Secure communication for mobile Adhoc network using (LPIT) Lagrange polynomial and Integral transform with Exponential Function

Sumee Rai
Student, CS
Shobhit University,
Meerut-250110

Nidhi Tyagi
Associate Professor, CS
Shobhit University,
Meerut-250110

Pradeep Kumar
Assistant Professor, CS
JSSATE, UPTU
Noida-201301

Abstract—Mobile adhoc network is collection of autonomous nodes that are frequently moving without the centralized control. Mobile adhoc networks are multi hop wireless networks without fixed infrastructure. Node frequently change topology, due to this type of behavior transformation of information from one node to another node is more complicated task. Decentralized nature of mobile adhoc network is more vulnerable to attack like denial of service (DOS) which consumes more bandwidth and resources. Security is major concern in adhoc network, so in this paper, we propose a new algorithm based on Lagrange polynomial and Laplace transform and inverse Laplace transform to enhance secure communication for MANET. This proposed algorithm provides security for transmission of information among node.

Keywords—Mobile adhoc network, Lagrange Interpolation, Threshold Cryptography, Modular Arithmetic, Integral Transform

I. INTRODUCTION

Adhoc network is self-dependable infrastructure less network. Every node moves independently and communicates with each other without the help of any central control. Connection among mobile nodes are made through waves, topology changes dynamically during over all process of communication. Due to inherent characteristic of MANETs: open medium, lack of centralized control, dynamic movement of node ,etc, MANETs are highly vulnerable to attacks.

Problem formulation: Main problem is highly secure communication among MANET node, so we proposed a secure algorithm based on Lagrange Polynomial and Laplace Transform.

II. BACKGROUND

Threshold Cryptography is the way to enhance security by creating partial secret shares and distribute among a set of n values based on node id. In a threshold cryptography scheme, out of n entities, we choose t (threshold value) entities (t<n) and calculate secret information on the basis of polynomial function.

Quantum Cryptography (QC) depends on the uncertainty principle of quantum with which it is impossible to for an eavesdropper to detect the data being transmitted without disturbing the transmission. This method is not based on mathematics instead it is developed on the base of physics. The changes made by the eavesdropper will anonymously introduce high error rate in the transmission between sender and receiver. It makes use of photons (light particles) to generate keys. Provably secure key distribution is achieved by using two channels between sender and receiver. Public and quantum channels are used to transmit encrypted data and key distribution respectively.

Integral transform has many applications in various fields such as Mechanics, Electrical circuit, Beam problems, Heat conduction, Wave equation, Transmission lines, Signals and Systems, Control systems, Communication Systems, Hydrodynamics, Solar systems. In this paper, we will discuss application of cryptography. In Shamir's idea of identity-based cryptosystem [3], the recipient's identity i is used to generate the encryption key, and the decryption key is derived from I and a random seed k. In an identity-based signature scheme, the signature key is generated from sender identity I and a random seed k, and the verification key is derived from sender's identity i.

Many IBC schemes [3,6] use threshold cryptography which originated from Shamir , for their key management. Shamir gives a solution to the problem of sharing a secret among a number of users. In his paper, he identifies the problem of how to divide data D into n pieces in such a way that D is easily reconstruct able from any t pieces, but even complete knowledge of $t-1$ pieces reveals absolutely no information about D.

In [8] a distributed pair wise key establishment scheme based on the concept of bivariate polynomials. In their method, any mobile node in an ad hoc network can securely communicate with other nodes just by knowing their corresponding IDs. The bivariate polynomials are shared in such a manner that the shares depend on the coefficient matrix of the polynomial, the requesting node's ID and the ID of the nodes that respond to the request.

