IOT applications for high security WSN using Elliptic Curve Cryptography Algorithm

Prof.Shamshekhar.S Patil
Assoc.Professor
Dept.of.CSE
Dr.AIT, Bengaluru,India

Ashwini .K.G
M.Tech
Dept.of.CSE
Dr.AIT, Bengaluru, India.

ABSTRACT:

In an earlier day's security protocols are not feasible for wireless sensor networks(WSN) because of their resource constraint nature, here security part is challenging and solution is required to be addressed. Now a day's wireless sensor networks are the active area of research and owed to large number of applications. The main aim is to increase the robustness of a network against attacks such as Man in Middle using the ECC (elliptic Curve Crypto system). Elliptic Curve Cryptography has been considered a feasible cryptographic technique due to its low computational overhead Securing WSN in the IoT application permits by proposing the mechanism that ensures the connectivity among devices and with lower costs in terms of consumption of energy and resource usage.

Keywords – Wireless Sensor Network (WSN), Internet Of Things(IoT), Digital Signature(DS), ECC(Elliptic Curve Cryptography).

INTRODUCTION:

In the Internet of things, wireless sensor network has been extensively discussed and security part is still in the list of relevant challenges and solution and it is need to mentioned and improved in the IOT (internet of things). WSN comprises of huge number of nodes and those nodes are jammed and set up either inside the occurrence or very near to it.

Wireless Sensor Network has low cost, low power devices used in sensing applications has several challenges, like security being conserved over the attacks and it update the data and communicate between sensors.

WSN has low cost, low power devices used in sensing applications has several challenges, like security being conserved over the attacks and it update the data and communicate between sensors.

WSN has low cost, low power devices used in sensing applications has several challenges, like security being conserved over the attacks and it update the data and communicate between sensors.

Using ECC in wireless sensor networks gives the efficient results because ECC use a smaller number of bits for authentications it will help in both hardware and software applications.

ARCHITECTURE OF WSN:

Components of WSN (Wireless Sensor Network) listed below:

1. **Security Manager**

   This component is responsible for generation, key storage and management.

2. **Network Manager**

   It is responsible for network configuration and management of Routing table and also schedule the communication among devices and update the stability of network.

3. **Field devices**

   Enables the network process and to be able of routing packets.

4. **Gateways**

   Gateway allows the communication among field devices and nodes.

We have creating two nodes for communication and input the values to that nodes and creating two private keys for that nodes and one prime value to be added , after enter all the input values to the equation we can import file for encryption if the values are fitted to the equation then it will be encrypt the message otherwise it shows the assertion error , when values will be fitted to equation we import file to encryption if it matches it gives the digital signature for the security purpose and message will be decrypted.

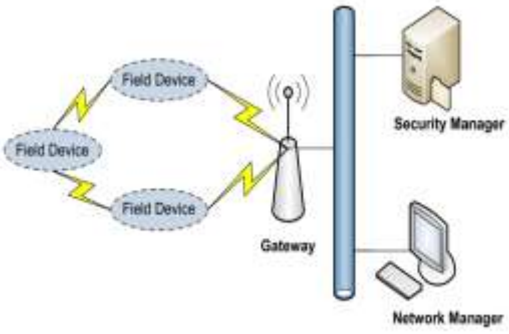


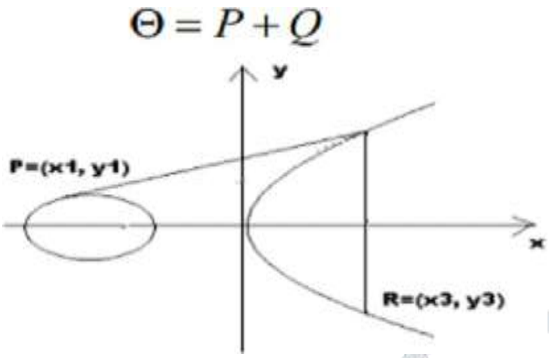
Figure 1. WSN Architecture.

PROPOSED METHOD:

In a proposed system is able to authenticate and also it manages the keys and communication between the sensors. In this approach we need three steps those are

- Deployment of network
- Encryption and decryption mechanisms
- Recognition of neighbor

These steps adopted to implement the project and encryption and decryption process ensures the security through digital signature.



According to resource constraints, the mechanism gives the security to data and attacks from internet will prevent. Each sensor will be integrated with wireless node those are call it as end devices. Those devices form a mesh networks and transfer the data through network.

Almost all the wireless networks connected through the gateways and they will be protected by powerful and in a unique gateway. To ensure the privacy and security innovative mechanism to be proposed.

