SECURITY IN WIRELESS SENSOR NETWORKS USING ELLIPTIC CURVE CRYPTOGRAPHY IN ARM 9

SECURITY IN WIRELESS SENSOR NETWORKS-

REAL TIME IMPLEMENTATION IN ARM 9

***Dr.T.P.Saravanabava** ****M.Gandhi**

bava@annauniv.edu gandhi.au004 @gmail.com

Department of EEE, Division of Embedded System Technologies, Anna University, Chennai-600 025, India

ABSTRACT:

Wireless sensor network is a kind of ad-hoc network which consists of distributed sensors to monitor physical and environmental conditions which are of autonomous type. WSN is not yet implemented widely for such applications due to its energy consumption, challenges in environmental conditions etc.Security in wireless sensor networks (WSNs) is an upcoming research field which is quite different from traditional network security mechanisms. In this paper, we propose an efficient PKC based security architecture. Key management plays an essential role in achieving security in WSNs.A Secure key management in WSN is a real challenging task for this we are choosing Elliptic Curve Cryptography. The parameters considered for the analytical study are the reduced key size, power consumption and the processing overhead and implemented in ARM 9(LPC3250).

Keywords: ECC, ECLIPSE IDE, LPC3250, ARM-LINUX-GCC.

1. INTRODUCTION:

1.1 Wireless Sensor Networks:

A wireless sensor network consists of distributed sensors to monitor physical and environmental conditions which are of autonomous type. The wireless sensors were initially used in military applications but nowadays it is used in many industrial and consumer applications for monitoring and controlling. The wsn has a group of nodes ranging from few to several hundred or even thousands. It consists of small light weighted wireless nodes called sensor nodes. A sensor node varies from the size of a shoebox to a grain of dust. The cost of sensor nodes is ranges from a few to

hundreds of dollars, depending on the complexity of the individual sensor nodes. The size and cost constraints on sensor nodes results in changes in constraints on resources such as energy, memory, computational speed and bandwidth. The topology of the WSNs can vary from a simple star network to multihop mesh network. The propagation technique between the hops of the network can either be routing or flooding. Energy, computation, memory and limited communication capabilities are the resource constraints of wireless sensor networks. All sensor nodes in the wireless sensor network are interacting with each other or by intermediate sensor nodes.

1.2 CHALLENGES IN KEY ESTABLISHMENT:

Sensor networks may consists of different types sensors such as seismic, visual, infrared, RADAR, thermal, magnetic etc to monitor wide range of parameters in real time. But WSN is not yet implemented in real time due to its various drawbacks such as low power transmitter, poor battery backup, large energy consumption and lack of security features etc. Our paper proposes a modification in ECC algorithm such that it increases the network security by replacing lifeless nodes by nodes having higher security key size. Various other problems in establishment of ECC algorithm include:

- In the key generation phase, an appropriate elliptic curve and the corresponding elliptic curve parameters are chosen to generate the elliptic curve points.
- Each node is assigned a unique seed key with which a key ring is generated by performing point doubling and addition operations over it. The key ring is pre-distributed into the sensor nodes prior to deployment.
- Another issue is the link formation between the nodes that share a common public key.

1.3 LITERATURE SURVEY:

[1] In this paper, the Elliptic Curve Digital Signature Algorithm is used to authenticate all broadcast Messages overhead and security of the proposed scheme are analyzed. [2] Study of Symmetric and asymmetric algorithms.ECC implementation for WSN in java sun spot devices.[3] To know about symmetric and asymmetric key management schemes open issues in broadcast authentication on WSNs. [4] Study of sensor motes interface with java real time problems facing while

programming with java for sensor motes [5] A key distribution schemes in ECC is explained with the help of seed key scheme.And also the performance is evaluated in terms of connectivity and resilience against node capture. [6] The key focus of this paper is in studying the hardware implementations of ECC in WSN, and emphasizing on the underlying finite field, representation basis, occupied chip area, consumed power, and time performances.[7]Two hardware architectures that improve performances of 8-bit microprocessors in the task of computing the basic ECC primitive, operation usually propose solutions Focused on reducing the execution time. [8] Differentiated key pre-distribution, where the idea is to distribute different number of keys to different sensors to enhance the resilience of certain links in the network.[9] Computational intelligence provides adaptive mechanisms that exhibit intelligent behavior in complex and dynamic environments like WSNs. [10] A group Key Management protocol was designed for cluster based WSN environment and calculated the complexity of each protocol.

