Secure Multicast Communications

T. Pugal

Abstract - Literature review revealed that multicast is used to deliver packets to group of users. To prevent users outside the group from eves dropping, a group is maintained to encrypt the group communication , and the group key is changed (rekeying) when a new member joins the group or an existing member leaves the group. Rekeying cost could be as high as n for a group with n members. This paper particularly addresses the problem of group key management in multicast communications. A secure multicast communication is important for application such as pay-per-view and secure video conferencing. The main issue in secure group communication is group dynamics and key management. A scalable secure group communication model ensures that whenever there is a membership change , new group key is computed and distributed to the group members with minimal computation and communication cost. Key management is the basis for providing common security services (data secrecy, authenticationand integrity) for group communication.