Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 8; April-June, 2015 pp. 22-25
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Network Security Issues of Mobile AD-HOC Networks using Elliptic Curve Cryptography

Bhavna Sharma[1] and Vandana Madaan[2]

[1]M.Tech (Computer Science) Hindu College of Engineering
[2]Hindu College of Engineering
E-mail: [1]sweetbhanu90@gmail.com, [2]vandana.madaan@gmail.com

Abstract—*Mobile Ad-hoc Networks or MANETs are a relatively new concept for wireless and infrastructure less dynamic network structure among a number of mobile nodes in absence of a centralized authority. These basic characteristics of MANETs make them a favorable alternative to the conventional networks in many circumstances but they are also prone to various network security attacks. Security of any network can be enhanced with the application of various cryptographic algorithms. A network dependent upon cryptographic algorithm intensifies the robustness of the network against various adversaries who aim to breach the network system. In this paper we have discussed the implementation of Elliptic Curve Cryptography (ECC) using GNU Multiprecision Library (GMP) and discussed their advantages for employment in MANETs to counter its security issues.*

Keywords*: MANET: Mobile Ad-hoc Networks, ECC :Elliptic Curve Cryptography, Threshold Cryptography (TC), GMP : GNU Multiprecision library.*

1. INTRODUCTION

As the advancement in the applications dependent on Internet has increased at a humongous rate, the need for availability for fast, reliable and stable network connection has increased simultaneously. Various wireless network systems have been designed to cater this issue but still these systems demand dependency upon wired networks which in some situations are difficult to obtain. Mobile Ad-hoc networks have been a latest trend in countering such challenges of network systems dependent upon wired connection even by minutest fraction. Mobile ad-hoc network is a relatively new concept and it involves spontaneous participation of users in an environment which supports dynamic networking architecture[1]. However with the availability of such network system poses various security issues that can hinder the proper performance of the system. Network attacks like Denial of service (DOS), Distributed Denial of Service (DDOS), Man-in-the-middle attack, compromised key attack, application layer attack, phishing and spamming [2]. Various measures have been proposed and implemented to tackle these attacks but the most favorable in many scenarios has been the security measures using Asymmetric Cryptography. In this paper we have discussed about Elliptic Curve Cryptography (ECC) and its possible applications in mobile ad hoc networks. Furthermore we have implemented ECC algorithm and analyzed its result to get a perspective of the capabilities which the ECC algorithm holds and its possible application in a mobile ad-hoc network. This paper consist of seven sections, the second section includes introduction to Ad-hoc networks. In the third and the fourth section we have provided with the description of Asymmetric Cryptography and ECC algorithm respectively. Implementation of the ECC algorithm is done in the fifth section followed by the sixth were its analysis has been done in the Result. Finally we have concluded the paper in the sixth section.

2. INTRODUCTION TO MOBILE AD-HOC NETWORKS (MANETS)

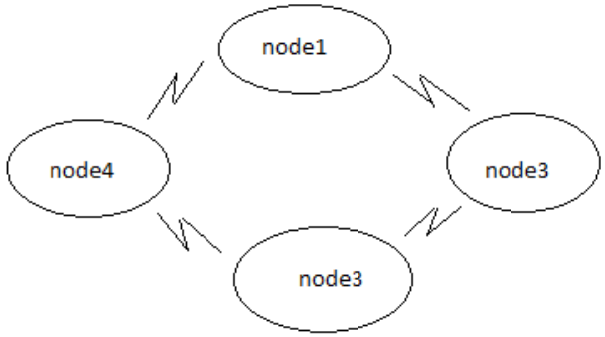


Fig. 1: A wireless mobile Ad hoc network

A Mobile Ad hoc network provides a platform for connecting mobile nodes operating beyond the reach of a fixed network. It is a self-configuring, infrastructure-less network of mobile devices connected by wireless links as shown in fig. 1.there is an ad-hoc network in which nodes are participating connected to each other via wireless links [2]. Each device in a MANET is free to move autonomously in each and every direction, and it reconfigures its links to the other devices frequently.

2.1 Advantages of MANETs

The advantages of Mobile Ad-Hoc networks are magnanimous because they deliver access to information as well as services indifferent to the geographical position. One of the peculiar advantages of MANETs is that they are free from central network administration due to self-configuration. Each of the system connected to a MANET are termed as Nodes. Nodes also act as routers and are cheaper than wired network. Scalability feature provides conformity for addition of more nodes. They have highly improved Flexibility. They are robust due to decentralized administration. The network can easily be set up at any of the place and time. Furthermore MANETs can be best recognized for their following assertive characteristics:

- Data Confidentiality: keeps data hidden and disclosed to outsiders
- Data Integrity: it ensures the data from being altered,
- Data update : it maintains data in the correct order and up-to-date,
- Data Availability :it provides data to be available on request,
- Data & Identity Authentication : checks that the data or request came from a valid sender, and
- Non-repudiation: it ensures a node cannot deny sending a message.

