification is performed using datas from point addition and point multiplication.

ADVANTAGES OF ECC TECHNIQUE

- Difficult to break the cryptographic system.
- Provides more security
- Less bit size and fast when compared to another cryptographic system
- Less key size when compared to existing algorithm like RSA
- By using LOEDAR scheme in this cryptography the hardware overhead 37./.
- Faster than RSA
- Good for handhelds and cell phone.

SOFTWARE USED

The performance parameters of our proposed techniques are throughput, packet delivery ratio , key generation time analysis ..

The software used to view the analyse the response is NS2. Here NAM window setup is used to view the simulation part and to view performance charactersistics.

STEPS FOR THE SIMULATION PROCESS

First by giving sender node and receiver node enter the data to be transmitted at that time NAM window opens and start the simulation process .

1. Network formation starts

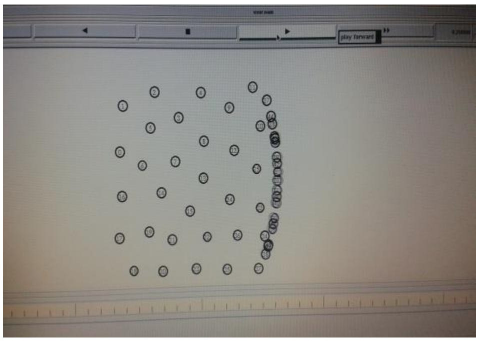
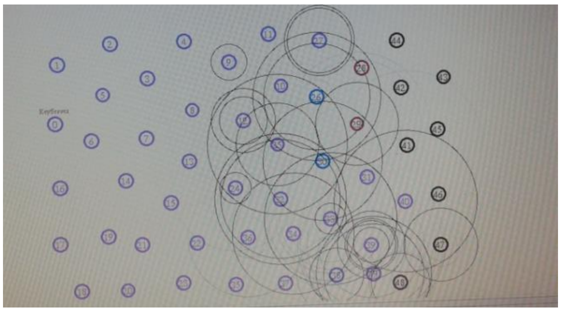


Fig 2. formation of nodes in network.

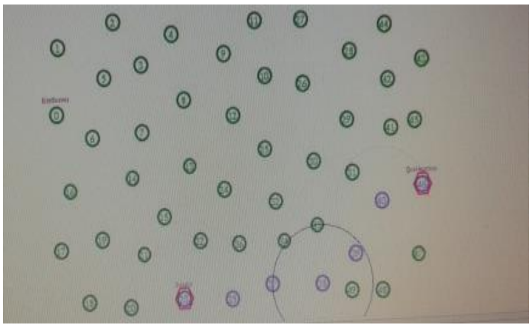
2. Broadcasting the public key to all the nodes in the network

Neighbour coverage process starts there in sensor network by which request sends from key server to all nodes in network



The above fig shows the diagram for sending neighbourhood coverage area.

3.data encryption and data decryption process.

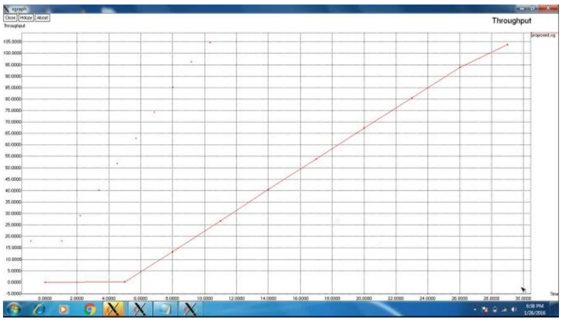


PERFORMANCE ANALYSIS

Performance features of our proposed work is analysed in graphical form with help of x window .

1. THROUGHPUT

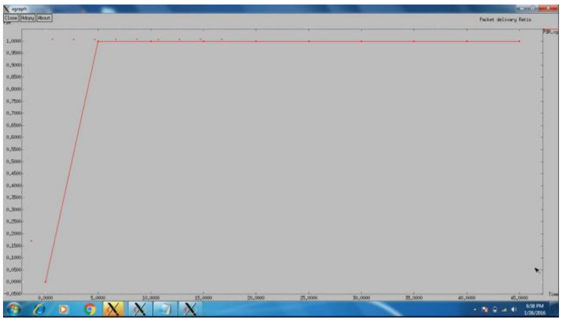
In this parameter it shows the efficiency of overall system designed. From the throughput efficiency of our proposed system is estimated.



Throughput parameters are analysed between two co ordinates they are time vs input.

