www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13346-13350

Enhancing Security of MANETs by Implementing Elliptical Curve based Threshold Cryptography

[1] Ms. Bhavna Sharma , [2] Mrs Vandana Madaan

[1]Department of computer science DCRUST Murthal
Hindu college of engineering ,Sonepat, Haryana
sweetbhanu90@gmail.com

[2]Assistant Professor , Department of computer science
Hindu college of engineering, DCRUST Murthal, Haryana
vandana.madaan@gmail.com

Abstract: ***Mobile Ad-hoc Networks or MANETs is a prominent technique in wireless networks which is receiving a great attention by different groups . A Mobile Ad-hoc network is a group of wireless mobiles nodes that tends to form a network without any fixed infrastructure having mobile and self-configuring nodes. Security in MANETs is a challenging issue hence it requires efficient security scheme to protect itself against malicious attacks and interceptions. Elliptical curve based threshold cryptography provides a promising solution to enhance the security of MANETs than other existing popular algorithms such as RSA. In this paper we have discussed the implementation of Elliptic Curve Cryptography (ECC) based threshold cryptography(ECC-TC) using GNU Multi precision 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 Multi precision library.

1. Introduction.

As the development in the applications dependent on Internet has enlarged at a humongous rate, the need for availability for fast, reliable and stable network connection has improved simultaneously. Various wireless network systems have been designed to provide secure and efficient technique in this issue yet these systems demand dependency upon wired networks which in some situations are hard to obtain.

Mobile Ad-hoc networks have been a new technique in countering such challenges of network systems dependent upon wired connection even by tiniest fraction. Mobile ad-hoc network is a relatively new concept and it involves spontaneous participation of users in an environment which supports dynamic networking structural design[1]. However with the availability of such network system poses various security issues that can hamper the proper performance of the system. Network attacks like Denial of service (DOS), compromised key attack, application layer attack, phishing and spamming [2].

Numerous methods have been proposed and implemented to block these attacks but the most favorable in many circumstances has been the security measures using Asymmetric Cryptography. In this paper we have discussed about Elliptic Curve Cryptography (ECC) and Threshold cryptography ,also their possible applications in mobile ad hoc networks. Furthermore we have implemented ECC-TC algorithm and analyzed its result to get a perspective of the capabilities which the ECC-TC 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-TC 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. Mobile ad-hoc networks (MANETs)

A Mobile Ad hoc network delivers a platform for connecting mobile nodes operating beyond the reach of a fixed network. It automatically configures, having no fixed infrastructure ,hence a network of mobile devices connected by wireless links.

As shown in Fig.2.1 there is an ad-hoc network in which nodes are participating connected to each other via wireless links [2]. Each device in a MANET independently moves from one point to another without restrictions in each and every direction, and it reconfigures its links to the other devices frequently

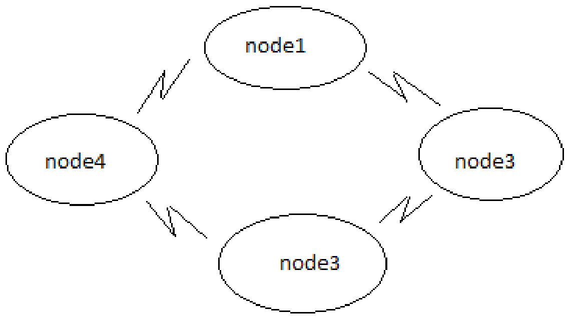


Figure 2.1: A wireless mobile ad hoc network

2.1 Advantages of MANETs

The advantages of Mobile Ad-Hoc networks are huge because they deliver access to information as well as services indifferent to the geographical location. One of the typical 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 conformism for addition of more nodes. They have highly enhanced 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 self-assured characteristics:

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

2.2 Applications of MANETs

There are various applications of MANETs. The application of MANETs with other network or operating systems gives it superior accessibility in wider domains such as

- *Defense services*: MANETs can be extremely advantageous 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.
- *Collaborative computing*: 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 for the information exchange among cross platforms using Bluetooth involving various nodes.
- *Educational Services:* MANETs efficiently provide an interactive medium in the educational environment, MANETs can be used to provide rapid and firm multimedia or data sharing within an enclosed environment.

