ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

Mutually Authenticated Control Scheme Using Enhanced ECC In Wireless Sensor Network

R.Ranjitha[#1], k. Indumathi[*2]

UG Student [#1],Assistant Professor, Department of Computer Science and Engineering [2]
AAA College of Engineering and Technology, Sivakasi, India
[1]ranjitharcse@yahoo.com, [2]kindumathicse@gmail.com

Abstract— Wireless sensor networks (WSN), sometimes called Wireless Sensor-Actuator Networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions and to cooperatively pass through the network to the main location. These motes in the network are restricted to memory and energy issues. Data encryption is an important issue and widely used in recent times to protect the data over internet and ensures security. One of the mostly used public key cryptography technique is the Elliptic Curve Cryptography. ECC is more efficient with the key size. It is less vulnerable to security threat attacks. A Modified effective implementing enhanced ECC with features like Elliptic Curve Digital Signature Algorithm (ECDSA) is to add more secure and effective data transfer along with key cipher of the text information. The enhanced scheme used in this ECC is Modified ElGamal Scheme over elliptic curves.

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called Wireless Sensor-Actuator Networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions and to cooperatively pass through the network to the main location. A usual WSN systems formed by combining these autonomous devices, or nodes with routers and a gateway.

The dispersed measurement nodes communicate wirelessly to a central gateway, which provides connection to the wired world where the user can collect, process, analyse and present your measurement data. Routers to gain an additional communication link between the end nodes and the gateway for extend distance and reliability in a wireless sensor network.

The Wireless sensor is networked and scalable, require very little power. It is also smart and software programmable, and also able to fast data acquisition, reliable and accurate over the long term, but costs little to purchase and install, and requires nearly zero maintenance. Collect, record and analyze data. In healthcare, able to collect patient.

The major issues that affect the design and performance of a wireless sensor network are as follows:

Security is quite challenging issue as WSN is not only being deployed in battlefield applications but also for surveillance, building monitoring, burglar alarms and in critical systems such as airports and hospitals. Confidentiality is required in sensor networks to protect information traveling between the sensor nodes of the network or between the sensors and the base station; otherwise it may result in eavesdropping on the communication. In sensor networks, it is essential for each sensor node and the base station to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. A false data can change the way a network could be predicted.

Quality of service is the level of service provided by the sensor networks to its users. WSN are being used in various real time and critical applications, so it is mandatory for the network to provide good QoS. Though, it is difficult because the network topology may change constantly and the available state information for routing is inherently imprecise. Sensor networks need to be supplied with the required amount of bandwidth so that it is able to achieve a minimal required QoS. Traffic is unbalanced in sensor network since the data is aggregated from many nodes to a sink node. QoS mechanisms should be designed for an unbalancedQoS constrained traffic. Many a time routing in sensor networks need to sacrifice energy efficiency to meet delivery requirements. Even though multihops reduce the amount of energy consumed for data collection the overhead associated with it may slow down the packet delivery. QoS designed for WSN should be able to support scalability. Adding or removing of the nodes should not affect the QoS of the WSN.

Wireless sensor networks once deployed should be able to work without any human intervention. It should be able to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

manage the network configuration, adaptation, maintenance, and repair by itself.

Sensor Networks consists of hundreds of thousands of nodes. It is preferred only if the node is cheap. Flash memory is advised to be used in sensor networks as it is inexpensive. The central processing unit of sensor node determines energy consumption and computational capabilities of a node. In order to provide the flexibility for CPU implementation, large number of micro-controller, microprocessor and FPGAs (field programmable gate arrays) are available.

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type [29] has an 16- bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. With such a limitation, the software built for the sensor must also be quite small.

II. Related Work

To reduce the resource use of sensors and enhance the security of WSN's, security enhanced user authentication protocol using ECC for WSN have been proposed. Even though this protocol provides security against session key attack, insider attack, Reply attack, Man in middle attack it takes more time consumption and it is not suitable for resource constrained WSN [3].

An unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves have been proposed to secure against adaptive chosen-message attack in the random oracle model. Here the key management is the major issue for this authentication scheme [4].

The public key algorithm such as ECC is considered as the advantage over other algorithms by means of energy consumption, minimum security key bits used and the bytes of data transmitted. Yet it has some patent problems, especially for binary curves. Standards aren't state-of-the-art, particularly ECDSA which is kind of a hack compared to schnorrsignatures [6].

In public key it's observed that ECC is a software base platform for typical WSN but it is complex. So the new cryptography like pairing based cryptography is considered for providing optimal solution for public key and it gives sufficient energy. Pairing security is low and also it have medium bonding, medium security and comparatively low efficiency [13].

III. Overview Of Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC includes a variants of many cryptographic schemes that were initially designed for modular numbers such as ElGamal encryption and Digital Signature Algorithm.