In figure 2 We have creating two nodes for communication and input the values to that nodes and creating two private keys for that nodes and one prime value to be added , after enter all the input values to the equation we can import file for encryption if the values are fitted to the equation then it will be encrypt the message otherwise it shows the assertion error , when values will be fitted to equation we import file to encryption if it matches it gives the digital signature for the security purpose and message will be decrypted.

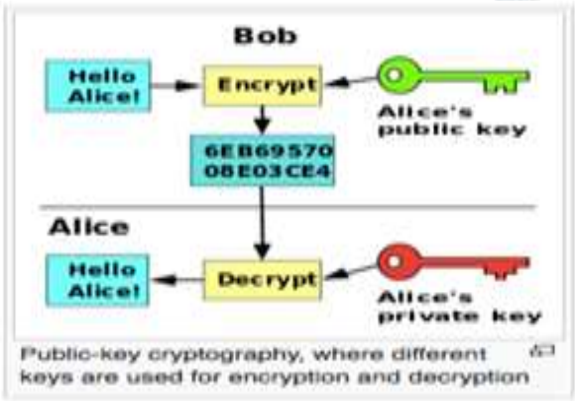


Fig.2 showing two sensor nodes communicating each other.

Equation of ECC $y2 = x3 + ax + b$ here A and B is having different values and varies in curves. ECC having a small key size as we know 162 bit key , p is a prime number

In ECC we are having smaller key size i.e, 160-bit key and it will be more secured compared to RSA , RSA is having 1024-bit key.

Point Multiplication

In this we have to do the multiplication of points those are point P multiplied with point K and Q in same elliptic curve.

$$Q = KP$$

Point multiplication is completed by two steps those are listed below.

STEP 1: Point Addition

In this we add points P and Q and result will be obtained in θ

$$\boldsymbol{\theta = P + Q}$$

STEP 2 : Point Doubling

Fig 3 : Here, we have to do addition of point P and it is obtained in Point R.

(R = 2P)

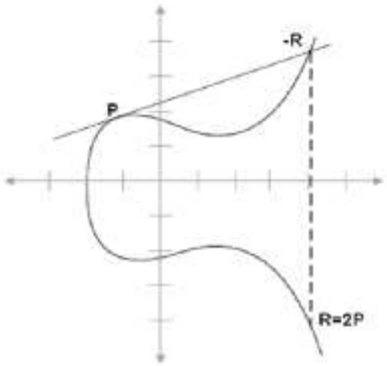


Fig 4 : Second point R on the curve; and the Point R is the point we want to compute.

ELLIPTIC CURVE DIGITAL SIGNATURE (ECDSA)

We use ECDSA i.e., operates on elliptic curve cryptography to communicate node A to node B both the nodes agree with Elliptic curve domain parameters.

ECDSA algorithm is used to provide the authentication between the hosts.

Stages of ECDSA is listed below -

- **Generate a key**
- **Generate a Signature**
- **Verification of Signature**

Generate a Key using ECDSA

An entity A's is An connected with a particular set of Elliptic curve domain parameters D= (a,b,n,h,G,q,FR). E is an elliptic curve, and q is a prime order i.e., E(Fq). Point A does the following steps.

Step 1 : choose any number for d to the interval[n-1, 1].

Step 2 : Calculate Q=dP

Where Q is Public key and A is private Key.

Generation of Signature in ECDSA

An entity A and message m and domain Parameters D.

Where D= (FR, a, b, n, h, G, q).

An entity A does the following steps

Step 1 : Select any number k in interval

[n-1,1].

Step 2 : Calculate $kP = X1, Y1$ and $r = X1$

mod (n), If r=0 then go back to step 1

Step 3 : Calculate k^(-1)mod (n).

Step 4 : Calculate s = $k^{-1\{h(m)+dr\}mod}(n)$,

if $s = 0$, go back to step1.

The signature for the message m is the pair of integers (r, s).

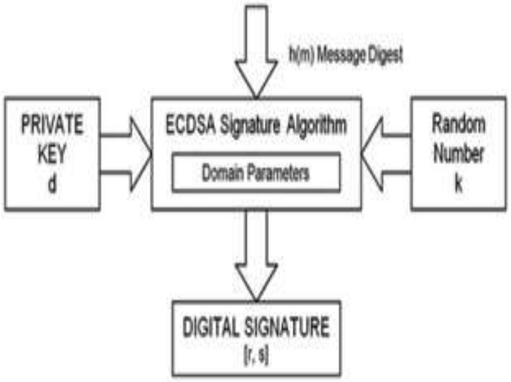


Fig 5 : Digital Signature Generation

Verification of Signature in ECDSA

Validate the verification of Signature

For A (r, s) on message m

For B, it will copy the domain of A and D = (FR, b, a, h, n, G) and public key Q.