3. Cryptography in network security

Network security issues are making a tremendous increase in the various dynamic, static or ad-hoc networks. These issues can be very well contained and handled by employing many cryptography based algorithm schemes into the key generation, encryption and decryption of various sensitive data that need to be provided with efficient security. Broadly these cryptographic algorithms are classified into three sub-groups namely RSA, ECC and Threshold. The diverse domain of the network security issues pave way for the application of these algorithms with respect to the degree of security required.

The comprehensive analysis and comparison of these cryptographic algorithms are essential for the determination of specific applicable algorithm to be employed to the respective network issues faced by the network.

3.1 Asymmetric cryptography algorithms

In the wide collection of network security protocols, Cryptography is a protruding domain where Asymmetric Cryptography has been the most promising because of the practice of two different keys, i.e. a public and a private key for the encryption and decryption of data respectively[3]. In order to service

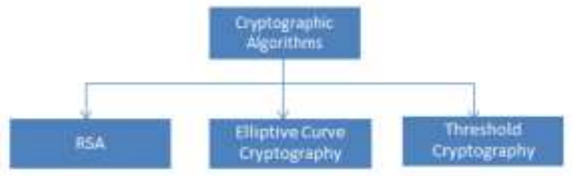


Figure 3.1 : Classification of Cryptographic algorithms

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.

3.2 Threshold Cryptography (TC)

Threshold cryptosystems are based on the modification of the information. These modifications in the information to be transmitted are done such that the message is broken into a number of shares and distributed among bunch of shareholders.

The formulation of threshold cryptographic systems is such that the generation, computation and the distribution of the secret key required for the encryption and the decryption process is to be done in such a fashion that only certain number of trusted parties among all the parties is required to perform the same. This marks as necessity for the generation of appropriate secret keys which are intended for the purpose of distribution. Advantage of such a cryptographic scheme allows the greater reliability toward the security of the data and protection from malicious party whose intent is to disrupt a significant data transaction. [8] In order to share and distribute a secret among a category of trusted parties, there are regulations which are to be abided; the secret is should carefully distributed to t+1 parties and only the honest t parties can formulate the secret. The condition is met such that no group of dishonest parties can deduce the secret even if provided with credible information about the secret itself. Here the generation of the secret can be interchanged with the generation of a message or a digital signature of the system.[3][4]

3.3 Elliptic Curve Cryptography (ECC)

ECC was first proposed by Niel Koblitz and Victor Miller, Elliptic Curve Cryptography (ECC) is one of the most efficient cryptosystems the current network security scenario today [6]. It involves the dependency on the characteristics of the elliptic curves and the data or messages are embodied as the function of an elliptic curve equation $y=x^2 + ax + b$. The properties of elliptic curves are chiefly point addition, point doubling. In point addition as mentioned

In Fig. 2 we assume two points say ‘X1’ and ‘X2’ on the elliptic curve ‘C’ and the line linking these two points has to intersect the elliptic curve itself at another point say ‘X3’, the point located on the exact opposite quadrant to ‘X_3’ is the additive sum of ‘X_1’ and ‘X_2’ i.e. $X_1 + X_2 = X_3$. As illustrated in the Fig.3 in point doubling we consider only a point ‘X’ whose reflection ‘R’ is taken on the opposite quadrant on the curve. A line which crosses this point ‘X’ 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’.

