Simulation of A Novel Scalable Group Key Management Protocol for Mobile Adhoc Networks

M. Sandhya Rani

Research Scholar at JNTUH and Assoc.Professor ,
Bhoj Reddy Engineering College for Women,
Hyderabad, Telangana state, India.
Email: sandhya_medi@yahoo.com

Dr.R.Rekha

Assoc. Prof, University College of Engineering & Technology,
MGU, Nalgonda, Telangana state, India.
Email: rrekhareddy@yahoo.com

Dr.K.V.N Sunitha

Professor, BVRIT Engineering College,
JNTU, Hyderabad, Telangana state, India.
Email:k.v.n.sunitha@gmail.com

Abstract— A Mobile Adhoc Network (MANET) is a collection of autonomous nodes that communicate with each other ,most frequently using a multi-hop wireless network. Secure and multicast group communication is an active area of research in MANETS. The main problem in secure group communication is group dynamics and key management. Group key management is crucial for multicast security. Member joining and member leaving from the group is the main challenge in designing secure and scalable group communication for dynamic update of keys. Most of the proposed solutions for wired networks are not considering this parameter and so suffer from the one-affects-n scalability problem. This paper presents the simulation of A Novel Scalable Group Key Management Protocol (NSGKMP) for wireless Adhoc Networks and demonstrates the simulation results through NAM(Network Animator) in NetworkSimulator2 (NS2). This NSGKMP for MANETs approach decreases number of rekeying operations when a member joins in to the group or leaves from the group i.e. dynamic updating of keys.

Keywords- *MANET*, NSGKMP, NAM, Rekeying, join and leave .

I.INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of self-configurable nodes or terminals which communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Many applications of adhoc networks involve collaborative computing among a large number of nodes and are thus group-oriented in nature. The conventional security solutions to provide key management through accessing trusted authorities or centralized servers are infeasible for this new environment since Mobile Adhoc Networks are characterized by the absence of any infrastructure, frequent mobility, and wireless links. In wired networks, many group key management protocols have been proposed and simulated[6,7],Efficient Group key(EGK), Tree Group Diffie-Hellman (TGDH), Logical key hierarchy(LKH),Skinny TRee (STR) and Computation and Communication Efficient Group Key (CCEGK) . However, these approaches are not directly applicable to ad hoc networks, because the communication cost per node can become very high for a large adhoc network with very dynamic group membership. So far very few group rekeying schemes have been proposed for ad hoc networks. They either use public-key techniques [8], or adapt the LKH scheme for ad hoc networks [9]. Public-key based schemes [8] are more expensive than symmetric-key based schemes in both communication and computation. The adapted LKH scheme [9] incurs the computational and communication cost that is of the same order as the LKH scheme .

In this paper, we present the simulation of a Novel Scalable Group Key Management Protocol(NSGKMP) for Wireless Mobile Adhoc Networks. In NSGKMP protocol, other than secure group communication forward secrecy and backward secrecy are maintained among the nodes. Forward secrecy prevents an accessing current communication by old member after it leaves from the group. Backward secrecy prevents an accessing of the communication sent before a new member joins to the group. To do so, a re-keying process should be performed after every join or leaving a member from the secure group. It consists in generating a new *TEK* and distributing it to all group members. The main problem with any re-keying technique

is scalability: as the re-keying process should be performed after every member join or leave from the group. The computational and communication overhead induced may be important in case of frequent join and leave operation to group.

NSGKMP for MANETS is based on the Chineese Remainder Theorem and a hierarchical graph B-Tree,in which each node contains two keys and a modulus[2,3]. The previous approach [2] is concentrated on to decrease number of re-keying operations, i.e. from $\log_2 n$ to $\log_m n$ when compared with [3], where n is the number of leaf nodes of tree and m is the order of the B-Tree. Here we are taken order of B-Tree is 3(i.e. *m*=3).In [1], NSGKMP for wired networks has been simulated. This paper presents brief introduction to NetworkSimulator2 (NS2) and simulation of NSGKMP approach for MANETs with the help of NetworkSimulator2 (NS2) NAM. And we showed that number of rekeying operations are less in NSGKMP for MANETS than SGKMP[3] through NAM visualizations.

