A CRT based Encryption Methodology for Secure Communication in MANET

Ditipriya Sinha
Calcutta Institute Of Engineering & Management
24/1A Chandi Ghosh Road, Kol-92

Uma Bhattacharya
Bengal Engineering And Science University,Shibpur
P.O.Botanic Garden,Shibpur, Howrah: 711103

Rituparna Chaki
West Bengal University Of Technology
BF-142, Sector-1, Saltlake

ABSTRACT
MANETs are well known for their flexibility and ease of communication. The communication is purely based on trust, without any need of authentication. This often leads to insecure communication, causing information tampering. The traditional means of security are not sufficient to safeguard against the inherent dangers of MANET. Researchers around the world are working in this issue. The preferred mode of securing data is through encryption. The process of encryption however is complex enough to increase the computational overhead. This paper proposes a secure encryption strategy using Chinese Remainder Theorem for shielding data from unauthorized access. The paper also includes a comparison of proposed method with existing methods

General Terms
CRT based key generation and secure route detection for secure communication.

Keywords
Chinese Remainder Theorem, Safety Key, Super Key, Lagrange's Interpolation.

1. INTRODUCTION
Security of information is a challenging issue in mobile ad-hoc network. Application of mobile ad-hoc networks are extended to military service, emergency service, confidential video conferencing etc. For this reason security plays [1] an inevitable role in this field. Every node in MANET is identical with respect to all functionalities. Ensure a secure environment in MANET is very challenging. Sharing of secret values in this network is inconsistent and computationally insecure. Key generation, encryption and decryption play an important role for providing secure routing in MANETs. However these schemes increase computational overheads for all nodes in the network.

Secret sharing in MANETs is a challenging issue due to its dynamic nature. Many researchers are involved in solving the secret sharing problem. Shamir's [2] proposal is one of the eminent secret sharing schemes. This scheme uses the concept of Lagrange's Interpolation method, a popular technique for polynomial evaluation. Shamir's scheme divides the data packet into n pieces such that it can be easily reconstructed from any k number of pieces.

Chinese remainder theorem uses the result about congruence in number theory [3] and its generalizations in abstract algebra. CRT is useful for key generation. In RSA-CRT, it is a common practice to employ the Chinese Remainder Theorem during decryption. It results in a decryption much faster than modular exponentiation. RSA-CRT differs from the standard RSA in key generation and decryption. For secret information leakage CRT is also used.

There exists many dimension of research on security in MANETs. There are mainly three objectives for secure routing. They are- 1) There are no single point failure.2) All nodes are authorized and trustworthy. 3) Data should be transmitted in secure and confidential way from source to destination. Proposed security protocol obeys above mentioned three objectives of secure routing.

This paper proposes a new security scheme in MANETs. This paper uses combination of RSA and CRT schemes for key generation, encryption and decryption of data. In this paper encryption is done using RSA scheme. On the other hand encrypted data is decrypted with the help of CRT scheme. Computational complexity of CRT is less than RSA modular exponentiation scheme. For this reason CRT scheme is used in this proposed scheme. Detection of secure routes is another goal of this proposed work. For secure route detection this paper creates safety key. This safety key is divided into n pieces in such a way that safety key is easily reconstruct from any k pieces. These pieces are shared among n different routes to detect whether the routes are secure or not. Secure paths are detected with the help of Shamir's secret sharing using Lagrange's Interpolation scheme. This algorithm combines the concepts of RSA, CRT and Shamir's secret sharing. These combinations provide secure environment in MANETs.

2. REVIEW
The ***Chinese Remainder Theorem*** [4] has been in use for quite a long time in the field of deterministic key pre-distribution. CRT generates key pool and key chain for key pre distribution. One of the applications of this theorem is encryption and decryption of data sequences. This technique is used in various secure routing protocols for key generation.

Chinese Remainder Theorem-Based RSA –Threshold Cryptography in MANET using Verifiable secret sharing. ***Scheme*** [4,5] is one of them. This paper implements Threshold cryptography based schemes for MANETs using Variable Secret Sharing Scheme. Threshold cryptography provides a promise securing network. This proposed scheme is based on Chinese Remainder Theorem under the consideration of Asumth-Bloom secret sharing. In this protocol key is generated using the concept of RSA key generation. Unlike RSA no public and private key generate in this algorithm. CRT is also used for key generation. Key is shared among network using Asumth-Bloom secret sharing scheme. Computational complexity for key generation is high in this algorithm.

