IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 4, Aug-Sept, 2013
ISSN: 2320 - 8791
www.ijreat.org

Location based Hierarchical Key Management System for Secure Group Communications in MANET based on number of Receivers

Saravanan TR[1], Sakthivel P[2]

[1] **Department of Computer Science and Engineering , Research Scholar, Sathyabama University, Chennai, TamilNadu 600019, India**

[2] **Department of Electronics and Communication Engineering , Associate Professor, Anna University, Chennai , TamilNadu 600025, India**

Abstract

In Mobile Ad Hoc Network (MANET), the secure communication basically depends on key management system. Though several cluster based keying mechanisms exists, the cluster head election is remains tricky. Hence in this paper, we propose a location based hierarchical key management system for secure group communication in MANET. Initially, group heads are selected based on stability index and they splits the nodes into clusters based on their location information. In each cluster, the cluster member with maximum stability index is chosen as cluster head. The procedure of data delivery is to encrypt the packet first by private key, and then encrypt and decrypt it again by cluster key and group key. When the new node wants to join or leave the network, re-keying of cluster and group key is performed. By simulation results, we show that proposed technique improves the network security and minimizes the cost.

Keywords: *Group communication, stability index, Mobile Adhoc Networks (MANET), clusters*

1. Introduction

Secure communication between two nodes in a network depends on reliable key management systems that generate and distribute keys between communicating nodes and a secure routing protocol that establishes a route between them. But due to lack of central server and infrastructure in Mobile Ad hoc Networks (MANETs), this is major problem to manage the keys in the network. In MANETs a mobile node operates as not only end terminal but also as an intermediate router. Therefore, a multi-hop scenario occurs for communication in MANETs; where there may be one or more malicious nodes in between source and destination. A routing protocol is said to be secure that detects the detrimental effects of malicious node(s in the path from source to destination).

In MANET there is no predetermined infrastructure such as base stations or mobile switching centers. The number of nodes in the network is not essentially preset. New nodes may join the network while existing ones may be compromised or become un-functional. The limited resources and mobility of nodes are bottleneck of MANET security. MANETs are highly vulnerable to various security threats, because they have the following inherent characteristics: open medium, absence of fixed central structure, dynamically changing topology, constrained capability, etc.

Cryptography is an important and powerful tool for security services, namely authentication, confidentiality, integrity and non-repudiation. Key management is a basic part of any secure communication. Key management deals with key generation, storage, distribution, updating, and revocation and certificate services, in accordance with security policies.

The size of MANETs increases, node joins and node leave will result in all MANETs nodes' key update. This will bring some problems such as the increase of traffic and computation quantity. The group key management protocol divides a group into region-based subgroups based on decentralized key management principles.

2. Hierarchical key management scheme

2.1 Problem Identification

In [6], the selection of the cluster head is not clearly mentioned. They have told that the node with the highest weight value will be selected as the cluster head, but how the weight value will be calculated is not mentioned. Also the formation of sub-group is not based on the current location which is any important criteria in highly mobile environment. In order to overcome these issues, in this paper, we propose to develop a Location based Hierarchical Key management system for secure group communications.

2.2 Related work

A new group key management protocol for wireless ad hoc networks was put forth by Rony et al. in [4]. They put forth an efficient group key distribution (most commonly known as group key agreement) protocol which is based on multi-party Diffie Hellman group key exchange and which is also password authenticated. The fundamental idea of the protocol is to securely construct and distribute a secret session key, 'K' among a group of nodes/users who want to communicate among themselves in a secure manner. The proposed protocol starts by constructing a spanning tree on-the-fly involving all the valid nodes in the scenario. It is understood, like all other protocols that each node is distinctively addressed and knows all its neighbors. The password 'P' is also shared among each valid member present in the scenario. This 'P' helps in the authentication process and puts off man-in-the-middle attack. Unlike many other protocols, the proposed approach does not need broadcast/multicast capability.

In Simple and Efficient Group Key (SEGK) management scheme for MANETs proposed in [5] group members compute the group key in a distributed manner.

A key management scheme for secure group communication in MANETs was described by Wang et al. in [6]. They described a hierarchical key management scheme (HKMS) for secure group communications in MANETs. For the sake of security, they encrypted a packet twice. They also discussed group maintenance in their paper in order to deal with changes in the topology of a MANET. Finally, they carried out a performance analysis to compare their proposed scheme with other conventional methods that are used for key management in MANETs. The results showed that their proposed method performed well in providing secure group communication in MANETs.