Security mechanisms that are frequently used and prove to be effectively useful in wired networks are not always applicable to MANETs. Attacks that can be effectively detected and prevented in wired networks have been big security challenges in MANETs [4]. For example, identity/address spoofing, message tampering, forgery, message replay. There are many security issues and threats that hinder the proper functionality of MANETS due to its characteristics such as lack of network infrastructure, frequent change in network topology and potential insider attacks.

2.2 Applications of MANETs

There are a number of applications of MANETs. The compatibility of MANETs with other network or operating systems gives it greater accessibility in wider domains such as

- Working in Collaboration: Computing based on collaborative methods give an edge to business meetings and information sharing outside the office environment when there are two different parties working on a same project.
- Bluetooth and Personal Area Networks: Short range MANETs can be used very well for the information exchange between cross platform using Bluetooth involving various nodes.
- Educational Services: In order to provide an interactive medium in the educational environment, MANETs can be used to provide swift and stable multimedia or data sharing within an enclosed environment.
- Defense services: MANETs can be extremely beneficial for the defense services as the need for a network in inhospitable and network challenged areas. The setup of a fast and reliable MANET can provide quality communication through a highly secure medium.

3. ASYMMETRIC CRYPTOGRAPHY ALGORITHMS

In the wide assortment of network security protocols, Cryptography is a prominent domain where Asymmetric Cryptography has been the most promising because of the usage of two different keys, i.e. a public and a private key for the encryption and decryption of data[3]. In order to employ Asymmetric cryptography in a network communication system, we need to merge its data with the asymmetric cryptographic algorithm which are varied on the basis of their application. [5]The data when applied in these cryptographic algorithms generate cipher texts which are transferred to the receiver through a secure communication media.

3.1 Elliptic Curve Cryptography (ECC)

First proposed by NielKoblitz and Victor Miller, Elliptic Curve Cryptography (ECC) is one of the most efficient cryptosystems the present network security scenario today [6]. It involves the dependency on the characteristics of the elliptic curves and the data or messages are represented as the function of an elliptic curve equation $y=x^2 + ax + b$. The properties of elliptic curves are basically point addition, point doubling. In point addition as mentioned in Fig. 1 we consider two points say 'P_1' and 'P_2' on the elliptic curve 'E' and the line joining these two points has to intersect the elliptic curve itself at another point say 'P_3', the point located on the exact opposite quadrant to 'P_3' is the additive sum of 'P_1' and 'P_2' i.e. $P_1 + P_2 = P_3$. As illustrated in the Fig.2 in point doubling we consider only a point 'P' whose reflection 'R' is taken on the opposite quadrant on the curve.

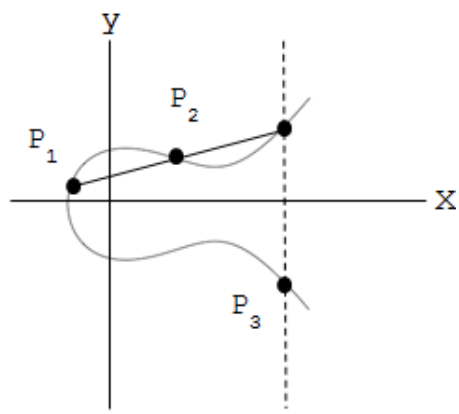


Fig. 2: Point Addition in ECC

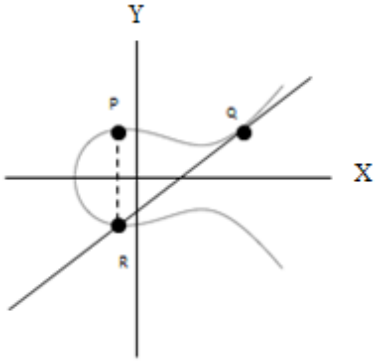


Fig. 3: Point Doubling in ECC

A line which crosses this point 'P' and also, o intersects the elliptic curve 'E' meets at another point 'Q'. This point 'Q' on the curve 'E' is the double of the singular point 'P'.

