International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 07, July-2019

An approach to ensure integrity of sensed data using elliptic curve cryptography scheme

T.Yasasvi[1], A.Vanathi[2]

[1]Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, JNTUK, A.P, India,
[2]Professor, Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, JNTUK, A.P, India,

Abstract: Now a days in many applications wireless sensor networks are used. In Wireless sensor networks set of nodes are distributed for recording and for monitoring the physical environmental conditions, and the data is collected and organized at the central location by using one or more neighboring nodes. In sensor networks, mainly the energy is consumed for the purpose of data transmission. In sensor nodes for reducing the consumption of energy data aggregation is an important approach. Hence it has emerged as a basic approach for reducing the number of transmissions of sensor nodes, where the overall power consumption in the network also minimizes. But while performing the processes of data aggregation the data can be easily compromised by number of attackers. Hence security must be provided while performing aggregation. An identity based aggregate signature (IBAS) scheme is shown based on the elliptic curve cryptography scheme, where it uses a smaller key for providing an equivalent level of security. Because of its key size length ECC obtains faster computation and lower power consumption and also requires only small memory and bandwidth.

Keywords: Data aggregation, wireless sensor network, identity-based, aggregate signature.

I. INTRODUCTION

Wireless sensor network contains sensor nodes which are used to monitoring and for recording the physical environmental conditions. The recorded data is collected and organized at a central location. Because of limited resources wireless sensor network have resource constraints like limited energy, limited memory space etc [1].In sensor network, for data transmission the maximum of energy will be consumed. If data transmission processes is optimized, then the network lifetime increases. The data transmission will be optimized by using data aggregation. Data aggregation in wireless sensor networks has different approaches. In that cluster based approach is one of the data aggregation approaches, where in this approach the entire nodes are grouped into different clusters in the network. Cluster members will selects the cluster head in each cluster. Data which is received by the members in the cluster is aggregated by cluster head and it is send to base station which results in low consumption of energy. So data aggregation is used for reducing the consumption of energy in wireless sensor network. But aggregation of data has some security issues like data integrity, data forging [2]. So there is a need of tight security in WSNs and in modern wireless communication security is most important.

Challenges in wireless sensor networks:

- **Power Consumption:**
  Wireless sensor node, is a microelectronic device, where the power source is limited. The lifetime of Sensor node, strongly depends on battery lifetime.

- **Memory and Storage space:**
  In wireless sensor network the major limitation is space for storage and memory. Sensor is a small device with very less amount of memory and storage space. So it is important that the sensor node should be quite small.

- **Self Management:**
  Wireless sensor networks once established should work without any human intervention. It should need to manage the maintenance, network configuration and should repair by itself.

- **Security:**
  The most challenging issue in WSN is security. To protect travelling information between the network sensor nodes or among the sensors and the base station in sensor networks the confidentiality is required. Data must be accurate, and should reach user end without any data change.

- **Key management:**
  In wireless sensor network for the secure communication key is used. Constraint such as small memory capacity in WSN needs the reliable and efficient key for secure communication between all relevant nodes.

- **Data aggregation:**
  The major challenging issue in wireless sensor networks is data aggregation. It is an approach in which information is collected and show in summary form. An aggregation process is for collecting more information about particular groups like age, profession etc.

II. RELATED WORK

In 1984, Shamir [3] brought the Identity based Cryptographi concept which is used to eliminate the public key certificates. In 2001, Franklin and boneh [4] introduced an ID-based encryption scheme based on bilinear maps on the elliptic curve. In 2003, Bone et. [5] proposes the aggregate signature scheme which is used to compress the many signatures which are generated by different users on different messages can be aggregated into one signature which can reduce the bandwidth and also the storage cost. In 2006, Herranz [6] a deterministic Id based signatures for partial aggregation is proposed, where it allows the aggregation only when the signature come from the same signer. In 2008, Wang et. in [7] a practical aggregate signature schemes with constant pairing operations is proposed, but it achieves only partial aggregation. After that many id-Based aggregate signature schemes are presented. An Id Based Aggregate signature Scheme using Diffie-Hellmans is done by merging the highlights of both aggregate signature schemes and the ID Based cryptography. Diffie –Hellman is one of the key exchange algorithm where it needs to exchange a key. In this maintaining of both the keys are necessary. In Diffie-Hellman, exchanging the keys securely and also the predistribution of keys are always not possible. The key size of Diffie-Hellman is large so it requires large amount of power resources and also the space.