An efficient and attack resistant key agreement scheme for secure group communications in mobile adhoc networks [6] is another example where CRT is used for key generation.

Main objective of this work is to reduce problems of secure group communication SGC and key management over MANETs. It identifies key features of SGC scheme over MANETs. This paper proposes Chinese Remainder Theorem based DH contributory key agreement protocol. This protocol gives the concept of Group Key GK. Here GK is generated by the contribution of all members in the group. This algorithm takes care of selection of group members. This protocol also concerns about problem of leave the member from the group. For security of group key this protocol uses the concept of CRT.

Shamir's Secret Sharing [2] is one of the pioneer papers in this area. It used Lagrange's Interpolation technique for encryption of data sequences. Shamir had proposed a method for dividing a data sequence D into n fragments in such a way that D can be easily reconstructed from any k pieces. This technique enables the construction of robust key management for cryptographic system. This scheme provides a secure key management scheme. This technique has been used by many researchers for secure routing in MANET.

Secure Routing Scheme in MANETs using Secret Sharing [5,7] proposes a secret sharing scheme using this method. Here secret is shared to detect malicious nodes in the network. For the key transmission RSA scheme is used in this paper. The key is encrypted using node's public key and then transmitted to them. The original secret key can be reconstructed by applying private key for their corresponding public key encrypted data. This scheme uses RSA modular expansion for decryption whose computational cost is high than CRT method.

Location Aided Secure Scheme In Mobile Adhoc Network [8] propose a routing scheme that uses geographical position information to reduce intermediate nodes that make a routing path. It gives guarantee of reliability and security of route establishment process. To achieve this protocol uses concept of projection line and shadow line. Here all nodes maintain a safety table. This table concerns about the behavior of neighbor nodes. This table detects all activities of misbehaving nodes. For route detection source node chooses secure path with the help of this safety table.

An Encryption Based Dynamic and Secure Routing Protocol for Mobile Adhoc Network [9, 10] prevent attackers and malicious nodes from tampering with communication process and also prevents a large number types of Denial Of Service Attack. It uses symmetric key cryptography. The goal of this protocol is to detect malicious activities of a node and mitigate them.

Key Management Scheme For Secure Communication In Hetarogenious Sensor [11] proposes a new key management scheme in heterogeneous sensor network. The first scheme proposes tree based scheme and second scheme is based on CRT based scheme. The proposed scheme describes how actually keys are changed in order to reconfigure compromised links when nodes are compromised.

Secure Routing for Wireless Mesh Network [12,13] proposes a security enhanced AODV routing protocol. This paper employs Blom's key predistribution scheme to compute the pairwise transient key to distribute group transient key. It is more effective in preventing routing attack.

3. SCOPE OF THE WORK

A successful approach for dealing with maintenance of mobile adhoc networks is security by generating keys in the network. Key generation and secret sharing help improve routing security. Very few routing protocols concern about security in the network.

The proposed algorithm addresses the problems of key generation and secret sharing. This protocol concerns on public and private key generation with less computational overhead and avoids routes which are not secure.

4. CASE STUDY

Figure 1 shows a network with six nodes. Suppose source node S wants to send messages to destination node E.

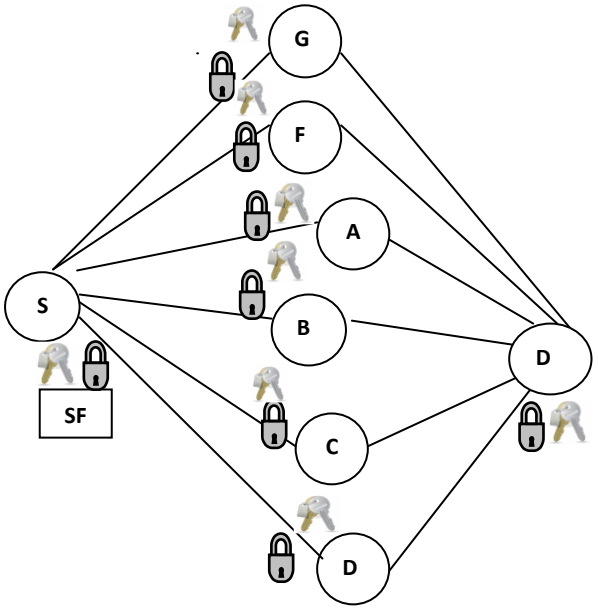

Figure 1: A network with six nodes

At first, S broadcasts RREQ message. Neighbors of S (A,B,C,D,F,G) receives this message from S. They again broadcast it to its neighbor. E receives this message from A,B,C,D,F,G. E compares destination node id with its id and discovers both of them are same. E sends ACK messages to S through those routes from which it receives RREQ message. On that basis S creates its own routing table for E.
Routing table of node S is shown below:

Table 1: Routing Table Of Node S

S	S->A->E
S	S–>B–>E
S	S->C–>E
S	S->D–>E
S	S->G–>E
S	S->F–>E

All nodes in the network maintains two keys, they are public and private. These keys are used for encryption and decryption of message respectively. S encrypts messages using its public key of destination node E.E decrypts messages using its private key of its own. For this reason each node maintains a KEY table. KEY table describes public key of all neighbor nodes in the network. For encryption S uses RSA algorithm and E decrypts the messages with CRT instead of modular expansion method of RSA due to its less computational cost.

At first S generates a safety key SF using CRT. S divides this safety key into 6 portions. Among these 6 portions [6/2]=3 portions can reconstruct safety key SF. S generates a polynomial F(x) of degree2 such that $F(x)=SF+a_0x+a_1x^2$. S generates different points from the polynomial F(x) in such a way that any three of them can be used to reconstruct the polynomial F(x).These six points are taken as $(x_0,F(x_0))$,$(x_1, F(x_1))$,$(x_2, F(x_2))$,$(x_3, F(x_3))$,…$(x_5, F(x_5))$.where $F(x_i) = y_i$.
Suppose S generates the number 1234 using CRT. Then a polynomial F(x) is created such that,

$$F(x) = 1234 + 166x + 94x^2$$

Suppose S uses two random numbers 166 and 94. Then SF=1234. The six points generated by S are as follows-

Table 2

x_0=1	y_0=1496
x_1=2	y_1=1942
x_2=3	y_2=2578
x_3=4	y_3=3402
x_4=5	y_4=4414
x_5=6	y_5=5614

S encrypts those six points and sends those six points to destination E through six available paths. The destination node E decrypts those points using its private key and CRT. E again encrypts those points with public key of S and sends through six different paths to source node S. S decrypts those points with its own private key.
S takes any three points from those six points and generates polynomial $F_1(x)$ using Lagrange's Interpolation Theorem.
Suppose S takes (2,1942) ;(4,3402);(5,4414)

$$l_0 = \left[\frac{(x-x_0)}{(x_0-x_1)}\right]\left[\frac{(x-x_2)}{(x_0-x_2)}\right]$$
$$= \frac{1}{6}x^2 - \frac{1}{2}x + 1$$

$$l_1 = \left[\frac{(x-x_0)}{(x_1-x_0)}\right]\left[\frac{(x-x_2)}{(x_1-x_2)}\right]$$
$$= \frac{1}{2}x^2 + \frac{3}{2}x - 5$$

$$l_2 = \left[\frac{(x-x_0)}{(x_2-x_0)}\right]\left[\frac{(x-x_1)}{(x_2-x_1)}\right]$$
$$= \frac{1}{3}x^2 - 2x + \frac{4}{3}$$

$F_1(x) = y_0l_0 + y_3l_1 + y_4l_2$

$$= 1496l_0 + 3402l_1 + 4414l_2$$
$$= 1234 + 166x + 94x^2$$

SF_1=1234

If $SF==SF_1$, these three points are valid and routes from which those three points are come also valid. Other wise any of points among three points are invalid and malicious nodes present on that routes from which those points are received by S. S again chooses another combination of three points among six available points and checks its validity. This way S finds secure routes and avoids non secure routes in network. Now, S sends all its messages to E through those secure paths.

