Abstract

A Secure digital conference scheme allows a group of people to communicate safely in different way. Dynamic participation is a key feature of the secure conference schemes that allows new conferees to join and the old conferees to leave. The conference key distribution scheme (CKDS) enables three or more parties to derive a common conference key to protect the conversation content in their conference. In this paper we study a conference scheme for mobile communications and find that the scheme is insecure against the replay attack. With our replay attack, an attacker with a compromised conference key can cause the conferees to reuse the compromised conference key, which in turn completely reveals subsequent conversation content.
Overview of Secure Conference Scheme for Mobile Communications


Index Terms

Computer Science

Mobile Communications

Keywords

Mobile Communications    Conference Scheme    Security    Dynamic Participation