3. Proposed Solution

3.1 Overview

In this paper, we propose to develop a location based hierarchical key management system for secure group communication. Initially, the nodes deployed in the network are split into groups and within the group the node with maximum stability index is chosen as group head. The group head splits the nodes into clusters based on the location information whose cluster head is selected based on stability index. When a source wants to transmit the data packet to destination node, then it transmits it in secure manner using double encryption technique. When the new node wants to join or leave the network, re-keying of cluster and group key is performed.

3.2 Estimation of metrics

3.2.1 Estimating Received Signal Strength

The received signal strength (RSS) is computed using the following formula

$$RSS = \delta * \Phi * P_{tx} \quad (1)$$

Where δ = constant that depends on the wavelength and antennas.

Φ = channel gain.

P_{tx} = Transmitter's signal power.

RSS in terms of dB and dBm (dB milliWatts) is expressed using the following Eq.(.

$$RSS\ [dBm] = 10 \log_{10} \delta + \Phi\ [dB] + P_{tx}\ [dBm] \quad (2)$$

3.2.2 Estimating Mobility

The mobility between the two nodes can be estimated from the ratio of RSS obtained among the two consecutive packet transmissions from a neighbor node. Thus the mobility metric Mo_j (i) of the node j with respect to i is computed using the following formula.

$$Mo_j(i) = 10 \log_{10} \frac{RSS_{i \to j}^{new}}{RSS_{i \to j}^{old}} \quad (3)$$

3.2.3 Link Quality

The ratio of number of error bits (b_{er}) to the number of received bits (b_{rx}) is termed as link quality (LQ) which is given below.

$$LQ = b_{er} / b_{rx} \quad (4)$$

The above computed value gets updated for every time t when a node receives a data packet. This value relies on the interference effect of the wireless channel, additive white Gaussian noise and signal transmission range.

3.2.4 Stability Index

Stability index (STI_{ij}) among the node i and j is computed based on the received signal strength, mobility and link quality (Using the section 3.2.1, 3.2.2, and 3.2.3) which is given using following Eq.(9)

$$STI_{ij} = \frac{RSS * LQ}{Mo_j(i)} \quad (5)$$

3.3 Cluster Formation

The steps involved in the cluster formation are as follows

1) Once the nodes are deployed in the network, each node broadcast the hello message with the node's stability index (Estimated in section 3.2.4) to its neighbor nodes within 2-hop neighbors. The format of hello message is as follows

Table -1 Format of Hello message

Node ID	One-Hop Neighbor	Two-hop neighbor	Stability index

2) After gathering the stability index of all the nodes, the node with maximum stability index is chosen as group head (GH). This is illustrated in fig 1

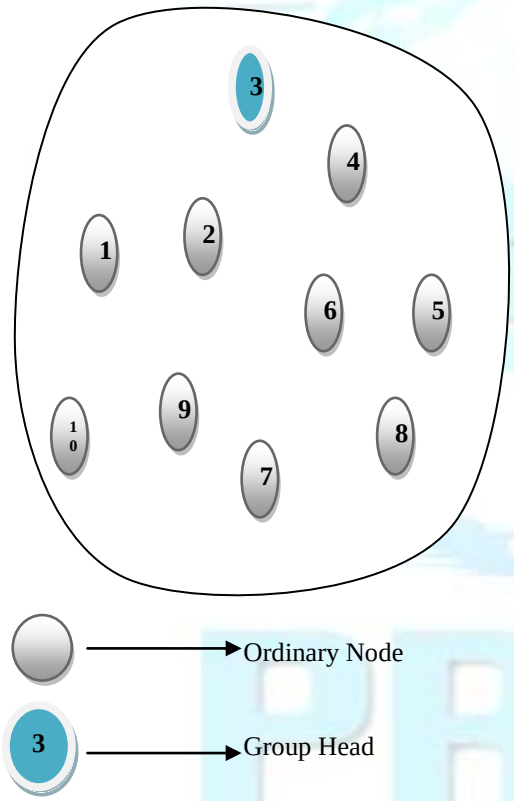


Fig 1 Selection of Group head

Fig 1 shows the selection of group head. Node 3 (N_3) with maximum stability index is chosen as group head. This means that N_3 has minimum mobility and contains less probability to move from the current group

3) At this moment, every other node enrolls itself with GH and transmits all its location information [10] to it.

4) GH upon receiving location information of all the nodes categorizes the nodes into two clusters C_1 and C_2.