2. ELLIPTIC CURVE CRYPTOGRAPHY:

Basically, it is "an approach to public-key cryptography based on the mathematics of elliptic curves" (Wikipedia). The good thing about Elliptic Curve Cryptography (or ECC), is that it can be faster than RSA and uses smaller keys, but still provides the same level of security. ECC is based on something called the elliptic curve discrete log problem, and it's a much harder problem than factoring integers. Because it's much harder, we can get away with fewer bits, so what we like to say is that ECC provides the most security per bit of any public key scheme.

2.1 ECC MATHAMATICAL CALCULATION:

Every cryptosystem is based on a hard mathematical problem that is computationally infeasible to solve. ECC relies on the difficulty of solving the discrete logarithm problem for the group of an elliptic curve over some finite field (such as integers modulo a prime number, or a Galois field of size a power of two).

Elliptic curves have cryptographic value because a user can 'multiply' a point by a number to produce another point on the curve, but cannot easily figure out what number was used – even with knowledge of the original point and the result.But first, the plaintext message needs to be mapped to a numerical value upon which mathematical operations can be performed;

which means that for this use, the message must be mapped to a point on an elliptic curve. To get the cipher text, it is necessary to perform elliptic curve operations. Where RSA would use modular multiplication, ECC makes use of the addition operation of elliptic curves; and ECC's multiple addition is the equivalent of RSA's modular exponentiation.

But first let's discuss elliptic curves. An elliptic curve over real numbers is a set of points (x, y) which satisfy an elliptic curve equation $y^2 = x^3 + ax + b$; where a, b, x, and y are real numbers. The elliptic curve changes with various choices of a and b.An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity.

So how do we perform the addition operation on the points of an elliptic curve? You have two points, P and Q on an elliptic curve, and P + Q = R. To determine R a line is drawn through points P and Q, and the line will intersect the elliptic curve at a third point, which is –R. The point –R is then reflected in the x-axis to point R. For example:

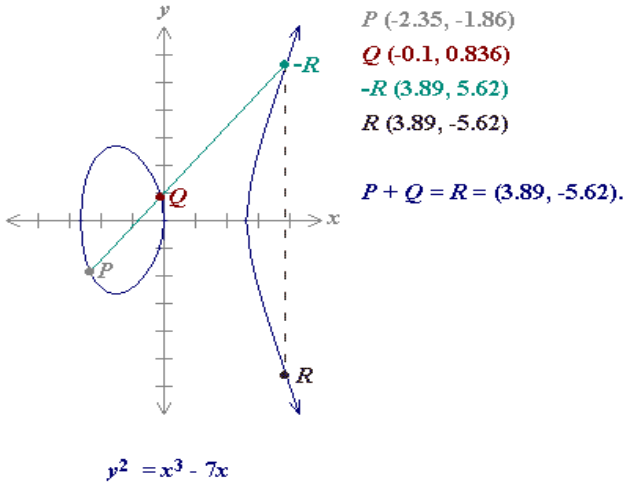

Figure 1. Point Addition

Figure 1. shows there are two exceptions where drawing a line through points P and Q will provide point –R. The first exception occurs when adding points P and –P, the second occurs when doubling point P. Since drawing a line through point P and –P will result in a vertical line (which will not cross through the elliptic curve at a third point), the point at infinity O is needed. By definition, P + (-P) = O, therefore, P + O = P . Now on to doubling point P. To add P to itself, a tangent line to the curve is drawn at the point P. The tangent line will intersect the elliptic curve at the point –R, if the y value of P is not 0. –R is then reflected into the x-axis to provide R. For example:

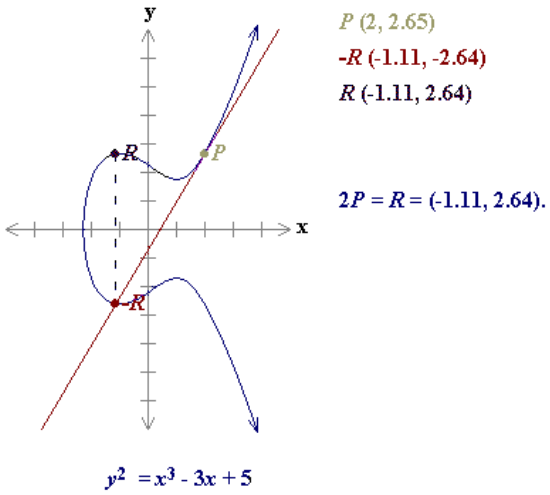

Figure 2.Point Doubling

Fig 2.shows "If a point P is such that yP = 0, then the tangent line to the elliptic curve at P is vertical and does not intersect the elliptic curve at any other point. By definition, 2P = 0 for such a point P"

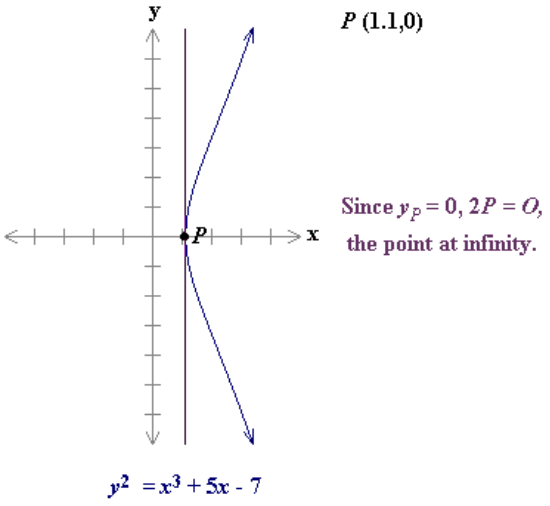

Figure 3. Point at infinity

Figure 3 .shows P = (x_1, y_1) and Q = (x_2, y_2), therefore P + Q = R = (x_3, y_3). $x_3 = m^2 - x_1 - x_2$ and $y_3 = m(x_1 - x_3) - y_1$. If P ≠ Q, then $m = (y_2 - y_1) / (x_2 - x_1)$, but if P = Q, then $m = (3x_1^2 + a) / (2y_1)$. (Note: m is the slope of the line through P and Q).

Since cryptography requires that a group has a finite number of points, the finite field of integers modulo a prime number is often used. It is not possible to use the graphs of this group to "connect the dots" for the geometric relationship, but the algebraic formulas have been adapted by performing them mod p. Therefore: $x_3 = m^2 - x_1 - x_2 \pmod p$ and $y_3 = m(x_1 - x_3) - y_1 \pmod p$; and if P ≠ Q, then $m = [(y_2 - y_1) / (x_2 - x_1)] \pmod p$, but if P = Q, then $m = [(3x_1^2 + a) / (2y_1)] \pmod p$.

2.2EXISTING SECURITY ALGORITHMS:

There are lot of public key security algorithms in practice for Wireless sensor networks such as RSA,Diffe-hellman key exchange,ECC etc. Each algorithm has their own advantages and drawbacks. Among all these algorithms ECC is considered to be good reduced key size meeting most of the requirements. The advantages and disadvantages of all existing algorithms are as follows.

RSA: This RSA based on exponentiation in a finite (Galois) field over integers modulo a prime and also uses large

integers (eg. 1024 bits) .It provides security due to cost of factoring large numbers.

Diffie-Hellman algorithm: It is based on exponentiation in a finite (Galois) field (modulo a prime or a polynomial). security relies on the difficulty of computing discrete logarithms and it is hard to break

ECC: Koblitz and Miller developed ECC in 1985. Its approach depends on the mathematics of elliptic curves. It was proved that ECC could provide same level of security when compared to RSA but with a smaller key size. For example, a 160-bit ECC key has the same security level as a 1,024-bit RSA and a 224-bit ECC key has the same security level as a 2,048-bit RSA key.

2.3 ECC& PROBLEMS:

Sensor nodes typically use irreplaceable power with the limited capacity, the nodes Capacity of computing, communicating, and storage is very limited, which requires WSN Protocols need to conserve energy as the main objective of maximizing the network lifetime. So it requires reduced key size algorithm to fulfil above requirements .