3.2 Threshold Cryptography (TC)

Public-private key mechanisms are being used by Mobile ad-hoc networks. In threshold cryptography, public key is known by all participants [7]. Various participants of the system share the private key. Public key of the elements is stored by each server which sign the replies asked using the private key of the entire system. Since adversary does not have much of reckoning power to rupture these cryptographic schemes so this system is impregnable.

For a secret to be shared and distributed amongst the participants, there are set of rules that need to be followed. The secret is distributed amongst k+1 participants and at least k participants are needed to decode the secret which is the threshold value [14].

4. ELLIPTIC CURVE CRYPTOGRAPHY (ECC) ALGORITHM

The ECC algorithm is a distinctive approach to cater the security issues of a network. The algorithm consists of three phases namely Key Generation, Encryption and Decryption as shown in fig.4. In this section we have discussed the characteristics of ECC in these phases.

a) Key Generation
i) Within the range of 'n' selection of a number'd'.
ii) Generation of Public key using the following equation : Q = d *P.

Where,
d = The random number that we have selected within the range of (1 to n-1).
P is the point on the curve.

'Q' is the public key and 'd' is the private key.
b) Encryption
i) Represent message 'm' on the curve. Let 'm' have a point 'M' on the elliptic curve 'E'.
ii) Randomly select 'k' from the range [1-(n-1)].
iii) C1 and C2be the two ciphertexts generated.
iii) C1 = k*P
iv) C2 = M + k*Q
v) C1 and C2 as ciphertexts to the receiver.

c) Decryption
i) Retrieval of the original message 'M'.
ii) M = C2 – d * C1.

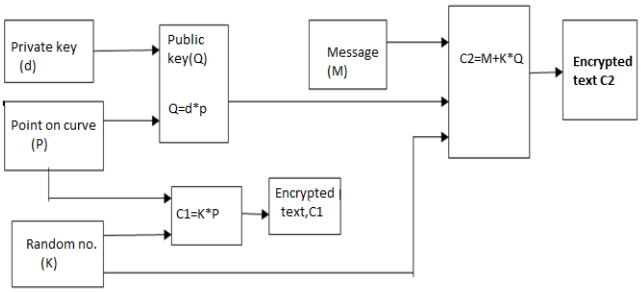
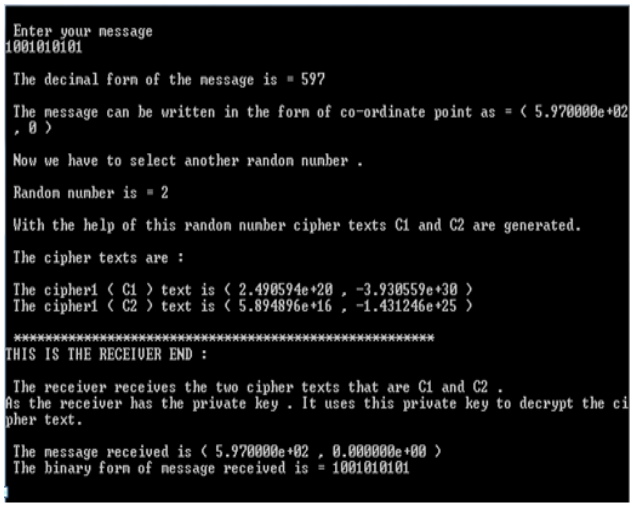


Fig. 4: Block diagram showing encryption process of ECC

5. IMPLEMENTATION OF ECC ALGORITHM USING GNU MULTI PRECISION LIBRARY (GMP).

GMP is an open source library providing operations on numerical, arithmetic, signed integers, rational and floating-point numbers . There is no specific and practical boundary to the calculations performed on GMP leaving the ones applied by the available memory on the machine in which GMP runs. GMP has an affluent set of functions, and the functions have a regular interfacing amongst them. There are colossal applications of GMP that includes cryptographic applications ,network security, security of internet applications, algebra systems, research of computational algebra.

5.1 ECC implementation



```
Enter your message
1001010101

The decimal form of the message is = 597

The message can be written in the form of co-ordinate point as = ( 5.970000e+02
, 0 )

Now we have to select another random number .

Random number is = 2

With the help of this random number cipher texts C1 and C2 are generated.

The cipher texts are :

The cipher1 ( C1 ) text is ( 2.490594e+20 , -3.930559e+30 )
The cipher1 ( C2 ) text is ( 5.894896e+16 , -1.431246e+25 )

*****************************************************
THIS IS THE RECEIVER END :

The receiver receives the two cipher texts that are C1 and C2 .
As the receiver has the private key . It uses this private key to decrypt the ci
pher text.

The message received is ( 5.970000e+02 , 0.000000e+00 )
The binary form of message received is = 1001010101
```

Fig. 5: Implementation of ECC using GMP with the message 1001010101

In this section we have provided the necessary structure of the ECC algorithm which can be utilized to stimulate on GMP to derive results.

