Efficient Rekeying Framework for SecureMulticast with Diverse-Subscription-Period Mobile Users

Abstract:

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. To design the optimal GKM, researchers have assumed that all group members have the same leaving probabilities and that the tree is balanced and complete to simplify analysis. In the real mobilecomputing environment, however, these assumptions are impractical and may lead to a large gap between the impractical analysis and the measurement in real-life situations, thus allowing for GKM schemes to incorporate only a specific number of users. In this paper, we propose a new GKM framework supporting more general cases that do not require these assumptions. Our framework consists of two algorithms: one for initial construction of a basic key-tree and another for optimizing the key-tree after membership changes. The first algorithm enables the framework to generate an optimal key-tree that reflects the characteristics of users' leaving probabilities, and the second algorithm allows continual maintenance of communication with less overhead in group rekeying. Through simulations, we show that our GKM framework outperforms the previous one which is known to be the best balanced and complete structure.