Identity-based cryptography specifies a cryptosystem in which both public and private keys are based on the identities of the users.[3,6] The idea of IBC was first proposed by Shamir in 1984.[7] Such a scheme has the property that a user's public key is an easily calculated function of his identity, while a user's private key can be calculated for him by a trusted authority, called a Private Key Generator (PKG).Compared to traditional PKI, it saves storage and transmission of public keys and certificates, which is especially attractive for devices forming MANETs. The identity based cryptosystem [9] and shared the session key among the nodes of MANET. Identity based cryptosystem provides a new but safe strategy for communication in MANET, Strategy uses Lagrange interpolation to share the session key among the nodes of MANET. This paper realizes the safe communication in the MANET. Integral transformation based encryption provide higher secure algorithm. In this process use Laplace and inverse Laplace transformation. Algorithm which makes it suitable for embedded systems that require high performance; ease of implementation, high speed, low power consumption and low cost beside security.

Proposed Security Architecture and Mechanism for wireless Information Transmission

The architecture and detailed mechanism is discussed in section discus below respectively.

III. SECURITY ARCHITECTURE

Figure illustrates the working architecture based on threshold cryptography, Lagrange polynomial and Integral transformation. The proposed architecture is divided into modules like Generate session key using node id at both sender and receiver side, encryption using Integral transformation and decryption done by inverse integral transformation method using exponential function.

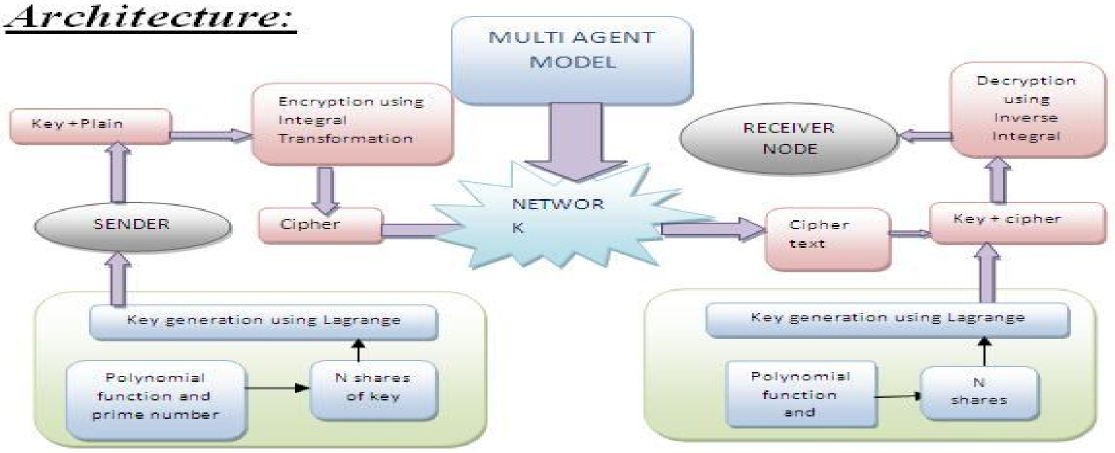
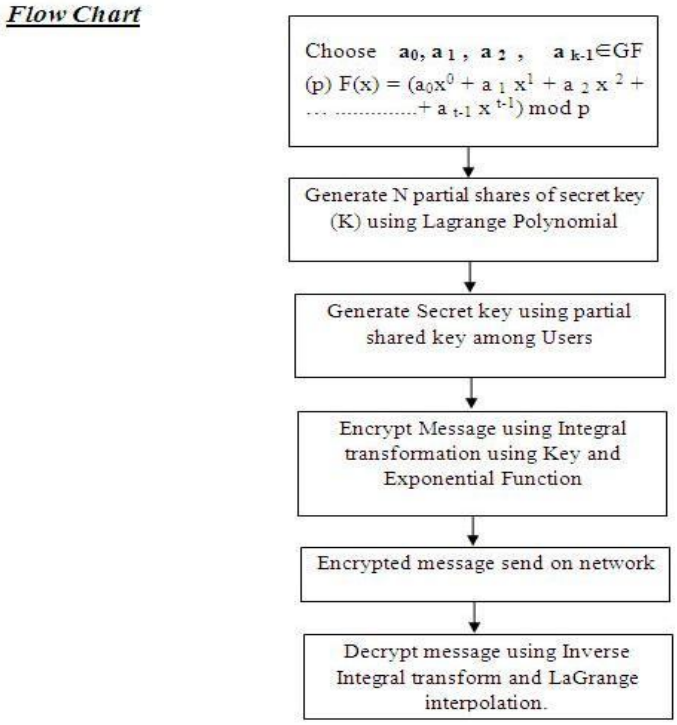

