Generalized ElGamal Cryptosystem using Elliptic Curves for Secure M2M Communications

B.Satyanarayana Murthy, L Sumalatha

Abstract*: Machine to Machine (M2M) is a technology that allows the communication between both wireless and wired systems. M2M allows us to exchange different types of data without participation of human beings and it plays an important role in both industry and business applications. Security is the important aspect in M2M communications, because the nodes are not fixed and they can acquire data from assorted devices. In addition, M2M devices have their limitations with respect to its memory and processing capabilities. Hence we need to incorporate an efficient scheme for securing M2M communications. In this paper we propose an ElGamal cryptosystem using Elliptic Curves to provide secure communications in M2M networks.

***Index Terms*: M2M Communications, ElGamal cryptosystem, Elliptic Curve Cryptography.**

I. INTRODUCTION

Machine to Machine (M2M) [1],[2] communication is a paradigm in which the two devices can communicate without human intervention. It is basically an integral part of Web of Things (WoT) and it is mostly used in business, scientific, industrial and engineering applications. M2M communication avoids the direct involvement of human beings. Hence it minimizes the maintenance cost in any business applications. Because of its autonomous functionality some sort of security problems may raised during the communication. There are millions of such M2M [2] devices may exist in the network and are able to exchange confidential information. In medicine applications such a device can carry medical records such that it should ensure the integrity of the data. That is, we have to protect the communication between M2M devices.

The figure 1 illustrates the paradigm of M2M communication.

The two M2M devices may communicate with each other through the use of radio interfaces and TCP/IP protocol. Sometimes there may be a chance to interact with wired networks also. The M2M [2] devices may use MobileIPs to communicate with other devices during its mobility. The communication also involves Global System for Mobile Communication (GSM) networks. That is, interaction between devices takes place through wired and wireless networks also.

In the subsequent sections we proposed an approach to protect the communication between devices from both intentional and unintentional modifications. That is, only the intended recipient can see the message, no other parties are able to see this.

Revised Manuscript Received on December 22, 2018.

B.Satyanarayana Murthy, BVC Engineering College, Andhra Pradesh.

Dr. L Sumalatha, Department of CSE, UCEK, Kakinada.

II. OVERVIEW OF ELLIPTIC CURVES

The main disadvantage of public key cryptosystem is the range of numbers used and they are being stored permanently. In the case of RSA public key cryptosystem, it is necessary to exchange public keys and with a little effort we can easily compute the secret key. The computational complexity of such algorithms is also more. Hence an alternative approach is required to overcome these scenarios. One of the best mechanisms to provide the same level security with little mathematical operations is the use of elliptic curve cryptography (ECC) [3],[4].

The main advantage of ECC, when compared to RSA is that it provides same security for a small key size with little processing overhead. The following table 1 illustrates the comparison between ECC[4] and RSA.

In ECC cryptosystem 163-bit encryption offers same level of security in RSA 1024-bit encryption. Similarly a 283-bit encryption in ECC offers equal security in RSA 3072-bit encryption. Hence, ECC almost reduces computing complexity with better security concerns.

An elliptic curve is described by an equation with two variables and coefficients. For a public key cryptosystem, the coefficients and variables are limited to elements in finite field.

For our purpose, we can consider cubic equations for elliptic curves of the for $y^2=x^3+ax+b$ where x,y and a,b are real numbers. The general form of curves is as shown in figure 2:

We can also define a point O is known as point at infinity in the definition of elliptic curve. There are set of pints E(a,b) contains all the points (x,y) which satisfies the elliptic curve equation that includes the element O. Taking a distinct value of the coordinates *(a, b)* gives different set *E(a, b).* The specific properties of non singular elliptic curves allow us to define an addition operation on the chosen curve points. The simple process is the addition of two points on the curve to get another point the curve i.e, R=P+Q, where P=(x1,y1) , Q=(x2,y2), and R=(x3,y3).