5. PROPOSED WORK

5.1 Description Of Proposed Work

Each node in the network creates two keys for encryption and decryption of messages. Every node generates one public key and one private key. For key generation all nodes in the network uses the concept of RSA as well as CRT(Chinese Remainder Theorem).Each node also creates another key which is different from public and private key. This key is called safety key. This safety key is used to detect the routes from source to destination where there are no malicious nodes. Source node determines this with the help of Largeness Interpolation Theorem and Shamir's Secret Sharing.
At first source node broadcasts RREQ message to all its neighbors. The neighbor nodes forward it and this process continues until destination node is found. Destination node receives different RREQ packets from different routes and returns ACK messages through those routes to source node. Source node creates routing table and stores all route information in this table.
Now source node generates the super-key (SF) using CRT. The SF is then divided into n part by the source node. A k-subset of these n parts can be used to reconstruct the SF. Source node determines value of n on the basis of available routes to the destination. Source node creates a polynomial F(x) with degree n and generates n number of points. It encrypts all those points with public key of destination node using RSA. All these encrypted n points are sent by source node to the destination node through n number of different routes. Destination node decrypts it with its private key using CRT (Chinese Remainder Theorem)[1,3]. It again resends all these points in encrypted form to source node with public key of source node through n number of different routes. Source node decrypts all the encrypted points with private key of it using CRT. Now source node using Larange's Interpolation Theorem reconstructs polynomial using k set of points from n set of points and determines constant with no coefficients (SF1).If SF1=SF, these k points are valid else they are invalid. This invalid set of k points is coming from k different paths. One of these paths is not secure due to the presence of malicious nodes. Source node avoids these k paths and accepts those k paths whose k points construct valid set. Source node sends messages to the destination node through these secure k paths in encrypted form. Receiver decrypts this message using CRT. This way all messages are sent to the destination node securely.

5.2 Key Generation

Each node maintains two keys, one is public key and another is private key. Keys are generated following ways:

1) Each node generates two prime numbers p,q.
2) N=pq.
3) Ǿ(N)=(p-1)(q-1).
4) Choose e such that e is not divisor of Ǿ(N) and 1<e< Ǿ(N).

5.3 Encryption

When source node wants to encrypt message for sending it to destination node, it uses public key of destination node using RSA following way:

$$C = M^e \pmod N$$

Where,
C=ciphertext.
M=plaintext
e,N=public key of destination node.

5.4 Decryption

When destination node receives the encrypted message it decrypts this encrypted message using CRT in the following manner:

$dp = d \bmod (p-1)$.
$dq = d \bmod (q-1)$.
$q_{inv} = q^{-1} \bmod p$.
$m_1 = C^{dp} \bmod p$.
$m_2 = C^{dq} \bmod q$.
$h = (q_{inv} * (m_1 - m_2)) \bmod p$.
$M = m_2 + h*q$

Where,
p,q= Two prime numbers such that N=p.q.
d,N=private key of destination node.

5.5 Safekey Generation

Before sending message source node generates Safekey using CRT. Generation of super key is determined following way:

1) Source node generates n integers $m_1,m_2,m_3,\ldots\ldots m_n$,such that $gcd(m_i,m_j)=1$.
2) $m= m_1 \bullet m_2 \bullet m_3 \bullet \text{-----} \bullet m_n$.
3) $a_1,a_2,a_3,\ldots\ldots a_n$ are set of integers.
4) $Z \equiv a_1 \pmod{m_1}$
   $Z \equiv a_2 \pmod{m_2}$
   •
   •
   •
   $Z \equiv a_n \pmod{m_n}$
   $Z= a_1y_1z_1 + a_2y_2z_2 + \ldots\ldots\ldots + a_ny_nz_n$
   $z_i = m/m_i$, $y_i = z_i^{-1} \pmod{m_i}$.
5) SF=m.
6) SF is the superkey of source node.

5.6 Description Of Algorithm

Input: A network with n number of nodes.

Output:

- Each node generates its public key and private key for encryption of message.
- It selects routes which are secure and source node sends messages to destination node through secure routes. Source node avoids routes which are not secure.

Variables used:

- **sid:** variable describes identity of source node.
- **desid:** variable describes identity of destination node.
- **(e_{id},N):**public key of id^{th} node.
- **(d_{id} ,N):** private key of id^{th} node.
- **SF:** variable describes safety key generated by CRT.
- **SF1:** variable describes safety key generated by polynomial of degree k through Lagrange's interpolation scheme.
- **R[i][j]**:It describes route between node i and j.
- **SEC[sid][k]**:It describes secure route between node sid and k^{th} node.
- **(x_i,y_i):**It describes x and y value of i^{th} point.

Modules Used:

KEYGENERATOR (id,(e_{id},N),(d_{id} ,N)): This module generates public and private key of id^{th} node. Public and private key generation of id^{th} node is described in section 5.2.

SAFEKEY(sid, SF): This module generates Safekey using CRT. This procedure is described in section 5.5 and returns Safekey SF.

