In Recent years, secure communications have become a important subject of research. The new service for wireless and wired networks is to provide confidentiality, authentication, authorization and data integrity. Security has always been a sensitive issue. In fact, this service becomes necessary to protect basic applications, especially E-commerce and bank transactions from a variety of attacks. An ad hoc network is a kind of wireless communication infrastructure that does not have base stations or routers. Each node acts as a router and is responsible for dynamically discovering other nodes it can directly communicate with. However, when a message without encryption is sent out through a general tunnel, it may be maliciously attacked. Securing group communication and group key establishment for ad hoc networks is covered in this paper. For a secure group communication in ad hoc networks, a group key is needed to be shared between group members to encrypt group messages. The main idea is to have group members actively participate to the security of the multicast group, therefore reducing the communication and computation load on the source. Since the group security is distributed among the group members, we propose a service right certificate, to verify that a node is authorized to join the group, and also a corresponding revocation mechanism.


Index Terms

Computer Science     Security

Key words

Secure Group communication     Multicast Key
distribution

Rekeying and Key Update

Key Tree