2.3.1 ECC ENCRYPTION AND DECRYPTION OF TEXT MESSAGE:

The procedures of decryption and encryption through elliptic curve analogous to ElGamal encryption scheme are described in the algorithms. The pure text m is first represented as a point M, and then encrypted by the addition to k Q, where k is an integer chosen randomly, and Q is the public key.

Algorithm: elliptic curve encryption

Input: Parameters field of elliptic curve (p, E, P, n), Public key Q, Plain text m

Output: Cipher text ($C1$, $C2$)

Begin

1. Represent the message m as a point M in E ($F\ p$)

2. Select $k \in R$ [1,$n-1$].

3. Compute $C1 = k\ P$

4. Compute $C2 = M + k\ Q$.

5. Return ($C1$, $C2$)

End

Algorithm: elliptic curve decryption

***Input*: Parameters field of elliptic curve (p , E, P, n), Private key d, Cipher text ($C1$, $C2$)**

Output: Plain text m

Begin

1. Compute $M = C2 - dC1$, and m from M.

2. Return (m).

End

2.4 ECC–S(PROPOSED ECC):

The problem due to load node is considered in our paper and a new proposal is made which is proved to be better in most aspects. The result is been proved using simulation and the result obtained proves that our ECC-S has good reduced key size and Good energy conservation than that of the existing ECC algorithm. Time consumption of various nodes are taken into account and they are compared for existing and proposed ECC-S and it is proved that the proposed method has low energy conservation over time. This in turn increases the network lifetime and also data aggregation is good.

3. SIMULATION SCENARIO:

The simulation environment that we have used is ECLIPSE IDE. It is a discrete event simulator for doing research All types of network can be simulated using this tool and it gives a wide support to do research under various algorithms such DSA,RSA and ECC. It uses Tool Command Language as scripting language and the tool is fully based on android basis. It supports both wired & Wireless Networks.

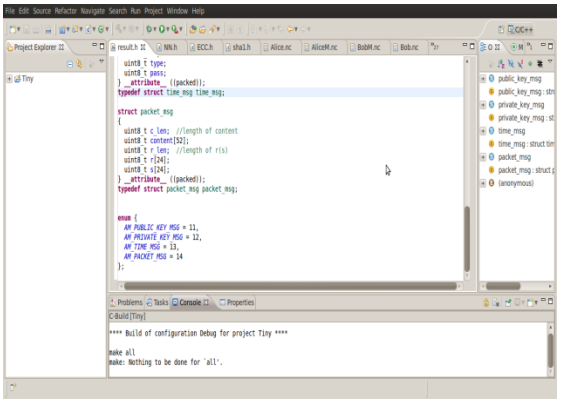

Fig.4 Eclipse input console

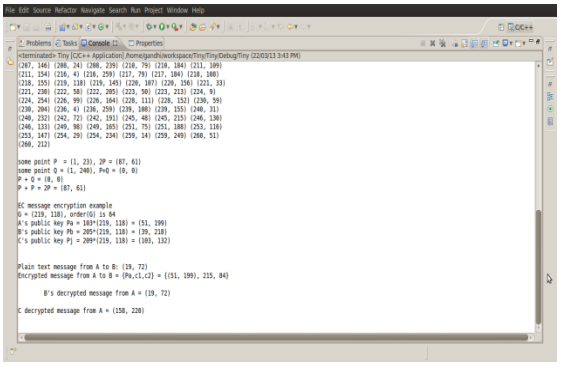

Fig.5 Eclipse output console

4. COMPARISION BETWEEN ECC (ECC& ECC -S):

Time consumption:

The time consumption is the ratio of real time consumption ,user time consumption and system time consumption at destination to the server. It is been proved that ECC –S has good time consumption than existing ECC algorithm. The observations made from simulation is tabulated below:

	EXISTING ECC	PROPOSED ECC
Real time	0.05S	0.00S
User time	0.08S	0.00S
System time	0.00S	0.01S

Table 4.1Time consumption ratio

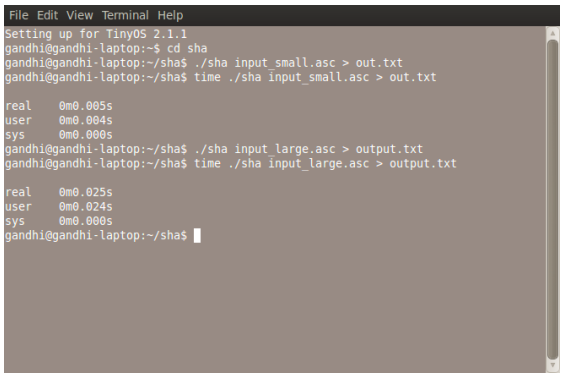

Figure 6: ECC algorithm time ratio

Figure 6. Illustrates time consumption of the existing ECC algorithm showed the above diagram.

