Abstract

Group communication plays a vital role in collaborative and group-oriented applications. It supports the dissemination of information from a sender to all the receivers in a group. The information needs to be encrypted using a secret key to ensure security in group communication over open networks. Group key establishment involves creating and distributing a common secret key for all group members. This paper proposes a group key agreement protocol that minimizes computation and storage overhead of nodes involved in group
communication. Hence this method is mainly suited for ad-hoc networks in which nodes have limited resources and short life time. Group member nodes form a logical tree structure among them. Group key is generated from the leaf to the root node. Then root node unicasts the computed key to every other member. This key is used for the encryption and decryption of group messages. The proposed scheme uses key tree structure to minimize the number of operations on each node. Elliptic Curve Diffie-Hellman minimizes computational overhead at each node and the key with smaller bit size can achieve higher security levels. The tree structure is always maintained as height balanced to minimize the key convergence time among group nodes.

**References**


**Index Terms**

Computer Science

Networks
Keywords