2. PACKET DELIVERY RATIO:

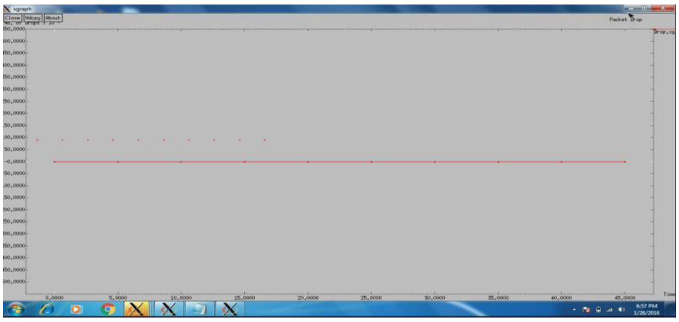
This parameter implies rate of packet delivery in the network system this shows rate of reduction in packet drop.



3. Packet drop:

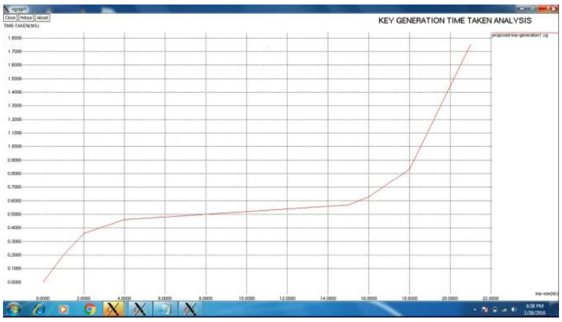
This graphical view shows the rate of packet drop in our proposed work.

Graph contains two co ordinates which is time vs number of drops



4. key generation time analysis:

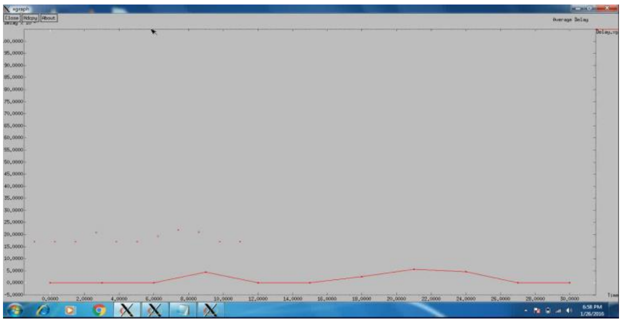
our proposed system undergoes encryption and decryption technique and it follows the public key cryptographic system the graphical representation tells the overall view for key generation for proposed technique.



The graph contains two coordinates they are time vs key generation in kbits/sec.

5. Average delay time:

Each system is possed with certain delay time to start up the certain mechanism the graphical view we analysed propsed system average delay with respsective time vs delay.



CONCLUSION:

In this paper, we proposed a framework to achieve privacy for data transmission between sender and receiver with help of the ECC cryptography. This approach provides a better security solutions than existing cryptographic methods. This method ensures privacy ,data verification , authentication ,non –repudation which are achieved by this process.

REFRENCES:

1. Salmina sulthana , Elisa bertino, Gabriel Ghintia “A light weight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks” IEEE transaction in MAY 2015.
2. Hyo-sang Lim ,Yang –sae Moon , Elisa bertino “ provenance baesd trustworthiness assessment in sensor networks”proc.seventh Intl workshop,pp. 2-7-2010.

3. S.Sultana, E.Bertino, M.Shehab, “A provenance baes mechanism to identify malicious packet dropping adversaries in sensor networks” .proc : Int’l workshoppp.332-338,2011.
4. Kanathakumar Polingalur, Zubin Abraham, AlexX.liu “ Securing sensor nodes against side channel attacks”in 2011.
5. KiranP, S Sathish kumar,and Dr Kaviya “ A novel frame work using elliptical curve cryptogrqphy for extremely secure transmission in distributed privacy preserving data minig” in advanced computing: An international journal vol3,no2, March2012.
6. E. Bhiam,and A.Shamir,”Differntial fault analysis of secret key cryptosystem.volume1294 pages 513-525,1997.
7. Nicola Constantinescu “ Elliptical curve scalar multiplication”in analysis of mathematics and computer sciencein volume37in 20012.
8. V.S.Miller, S Sathish kumar “ use elliptic curves in advance cryptogoly-proceedings crypto’85 springerverlag 1986.
9. Kunma, Kaijie wu in “ LOEDAR: Low cost error detection and recovery scheme for ECC.
10. I.Bheriel,B.Meyer,V.Muller,”Differntisl fault attacks on elliptical curve cryptosystem” lecture notes in computer science”, springer – verlag 2000 pp 131-146.
11. A.Dominguez-oviedo and M.Anwar hasan “Errir detection and fault tolerancein ECSM using input randomization” IEEE transaction on dependable and secure computing,vol62009.