Architecture:
MULTI AGENT MODEL
Key+Plain
Encryption using Integral Transformation
SENDER
Cipher
NETWOR K
Cipher text
Key + cipher
Decryption using Inverse Integral
RECEIVER NODE
Key generation using Lagrange
Polynomial function and prime number
N shares of key
Key generation using Lagrange
Polynomial function and
N shares

Fig. 1 Secure Architecture based on Threshold Cryptography


Flow Chart
Choose $a_0, a_1, a_2, \quad a_{k-1} \in GF(p)$ $F(x) = (a_0x^0 + a_1 x^1 + a_2 x^2 + \ldots \ldots + a_{t-1} x^{t-1}) \bmod p$
Generate N partial shares of secret key (K) using Lagrange Polynomial
Generate Secret key using partial shared key among Users
Encrypt Message using Integral transformation using Key and Exponential Function
Encrypted message send on network
Decrypt message using Inverse Integral transform and LaGrange interpolation.

Flow Chart

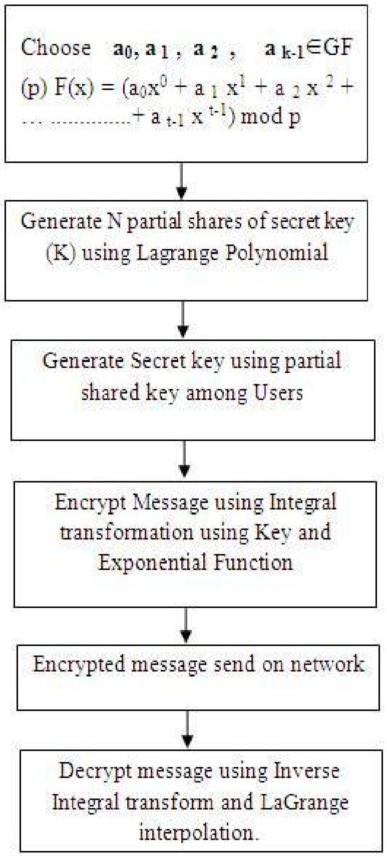

Choose $a_0, a_1, a_2, \quad a_{k-1} \in GF$ (p) $F(x) = (a_0x^0 + a_1 x^1 + a_2 x^2 + \ldots \ldots\ldots\ldots + a_{t-1} x^{t-1}) \bmod p$
Generate N partial shares of secret key (K) using Lagrange Polynomial
Generate Secret key using partial shared key among Users
Encrypt Message using Integral transformation using Key and Exponential Function
Encrypted message send on network
Decrypt message using Inverse Integral transform and LaGrange interpolation.

Fig. 1 Flow Chart for generating partial keys, Encryption and decryption

IV. KEY GENERATION, ENCRYPTION AND DECRYPTION

Step -1 Key Generation

In the first Module of key generation we explain about how we generate the session key by using threshold cryptography and Lagrange interpolation with modularithmetic to generate session key required Minimum t_{Th} (**Threshold value**) no of node in cluster. Consider a Polynomial equation GF (p) is Finite field p>n

Choose $\mathbf{a_0, a_1, a_2, \quad a_{k-1}} \in GF$ (p)

$$F(x) = (a_0x^0 + a_1 x^1 + a_2 x^2 + \ldots \ldots\ldots\ldots + a_{t-1} x^{t-1}) \bmod p$$

