existing root of the subtree and one unicast to inform the new user the existing keys. When the user joins the first service group two nodes in the DG part gets affected. The worst case rekeying cost occurs in the case when the user joins the last service group at an insertion point h-1 where h is the height of the last service group. The rekeying cost for this case is $2(h+l)-1$.

Table.3.Rekeying message costs for deletion

Delete	Best	Worst
Binary Tree	h	$h+2l-3$
2-3 tree	$(h-1)d$ $+4$	$d+mh$ $+2(l-1)$
NSBHO	3	$d+mh$ $+2(l-1)$

The rekeying costs for leave case are also listed in table.3 and the case where user leaves from the first service group results in best case rekeying cost and the user leave from the last service group results in the worst case rekeying cost, when the service groups are considered in left right order.

5. Conclusion and future work

Key management is important in group communications and this paper has dealt with managing keys using B-trees and NSBHO trees for multi-privileged groups. Algorithms for join and leave in both B-trees and NSBHO trees are provided and rekeying algorithms for the same respectively have also been developed. Bounds for the tree heights have been proved as lemmas. A performance comparison of the Multi-privileged key management using B-trees and NSBHO trees has been provided which shows that NSBHO gives better results. The applications discussed can be implemented as future work using NSBHO trees.

References

[1] Banerjee, S.; Bhattacharjee, B., Scalable secure group communication over IP multicast, *IEEE Journal on Selected Areas in Communications*, vol.20, no.8, pp. 1511-1527, Oct 2002.

[2] D.Ma,Y.Wu,R.Deng,T.Li, Dynamic access control for multi-privileged group communications,Proceedings of 6th International Conference on Information and Communications Security, *Lecture Notes in Computer Science(LNCS)*,3269(2004)508-519.

[3] Eskicioglu. A.M., Multimedia Security in Group Communication: Recent Progress in Key Management, Authentication and Watermarking, *ACM Multimedia Systems J., special issues on multimedia security*, pp. 239-248, Sept. 2003.

[4] Guojun Wang; Jie Ouyang; Hsiao-Hwa Chen; Minyi Guo, ID-Based Hierarchical Key Graph Scheme in Multi-Privileged Group Communications, *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE* , vol., no., pp.172-176, 26-30 Nov. 2007.

[5] Justin Goshi and Richard E. Ladner. 2003. Algorithms for dynamic multicast key distribution trees. In *Proceedings of the twenty-second annual symposium on Principles of distributed computing* (PODC '03). ACM, New York, NY, USA, 243-251.

[6] Josep Pegueroles, Francisco Rico-Novella, Balanced Batch LKH: New Proposal, Implementation and Performance Evaluation., iscc, *Eighth IEEE Symposium on Computers and Communications, 2003*. vol.2 pp. 815 - 820 vol.2

[7] Li, X. S., Yang, Y. R., Gouda, M. G., and Lam, S. S. 2001. Batch rekeying for secure group communications. *In Proceedings of the 10th international Conference on World Wide Web* (Hong Kong, Hong Kong, May 01 - 05, 2001). WWW '01. ACM, New York, NY, 525-534.

[8] Lu, H. 2005. A Novel High-Order Tree for Secure Multicast Key Management. *IEEE Trans. Comput. 54*, 2 (Feb. 2005), 214-224.

[9] Moyer.M.J., Rao J.R., and Rohatgi .P., "Maintaining Balanced Key Trees for Secure Multicast," *Internet Research Task Force (IRTF), Internet draft, draft-irtf-smug-key-tree-balance-00.txt*, June 1999.

[10] Ng, W. H., Howarth, M., Sun, Z., and Cruickshank, H. 2007. Dynamic Balanced Key Tree Management for Secure Multicast Communications. *IEEE Trans. Comput.* 56, 5 (May. 2007), 590-605.

[11] Ng, W.H.D.; Zhili Sun, "Multi-layers balanced LKH," *Communications, 2005. ICC 2005. 2005 IEEE International Conference on* , vol.2, no., pp. 1015-1019 Vol. 2, 16-20 May 2005.

[12] O. Rodeh, K. P. Birman, and D. Dolev. Using AVL trees for fault tolerant group keymanagement. *International Journal on Information Security*, pp 84-99, 2001.

[13] Rafaeli, S. and Hutchison, D. 2003. A survey of key management for secure group communication. *ACM Comput. Surv.* 35, 3 (Sep. 2003), 309-329.

[14] Sanjeev Setia , Samir Koussih , Sushil Jajodia , Eric Harder, Kronos: A Scalable Group Re-Keying Approach for Secure Multicast, *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, p.215, May 14-17, 2000

[15] Sherman, A. T. and McGrew, D. A. 2003. Key Establishment in Large Dynamic Groups Using One-Way Function Trees. *IEEE Trans. Softw. Eng*. 29, 5 (May. 2003), 444-458.

[16] Sun, Y. and Liu, K. J. 2007. Hierarchical group access control for secure multicast communications. *IEEE/ACM Trans. Netw.* 15, 6 (Dec. 2007), 1514-1526.

[17] Wang, G., Ouyang, J., Chen, H., and Guo, M. 2007. Efficient group key management for multi-privileged groups. *Comput. Commun* .vol.30, 11-12 (Sep. 2007), pp 2497-2509.

[18] Wee Hock Desmond Ng, Haitham S. Cruickshank, Zhili Sun:, "Scalable Balanced Batch Rekeying for Secure Group Communication," *Elsevier Computers and Security*, vol. 25, pp. 265-273, June 2006.

[19] Wong, C. K., Gouda, M., and Lam, S. S. 2000. Secure group communications using key graphs. *IEEE/ACM Trans. Netw.* 8, 1 (Feb. 2000), 16-30.

[20] Yan Sun; Liu, K.J.R., "Scalable hierarchical access control in secure group communications," *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies* , vol.2, no., pp. 1296-1306 vol.2, 7-11 March 2004.

[21] Zhang, X. B., Lam, S. S., Lee, D., and Yang, Y. R. 2003. Protocol design for scalable and reliable group rekeying. *IEEE/ACM Trans. Netw.*11,6(Dec.2003),908-922.

[22] Zhang.Q.,Wang.Y., A centralized key management scheme for hierarchical access control, *Proceedings of Global Telecommunications Conference4 (2004)* 2067-2071.

Ms.A. Muthulakshmi has six years of teaching experience and has guided five PG projects. She has attended 10 National/International conferences and workshops in the area of cryptography and security in computing. She is a member of Cryptology Research Society of India.

Dr. R. Anitha is an Associate Professor in the Department of Mathematics and Computer Applications. She has 24 years of teaching experience. She has guided 3 PhDs and 1 M.Phil in Applied Mathematics. At present she is guiding 9 research scholars. She is the Program Coordinator of the five year integrated M.Sc. Theoretical Computer Science programme. Currently she is the principal investigator (PSG Tech) of the CDBR-Smart and Secure Environment project, funded by NTRO, which is a collaborative research work of eight Institutions. She has rendered seven years of service for NSS. She is a member of ISTE, CRSI and ACM. She has visited France and Australia on academic grounds .Cryptography and Security in Computing are her areas of interest.

Ms. M. Sumathi is a Lecturer in the Department of Mathematics and Computer Applications. She has three years of teaching experience. Her area of interest is Optimization Techniques.