An Implementation of Elliptic Curve Cryptography Algorithm for Secured Data Transmission In Wireless Sensor Network

Binay Kumar Pradhan
IIIT Bh
Odisha,India 751003
ID:B415019@iiit-bh.ac.in:

Pritish Gupta
IIIT Bh
Odisha,India 751003
ID:B415039@iiit-bh.ac.in:

Rudra Narayan Panda
IIIT Bh
Odisha,India 751003
ID:B415045@iiit-bh.ac.in:

Supratik Samal
IIIT Bh
Odisha,India 751003
ID:B415059@iiit-bh.ac.in:

Srichandan Sobhanayak
IIIT Bh
Odisha,India 751003
ID:srichandan@iiit-bh.ac.in:

Laxmikanta Mohanty
IIIT Bh
Odisha,India 751003
ID:laxmikantamohanty@gmail.com:

Sandeep Nigam
IIIT Bh
Odisha,India 751003
ID:A116018@iiit-bh.ac.in:

I. ABSTRACT

Remote sensor systems are a standout among the most exceptional advances in the most recent years of Computer Science and there are many research works that have satisfied the various security and energy needs of the sensor network. Since the data between the nodes are channelized through every other node in the network, wireless mesh topology is less secured and have many security and energy issues. In order to ensure correct system behavior and to eliminate the possibilities of network attack or interception, Encryption is used. Because of the nature of the sensor systems, their security prerequisites rely on the application being used and even the geological organization of the hubs. Diverse applications functioning over a same wireless sensor network stage generally have distinctive security necessities. Smaller key sizes can be used for less sensitive data which is a satisfactory way to limit the energy utilization.(unlike RSA and AES where computation time and memory were greatest issues) This paper centers around the execution of the scalar point multiplication, and this is the basic task of public key Elliptic Curve Cryptography(ECC). This cryptosystem has high security furthermore, great execution offered by ECC, compared to other options, for example RSA.Besides, this task can be utilized in digital signature(ECDSA), establishment of key(ECDH) and various encryption/decryption(ECIES) protocols.

Keywords-Message forwarding; RSA, ECC, Sensor Networks, ECDSA, ElGamal

II. INTRODUCTION

Remote Sensor System, where verification and Security is the real issue, for example, bits in the system which sends the sensor contributions to the client which they conveyed in a remote access. In view of the level issues and dangers are tended to.

The security in Wireless Sensor Networks share numerous qualities with customary remote specially appointed systems, there are key contrasts between the make-up and points of the two kinds of systems [1]. Although WSNs are monetarily practical, however in the meantime their computational necessities keep the immediate use of existing exceptionally dependable conventional remote security methods. Conventional remote system security principles are not appropriate for sensor arrangement as they are all, more demanding in memory, vitality and are computationally escalated. An essential angle is that the sensors in WSNs are unattended, conveyed in antagonistic condition, have limited energy and network topology is unknown making them prone to different types of attacks like eavesdropping, compromised node attacks, traffic-analysis, etc. These gadgets are extremely constrained in their vitality, calculation processor, data transfer capacity and correspondence abilities that impose strong restrictions on the processing capabilities and available memory for security, based on the executions. Various security procedures have been proposed to increase energy efficiency for designing better security protocol. By utilizing public key cryptography on exceptionally asset compelled gadgets which are because of impediments, for example, energy and memory limitations. It is derived that symmetric cryptography is favourable for applications that can not manage the cost of computational complexity. Effective cryptographic calculations with streamlined usage, regarding vitality utilization and computational overhead, are basic to amplify the battery lifetime of sensor hubs. Verification comes into the issue where every hub will confirm with the other hub through security codes. As WSN, where multiple motes deployed in the surveying region, it is hard to verify each bit as we think about it as a mesh topology. In order to make it more powerful, Public key

cryptography comes to be helpful. It is utilized and proposed from different encryption strategy which advanced from Das protocol, Adleman Calculation ,"Ron Rivest, Adi Shamir and Leonard specified in [3].(RSA)" and Diffe-Helman calculation with Dynamic client confirmation convention utilizing hash work, smart card through gateway. The few above can not ready to address or understand the insider attack.