Step 1 : Substantiate r and s are numbers in the

interlude [n-1,1]

Step 2 : Calculate $w = s^{-1}mod\ (n) and\ h(m)$

Step 3 : Calculate $u1 - h(m)mod(n)$.

Step 4 : Calculate $u2 = rW\ mod\ (n)$.

Step 5 : Calculate $u1P + u2Q = (x0, y0) and\ v = x0\ mod\ (n)$.

$if\ v = r$ then signature will be accepted.

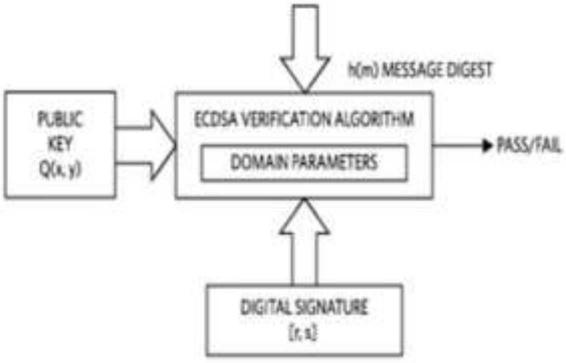


Fig 6 : Digital Signature Verification

ECDH (Elliptic Curve Diffie Hellman)

An unsigned agreement of key protocol agrees two parties in Diffie Hellman Elliptic Curve, those two parties having a private and public key in elliptic curve, to launch the shared secrete key, and the channel is not secured. The shared secrete is used directly as key or it may use different key for encryption using symmetric key cipher.

Using Public and Private keys, Public information that is shared between the two parties

Shared secrete keys is do not give the permission to access of private details for third parties and also not have permission to access public data. Those two parties will compute the shared secrete.

ECDH Overview

By using Diffie Hellman Elliptic Curve parameters we can create the shared secrete between the two parties A and B.A and B have to agree with the elliptic curve domain parameters.

Private Keys dA and QA and Public Keys dB and QB are the two key pairs of B. A and B Consist of Private key d, and Public Keys $Q = dG$

Step 1 : A calculates $k = dA \times QB = (xK, yK)$

Step 2 : B calculates $L = dB \times QA = (xL, yL)$

- Hence dBdAG=dAdBG=dAQB=dBQA.
- Therefore $L = K\ and\ xL = xK$

The Shared Secrete key is xK

We are not able to find the public key K i.e., private key of (dA or dB) and the third party will not be obtaining the shared key.

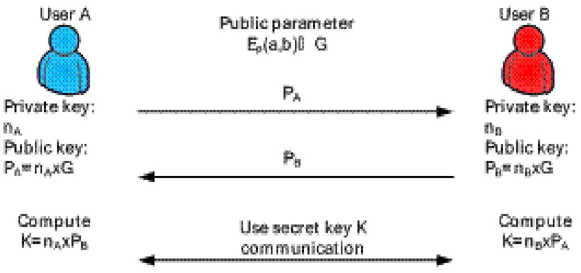
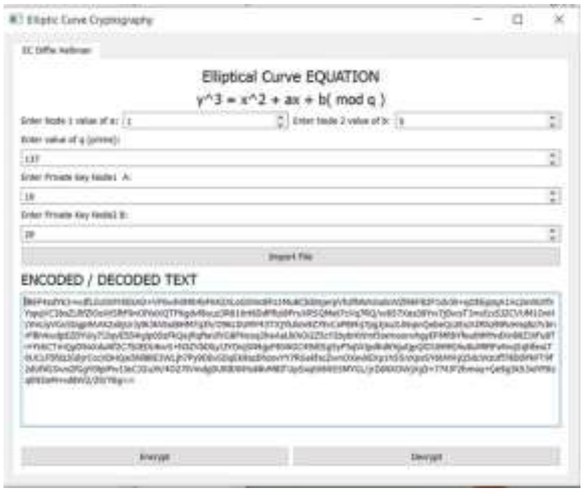


Fig 7 : Private and Public Keys Generation

RESULT:



Elliptical Curve EQUATION

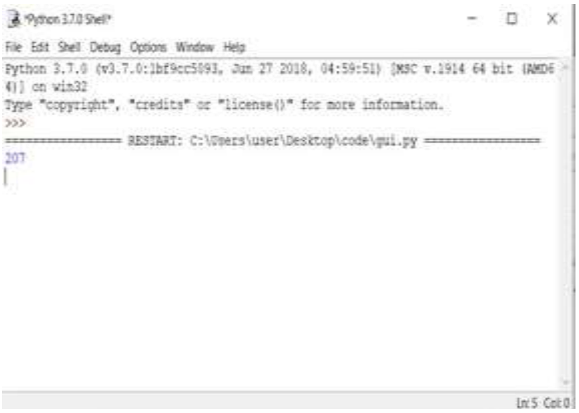
y^3 = x^2 + ax + b(mod q)