F(0)= a_0=secret key (SK) and p is a huge prime number and $a_1, a_2\ldots$, and a_{k-1} are arbitrarily chosen from Z/PZ. Then each user of identity id is provided with it partial key

S_i = f (idi). Their shares provide t distinct points (x, y) = (i, S_i) calculate polynomail by using lagrange interpolation [5]

$F(x) = \sum_{i=1}^{k} Y_i \prod_{1\le j\le k, j\ne i} \frac{X-X_j}{X_i-X_j}$Eq-1

Lagrange interpolation Since f (0) = a0 = S, the shared secret can be expressed as

$$k = \sum_{i=1}^{k} D_i Y_i$$

Where

$$D_i = \prod_{1\le j\le k, j\ne i} \frac{X_j}{X_j - X_i}$$

Secret key is genrated by t arbitary node(minimum no of threshold node) by using F(0)=$a_0$modp=(SK)

Step-2 Encryption Process

Introduction to the Integral Transform Method

The foundation of Integral theory is Lerch's cancellation law. The direct Integral transform or the integral of a function f (t) defined for $0 \le t < \infty$ is the ordinary calculus integration problem

L\{f(t)\}= F(s)= $\int$ f(t)e^{-st}dt
L^{-1} \{F(S)\}=f(t)
L^{-1} is inverse Integral transform.
Integral transformation is linear function that satisfies following

1. L{f(t) ±g(t)}= L{f(t)} ± L{g(t)}
2. L{d$_1$f(t) = d$_1$L{f(t)} d$_1$ is constant.

There are many application of Laplace transform like to solve differential equation, in physics and engineering. In this paper we use Laplace transformation to provide the security of information during transmission from one node to another node in mobile Adhoc network inter and intra communication.

Using exponentail function

$$e^{kx} = 1 + \frac{kx}{1!} + \frac{(kx)^2}{2!} + \frac{(kx)^3}{3!} + \cdots,$$

k any real no.Multiply both sides by x

$$xe^{kx} = x(1 + \frac{kx}{1!} + \frac{(kx)^2}{2!} + \frac{(kx)^3}{3!} + \cdots),$$

k any real no.

$$xe^{kx} = x1 + \frac{kxx}{1!} + \frac{x(kx)^2}{2!} + \frac{x(kx)^3}{3!} + \cdots,$$

k is shared key generated by LaGrange polynomial.

A	B	C	D	-	-	Z
0	1	2	3	-	-	25

Let us consider plain text

$$f(x) = Pxe^{kx} = P0x1 + P1\frac{kxx}{1!} + P2\frac{x(kx)^2}{2!} + P3\frac{x(kx)^3}{3!} + P4\frac{x(kx)^4}{3!} + P5\frac{x(kx)^5}{3!} \ldots,$$

$$f(x) = Pxe^{kx} = x(P01 + P1\frac{kxx}{1!} + P2\frac{(kx)^2}{2!} + P3\frac{(kx)^3}{3!} + P4\frac{(kx)^4}{3!} + P5\frac{(kx)^5}{3!} \ldots),$$

$f(x) = \sum_{n=0}^{\infty}(Pn\ 2^n x^{n+1} / n!)$

Taking Integral transform both side

$$\mathrm{L}f(x)\} = L\{Pxe^{kx}\} = L\{x(P01 + P1\frac{kxx}{1!} + P2\frac{(kx)^2}{2!} + P3\frac{(kx)^3}{3!} + P4\frac{(kx)^4}{3!} + P5\frac{(kx)^5}{3!} \ldots),\}$$

$$\mathrm{L}\{f(x)\}=\left(\frac{G0}{Sn} + \frac{G1}{S3} + \frac{G2}{S4} + \frac{G3}{S5} + \frac{G4}{S6} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \right)$$

Modular Arithmetic

Modular Arithmetic discovered by K.F. Gauss. Two numbers a and b are said to be equal or congruent modulo n iff n|(a-b), i.e. iff their difference is exactly divisible by n. Usually a, b, are nonnegative and n a positive integer.