It is believed that the discrete logarithm problem is much harder when applied to points on an elliptic curve. This prompts switching from numbers modulo p to points on an elliptic curve. Also an equivalent security level can be obtained with shorter keys if we use elliptic curve-based variants. The shorter keys result in two benefits −

- Ease of key management
- Efficient computation

These benefits make elliptic-curve-based variants of encryption scheme highly attractive for application where computing resources are constrained.

History Of ECC

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths.

At the time of its discovery, the ECC algorithm was described and placed in the public domain. What others found was that while it offered greater potential security it was slow. Certicom focused its efforts on creating better implementations of the algorithm to improve its performance. After many years of research, Certicom introduced the first commercial toolkit to support ECC and make it practical for use in a variety of applications.

Certicom ECC Challenge offers an opportunity for people around the world to create new methods of attacking the algorithm and exposing any weaknesses. The longer an algorithm stands up to attack the more confidence developers have in its ultimate security. The ECC Challenge started in November 1997 and still runs today.

ECC Key Generation:

The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

$$Q=d*P$$

Where

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

d = The random number that selected within the range of (**1 to n-1**).

P = The point on the curve.

Q = The Public key.

d = The Private key.

ECC Encryption:

Step1:Define a Curve

Step2:Generate public private Key pair using that curve, for both sender and receiver

Step3:Generate a Shared secret key from the key pair

Step4:From that shared secret key, generate an encryption key

Step5:Using that encryption key and symmetric encryption algorithm, encrypt the data to send

Let 'm' be the original message and 'm' has the point 'M' on the curve E,k be the randomly selected number ranging from[1-(n-1)].

Two ciphers c1,c2 be generated by using

C1 = k * P

C2 = M + k * Q

ECC Decryption:

The sender will either share the curve with receiver or sender and receiver will have the same use for the same curve type. Also, sender will share its public key with receiver.

Step1:Generate public private Key pair using the same curvefor that curve.

Step2:Regenerate a shared secret key using private key of receiver and public key of sender.

Stepe3:From that shared secret key, generate an encryption key.

Step4:Using that encryption key and symmetric encryption algorithm, decrypt the data.

C1, C2 can be decrypted by using the following formula:

M = C2 – d * C1 where M is original message

IV. PROPOSED SYSTEM

The enhanced scheme used in this ECC in the multihop protocol classified based on the simple features of using Modified ElGamal Scheme over elliptic curves. Where modified Elgamal states that using the ElGamal mathematical formula used with the functionalities of using the pre-computational of generating the Elliptic curve points over Fp which are defined as the E which all these are represented as the G=(xG,yG) as the base point on the E(Fp) whose order is a very large value N. User selects a random integer dA which is of the range. Where the implementing the SHA-1 for hash value generation for signature generation and verification. Here the algorithm which uses private key value to encrypt the

Step 1: Verify r and s are integers in the range [1, n –1]

Step 2: Compute e = SHA-1(m).

Step 3: Compute $w = s_{-1} \bmod n$.

message also with secured signature authentication as well as secured message transmission, while the same key value as kA is used to decrypt the message. As the proposed algorithm uses Elliptic curve over Elgamal method.

A. Enhanced Elliptic Curve Algorithm

This involves two main features solving authenticity of the node sending message by signature method and effective message encryption.

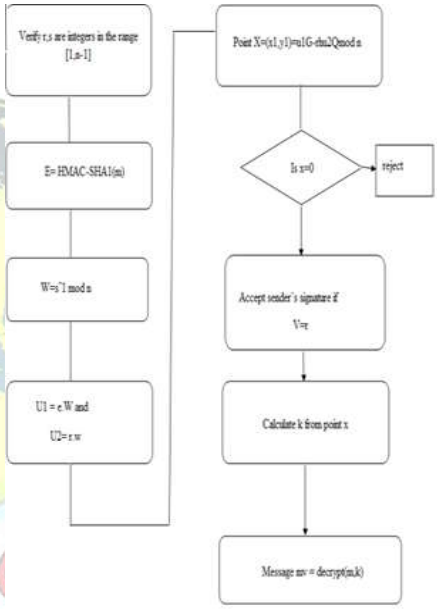

Fig 1.Enhanced ECC signature generation algorithm

The below algorithm for signature generation algorithm represented in Fig. 1.

Step 1: Selects a Random number k □ [1, n – 1].

Step 2: Computes Point kG = (x, y) and r = x mod n, if r = 0 then goto Step 1.

Step 3: Compute t = kA–1 mod n.

Step 4: Compute e = SHA-1(m,r), where SHA-1 denotes the 160 bit hash function.

Step 5: Compute s = r*d*hA + kA mod n, if s = 0 goto Step 1.

Step 6: The signature of message m is the pair (r, s).