5) The nodes within C_1 broadcast the hello message to its neighbors and gather the stability and the node with maximum stability index is chosen as cluster head CH_1 (Similar to step 1). Similarly, CH_2 is selected for C_2. This is illustrated using fig 2. The cluster heads helps in communicating with other clusters and GH.

Using the above steps, several groups are formed with the various clusters.

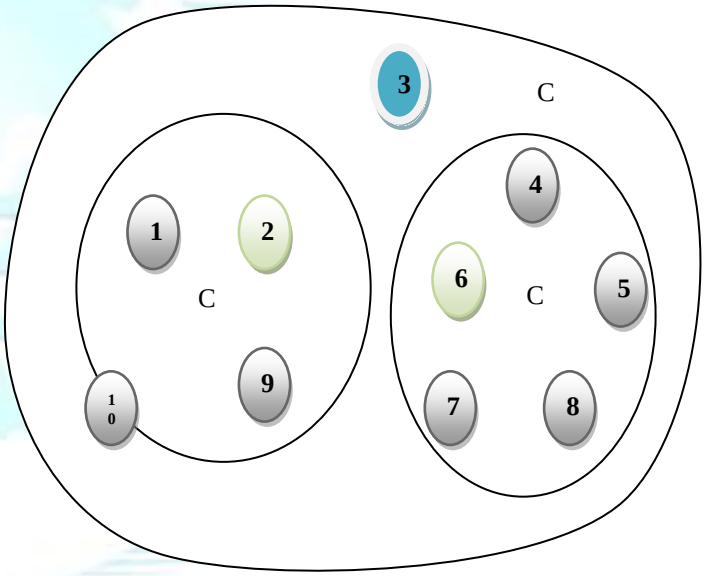


Fig 2 Cluster formation

Fig 2 illustrates the formation of clusters. Based on the location information received by N_3, two clusters C_1 and C_2 with cluster members (N_1, N_2, N_9 N_{10}) and (N_4, N_5, N_6 N_7, N_8) respectively. C_1 selects N_2 containing maximum stability index as CH_1 and C_2 selects N_6 containing maximum stability index as CH_2.

2.4 Group key Management

3.4.1 Rivest, Shamir and Adleman (RSA) algorithm

The RSA algorithm is mainly used for executing public key cryptography. The public keys are identified by each node in the network and it is utilized for encrypting messages. While the message encrypted using public key can only be decrypted using private key. These public and private keys are generated using the following method. [8] .Let x and y be the distinct prime numbers. Let p be an integer. The modulus for both public and private keys is

are generated using the following Equation

$$|r| = x*y \quad (6)$$

Following the computation of modulus, the Euler's totient function (ε) is computed using Eq. (7)

$$\varepsilon(x*y) = (x-1)(y-1) \quad (7)$$

The integer p is the range $1 < p < \varepsilon(x*y)$. p and $\varepsilon(x*y)$ do not share any divisors other than 1. Hence p acts as public key component. (represented as K_{pu})Then b is estimated using modular arithmetic technique which fulfills congruence relation.

$$bp \equiv (\text{mod } \varepsilon(x*y)) \quad (8)$$

Here bp-1 can be evenly divided by the quotient (x-1)(y-1) which is computed using Euclidean algorithm. Hence b is declared as private key component (Represented as K_{pr})

3.4.2 Secure communication

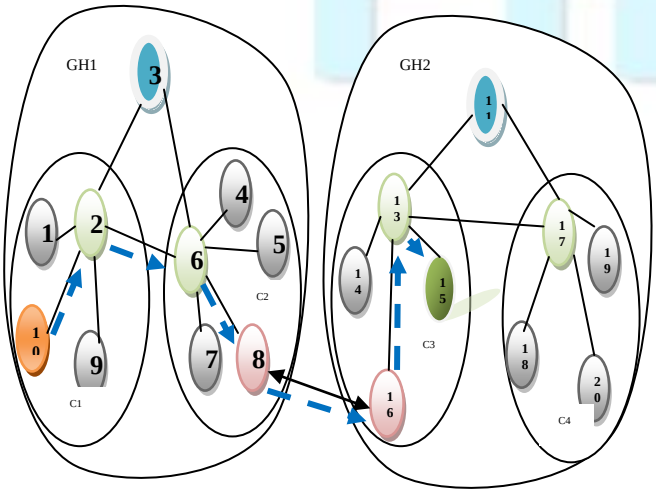
Let DP be the data packet.GH generates a group key K for each group and transmits it to all the nodes in the clusters. This is used to encrypt all the nodes in the cluster.