The geometric interpretation of elliptic curve addition, as follows:

1. In the first case the points P=(x1,y1) and Q=(x2,y2) have distinct x and y coordinates. The coordinates of the point R, x3 and y3, can be found by first finding the slope

of the line $\lambda=(y2-y1)/(x2-x1)$; $x3= \lambda^2-x1-x2$ and $x3= \lambda(x1-x3)-y1$.

2. In the second case ,the two points overlap (R=P+P). Then : $\lambda=(3x^2+a)/(2y1)$; $x3= \lambda-x1-x2$; $y3= \lambda(x1-x3)-y1$.
3. In the third case, the two points are additive inverses of each other. The intercepting point is at infinity.

III. ELGAMAL CRYPTOGRAPHY USING ELLIPTIC CURVES

ElGamal cryptosystem [8] is a public key cryptosystem developed by Taher ElGamal and is based on discrete logarithm problem. In M2M communications there are different nodes exists in a network. For example, if two nodes namely M2M Node 1 and M2M Node 2 want to communicate with one another, then the nodes can select a rigid curve C, a permanent prime number *p* and a point on curve P(x,y). In this, we used Java Elliptic Curve Cryptography Library [5],[6] to develop a cryptosystem. The security of any cryptosystem is depends up on the size of key used to encrypt and decrypt the message. Many algorithms like RSA use 1024-bit key. We can select the larger key size to offer more security, but which can reduces the performance of the algorithm. To avoid this we have to choose alternative methods like ECC.

Encryption:

An input text P of variable length is split into equal length blocks (p*0*, p*1*…..pn). We guess the input message to be *ASCII* characters and each letter of message can be encoded using a 8-bit integer(0,255) at the sender and similarly decoded at the receiver. The encoded message is then embedded into the *x,y* - coordinates such that *(x,y)* lies on the given elliptic curve. The M2M Node 2 chooses E(x,y) with an elliptic curve over f group G and e1(x1,y1), a point on the curve, a secret key, d for decryption. Then the node computes e_2 such that $e_2(x_2, y2)=dxe1(x_1, y_1)$ and send its public elements such as E, e_1 and e_2 to the other node (M2M Node1). Now, the M2M Node 1 can encrypt the given message block p_i by taking a random integer k as follows

$$C_{i1}=kxe1 \quad \text{and} \quad C_{i2}=p_i+kxe_2$$

The final cipher text is obtained by combining all intermediate cipher text blocks (C1,C2,C3,……, C_n).

Decryption:

After converting plain text into cipher text at the M2M Node 1 side, it can send the cipher text to the intended recipient. At the other end, M2M node 2 can obtain plain text from the following equation : $P= C_{i2}-(dxC_{i1})$.

The encryption and decryption process of above mentioned cryptosystem can be represented as shown in figure 3.

IV. PERFORMANCE ANALYSIS

We have been tested the development of our scheme with ASCII input file type of various sizes and also measured the time required for encryption and decryption. The decryption process takes less time when compared to encryption. Decryption was observed that it is eight times faster than encryption because it involves less number of multiplications than encryption [10]. The figure 4 shows the performance comparison between encryption and decryption speed for a block size of120KB.

The encryption process speed is little slow when compared with decryption process. However the scheme offers equal security as compared with RSA. The speed of an encryption is the most deciding factor for choosing a security scheme. Symmetric key encryption algorithms like AES and DES are faster because of its limited key size but those are non resistant to brute force attacks. Our scheme is better for security even it will take more time to encrypt the message. The decryption is faster as compared with DEA and AES [9],[11].

This approach not only offers security, it is more generalized due to its efficient computational capability when compared to other approaches like RSA and Diffie-Hellman. The table 2 shows ratio of computation of RSA to elliptic curves for different sizes of keys:

V. CONCLUSION AND FUTURE WORK

Most of the security schemes are based on the illusion that the underlying mathematical problems are complex. The security of an cryptography system is depends up in such an illusion. In most of the cases we can easily solve such a mathematical problem. This results in compromising the keys.