The remainder of the paper is organized as follows. Section II presents Structure Of MANET nodes for Proposed Approach , Section III presents Simulation Environment, Section IV presents Simulation Results, Section V presents performance of the protocol and Section VI gives the conclusion.

II. Structure Of MANET nodes for Proposed ApproachS

Several Group Key management schemes have been proposed with different network structures and topologies: random fashion, tree structure, hierarchical and hybrid[4,8].In this paper we present the B-Tree structure as shown in Fig. 1 for group communication to deploy the MANET nodes . In B-Tree of order m, each node contains at most *m-1* elements and each node contains at least $\lceil m/2 \rceil$-1 elements. The Fig. 1 describes that a B-Tree of order 3, so each node consists of at most 2 elements, And maintaining users of the group at leaf nodes of B-Tree. So each leaf node consists of 2 users. i.e. *node21* consists of user's u1 and u2 , *node22* consists of user's u3 and u4 n*ode29* consists of user's u17 andu18 .

In the Fig. 1 user u18 wants to join into the group. After joining in to the group to provide backward secrecy we are changing the parent's key from leaf to the root node that was indicated in the Fig. 1. After changing the parent's keys, the changed keys are sent to the corresponding children's that was shown in the simulation. In [3], binary tree structure is used. When the group is large, the number of levels in the binary tree will be more which increases number of keys at member. Extending this scheme to B-Tree will reduce the height of the tree reducing number of keys at each member. At the same time we should consider server side storage i.e. number of keys at the level of the tree. In [3], $\log_2 n$ keys are maintained by the every member in the tree, extending the scheme to B-tree will result in maintaining $\log_m n$ keys by the members of the B-tree (where *m* is the order of B-tree and n is the number of leaf nodes).

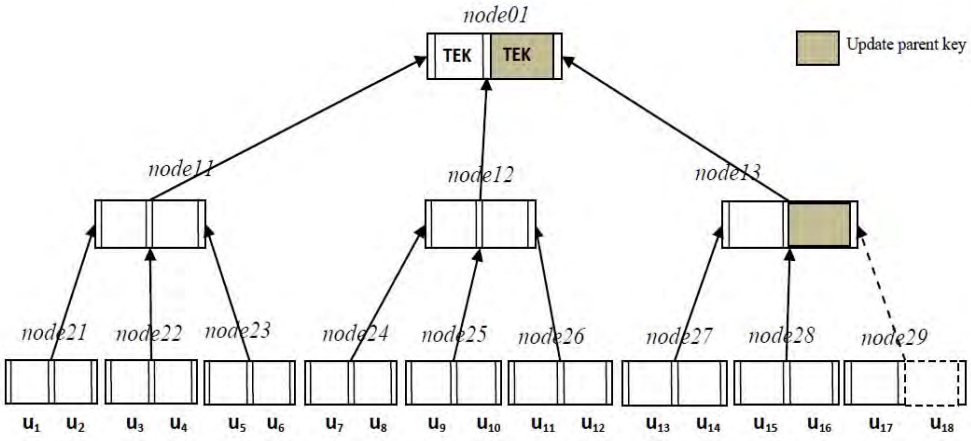

Fig. 1 Group Structure in B-Tree format

III. Simulation Environment

A.Simulation Model

Our proposed protocol simulations have been carried out using Network Simulator version 2 (NS-2.35) and its associated tools for animation and analysis of results.NS2 is an event driven network simulator tool. We chose a Linux platform i.e. UBUNTU 12.10, as Linux offers a number of programming development tools that can be used with the simulation process. NS-2 allows a user to emulate network traffic as it actually occurs on physical networks. We used ftp traffic for packet transmission to implement our proposed protocol. The software simulates switches, routers, connections and traffic sources of various kinds. Traditionally, NS2 is used to model new versions of communication protocols like Transmission Control Protocol (TCP) and Ethernet, and it can also model new forms of traffic generation, like the group key management simulation for

wired and wireless networks. We analyzed our experimental results in NAM(Network Animator) trace file. To evaluate the performance of NSGKMP for MANETs, we find the Rekeying path and number of rekeying messages in a group of nodes through NAM animation .