We write a = b (mod n).

C$_i$=G$_i$ mod26 for i=0, 1, 2, 3……………………n
Ci=G$_i$-26d$_i$for i=0, 1, 2, 3……………………n
All d$_i$ for i=0, 1, 2, 3……………n Sharable between sender and receiver .
C$_0$, C$_1$,C$_2$, C$_3$, C$_4$ ……..Cn are Cipher text of Plain text P$_0$, P$_1$, P$_2$,P$_3$, P$_4$…………….Pn

Step-3 Decryption Process

G$_i$=Ci+ 26d$_i$for i=0, 1, 2, 3……………………n using d$_i$ generate all G$_i$

$\mathrm{L}\{f(x)\}=\left(\frac{G0}{S1} + \frac{G1}{S3} + \frac{G2}{S4} + \frac{G3}{S5} + \frac{G4}{S6}\right)$

Taking inverse Laplace transforms both sides
using LaGrange interpolation generate session key and generate P$_0$, P$_1$, P$_2$,P$_3$, P$_4$……….Pn

Mechanism for secure Information transmission

The proposed mechanism is divided into main three phases as follows.

PHASE-1: Secret Key Generation using LaGrange interpolation polynomial

- Random no generator generate node id.
- Using node id Generate shared information of secret key

- We fixed threshold no of node id ,to regenerate secret key
- Consider a Polynomial equation GF (p) is Finite field p>n
- Choose **a_0, a_1 , a_2 , a_{k-1}**∈GF (p)

$$g(x) = (a_0x^0 + a_1 x^1 + a_2 x^2 + \dots + a_{t-1} x^{t-1})\ \textbf{mod p}$$

```
Total No of user=N;
    for(i=0; i<t; i++)
            {Id[i];
            }
    for(i=0; i<t; i++)
    { nr=1;
    dr=1;
    for(j=0; j<t; j++)
                  {
    If($j \neq i$)
                  {
    nr=nr*(x-Id[j]);
    dr=dr*(Id[i])- Id[j]);
    g(x)=(nr/dr)*FId[i]));  /*Polynomial Equation generated by node id*/
                  }
                  Put the value of x and Generate Secrete KEY;
         Sk=g(x)mod p;  /*SK-Session Key*/
/*session key use for secure communication among nodes.*/
```

PHASE-2: Encryption

- Secret key generate from LaGrange polynomial use as key in Integral transform
- Generate secure message using Integral transform.

PHASE-3: Decryption

- Generate session key using shared partial information
- Decrypt message using inverse integral transformation.

EXAMPLE

Key Generation

Choose **a_0, a_1 , a_2 , a_{k-1}**∈GF (p)

$$F(x) = (a_0x^0 + a_1 x^1 + a_2 x^2 + \dots \text{.............}+ a_{t-1} x^{t-1}) \text{ mod p}$$

$a_0 =2$, $a_{1,}$ $a_{2=1\ ,a3=1}$

let us consider node id generated by random no generator

consider 4 node

id0=0 id1=1,id2=2,id3=3 prime no p=5,

plynomail equation

f(x)=(x3+x2-x+2)mod5

generate partial key using lagrange polynomail

f(0)=2, f(1)=3, f(2)=12, f(3)=5, these partial key send to reciver side ,reciver generate session key using these partial key.