$$GH \xrightarrow{K} N_i \quad (9)$$

Each CH generates cluster key (K_{CH}) which is known only by the nodes within the cluster (N_{Ci}).

$$CH \xrightarrow{K_{CH}} N_{Ci} \quad (10)$$

When a data is to be transmitted among the nodes in different clusters, then the respective cluster head transmits the data to the GH. Then GH generates a secret key K_{sec}. This key is used for encrypting and decrypting the messages among two nodes.When CH knows the location of destination node, then a private key is generated K_{pr} (Estimated in section 3.4.1) which only belongs to the source and destination node. When the packet is to be transmitted, it is first encrypted with K_{pr}. Hence the data packet will not be intercepted by any other nodes. This is illustrated using the following example



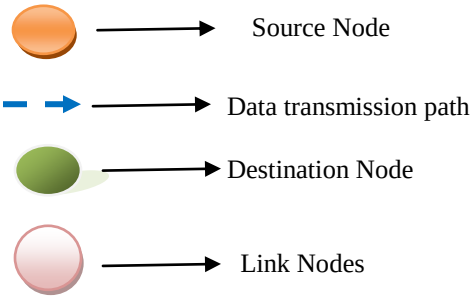


Fig 3 Secured Communication among the nodes in two different groups

Consider figure 3. It demonstrates the data transmission path (N_{10} (S) $\rightarrow$ CH_1 $\rightarrow$ CH_2 $\rightarrow$ N_8 $\rightarrow$ N_{16} $\rightarrow$ CH_3 $\rightarrow$ N_{15}(D)) from source to destination in the secured manner. GH_1 generates a group key K_1 and transmits it to all the nodes in the clusters within group G_1. Similarly GH_2 generates a group key K_2 and transmits it to the nodes in the clusters within group G_2. CH_1, CH_2, CH_3 and CH_4 generate the cluster keys K_{CH1}, K_{CH2}, K_{CH3} and K_{CH4}. Let N_{10} and N_{15} be the source and destination node respectively. When N_{10} wants to transmit DP to N_{15}, it initially generates private key K_{pr} and encrypts it. Then DP is again encrypted using K_{CH1}. The encrypted message is transmitted to CH_1.

$$N_{10} \rightarrow CH_1: \text{Enc } \{[DP]\ [K_{pr}]\ [K_{CH1}]\}. \quad (11)$$

CH_1 upon receiving the encrypted message decrypts it using K_{CH1} and encrypt it using K_1 and transmits to CH_2.

$$CH_1: \text{Dec } [KCH_1]\ \{[DP]\ [K_{pr}]\ [K_{CH1}]\}. \quad (12)$$
$$CH_1 \rightarrow CH_2: \text{Enc } \{DP\ [K_{pr}]\ [K_1]\} \quad (13)$$

CH_2 decrypts message using K_1 and encrypts it using K_{CH2} and transmits to Link node N_8.

$$CH_2: \text{Dec } [K_1]\ \{DP\ [K_{pr}]\ [K_1]\} \quad (14)$$
$$CH_2 \rightarrow N_8: \text{Enc } \{DP\ [K_{pr}]\ [K_{CH2}]\} \quad (15)$$

N_8 decrypts the message using K_{CH2} and encrypts it using K_{sec} and transmit to the link node N_{16}.

$$N_8: \text{Dec } [KCH_2]\ \{DP\ [K_{pr}]\ [K_{CH2}]\} \quad (16)$$
$$N_8 \rightarrow N_{16}: \text{Enc } \{DP\ [K_{pr}]\ [K_{sec}]\} \quad (17)$$

N_{16} decrypts the message using K_{sec} and encrypts it using K_2 and transmits to the CH_3.

$$N_{16}: \text{Dec } [K_{sec}]\ \{DP\ [K_{pr}]\ [K_{sec}]\} \quad (18)$$
$$N_{16} \rightarrow CH_3: \text{Enc } \{DP\ [K_{pr}]\ [K_2]\} \quad (19)$$

CH_3 decrypts the message using K_2 and encrypts it using K_{CH3} and transmits it to the destination node N_{15}.

$$CH_3: \text{Dec } [K_2] \{DP [K_{pr}] [K_2]\} \quad (20)$$
$$CH_3: N_{15} \text{ Enc } \{DP [K_{pr}] [K_{CH3}]\} \quad (21)$$

N_{15} decrypts the message using KCH_3 and K_{pr} and obtains DP.