B. Simulation Parameters

The simulation parameters used in our work are listed in Table 1.

TABLE I. SIMULATION PARAMETERS

Parameters	Value
Simulator	NS-2(Version 2.35)
Channel Type	Channel/Wireless Channel
Routing protocol	AODV
Traffic type	FTP
Simulation Duration	300ms
MAC Layer Protocol	802.11
Max. No. Nodes	26
Transmission Range	1000x1000m
Packet Size	512 Bytes

C. NAM Animation

Nam is a Tcl/Tk based animation tool that is used to visualize the ns simulations and real world packet trace data. The first step to use nam is to produce a nam trace file. The nam trace file should contain topology information like nodes, links, queues, node connectivity etc as well as packet trace information. We showed our new protocol NSGKMP for MANETs using NAM animations. Animation permits the user to promptly see the status of each part of the network. NAM lets users change the animation speed and play it forward or backward, fast forward, fast backward, making it easy to find and inspect appealing occurrences.

IV. SIMULATION RESULTS

B-Tree of order 3 was constructed using NS2 simulator. According to B-Tree(order 3) property each node consists of two elements. In the Fig. 2, green hexagon shape node pairs are treated as root node. i.e. labels (1) and (2). The blue square shape node pairs i.e. labels (4) and (5), (6) and (7), (8) and (9) are treated as intermediate nodes of a tree. Leaf circle shape node pairs are labeled with (16) and (17), (18) and (19), …….. (36) and (37) treated as users of the group.

We are showing in our simulations that a node labeled with (20) joining in to the group and a parent node changes it's key after joining the new node and it sends the new key to it's children. The following are the snapshots of our NAM simulation The following Fig. 2 showing the group of MANET nodes in B-Tree format of order 3.Thus we placed 2 elements at each node.

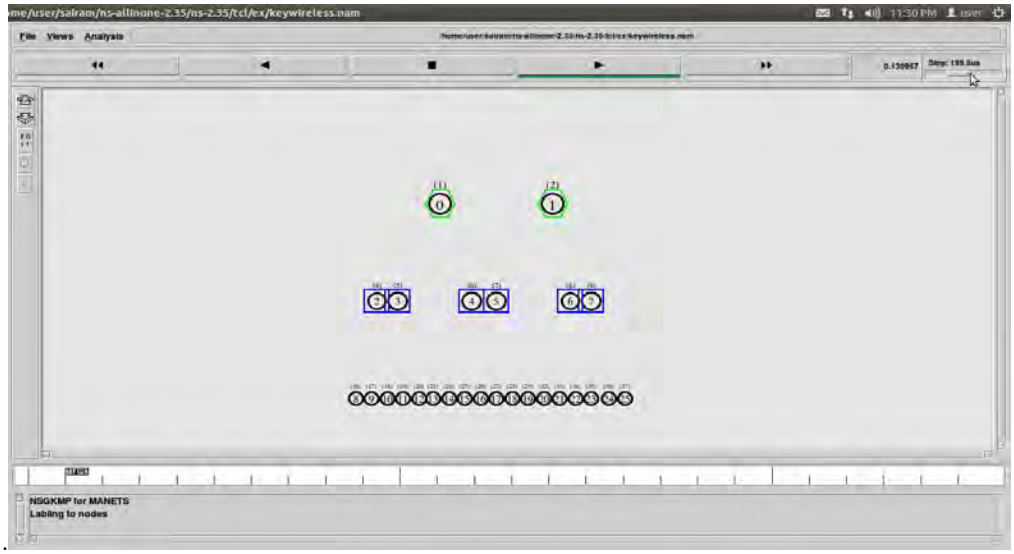

Fig 2. Creation of MANET nodes in B-Tree format and Labeling to nodes

In Fig. 3 user 20 wants to join to the group that is indicated by orange color.