III. PROPOSED WORK

The proposed method was implemented in Wireless sensor network model by using the modules a sensor node, the base station and an aggregator node. The sensor nodes are grouped into different clusters. In that cluster head is one of the designated node in the cluster, where it also called as an aggregator node. The sensor node obtains the data and it is processed and will be transmitted to the aggregator node. Once the data from, all the nodes belongs to cluster has received then the aggregation process starts by the aggregator. Now the data which is aggregated will be encrypted by using the Elliptic Curve Cryptography algorithm which is a public key cryptography based security algorithm. In wireless sensor networks the main purpose of security is for not message encryption but from the prevention of changing the message content.

Elliptic Curve Cryptographic (ECC) Scheme:

In public key cryptography, Elliptic Curve Cryptography (ECC) is one of the cryptographic algorithm, in this Public key and a private key are the pair of keys, where the set of operations are associated with these keys in ECC for the cryptographic operations. In ECC only a particular user will knows the private key whereas for all the users who are the part of communication, the public key is distributed. Without exchanging the secret key, Elliptic Curve Cryptography (ECC) will provide secure communication. Nowadays in public-key cryptographic system the most popular system is Elliptic Curve cryptography (ECC). Main advantage of the elliptical curve cryptography is providing the same level of security using the small keys.

ID Based Aggregate Signature scheme using ECC:

Setup Phase:

In setup phase our proposed scheme contains a systemparameters param, and an initialization of a Master secret key (msk) and a security parameter I.

Key Generation Phase:

Generation of keys is an important phase were it is need to generate two keys they are public key and a private key using ECC 160 bit algorithm.

- Private key is generated by selecting an random integer‘d’ within a range [1, n-1].
- Public key is generated, using the formula u=d*p
  Where point on the curve is p
- Security Key I=u*d.

Signature Generation:

Generating the signature for a message (m) user inputs the senor id, corresponding private key and hash function.

h =HASH (m)
Where, HASH is an cryptographic hash function such as SHA-1

- For generating a signature select a random integers K.
  r =x1(mod n) [where x1=I*p]
  s =k-1(h+d*r)
- Signature of a message is (r,s).

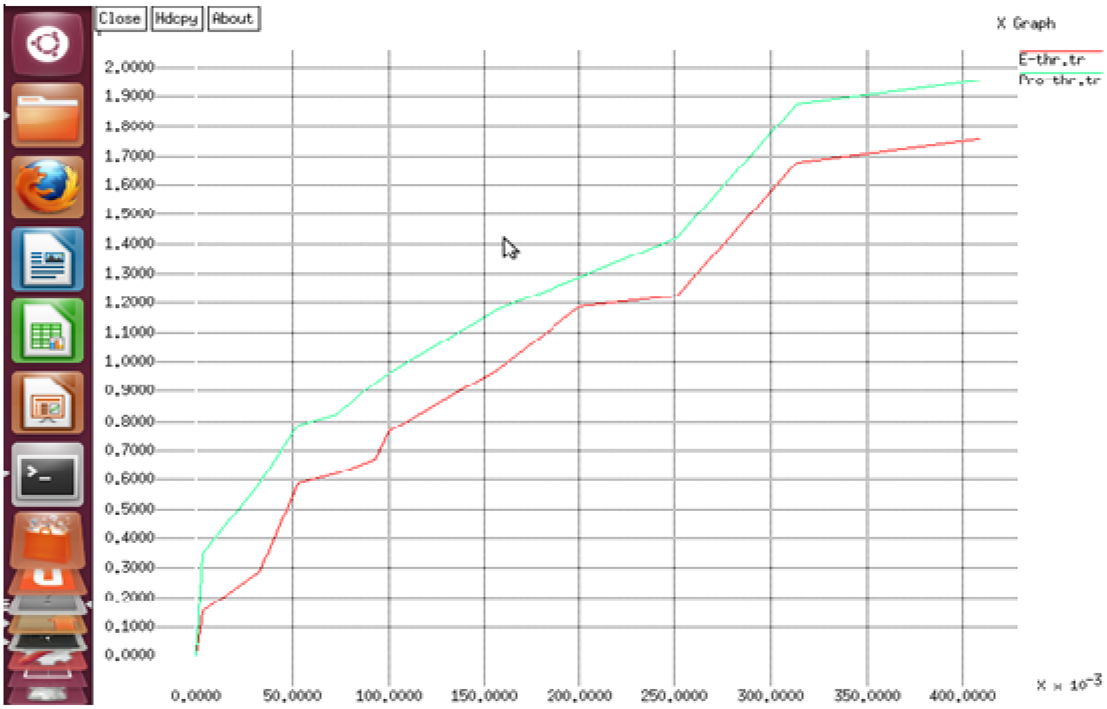
Signature Verification:
After receiving the signature the algorithm again calculates the hash function. Then it should be x1 =r (mod n). Therefore signature is valid otherwise it an invalid.