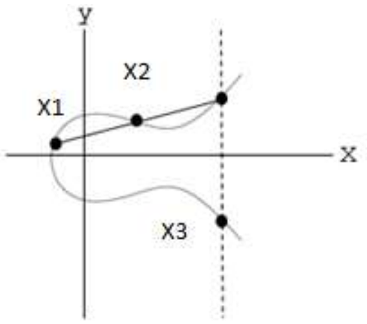


Figure 3.2(a): Point Addition in ECC

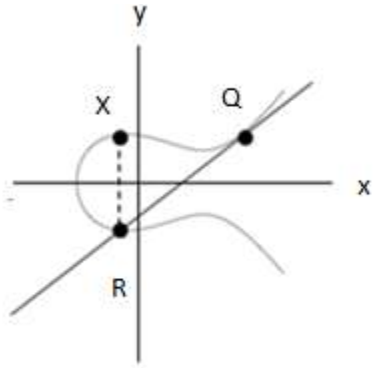


Figure 3.2(b): Point Doubling in ECC

4. Elliptical curve based Threshold cryptography scheme(ECC-TC)

The ECC-TC 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.. 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 = represents the number selected randomly from the range (1 to n-1).
P = point on the curve.
Q = Public key and
‘d’= 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 C2 be the two cipher texts generated.
iii) C1 = k*P
iv) C2 = M + k*Q
v) C1 and C2 as cipher texts to the receiver.

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

As shown in Fig. 4.1 First of all the message is divided into n no of shares using Threshold cryptography furthermore using the ECC cryptography ,the corresponding cipher texts are generated of different shares. The encrypted message is then transmitted to the sender’s site

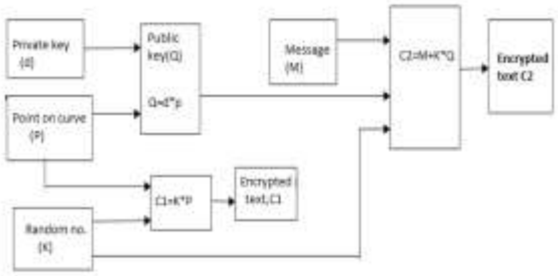


Figure 4.1: Block diagram showing encryption process of ECC

Here, At the receivers end as shown in Fig 4.2 the shares are reconstructed using Shamir’s n out of t scheme and the message is decrypted using sender’s private key. The encrypted texts are reverted back to the original text by using private key ‘d’ of the receiver

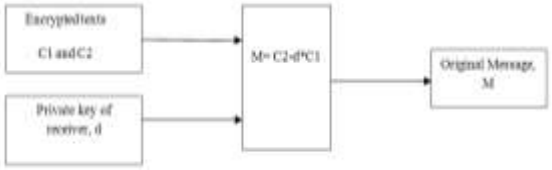


Figure 4.1 : Block diagram showing decryption process of ECC

5. Implementation of ECC-TC 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-TC implementation on GMP

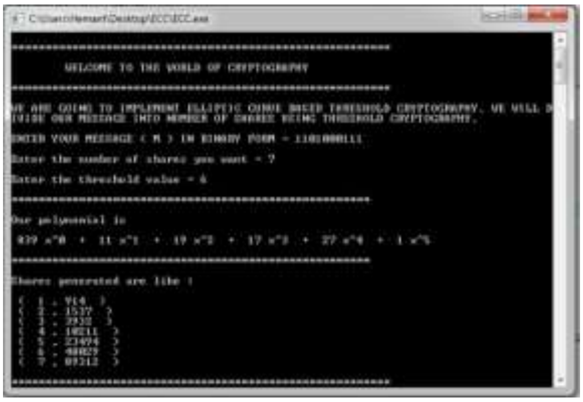
The GMP consists of various enriched libraries that contains functions of mathematical computations functions required to perform calculations in the ECC algorithm [13].Therefore the cryptanalysis has been done using GMP Library.

The Implementation involved simulations of MANET by forming a network with 'n' no. of mobile nodes comprising sender nodes as 'S', receiver nodes as 'R' and other participating mobile nodes called shareholders(SH). First of all the user is asked to enter a message in binary form then the user is asked to enter the number of shares in which he wants to distribute the message after that the threshold value is entered by the user which is the minimum number of users required to retrieve the original message. The polynomial equation generated by finite field curve of x, y coordinates is used for generating the cipher texts based on the shares.

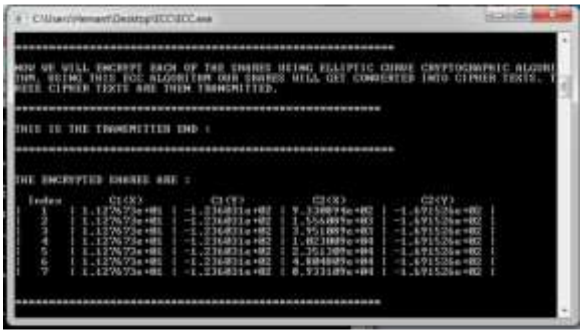
Now at the transmitter end the encrypted shares are generated which are in x , y coordinates and are transmitted to the receiver.