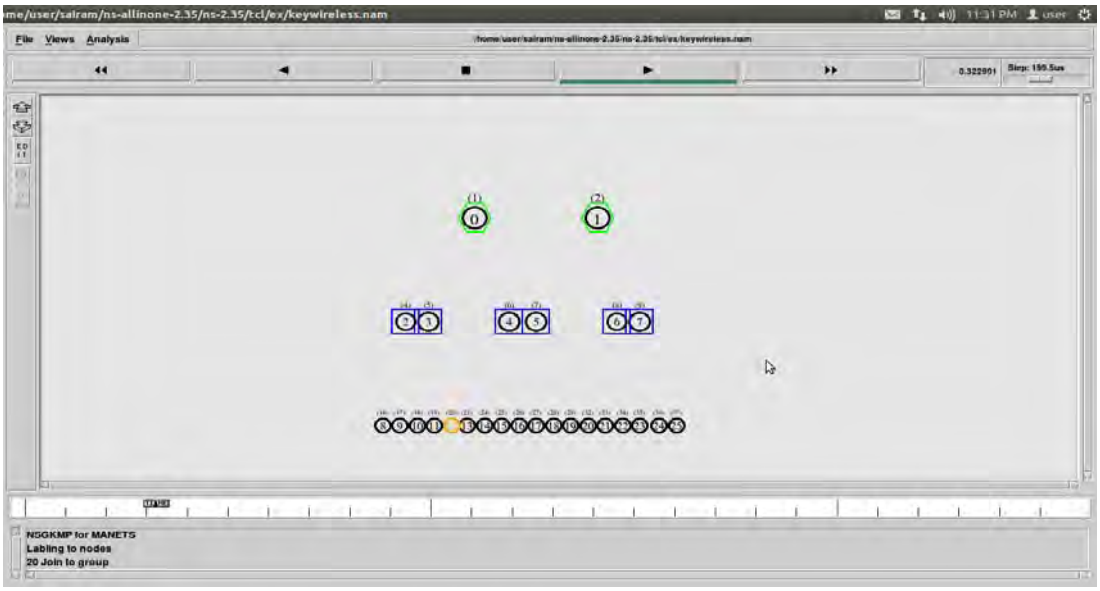

Fig 3. User 20 wants to join to the group

After user 20 joins in to the group his parent i.e. (5) was changed his key. It is shown with Red color.

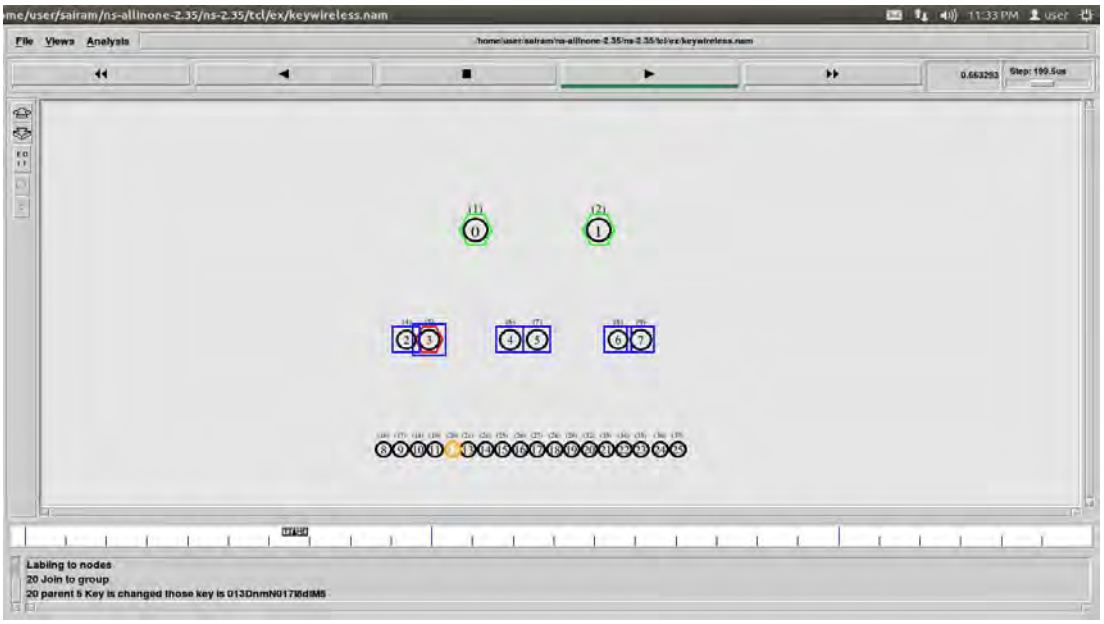

Fig 4 Node 5 changed it's key

After changing the parent's key, the changed key was sent to the corresponding children , i.e. (20) and (21)