Enter Node 1 value of a: 1
Enter Node 2 value of b: 5
Enter value of q (prime):
137
Enter Private key Node1 A:
18
Enter Private key Node2 B:
29

ENCODED / DECODED TEXT

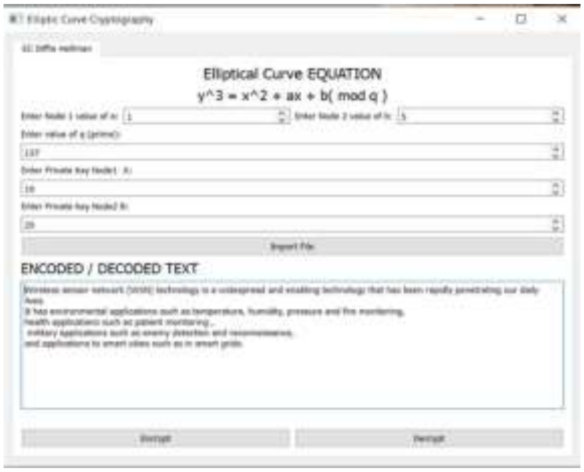
[illegible]

Encrypted Text for Decoding



```
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:59:51) [MSC v.1914 64 bit (AMD6
4)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
================== RESTART: C:\Users\user\Desktop\code\gui.py ==================
207
```

Calculated Private Key for decryption and gives Digital Signature



Elliptical Curve EQUATION

y^3 = x^2 + ax + b(mod q)

Enter Node 1 value of a: 1
Enter Node 2 value of b: 5
Enter value of q (prime):
137
Enter Private key Node1 A:
18
Enter Private key Node2 B:
29

ENCODED / DECODED TEXT

Wireless sensor network (WSN) technology is a widespread and enabling technology that has been rapidly penetrating our daily lives.
It has environmental applications such as temperature, humidity, pressure and fire monitoring,
health applications such as patient monitoring.,
military applications such as enemy detection and reconnaissance,
and applications to smart cities such as in smart grids.

Decrypted Secret Text

CONCLUSION:

In an Elliptic Curve Cryptography, a strong security mechanism over the attacks will be recommended to avoid Man-in-Middle Attack, we use public key authentication mechanism and create a secrete key (private key) between the nodes. We require 160-bit authentication of a message for a single modular exponentiation and also a single scalar multiplication, and it reduces the cost of the authentication. It also verifies the digital signature.

REFERENCE:

[1] H. Aoudia, Y. Touati, A. Ali Cherif and P. Greussay, Hieararchical Routing Approach-based energy optimization in Wireless Sensor Networks. Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access (MOBIWAC), 2012.

[2] C.P. Mayer. Security and Privacy Challenges in the Internet of Things. KiVS Workshop on Global Sensor Network, pp.131-134, 2009.

[3] P. Nandu and N. Shekokar, An Enhanced Authentication Mechanism to Secure Re-programming in WSN. International Conference on Advanced Computing Technologies and Applications (ICACTA), vol.45, pp.397-406, 2015.

[4] M.A. Haque-Chowdhur and K. Ki-Hyung, A survey of flash memory design and implementation of database in fash memory. Proceedings of the 3rd International Conference on Intelligent System and Knowledge Engineering, vol.1, Xiamen (China), pp.1256-1259, 2008.

[5] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, 2002.

[6] Z. Benenson, N. Gedicke, and O. Raivio, “Realizing robust user authentication in sensor networks,” in Proc. Workshop on Real-World Wireless Sensor Networks, 2005.

[7] H. Wang, B. Sheng, and Q. Li, “Elliptic curve cryptography-based access control in sensor networks,” Int. J. Security and Networks, vol. 1, nos. 3/4, pp. 127–137, 2006.

[8] N. Gura, A. Patel, A. Wander, H. Eberle, and S.C. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs,” in Proc. CHES, 2004, vol. 3156, LNCS, pp. 119–132.

[9] Fan Ye.Haiyun Luo, “Statical En-Route Filtering Of Injected False Data In Sensor Network,” vol.23,No 4,pp.83 850,April 2005

[10] Theodore Zahariadia and Panagiotis trakades, “Efficient Detection of Routing Attack in Wireless Sensor Network” 978-1-4244-4530-1/09 C 2010 IEEE.