The GMP consists of various enriched libraries that contains functions of mathematical computations functions required to perform calculations in the ECC algorithm [13].

In this implementation the user asked to enter a message in binary form. This message is then converted into a decimal form, which further is represented in the terms of x-y coordinates. After this representation a random number is chosen from a group with a predefined range. This random number is essential for generating the ciphertexts. The receiver which receives the ciphertexts can decipher them using private key.

6. RESULT

In the implementation of the ECC algorithm in the above section gives us the proper functionality of an efficient, fast and reliable algorithm with exceptional rate of key generation, encryption and decryption. After application of the message 1000101001 to this algorithm firstly we have a decimal representation of the message as 597 and further a coordinate representation as 5.9700000e+02.There are two ciphertexts C1: 2.49059e+20,-3.939559e+30 and C2: 5.4894896e+16,-1.431246e+25 which are generated as the public key is applied for the encryption. These ciphertexts are received by the user and then converted into its original form by the use of the private key[13].

7. CONCLUSION

In the end we would like to conclude by mentioning the fact that with the ever changing technology and the need for availability of robust networking systems in every environment are ideal conditions for Mobile Ad-hoc Networks to flourish and accepted as a reliable alternative to the present networks. However the security of the MANETs has been an issue of prime importance. The employment of Asymmetric Cryptographic algorithms such as RSA and Elliptic Curve Cryptography will increase the security of a MANET drastically. Furthermore integration of ECC with Threshold Cryptography (ECC-TC) also can enhance the security and reduce risk of a MANETs.

REFERENCES

[1] L. Zhou and Z. J. Haas, “Securing ad hoc networks” ,*IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, November/ December 1999

[2] Sarvesh Tanwar *et al* ” Threats & Security Issues in Ad hoc network: A Survey Report” *IJSCE*, Vol.2, Issue-6, Jan 2013.

[3] Vanesa Daza a, Javier Herranz b, Paz Morillo c,, Carla Rafols ”Cryptographic techniques for mobile ad-hoc networks”*Elsevier,Computer Networks 51 (2007) 4938–4950*

[4] Shalini Saini, Asst. Professor Abhishek Shukla, Dr. Manish Verma “A Survey of Security in Mobile Ad-Hoc Networks using Cryptography” *IJARCSE*, Vol. 4, Issue 10, Oct 2014.

[5] A. Shamir, “How to share a secret”, Communications of the ACM, Vol. 22, No. 11, November 1979.

[6] Vishwa gupta “Advance cryptography algorithm for improving data security” *Int. J of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 2, Issue 1, January 2012

[7] Sonali Nimbhorkar1, Dr. L.G.Malik,” Prospective Utilization of Elliptic Curve Cryptography for Security Enhancement”, *IJAIEM* , Vol.2, Issue 1, January 2013 ISSN 2319 – 4847.Gemmell P. S.

[8] “An Introduction to Threshold cryptography”, *Cryptobytes,1997*

[9] Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta,” Performance Based Comparison Study of RSA and Elliptic Curve Cryptography” *International Journal of Scientific & Engineering Research*, Volume 4, Issue 5, May-2013,ISSN 2229-5518.

[10] S.M. Sarwarul *et al* ” Security of Mobile Agent in Ad hoc Network using Threshold Cryptography” *World Academy of Science, Engineering and Technology* Vol:4 2010-10-27

[11] Marianne A. Azer *et al* “Threshold Cryptography and Authentication in Ad Hoc Networks Survey and Challenges” *IEEE, Second Int. Conference on Systems and Networks Communications (ICSNC 2007)0-7695-2938-0/07*

[12] Jesse Russel, Ronald Cohn, “Gnu Multiple Precision Arithmetic Library”,2012.

[13] Menezes .A.*et al* “Hand book of Applied Cryptography,”CRC Press 1996

[14] Dr. (Mrs). G.Padmavathi, Ms. B. Lavanya” Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for Small” *Int. J. Advanced Networking and Applications* Volume: 03, Issue: 04, Pages:1245-1252 (2012)

[15] L. Ertaul and N. Chavan, “Security of Ad Hoc Networks and Threshold Cryptography”, in *MOBIWAC 2005*.Mobile Adhoc Networks.