Section II manages the requirement for the security and different approaches to unravel those issues inside the restricted needs. In Section III we clarify the outline of the Elliptic bend cryptography. We clarify the plan of our proposed plot alongside the methods utilized as a part of Area IV, while the verification of recreation results and execution measures are broke down in Segment V.

III. RELATED WORK

Different client validation conventions have been put forward for securing WSNs which limits the utilization of sensors. The receiver receives these tag pair. After verifying it accepts, else it disregards the message. It is hard to verify each bit as we think of it as mesh topology. Thus ECC(Elliptic Curve Cryptography calculation) which is recommended to comprehend this issue successfully and all the more proficiently recommended here in which can be conveyed to tackle the issue of public key encryption. But a few issues, for example, energy utilization is the significant issue with confinements of the SAMA (Source Anonymous Message Authentication) alongside elliptic curve in light of the Modified El Gamal Scheme [4]. The security issues are planned to comprehend the privacy, confirmation and respectability offering both link-layer and end to end security nodes. It is said to accomplish the conclusion to end security in multihop match keys shared between hubs from source and goal. This area based key administration plot for the remote sensor arrange work for the safe neighborhood verification on the multihop pairwise key strategy which are conveyed as the calculation [4].

Authentication scenarios analysis of the cost on the security services provided with an assumed unique device IDs of the 4-bytes and 16-bytes challenge as with ECDSA-160 requires 89.3 percent yet RSA-1024 of the 97.5 percent of energy utilization [6]. MoTE-ECC library is equipped with an AVR processor of 8bit capacity. Although it is a highly optimized ECC library, it is quite scalable for Memsicâs MICAz motes and other sensor nodes. [5] which solves the library related issues based on computation limits with better authentication features. In [3] displayed the rest client confirmation convention that utilizations elliptic bend cryptography (ECC) in WSN conditions, which is more secure in execution as the key size is little nearly to Ron Rivest, Adi Shamir and Leonard Adleman Algorithm (RSA) and calculation issue in the asymmetric or public key cryptography is likewise settled to the restriction as similarly appeared in the Table.1. ECC relatively considered with Public Key Cryptography(PKC) conspire and different calculations which are similarly arranged based on the security and danger rates and time to break the code where size of key

TABLE I: TABLE I. KEY SIZES OF ECC IN COMPARISON WITH OTHER PUBLIC KEY CRYPTOGRAPHY

BITS	ECC	RSA/DSA	MIPS-years to attack	Protection on life time
80	160	1024	10^12	Until 2010
112	224	2048	10^24	Until 2030
128	256	3072	10^28	Beyond 2031
256	512	15360	10^66	Beyond 2031

in bits as in the primary segment and assurance till the best machine deciphering the code as the validity said in the last section. In Shi et al's. convention, the sensor does different cryptographic tasks, for example, hash work assessments(one way), scalar-point multiplications, arbitrary number creations, and map to-point hash work assessments in Elliptic curve cryptography calculation. Scalar-point multiplications are considerably more costly than hash work assessments. In like manner, it is important to change the convention with the goal that the sensor can examine if the information is from a genuine client, not from a traded off mote[4]. The significant issue in the remote sensor network discusses the vitality preservation of the bit. It evaluates the energy expenses of verification and key trade in light of public key cryptography on a different stages [8] The advantages of transmitting smaller ECC keys and testaments will thus be more critical and perfect.

IV. OVERVIEW OF ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic bend cryptography is a cryptography strategy which incorporates the utilization of the elliptic curve numerical measures in the cryptography. Cryptography provides confidentiality, Confirmation, Non-repudiation and Integrity. The pith of any computation under cryptography is the "seed" or the "key" used for scrambling/unscrambling the information. In perspective of the key, cryptosystems can be organized into two characterizations: "Symmetric"and "Asymmetric". In Symmetric Key Cryptosystems, we use a similar key that is used for both encoding and furthermore the relating unscrambling. This system of key open key encryption as showed up in the Fig.1.