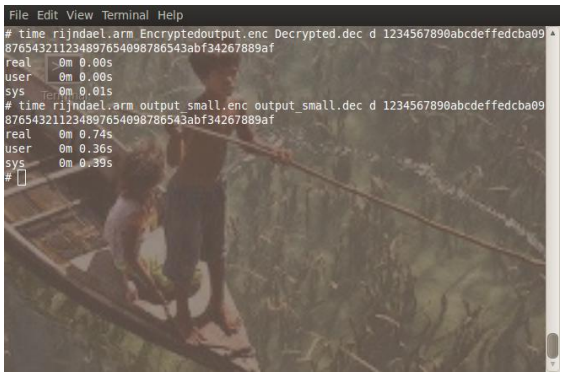

Figure 7.ECC –S algorithm time ratio

Figure 7. Illustrates that the time consumption of the proposed ECC-S algorithm

6. CONCLUSION & FUTURE WORK:

The modifications made in ECC algorithm has improved its Time consumption which in turn increases over all network life time. Thus ECC algorithm appears to be efficient in most aspects such as data aggregation, time consumption , speed ,processing overhead etc. In future a sleep mechanism can be induced among the nodes in clusters which in turn can further increase the network lifetime. The awaken nodes with no data transfer can be taken into sleep node using ASLEEP (Adaptive Staggered LEEP Protocol) which in turn increase the lifetime of Sensor nodes. The integration of ASLEEP protocol into ECC can yield a prolonged network lifetime .

7. REFERENCES:

1. Yong Sheng , Jie Li , Mohsen Guizani, "PKC Based Broadcast Authentication using Signature Amortization for WSNs", IEEE Transactions on Wireless Communications,2106-2115(2012)

2. Bhisham Sharma,Yogesh Kumar,Vandana Ladha," Design and Develop ECC for Wireless Sensor Network" , International Journal of

Computer Applications(0975-8887),1-7(2012)

3. Lie Jiang, Li Yu, Zilong Chen," Network Calculus based QoS Analysis of NetworkCoding in Cluster-tree Wireless Sensor Network", IEEE conference paper ,1-6(2012)

4. Yun Zhou ,Yuguang Fang,Yanchau Zhang," Securing Wireless Sensor Networks: A Survey", IEEE Communication Surveys & Tutorials,6-28(2008)

5. Homin Kwon,Venkataraman Atti, Andreaws Spanias", Experiments With Sensor Motes and Java-DSP", IEEE Transactions On Education,257-262(2009)

6. Eleni Klaoudatou, Elisavet Konstantinou, Georgios Kambourakis, Stefanos Gritzalis," A Survey on Cluster-Based Group Key AgreementProtocols for WSNs", IEEE Communications Surveys & Tutorials,429-442(2011)

7. J.-L. Chen, Y.-W. Ma, X. Wang, Y.-M. Huang, Y.-F. Lai," Time-division secret key protocol for wireless sensor networking", IET Commun.,Vol.5.Iss 12,1720-1726(2011)

8. J. Portilla, A. Otero, E. de la Torre,T. Riesgo, O. Stecklina, S. Peter, P. Langend¨orfer ," Adaptable Security in Wireless Sensor Networks by Using Reconfigurable ECC Hardware Coprocessors", International Journal of Distributed Sensor Networks,1-12 (2010)

9. Xu Huang, Dharmendra Sharma, Mohammed Aseeri, Sultan Almorqi," Secure Wireless Sensor Networks with Dynamic Window for Elliptic Curve Cryptography", Fourth International Conference on Network and System Security , 600-605(2010)

10. Hilal Houssain, Mohamad Badra, Turki F. Al-Somani,"Hardware Implementations of Elliptic Curve Cryptography in Wireless Sensor Networks" International Conference on Internet Technology and Secured Transactions,1-6(2011).