Aggregation Phase:
In this phase a set of sensor nodes belongs to one cluster, with different signatures from different users will run the algorithm to generate a aggregate signature from the setof (message m, id), pairs (r,s).

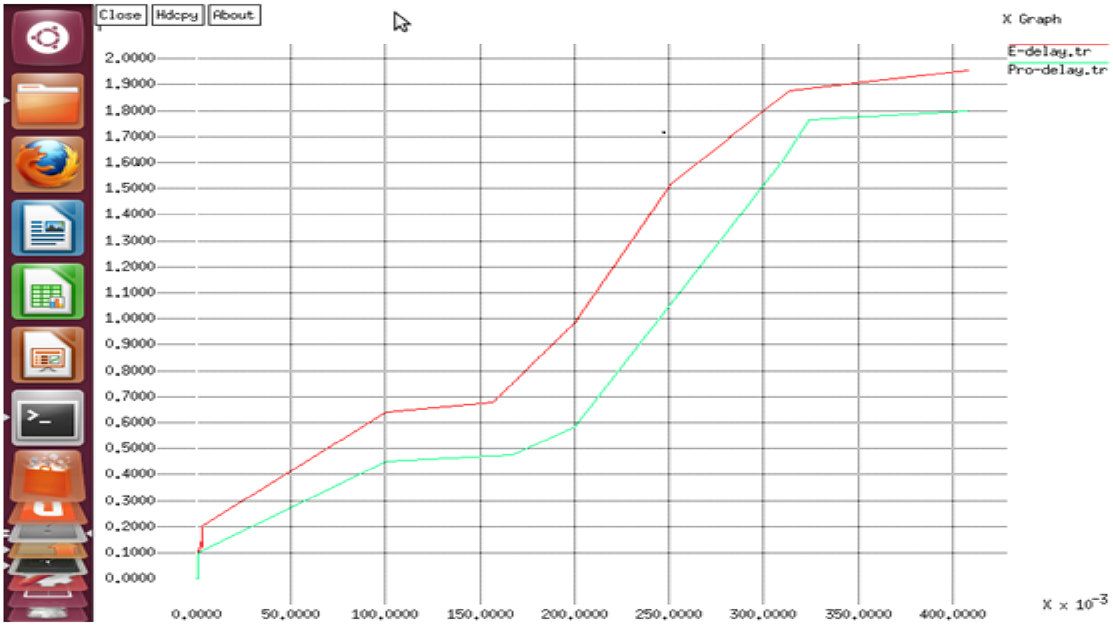
Aggregate Verification:
Verification of an aggregate signature scheme can be done by set (message m, id) and params. The algorithm checks whether the aggregate signature is valid or not on message m by id.

IV. PERFORMANCE REULTS

Throughput:
Throughput is defined as the maximum rate of production. When coming to the communication network, network throughput or the throughput is depends on the rate of successful message deliver over the network communication channel. When the number of packets is increased in the network, then the packets processed by each node per unit of time also increases, which results in the increase of throughput.

