MIS Review Vol. 18, No. 1, September (2012), pp. 71-91

Key Management Scheme for Cumulative Member Removal and Bursty Behavior in Secure Group Communication using *m-ary* Tree

R. Aparna[1], B.B. Amberker[2]

[1]*Deptartment of Computer Science and Engineering, Siddaganga Institute of Technology*

[2]*Department of Computer Science and Engineering, National Institute of Technology*

ABSTRACT: *Secure group communication is an important research area and numerous applications are relied upon secure group communication model. Since the group is dynamic in nature, rekeying must be carried out in an efficient manner. Member leave event should be handled carefully compared to member join event. In some applications like pay-per-view, periodical electronic information distribution etc., many users join and leave the group at the same moment known as bursty behavior. In this paper, we propose schemes for handling cumulative member removal and bursty behavior. We use m-ary key tree for managing the secure group and maintain only m keys at each level of the key tree. We start with a scheme for cumulative member removal and then we handle all the possible bursty behavior scenarios. We analyze the communication and computation costs for worst cases. We compare the costs of our scheme with the schemes proposed by Li et al. (2001) and binary key tree scheme of Zou, Magliveras, and Ramamurthy (2002). We show that in our scheme the number of new keys generated and encryptions performed are less compared to Li et al. (2001) and Zou, Magliveras, and Ramamurthy (2002) schemes.*

KEYWORDS: *Secure Group Communication, m-ary Key Tree, Key Distribution Center, Cumulative Member Removal, Bursty Behavior, Encryption Keys.*