3.4.3 Group member Join and Leave operation

In this section, the first phase illustrates the node joining the group and second phase illustrates the node leaving a group.

3.4.3.1 Group member Join

1) When a new node N_i wishes to join a cluster C_i, it broadcasts the hello message to inform that it is going to join C_i. The format of hello message is as follows.

Table -2 Format of hello message

Node ID	Nodes Location

2) Following the reception of hello message, the neighboring nodes forwards them to CH_i which in turn authenticates N_i's ID based on N_i's k_{pu}.
3) At this moment, GH_i functions as controller node among the cluster members including N_i in order to execute Group Diffie–Hellman (GDH). By executing this keying scheme, a new cluster key K_{CHnewi} is generated.
4) CH_i then updates all cluster member list and broadcasts the updated list to the members within the clusters.
5) K_i is also re-keyed as a new joining as occurred. This is done as follows
6) CH_i reports the information about the new node to all other cluster heads within the group for them to apply the following MAC function to generate new group key

$$K_{newi} = MAC (K_{CHi}, n)$$

Where MAC is the cryptographically secure hash function ,K_{CHi} is the existing cluster key used as secret key for MAC,n is the counter which gets incremented for every joining event.

3.4.3.1 Group member Leave

1) When a node N_i leaves a cluster C_i, it sends C_leave messge to CH_i.

$$N_i \xrightarrow{C\_leave} CH_i$$

2) CH_i upon hearing this message updates its member list and distributes the message to all its members.
3) Using GDH, a new cluster key K_{CHnewi} is generated and distributed to all the cluster members.
4) Further, the CH_i informs other cluster heads about the member leave event.
5) The cluster heads upon receiving message broadcasts to its cluster members.
6) Finally, CHs regenerate a group key K_{newi} and distributes it to their corresponding cluster members by encrypting the group key with their K_{CHnewi}.

4. Simulation Results

4.1 Simulation Model and Parameters

We use NS2 [11] to simulate our proposed protocol. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.In our simulation, 50 mobile nodes move in a 1000 meter x 1000 meter region for 100 seconds simulation time. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is varies from 2m/s to 10m/s. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in Table 3

Table - 3 Simulation Parameters

No. of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Routing Protocol	AODV
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	500 bytes

Mobility Model	Random Way Point
Speed	2,4,6,8 and 10 m/s
No. of Receivers	2,4,6,8 and 10.
Pause time	5 s

4.2. Performance Metrics

We evaluate mainly the performance according to the following metrics.

4.2.1 Average Packet Delivery Ratio

Average Packet Delivery Ratio is the ratio of the number .of packets received successfully and the total number of packets transmitted.

4.2.1 Packet Drop

Packet Drop is the number of packets dropped during the data transmission.

4.2.1 Resilience against Node Capture

In Resilience against Node Capture we are going to calculate how a node capture affects the rest of network resilience. It is calculated by estimating the fraction of communications compromised between non compromised nodes by a capture of x-nodes.

We compare our Location based Hierarchical Key Management System (LHKM) with the Hierarchical Key Management System (HKM) scheme. The simulation results are presented in the next section

4.1 Simulation Results

In our initial experiment we vary the number of receivers as 2,4,6,8 and 10.

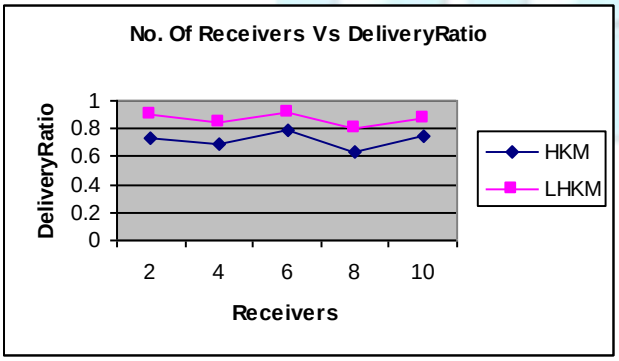


Fig 4: Receivers Vs Delivery Ratio

From figure 4, we can see that the delivery ratio of our proposed LHKM is higher than the existing HKM protocol. For varying number of receivers 2,4,6,8,10 delivery ratio is increased in compared with existing Hierarchical Key Management System (HKM) scheme