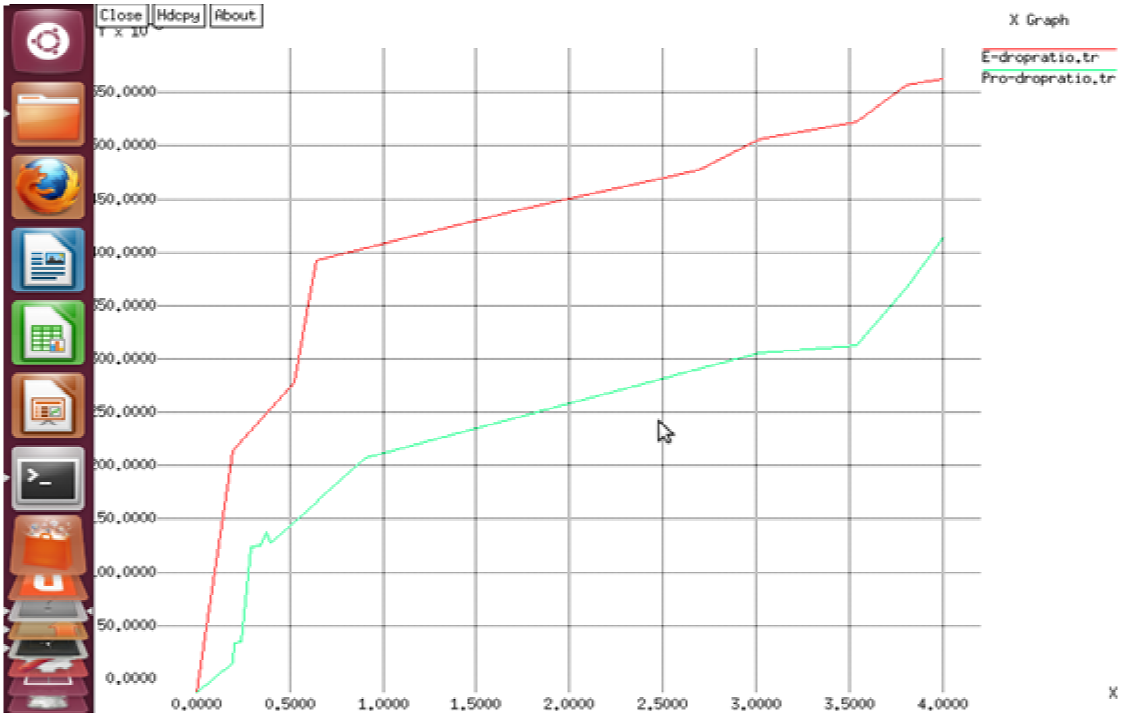


Packet Delay:
The packet delaying in a network is defined as the time taken for a packet to reach the destination after it leaving the source. To measure a packet delay, it is important to scaling the size of the packet which is depending ons the throughput. Delay of the packet is decreased when the throughput is increased.



Drop Ratio

If the node is compromised then the node which is compromised will drops all or some of the packets that are need to be forwarded. Sometimes the compromised node may also drop the data which is generated by it.



V. CONCLUSION

Elliptic Curve Cryptography (ECC) is a promising approach for meeting the security requirements in WSNs. The computational cost and also the speed of this algorithm are comparatively better than Diffe-Hellman. The key size of 160 bit elliptic curve cryptography provides the same level of security as Diffie-Hellman. Many advantages can obtain by ECC with the help of small key sizes which includes storage, bandwidth, speed and also an efficient power use. Using an shorter keys will lower the storage space requirement for key and fast arithmetic operations.

REFERENCES

[1]. Waltenegus-Dargie, Christian Poellabauer," Fundamentals of Wireless Sensor Networks", Wiley Series on Wireless Communications and Mobile Computing.

[2]. Xiaojiang Du, North Dakota State University and Hsiao-Hwa Chen, National Cheng Kung University "Security in Wireless Sensor Networks" IEEE Wireless Communication August 2008.

[3]. A.Shamir. identity-based cryptosystems and signature schemes. Proceedings of Crypto'84, LNCS Vol.196, pp.47-53,Springer-Verlag,1985.

[4]. D.Boneh and M.Franklin. Identity Based encryption from Weil Paring. Proceedings of Crypto' 01, LNCS,Vol.2139,pp.213-229,Springer-Verlag,2001.

[5]. D.Boneh, C.Gentry, B.Lynn and H.Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. Advances in Cryptology -Eurocrypt 2003, LNCS Vol. 2656, pp. 416-432, Springer-Verlag, 2003.

[6]. J.Herranz. Deterministic identity- based signatures for partial aggregation[J]. Computer Journal, 49(3): 322-330,2006.

[7]. Z.Wang, H.Chen, D.Ye, et al. practical identity- based aggregate signature scheme from bilinear maps. volume 13(6), pages 684-687. Shanghai Jiao Tong University Press 2008.

AUTHORS PROFILE

Tadi Yasasvi received the B.Tech Degree in Information Technology from Aditya College of Engineering & Technology, affiliated to Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India. Presently working for M. Tech Degree in Computer Science & Engineering at Aditya Engineering College, affiliated to Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India

Prof.A.Vanathi, Received her B.E in CSE from Bharadhidasan University, Trichy, T.N, India and M.E., in CSE from Anna University Chennai, TN, India. She is currently pursuing Ph.D in Acharya Nagarjuna University, Guntur. She was a lecturer, Assistant Professor and currently working as an Associate professor and Head Of the Department CSE, Aditya Engineering College, Surampalem, AP, India. Her research interests include Information Security, Mobile Computing, WSN and IoT. She is a Lifetime Member of CSI and ISTE.