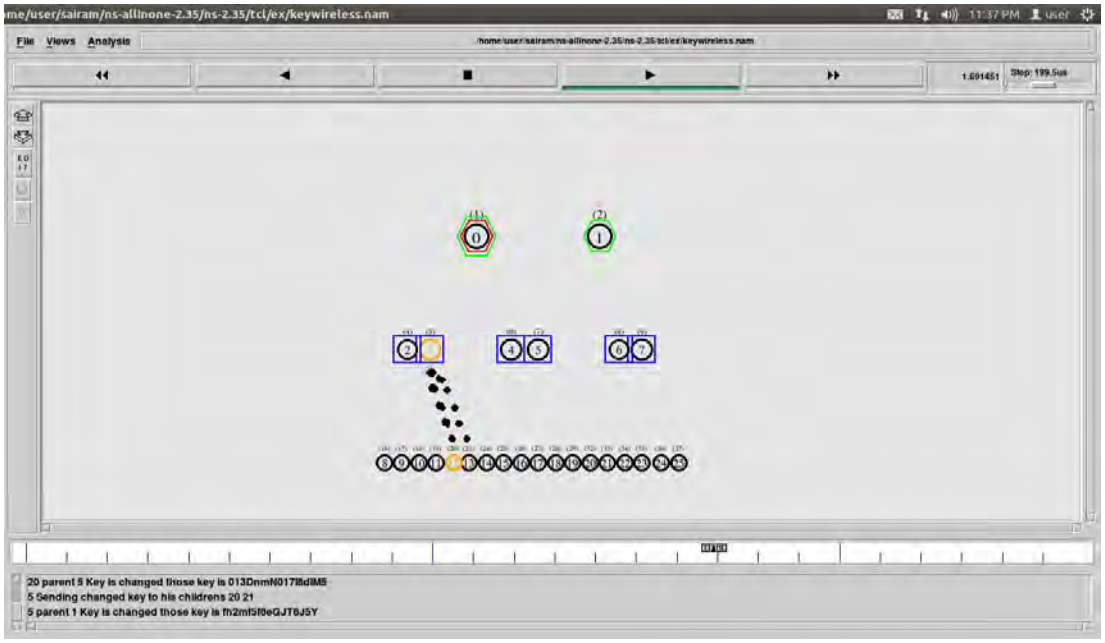

Fig 5. Node 5 sending changed key to it's children 20 & 21

After changing the key of (5), his parent (1) key also changed, so the changed key was sent to his children (4), (5), (6) and (7), that was shown in the Fig. 6.