POINTGENERATOR(sid,R[[n],SF,desid, (x_0,y_0),……,(x_{n-1} , y_{n-1})): This module generates n points for all available n paths with the help of Shamir's Secret Sharing using polynomial interpolation

. a. Source node sid divides super key SF into n parts where any subsets of $\left\lfloor \frac{N}{2} \right\rfloor$ (k) pats reconstruct the super key.
b. Source node generates (k-1) random numbers.
c. It creates a polynomial of k degree.

$$F(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$$

Where,
a_0=SF .
$(a_1, a_2 \ldots\ldots, a_{k-1})$are random numbers generated by source node. Now, source node sid generates n points. Each point contains with (x,F(x)) where source node generates x randomly. For distinct x_i's there is one and only one
$F(x_i)=y_i$. for all i.
This module returns n number of points from (x_0,y_0) to (x_{n-1}, y_{n-1}).

SECUREROUTE(sid,(x_0,y_0),……,(x_{k-1},y_{k-1}) ,SF_1):
This module generates Lagrange basis polynomials using following equation

$$F_1(x) = \sum_{r=0}^{k-1} y_r \prod_{i=0, i\neq r}^{k-1} \frac{(x-x_i)}{(x_r-x_i)}$$

SF_1 stores constant part of $F_1(x)$ and returns it.

Algorithm:

i) Source node broadcasts RREQ packets.
ii) Neighbors of source node receive these packets and again broadcast it.
iii) Step (ii) is repeated until destination node is found.
iv) After receiving RREQ destination node sends ACK message through those routes to source node.
v) Source node creates routing table R[][] on the basis of ACK messages it receives from destination node.

vi) Source node calls KEYGENERATOR(sid,(e_s,N),(d_sN)) for generation of public and private key of source node and broadcasts its public key (e_s,N)to all nodes in the network.

vii) Destination node also calls KEYGENERATOR(desid,(e_d,N),(d_d, N)) for generation of public and private key of destination node and broadcasts its public key ,(e_d,N)to all nodes in the network.

viii) Source node generates Safety Key and calls SAFEKEY(sid, SF) module.

ix) Now, source generates n number of points among n number of available routes by calling POINTGENERATOR(sid,R[][n],SF,desid, (x_0,y_0),……,(x_{n-1} , y_{n-1})).

x) Source node encrypts all these n points by calling ENCRYPTION(sid, (e_d,N),(x_0,y_0),…,(x_{n-1} , y_{n-1})) and sends all theses encrypted n points through n different routes with the help of routing table R[][n].

xi) Destination node decrypts all those n points by calling DECRYPTION(desid,(d_d,N),(x_0,y_0),…….,(x_{n-1},y_{n-1})).

xii) Now destination node again sends these n points to source node through those n routes in encrypted form by calling ENCRYPTION (desid, (e_s,N) ,(x_0,y_0),…….,(x_{n-1} , y_{n-1})).

xiii) Source node decrypts those n points by calling DECRYPTION (sid,(d_s N), (x_0,y_0),…,(x_{n-1},y_{n-1})).

xiv) Source node selects k number of points among n number of points.

xv) It verifies whether k routes are secure or not by calling SECUREROUTE (sid,,(x_0,y_0),……..., (x_{k-1},y_{k-1}),SF1).

xvi) If SF==SF1,

k routes from which k points are received by source node are secure and stores in SEC[sid][k].

Else

k routes from which k points are received by source node are not secure and source node repeats steps from(xiv) to(xv) until secure k routes are found.

xvii) Source node sends messages through k secure routes to destination node.

6. PERFORMANCE ANALYSIS

Performance metrics used to evaluate our proposed protocol is-computational complexity. We have compared the performance of proposed protocols with other existing protocol such as Secure Routing Scheme Using Secret sharing. Main objective of this routing protocol is key generation and secret sharing.

6.2 Simulation Environment And Result

6.2.1 Simulation setting

Table 3. Simulation Setting Of The Network Environment.

Name	Value
Channel	Wireless
Propagation	Two Way
Network Interface Type	Wireless Phy
Antenna	Omni Antenna
No of nodes	40
MAC	IEEE 802.11
Simulation Area	600*600 m^2