k=f(0)=2mod5=2

Encryption Process

Let us consider plain text
MONDAY
P_0=12, P1=14,P2=15,P3=3,P4=0,P5=24

$$f(x) = Pxe^{kx} = P0x1 + P1\frac{kxx}{1!} + P2\frac{x(kx)^2}{2!} + P3\frac{x(kx)^3}{3!} + P4\frac{x(kx)^4}{3!} + P5\frac{x(kx)^5}{3!} \dots,$$

$$f(x) = Pxe^{kx} = x(P01 + P1\frac{kx}{1!} + P2\frac{(kx)^2}{2!} + P3\frac{(kx)^3}{3!} + P4\frac{(kx)^4}{3!} + P5\frac{(kx)^5}{3!} \ldots),$$

for k=2

$$f(x) = Pxe^{kx} = x(12 + 14\frac{kx}{1!} + 15\frac{(kx)^2}{2!} + 3\frac{(kx)^3}{3!} + 0\frac{(kx)^4}{4!} + 24\frac{(kx)^5}{5!} \ldots),$$

by using Integral transformation ,taking Integral transform both side of give equation consider k generated by Lagrange polynomial,

$\mathrm{L}\{f(x)\} = L\{Pxe^{kx}\} = L\{x\left(12 + 14\frac{kx}{1!} + 15\frac{(kx)^2}{2!} + 3\frac{(kx)^3}{3!} + 0\frac{(kx)^4}{4!} + 24\frac{(kx)^5}{5!} \ldots\right)\}$,

for k=2

$\mathrm{L}\{f(x)\} = L\{Pxe^{2x}\} = L\{x\left(12 + 14\frac{2x}{1!} + 15\frac{(2x)^2}{2!} + 3\frac{(2x)^3}{3!} + 0\frac{(2x)^4}{4!} + 24\frac{(2x)^5}{5!} \ldots\right)\}$,

taking Integral transform both side

$=\frac{12}{s2} + \frac{56}{s3} + \frac{120}{s4} + \frac{136}{s5} + \frac{0}{s6} + \frac{4608}{s7}$

q0=12, q1=56,q2=120,q3=136,q4=0,q5=4608

12=26(0)+12, 56=26(2)+4, 120=26(4)+22, 136=26(6)+0 , 0=26(0)+0 , 4608=26(177)+4

C0=12, C1=4, C2=22 ,C3=0, C4=0 , C5=4 are cipher text

for i=0,1 2 , 3, 4 ,5 ,6 ………… di= 0, 2, 4, 6, 0, 177 shared between sender and receiver.

messages ‘MONDAY’ converted to ‘ MEWAAD’.

Decryption Process

1. using shared partial key generate secured key
   f(0)=2, f(1)=3, f(2)=12, f(3)=5,

   (X0=0 , Y0=2), (X1=1 , Y1=3), (X2=2 , Y2=12) , (X3=3 , Y3=5)

$$F(x) = \sum_{i=1}^{k} Y_i \prod_{1\le j\le k, j\ne i} \frac{X - X_j}{X_i - X_j}\ Modp$$

f(x)=(x^3+x^2-x+2)mod5

f(0)=(0+0-0+2)mod5=2 ,k=2

for i=0,1 2 , 3, 4 ,5 ,6 ………… di= 0, 2, 4, 6, 0, 177

Received message is **MEWAAD**

q0= 26*0+12 =12 q1=26*2+4=56 q2=26*4+22=120q3=26*6+ 0=136

q4=26*0+0=0 q5=26*177+4=4068

$\mathrm{L}\{f(x)\} ==\frac{12}{s2} + \frac{56}{s3} + \frac{120}{s4} + \frac{136}{s5} + \frac{0}{s6} + \frac{4608}{s7}$

taking inverse integral transform both side using k=2

$$f(x) = Pxe^{2x} = x(12 + 14\frac{2x}{1!} + 15\frac{(2x)^2}{2!} + 3\frac{(2x)^3}{3!} + 0\frac{(2x)^4}{4!} + 24\frac{(2x)^5}{5!} \ldots),$$

messages ‘ MEWAAD’ converted to. ‘MONDAY’

V. CONCLUSION

This proposed algorithm is more secure because it is light weighted and in this algorithm first we secure the secret key using Lagrange polynomial and integral transformation this higher secure method to secure key using node id in mobile adhoc network. And after producing key we use this key for encryption and decryption that algorithm based on Laplace transformation and modular arithmetic. Algorithm provides higher security.