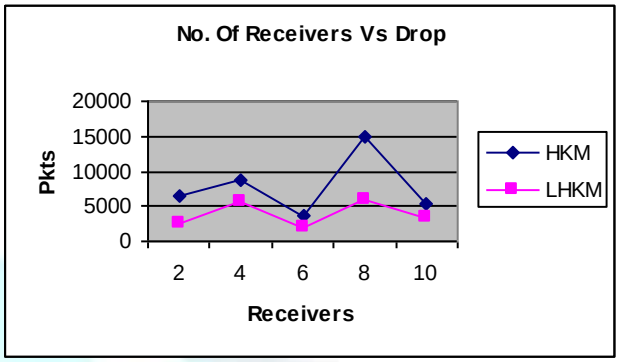


Fig 5: Receivers Vs Drop

From figure 5, we can see that the packet drop of our proposed LHKM is less than the existing HKM protocol

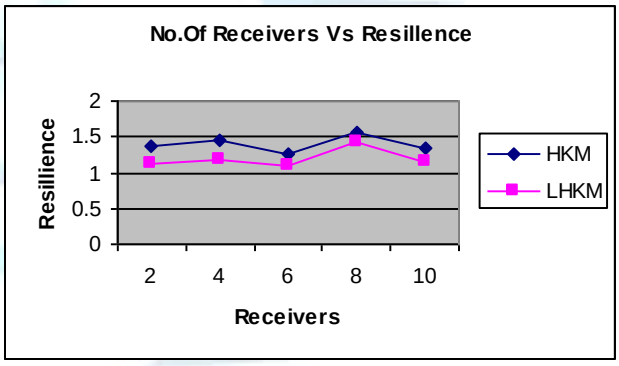


Fig 6: Receivers Vs Resilience

From figure 6, we can see that the resilience of our proposed LHKM is less than the existing HKM protocol

5. Conclusion

In this paper, we have proposed a location based hierarchical key management system for secure group communication in MANET. Initially, group heads selected based on stability index which splits the nodes into clusters based on their location information. In each cluster, the cluster member with maximum stability index is chosen as cluster head. In case, the source node has to transmit the data to the destination node, the procedure of delivery is to encrypt the packet firstly by private key, and then encrypt and decrypt it again by cluster key and group key. When the new node wants to join or leave the network, re-keying of cluster and group key is performed. By simulation results, we have shown that proposed technique improves the network security and minimizes the cost. The main advantage of this approach is that it improves data confidentiality and integrity.

References

[1] N. Vimala, B. Jayaram, Dr. R. Balasubramanian, "An Efficient Rekeying Function Protocol with Multicast Key Distribution for Group Key Management in MANETs", April 2011.
[2] Wan An Xiong, Yao Huan Gong, "Secure and Highly Efficient Three Level Key Management Scheme for MANET", 2011.
[3] Kamal Kumar Chauhan and Amit Kumar Singh Sanger, "Securing Mobile Ad hoc Networks: Key Management and Routing", April 2012.
[4] Rony H. Rahman, and Lutfar Rahman, "A New Group Key Management Protocol for Wireless Ad-Hoc Networks", International Journal of Computer and Information Science and Engineering, vol. 2, no. 2, pp. 74-79, 2008.
[5] Bing Wu, Jie Wuand Yuhong Dong, "An efficient group key management scheme for mobile ad hoc networks", Int. J. Security and Networks, 2008.
[6] Nen-Chung Wang, and Shian-Zhang Fang, ―A hierarchical key management scheme for secure group communications in mobile ad hoc networks,‖ Journal of Systems and Software, vol. 80, no. 10, pp. 1667-1677, 2007.
[7] Jin-Hee Cho, Ing-Ray Chen, Ding-Chau Wang, "Performance optimization of region-based group key management in mobile ad hoc networks", 26 July 2007.
[8] Prasad Lokulwar and Vivek Shelkhe, " Security Aware Routing Protocol For MANET Using Asymmetric Cryptograpy using RSA Algorithm", BIOINFO Security Informatics, Volume 2, Issue 1, pp.-11-14, 2012.
[9] Rajashekhar Biradar, Sunilkumar Manvi, Mylara Reddy, "Mesh Based Multicast Routing in MANET: Stable Link Based Approach", International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010.
[10] Xu Li, Nathalie Mitton, and David Simplot-Ryl, "Mobility Prediction Based Neighborhood Discovery in Mobile Ad Hoc Networks", Networking, pp 147-159, 2011.
[11] Network Simulator: http:///www.isi.edu/nsnam/ns