6.2.2 Result

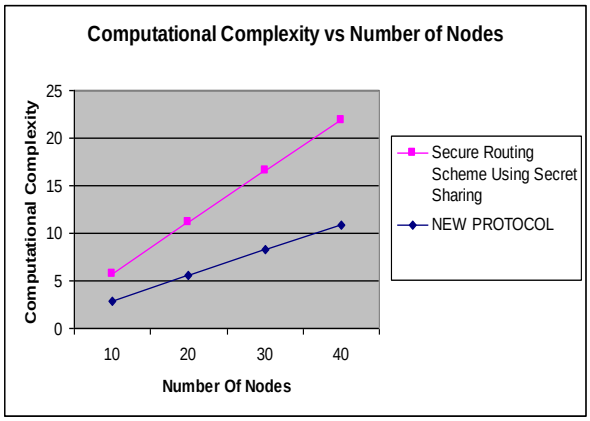

Figure 2: Computational Complexity vs Number Of Nodes

When number of nodes is from 0 to 10, performance of proposed protocol is approximately same with Secure Routing Scheme Using Secret Sharing scheme. After that when number of nodes increase computational complexity of both algorithms increase. Computational complexity of Secure Routing Scheme is always higher than proposed routing protocol. Secure Routing Scheme uses RSA modular expansion for decryption. New protocol uses CRT for decryption whose computational complexity is lower than RSA modular expansion technique. For this reason performance of proposed protocol is always better than Secure Routing Scheme Using Secret Sharing.

7. CONCLUSION

Secure routing is one of the major research areas in MANET. This involves routing of packets in a confidential manner. Much work has been done in this area, most of the researchers have considered RSA algorithm for key encryption. The use of RSA has however increased the overload on the network. This paper proposes the use of Chinese Remainder theorem along with Shamir's secret sharing to reduce the encryption complexities. Secure path detection, encrypted message transformation are main objective of this protocol. This paper

uses Shamir's secret sharing scheme to detect secure routes among all available routes. Source node sends the messages in encrypted form using these secure routes. Thus the proposed protocol not only generates key for encryption and decryption but also generates secure routes for transmitting messages in encrypted form. The simulation results show that performance of proposed protocol is better than Secure Routing Scheme Using Secret Sharing with increase in the number of nodes in the network. More simulation work is being undertaken to taste the overall performance of the proposed scheme.

8. REFERENCES

[1] Y.C.Hu, A Perrig, "A survey of Security Wireless AdHoc Routing",IEEE Security and Privacy ,vol-2,2004.

[2] A.Shamir, "How to share a secret? ", Comm.ACM, vol.22, No-11, 1979.

[3] Tom.M.Apostol, "Introduction To Number Theory", Springer-verlag, 1976.

[4] S.Sarkar,B.Kisku,S.Misra and M.S Obaidat " Chinese Remainder Theorem-Based RSA-Threshold Cryptography in MANET using Verifiable Secret Sharing Scheme" IEEE International Conference On Wireless and Mobile Computing,Networking and Communications,2009.

[5] A.Amuthan and B.Arvind Baradwaj "Secure Routing Scheme in MANETs using Secret Key Sharing", International Journal of Computer Applications(00975-8887) volume 22-No.1,May 2011.

[6] Ravi K.Balachandan,Xukai Zou,Bytrav Ramamurthy,Amardeep Thukral "An efficient and attack resistant agreement scheme for secure group communications in mobile ad-hoc networks",Wireless Communication And Mobile Computing in Willey Interscience,2007.

[7] CK.Kaya and A.A.Seluck, "A Verfiable Secret Sharing Scheme Based On the Chinese Remainder Theorem", INDOCRYPT 2008,LNCS 5365.

[8] Do-hyoen Lee,Sun Choi,Ji-hyoen Choi and Jae-il Jung "Location Aided Secure Routing Scheme in Mobile AdHoc Networks",Springer-Verlag Berlin Heidelberg 2007.

[9] P.Feldman "A practical scheme for non interactive verifiable secret sharing",IEEE Symposium On Foundation of Computer Science.

[10] Pankaj Kumar Sehgal,Rajdeep Nath "A Encryption Based Dynamic and Secure Routing Protocol for Mobile Adhoc Network",International Journal of Computer Science and Security(IJCSS),volume 3-No.1.2009.

[11] A.S Purnima,B.B Amberkar," Key Management Scheme For Secure Communication In Hetarogenious Sensor Network" Techniques for MANETs",International Journal of Recent Trends In Engineering ,volume.1,No-1,May 2009.

[12] P.Papadimitoras and Z Hass, "Secure Data Transmission in Mobile Adhoc Networks",ACM workshop on Wireless Security,Proc of 2003.

[13] Celia Li, Zhuang Wang and Cungang Yang,"Secure Routing for Wireless Mesh Network",International Journal of Network Security,volume.33,No-2,sept 2011.