International Journal of Network Management
13(6): 419-425

A Scalable Key-management Scheme with Minimizing Key Storage for Secure Group Communications

Tseng, Yuh-Min

Abstract

Recently, many group communication services have become the focus for future developments in the Internet and wireless network applications, such as video-conferencing, collaborative work, networking games or online videos. In particular, these applications require data delivery from one sender to a large number of authorized receivers. Therefore, secure multicast communication will become an important networking issue in the future. Using a common encryption key only known by authorized members to encrypt transmitted data is a practical approach. But, whenever a group member joins or leaves the group, the common encryption key must be updated to ensure both past and future secrecy. As a result, minimizing key update communication cost and the key storage requirement of a group controller is a critical issue in a scalable and dynamically changing large group. A new key-management scheme is proposed to reduce the key storage requirement of a group controller to a constant size, which is far better than that of the previously proposed schemes, while retaining the same key update communication cost. In addition, the correlation between the key storage requirement of each group member and key update communication cost are also presented.