VI. FUTURE WORK

In this paper, a secure system for MANET is presented, which solves the problem of scalability of nodes in MANET. We can improve the performance of the system by reducing the communication overhead among nodes.

REFERENCES

[1] M. B. Abdelhalim , M. El-Mahallawy , M. Ayyad , A. Elhennawy , Design & Implementation of an Encryption Algorithm for use in RFID System , International Journal of RFID Security and Cryptography (IJRFIDSC), Volume 1, Issues 1/2, March/June 2012

[2] Mamatha.T , Network Security for MANETS International Journal of Soft Computing and Engineering (IJSCE) , Volume-2, Issue-2, May 2012

[3] Shushan Zhao, Akshai Aggarwal, Richard Frost, Xiaole Bai , A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks , IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 2, SECOND QUARTER 2012

[4] Lu Li, Ze Wang, Wenju Liu and Yunlong , A Certificate less Key Management Scheme in Mobile Ad Hoc Networks 2011 IEEE

[5] A.Rajaram , Dr.S.Palaniswam, A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks , International Journal of Computer Science Issues, Vol. 7, Issue 4, No 5, July 2010

[6] EDUARDO DA SILVA, ALDRI L. DOS SANTOS, AND LUIZ CARLOS P. ALBINI , Identity based key management in
mobile adhoc networks and applications, IEEE Wireless Communications • October 2008

[7] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” CRYPTO’84, LNCS, 1985,

[8] Anindo Mukherjee, Hongmei Deng, Dharma Agrawal , Distributed Pairwise Key Generation Using Shared Polynomials for Wireless Ad Hoc Networks , Center of Distributed And Mobile Computing,University Of Cincinnati, Cincinnati

[9] Li Wang, Jiu Hui Zhang “ Security Strategy of MANET Based on Identity- Based Cryptosystems” 2010 IEEE

[10] XU Xiao-long XIONG Jing-Yi, CHENG Chun-Ling “The Model and the Security Mechanism of the Information Retrieval System based on Mobile Multi- Agent” 2010 IEEE

[11]Derek Williams ,The Tiny Encryption Algorithm (TEA)CPSC 6128 – Network SecurityColumbus State UniversityApril 26, 2008

[12] A. V. Reddy, “A Cryptanalysis of the Tiny Encryption Algorithm”, Master of Science, Department of Computer Science in the Graduate School, The university of Alabama, 2003.

[13].A. P. Hiwarekar* VidyaPratishthan’s A NEW METHOD OF CRYPTOGRAPHY USING LAPLACE TRANSFORM College of Engineering, Vidyanagari, M.I.D.C. Baramati, Dist.Pune, Maharashtra, 2012

[14].Mohammed A. Shreef, Image Encryption Using Lagrange-Least SquaresInterpolation 2013

ABOUT THE AUTHORS

Sumee Rai completed her B.Tech (Information Technology) with Hons. in 2011 from Mahatma Gandhi Mission’s College of Engineering and Technology, Noida (U.P) and currently pursuing M.Tech (Computer Engineering) from Shobhit University, Modipuram, Meerut. Her research interest includes Mobile Adhoc Network, Algorithm analysis and Mobile Communication.

Nidhi Tyagi received her Ph.D. in Computer Engineering & IT, from Shobhit University, Modipuram, Meerut. Presently she is working as Associate Professor at Shobhit University, Meerut. Her area of interest includes system software, Data Structures and web technologies.

Pradeep Kumar is working as an assistant professor in JSS Academy of Technical Education, Noida (U.P). He received his M.Tech. in Computer Engineering from Shobhit University, Meerut in 2011 and completed his B-Tech from College of Engineering, Roorkee, Uttrakhand in 2005. His area of interest includes MANET and Network Security.