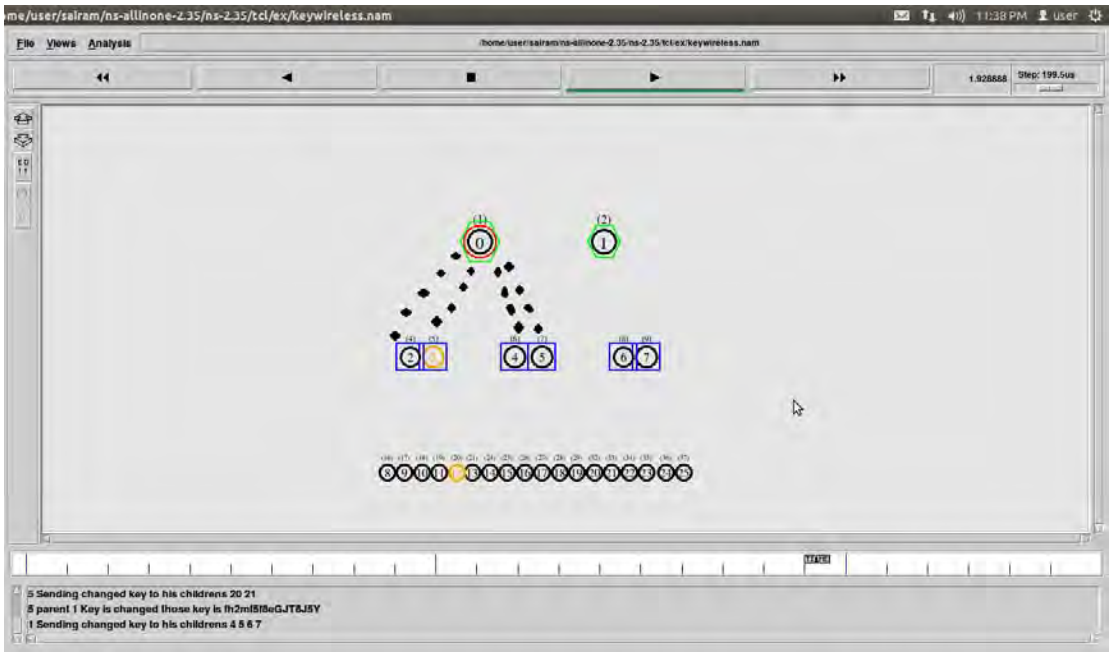

Fig 6. Node 1 sending changed key to it's children 4,5,6,7

Finally the number of re-keying operations from leaf to the root node indicated by Orange color nodes shown in Fig 7.

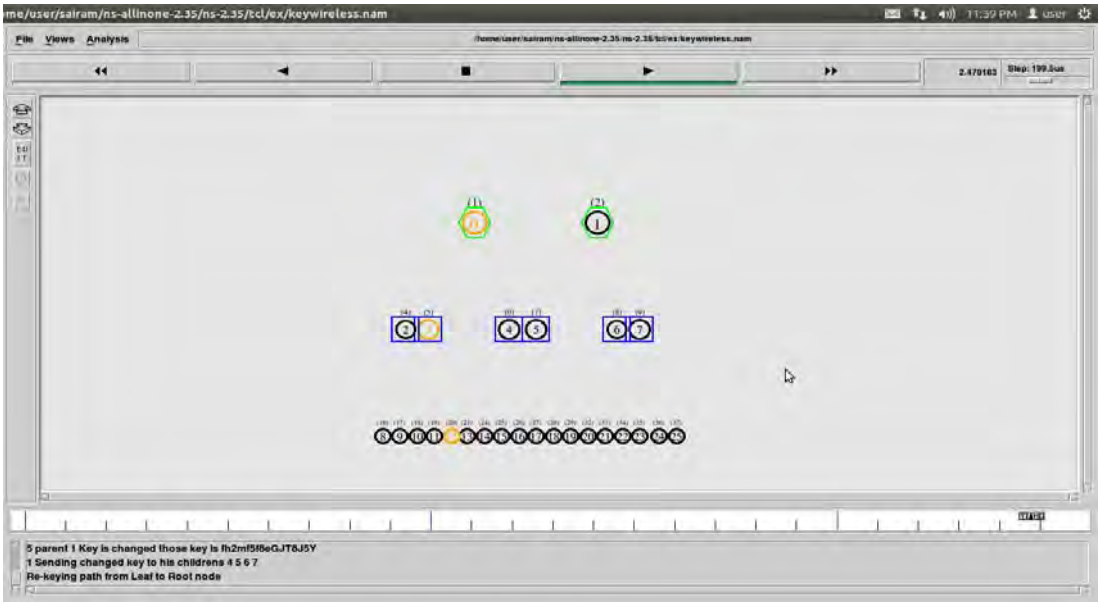

Fig 7. Rekeying operations performed at nodes 5, 1

V. PERFORMANCE OF THE NEW PROTOCOL

This session provides the performance of our proposed approach for MANETs , by comparing with the protocol of [3]. Table 2 gives the comparison between our approach and [3].It is shown from Fig. 7 that NSGKMP for MANETs has less number of Re-keying operations when a member joins to the group.(i.e only 2 operations).