Step 7: Source node sends Sink node the message m and her signature (r, s).

Step 8: Message encryption with kA using block obtaining a encrypted message.

Step 4: Compute $u_1 = e.w$ and $u_2 = r.w$.

Step 5: Compute Point $X = (x_1, y_1) = u_1G - rhu_2Q \bmod n$. If X = O, then reject the signature.Else compute $v = x_1 \bmod n$.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

Step 6: Accept Source node's signature if v = r.

Step 7: Message decryption with calculating the k_A as a key for block cipher decryption.

V. Simulation Result

Performance measure of the algorithm are done with the implementation of the concept in the Nerwork Simulator. In the following experimentation of this implemented algorithm which analyzed based on the packet delivery ratio and packet transfer delay as the measuring parameters. For better encryption and decryption result output

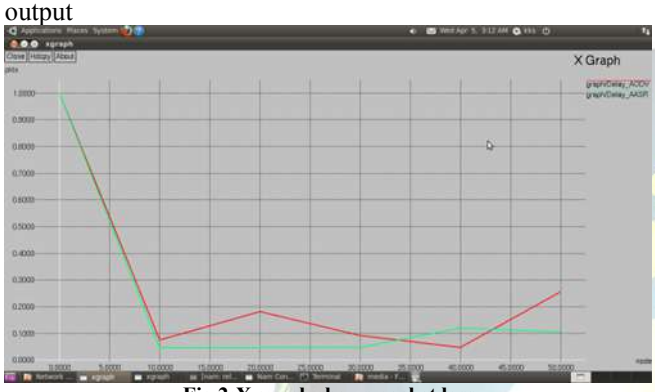

Fig 2:X graph shows packet loss

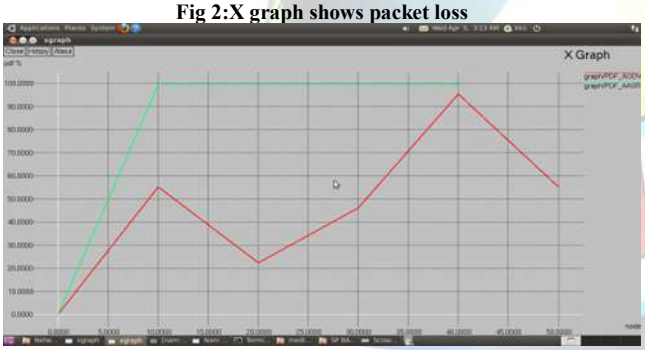

Fig 3: X graph shows packet delivery ratio

VI. Conclusion And Future Work

As the large demands of security features needed for the wireless sensor network with Network simulator and using Elliptic Curve Cryptography with enhanced features such as key generation and signature verification is done and analyzed with other public key cryptography scheme and compared along with the enhanced scheme with limited computation and a delay in the communication between the source and sink through the intermediate nodes in the mesh topology is analyzed and compared.

As a part of future work, it is to be implemented with high security which is provided by any signature algorithm like SHA-512. And also to test our proposed technique on large environment system with various attacks like Sybil attack, wormhole attack.

Acknowledgement

The author wish to thank the Management and Principal of AAA College of Engineering and Technology, for the support in carrying out this project work.

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,(2014),' Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography', Sensors 2014, 14, pp. 10081-10106.

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

[5]. Ms.Sneha M. Sakharkar (2014), Prof. R. S. Mangrulkar, Dr. Mohammad Atique.' A Survey: A Secure Routing Method for Detecting False Reports and Gray-hole Attacks along with Elliptic Curve Cryptography in Wireless Sensor Networks. 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[6]. 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. PerCom 2005. Third IEEE International Conference, pp.324-328.

[7]. Asha Rani Mishra, Mahesh Singh (2012).' Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network..In International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 1 Issue 3.

[8]. Ravi Kishore Kodali(2014).' ECC with Hidden Generator Point in WSNs '.In 2014 IEEE Region 10 Symposium 978-1-4799-2027-3/14

[9]. Merad Boudia Omar Rafik, Feham Mohammed (2013).' The impact ofECC's scalar multiplication on wireless sensor networks'.

[10]. Daehee Kim, Student Member, IEEE, and Sunshin an, Member, IEEE (2016).' PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks'. IEEE sensor journal, VOL. 16, NO. 8, APRIL 15, 2016

[11]. Ibrahim Nadir,(2015).'Establishing Symmetric Pairwise-keys Using Public-Key Cryptography in Wireless Sensor Networks (WSN)'.

[12]. Y. Bevish Jinila, K. Komathy (2014), "Distributed and secured dynamic pseudo ID generation for privacy preservation in Vehicular ad hoc networks", Journal of Applied and Theoretical Information Technology, Vol. 66, No.1, pp. 126 – 134, ISSN : 1992-8645.