Elliptic Curve (EC) frameworks as connected to cryptography were first released in 1985 autonomously by "Neal Koblitz and Victor Miller" [7]. The discrete logarithm issue on elliptic bend bunches is accepted to be more troublesome than the comparing issue in (the multiplicative gathering of nonzero components of) the hidden limited field.

A. Definition of Elliptic Curves

An elliptic curve over a field K is a non singular cubic curve with 2 factors, f(x,y) =0 having a rational point (which might be a point at infinity). The field K is normally taken to be real, rational, complex numbers and mathematical expansions of rational, p-adic numbers, or a limited field. Elliptic bends bunches for cryptography are checked with the fundamental fields of Fp (where p greater than 3 is a prime) which typical bend condition are specified in the Fig.1. also, F2m (portrayal in binary with 2m number of components). An elliptic curve

is a plane bend characterized by an equation of the form(1). $y^2 = x^3 + ax + b...(1)$

An elliptic curve E (Fp) over a limited area Fp is specified by the variables a, b component of Fp (a, b satisfies the relationship 4a3+27b2! = 0), comprises of the range of points (x, y) belonging to Fp, fulfilling the equation $y2 = x3+ax+b$ The group of points on E (Fp) incorporate point O, and that is the point found at infinity and that is the identity component under addition. The Addition operator is explained over E(Fp) and it can be visible that E(Fp) forms an abelian group under addition.

Algorithm for encryption:

- Enter a prime no p which is used to keep the points in GF (n=1)
- Collect the points(y*y) which are quadratic residue of (x*x*x)+ (a*x)+b
- Enter e1
- A random number d is generated which is private key
- Find public key e2=d*e1
- Enter the message P
- A random number r is generated for encryption
- Find c1=r*e1
- Find c2=P+(r*e2)
- c1 and c2 are the encrypted points

Algorithm for decryption:

- Enter encrypted points c1 and c2
- Enter curve parameter a and b to form the same curve as encryptor
- Enter the prime no p to keep points in GF (n=1)
- Enter private key d
- Decrypted message (P) = c1-(d*c1)

V. PROPOSED SYSTEM AND SIMULATION

Message encryption at the host before routing it over network using RSA is an example. The upgraded plot is utilized as a part of this ECC in the multihop protocol in view of the basic highlights of utilizing Modified ElGamal Scheme [4] over elliptical curves. Adjusted ElGamal states that utilizing the numerical formula with the functionality of using the pre-computational of producing the elliptic curve focuses over Fp which are defined as the E which all these are represented as G=(xG,yG) as the base point on the E(Fp) whose order is very large value N. Client chooses an irregular whole number dA within the range where the executing SHA-1 for hash value is generated for signature and confirmation. Here the calculation which utilizes private key is incentive to scramble the message with secured signature validation and additionally secured message transmission. An indistinguishable key an incentive from kA is utilized to decode the message. The proposed calculation utilizes elliptical curve over ElGamal method.

Elliptic Curve involves two main features solving authenticity of the node sending message by signature method and encryption of message with higher bit at less computational time. Here we propose the encryption of message at a node before transmission. The data packet route is simulated using two nodes in a network. Another node is present in the network during simulation for capturing the packet lost during the transmission.

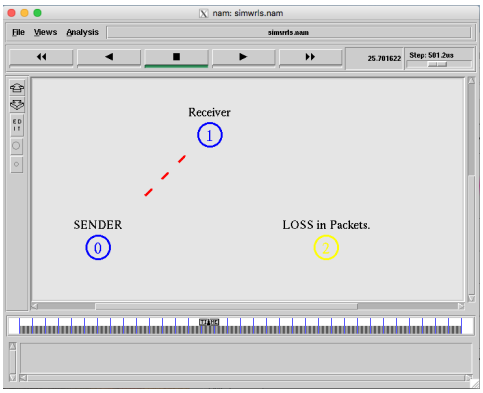

Fig. 1: Packets sent

In Fig. 1, a duplex link is established between two nodes and sender sends data to the receiver using TCP of transport layer protocol.