TABLE II. COMPARISON OF NEW PROTOCOL WITH SGKMP

Scalability metrics	**Number of Re-keying operations**	
Protocols	**join**	**Leave**
NSGKMP for MANETs	$\log_{m} n$	
SGKMP	$\log_{2} n$	

VI. CONCLUSION

To improve the scalability in Group communication, we proposed A Novel Scalable Group Key Management Protocol for MANETs and demonstrated that it has better scalability in terms of number of Re-keying operations. And also Our approach satisfies all the Security attributes of the Group key management System during the Rekeying process. The process of entire approach was simulated in network simulator NS2 and presented the simulation results through NAM. Finally we conclude that if we increase the order of B-Tree, then automatically we can decrease the number of re-keying operations further more. As a future work, instead of unicasting the rekeying messages to the nodes, broadcasting may be done that will reduce the number of messages sent through the network.

REFERENCES

[1] Amruta sagar Kavarthapu and Aswini Kavarthapu , "Simulation of A Novel Scalable Group Key Management Protocol", International Journal of Computer Applications, vol. 68 , pp. 18-22, April 2013.
[2] Amruta sagar Kavarthapu and Seshagirirao Ganta , "A Novel Scalable Group Key Management Protocol ", International Journal of Computer Applications, vol 39, pp. 535-538, February 2012.
[3] Ronggong Song and George O. M. Yee, "A Scalable Group Key Management Protocol (SGKMP)", IEEE Communication Letters, vol. 12 , pp.541-543 , July2008.
[4] Renuka A and Dr. K .C .Shet , "Hierarchical Approach for Key Management in Mobile Adhoc Networks" ,International Journal of Computer Science and Information Security ,vol. 5, No.1, 2009.
[5] D.SAMANTHA , Classic Data Structures, Prentice- Hall of India Private Limited, New Delhi-110001, 2006.
[6] S. Zheng , D. Manz , J. Alves -Foss, and Y. Chen. "Security and performance of group key agreement protocols" ,In Proc. IASTED Networks and Communication Systems, pp 321–327, Mar 2006.
[7] David Manz, Jim Alves-Foss, and Shanyu Zheng , "Network Simulation of Group Key Management Protocols" ,Journal of Information Assurance and Security , pp 67-79, January 2008.
[8] T. Kaya, G. Lin, G. Noubir, A. Yilmaz ," Secure Multicast Groups on Ad Hoc Networks", In Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03) , 2003.

[9] L. Lazos and R . Poovendran ," Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information " , In Proc. of IEEE ICASSP'03 , Hong Kong , China, April 2003.

AUTHORS' PROFILE

M.Sandhya Rani obtained her B.Tech in CSE from JNTU in 2002 and M. Tech in CSE from OU in 2008. She is pursuing Ph.D, in CSE from JNTUH, Hyderabad. She is working as Associate Professor in Bhoj Reddy Engineering College for Women and has 12 yrs of teaching experience. Her areas of interest include Network security and Mobile Computing.

Dr. Rekha Redamalla obtained her M.Tech(CS) from JNTU Hyderabad. She received Ph.D (CS) from University of Udine(ITALY) in 2006. She has 18 years of Teaching Experience and presently the Principal, University college of Engineering & Technology, Mahatma Gandhi University, Nalgonda, Telangana state, India, Her areas of Interests are Semantics of OOL, Network Security and DMDW. She published more than 15 papers in International & National Journals and conferences.

Dr.K.V.N.Sunitha obtained her B.Tech ECE from Nagarjuna University, M.Tech Computer Science from REC Warangal and Ph.D from JNTUH in 2006. She has 21 years of Teaching Experience, working as Professor & Principal, BVRIT college . She is a recipient of Academic Excellence award by GNITS in 2005. She has received "Best computer Science Engineering Teacher award" by ISTE (Indian society for Technical education) in Feb 2008. She is guiding 12 PhD scholars & published more than 65 papers in International & National Journals and conferences. She has authored three text books. She is Board of Studies member for many other Engg. colleges. She has received funding for her research proposal from CSI Computer society of India. Her auto biography is listed in Marquis who is who in the world , 28th edition 2011.She is a fellow of Institution of Engineers, Sr. Member for IEEE & Life member for CSI.