

109. EFFICIENT REKEYING FRAMEWORK FOR GROUP KEY MANAGEMENT IN MOBILE COMMUNICATION

R.J. Remy Janet, X. Anitha Sarafin

M.E. Scholar, Associate Professor

Department of Computer Science and Engineering, M.N.M Jain Engineering College

janetemy@gmail.com, readyanita@gmail.com.

Mobile communication is playing a vital role in the current technical world and becoming more popular and prevalent across the world everyday at one end and many security problems are arising at the other end. To overcome these security problems many security mechanisms for mobile communications have been introduced. Group key management (GKM) in mobile communication is important to enable access control for a group of users. A major issue in GKM is how to minimize the communication cost for group rekeying. Large and dynamic user group can be managed by GKM. Multicast service will be a key application for supporting a large group of subscribers. Communication overhead can be maximized for the optimal tree structure by analyzing the condition such as arbitrary number of members, non equal leaving probability and non balanced and complete tree structure. The new framework is proposed, it consists of two main algorithms: the first algorithm can generate a key tree that correspond to the optimal key tree. The second algorithm is an optimal key tree maintenance algorithm that is used for group membership changes.

Index Terms— multicast, security, group key, group key management, key distribution, rekeying, group dynamics, Multicast and Broadcast Rekeying Algorithm.

Journal of Science and Innovative Engineering & Technology