In most of the cases public key cryptography is preferable scheme for data transfer, because there is no need to exchange secret key before actual communication starts. One of such scheme is ECC. It overcomes the problem of secret key exchange and makes the cryptosystem complex. Here we can share only public elements. And the computations are faster and also more practical. Our schemes also performs better for variable size input blocks of plain text and it takes lesser memory and processor requirements. Hence this scheme is more suitable for M2M communications. Due to the limitations in the M2M nodes this type of lightweight cryptosystems are preferable.

We limited the elliptic curve to certain operations. In the future we can extend the algorithm to include all points on the elliptic curve and perform all operations. It is necessary to extend the approach to take variable size input blocks and reduced encryption time complexity. And the major enhancement for this approach is we have to incorporate this type of lightweight cryptosystems in Ultra dense networks where the number of devise per a square feet is more than ten.

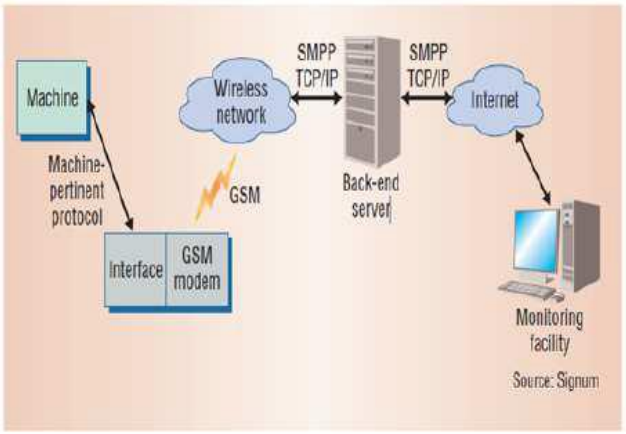

Figure 1:

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

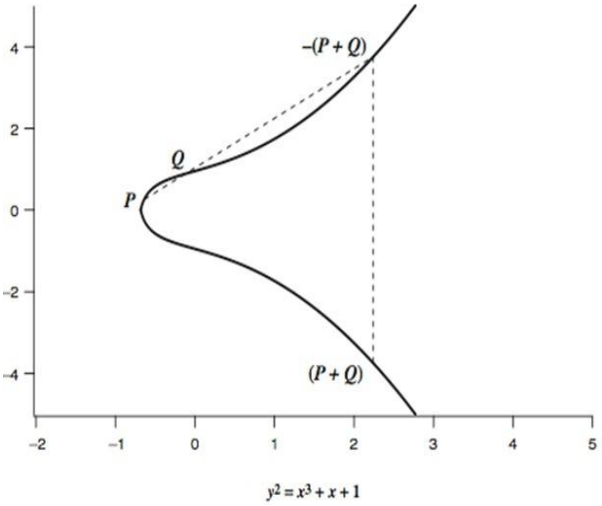

Figure 2:

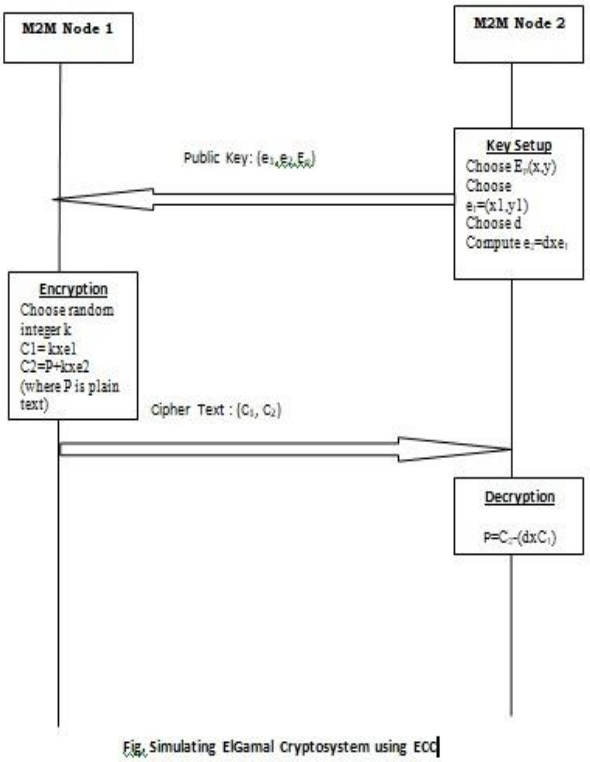

Fig. Simulating ElGamal Cryptosystem using ECC

Figure 3:

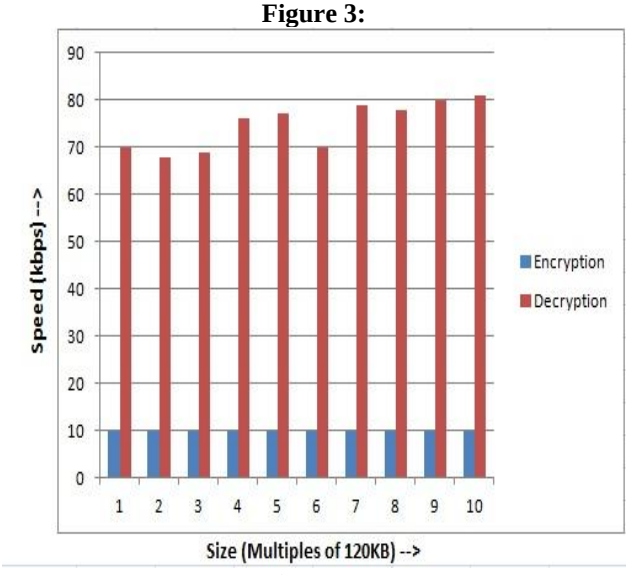

Figure 4:

Table 1:

Symmetric	ECC	RSA/DSA
80	163	1024
128	283	3072
192	409	7680
256	571	15,360

Table 2:

Security Level(bits)	Ratio of RSA cost: EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

REFERENCES

1. B satyanarayana Murthy, Dr. L Sumalatha ,"Security and Privacy in Machine-to- Machine Communications– A Survey", IJETSR,ISSN 2394 – 3386,Volume 4, Issue 11,November 2017
2. B.Satyanarayana Murthy, Dr. L Sumalatha, "A Distributed Authentication and Key Exchange Approach for Secure M2M Communications", 978-1-5386-1144-9, 2016, IEEE.
3. Koblitz, Neal. "Elliptic curve cryptosystems." *Mathematics of computation* 48.177 (1987): 203- 209. Bos, Joppe W., et al. "Elliptic curve cryptography in practice." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2014. 157-175.
4. Java Elliptic Curve Cryptography(JECC) software : http://jecc.sourceforge.net/
   JavaPlot Library:- http://vase.essex.ac.uk/software/JavaPlot/
5. V. Gupta, S. Gupta, and S. Chang, "Performance Analysis of Elliptic Curve Cryptography for SSL," CM Wksp. Wireless Security, Mobicom 2002, Atlanta, GA, Sept. 2002,
6. Rosy Sunuwar, Suraj Ketan Samal " Elgamal Encryption using Elliptic Curve Cryptography ",CSCE 877 - Cryptography and Computer Security University of Nebraska- Lincoln.
7. J. Guajardo and C. Paar, "Efficient Algorithms for Elliptic Curve Cryptosystems," B. S. Kaliski Jr., Ed., Advances in Cryptology — CRYPTO, 1997, LNCS, vol. 1294, Springer-Verlag, 1997, pp. 342–56.
8. M. Ciet et al., "Trading Inversions for Multiplications in Elliptic Curve Cryptography," preprint, 2003, http://eprint. iacr.org/
9. K. Eisentraeger et al., "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," M. Joye, Ed., Topics in Cryptology — CT-RSA 2003, LNCS, vol. 2612, Springer-Verlag, 2003, pp. 343–54.