At the receiver's end the user is asked to enter the number of shares needed to recover the message followed by the index number of the shares by which the receiver can decipher the cipher texts using private key.

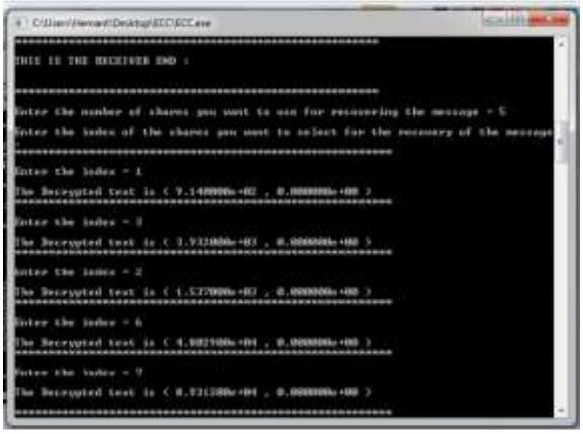
5.2 Screen shots of implementation of ECC-TC



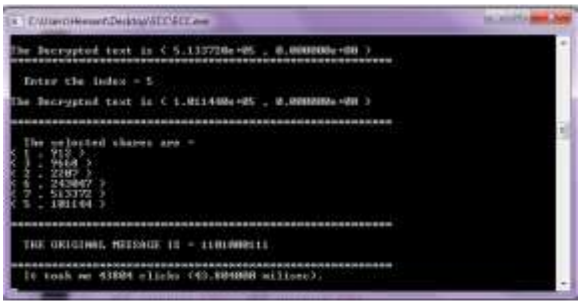
```
************************************************************

        WELCOME TO THE WORLD OF CRYPTOGRAPHY

************************************************************

WE ARE GOING TO IMPLEMENT ELLIPTIC CURVE BASED THRESHOLD CRYPTOGRAPHY. WE WILL D
IVIDE OUR MESSAGE INTO NUMBER OF SHARES USING THRESHOLD CRYPTOGRAPHY.

ENTER YOUR MESSAGE ( M ) IN BINARY FORM - 1101000111

Enter the number of shares you want - 7

Enter the threshold value - 6

*******************************************************

Our polynomial is

 839 x^0  +  11 x^1  +  19 x^2  +  17 x^3  +  27 x^4  +  1 x^5

*******************************************************

Shares generated are like :

 (  1 , 914  )
 (  2 , 1537  )
 (  3 , 3932  )
 (  4 , 10211  )
 (  5 , 23494  )
 (  6 , 48029  )
 (  7 , 89312  )

************************************************************
```



```
************************************************************

NOW WE WILL ENCRYPT EACH OF THE SHARES USING ELLIPTIC CURVE CRYPTOGRAPHIC ALGORI
THM. USING THIS ECC ALGORITHM OUR SHARES WILL GET CONVERTED INTO CIPHER TEXTS. T
HESE CIPHER TEXTS ARE THEN TRANSMITTED.

**********************************************************

THIS IS THE TRANSMITTER END :

************************************************************


THE ENCRYPTED SHARES ARE :

  Index        C1(X)          C1(Y)            C2(X)            C2(Y)
|   1    | 1.127673e+01 | -1.236031e+02 | 9.330000e+02 | -1.691526e+02 |
|   2    | 1.127673e+01 | -1.236031e+02 | 1.556000e+03 | -1.691526e+02 |
|   3    | 1.127673e+01 | -1.236031e+02 | 3.951000e+03 | -1.691526e+02 |
|   4    | 1.127673e+01 | -1.236031e+02 | 1.023000e+04 | -1.691526e+02 |
|   5    | 1.127673e+01 | -1.236031e+02 | 2.351300e+04 | -1.691526e+02 |
|   6    | 1.127673e+01 | -1.236031e+02 | 4.804800e+04 | -1.691526e+02 |
|   7    | 1.127673e+01 | -1.236031e+02 | 8.933100e+04 | -1.691526e+02 |

**********************************************************
```



```
**********************************************************

THIS IS THE RECEIVER END :

**********************************************************

Enter the number of shares you want to use for recovering the message - 5

Enter the index of the shares you want to select for the recovery of the message
:
************************************************************

Enter the index - 1

The Decrypted text is ( 9.140000e+02 , 0.000000e+00 )
************************************************************

Enter the index - 3

The Decrypted text is ( 3.932000e+03 , 0.000000e+00 )
************************************************************

Enter the index - 2

The Decrypted text is ( 1.537000e+03 , 0.000000e+00 )
************************************************************

Enter the index - 6

The Decrypted text is ( 4.802900e+04 , 0.000000e+00 )
************************************************************

Enter the index - 7

The Decrypted text is ( 8.931200e+04 , 0.000000e+00 )

************************************************************
```



```
The Decrypted text is ( 5.133720e+05 , 0.000000e+00 )
************************************************************

 Enter the index - 5

The Decrypted text is ( 1.811440e+05 , 0.000000e+00 )

************************************************************

 The selected shares are -
( 1 , 912 )
( 3 , 9668 )
( 2 , 2207 )
( 6 , 243047 )
( 7 , 513372 )
( 5 , 181144 )

************************************************************

 THE ORIGINAL MESSAGE IS - 1101000111

************************************************************
 It took me 43004 clicks (43.004000 millisec).
```