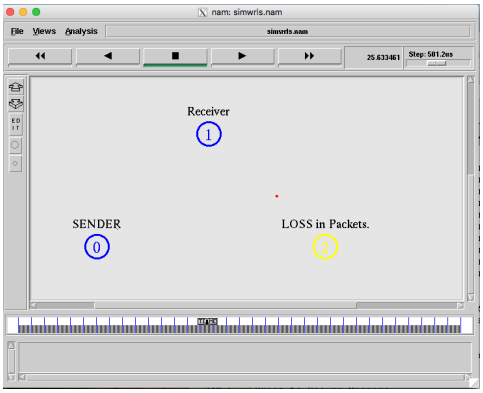

Fig. 2: Lost Packets

Fig. 3: Data route

In Fig. 2 a simplex link is established between the sender and another node in the network that acts as a sink for every loss packets. The connection between them is set using UDP of transport layer protocol. In wireless sensor network after

transmission of data is complete at sender and receiver using private key decrypts the message using the same elliptic curve the data route is plotted using X-graph in Fig. 3 with packet size vs time interval.

VI. FUTURE WORKS AND CONCLUSION

The future work includes C++ implementation of ECC algorithm need to be implemented using tcl script so as to allow a node to encrypt the message and allow another node to decrypt the message.Evaluating the performance in terms of delay in encryption and decryption.Enhanced ECC Algorithm allowing authentication of a node during decryption.

In this paper, Transmission of data is simulated using NS2 and data (message in terms of points from the Elliptic Curve) is encrypted using ECC Algorithm. Final output generated is a simulation of data transmission between 2 nodes and a third node is defined as a sink for capturing loss in packets using NAM and data delivery between the 2 node is plotted in X-graph and displayed. Also encryption and decryption using C++ using RSA and ECC algorithm is submitted.The projects aimed to implement a high security algorithm(ECC) to overcome the size and energy issues present in aforementioned algorithms.

VII. REFERENCES

[1] Doomun, M. Razvi, and K. M. S. Soyjaudah."Analytical Comparison of Cryptographic Techniques for Resource- constrained Wireless Security", IJ Network Security 9.1 (2009): 82-94.

[2] Mana, Mohammed, Mohammed Feham, and Boucif Amar Bensaber", Trust Key Management Scheme for Wireless Body Area Networks", IJ Network Security 12.2 (2011), pp. 75-83.

[3] Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung , Junghyun Nam and Dongho Won, "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", Sensors 2014, pp. 10081-10106.

[4] Jian Li, Yun Li, Jian Ren, Senior Member, IEEE and Jie Wu, Fellow, "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks", IEEE, Vol 25 (2014) , pp. 1223- 1232.

[5] Liu Z., Wenger E. Grobschaadl J. "MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks", In Applied Cryptography and Network Security, (2014) pp.361-379.

[6] Tsiftes N., Dunkels A., He Z. and Voigt T. "Enabling large-scale storage in sensor networks with the coffee file system", In Proceedings of the 2009 International Conference on Information Processing in Sensor Networks (2009), pp. 349-360.

[7] Osterlind F., Dunkels A., Eriksson J., Finne N., Voigt T. (2006, November). "Cross-level sensor network sim-ulation with cooja". In Local Computer Networks, Proceedings 2006.

[8] Wander A. S., Gura N., Eberle H., Gupta V. and Shantz S. C. (2005). "Energy analysis of public-key cryptography for wireless sensor networks". In Pervasive Computing and Communications, 2005.

[9] Yao, Wenbin, Si Han and Xiaoyong Li. "LKH++ based group key management scheme for wireless sensor network." Wireless Personal Communications 83.4 (2015): 3057-3073.

[10] Liu, Yuxin et al. "ActiveTrust: Secure and trustable routing in wireless sensor networks". IEEE Transactions on Information Forensics and Security 11.9 (2016): 2013-2027.