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

6. Observations

After implementation of the algorithm we observed cases of outputs which include the encryption and decryption of plaintext 'm' and the time taken for the operation. The outputs are are represented in a tabular form in the Table 6.1.

Table 1: Total Encryption and decryption time

Message bit in binary	Shares(n)	Threshold value (t)	No. of shares to recover message	Time in mili Secs
11000110	5	3	3	11.52 s
110111000	6	4	4	16.19 s
001111110	7	5	5	21.46s
1111110000	8	7	6	22.42s
11010110000	9	6	5	24.21 s
10000011010	10	7	7	29.78s
110010	11	8	6	33.04s

The values of the time taken by each operation such as encryption and decryption in association with the number of shares , threshold values and number of shares to recover the original message bit are further represented in a graphical format in the figure 6.1.

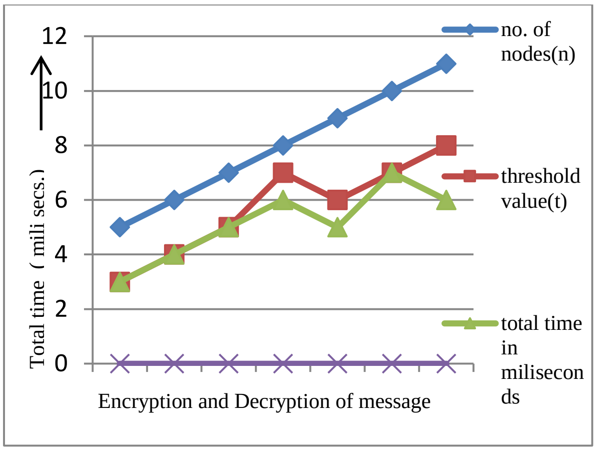


Figure. 6.1 Graph showing total time taken by ECC-TC algorithm

In the figure 6.1 we have represented the time taken for Encryption and Decryption with respect to the original message in the x axis. The y axis of the graph represents the clock cycles that are time taken by the above mentioned operations.

7. Result

With the observations incorporating the implementation of ECC-TC algorithm we can deduce to a result that the security provided by ECC algorithm is enchanced by its integration of threshold cryptographic schme(TC).The implementation of the ECC-TC algorithm in the above section gives us the proper functionality of an efficient, fast and reliable algorithm with exceptional rate of encryption and decryption time and storage efficiency. This technique proves to be robust and hard to break algorithm for securtiy which is majorly in demand.[9]

8. 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.

9. 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 .