Abstract

Maintaining security is a critical issue in any group communication protocols. The objective of security in a group communication is to ensure the access only to the legitimate members of the multicast group. The entry and eviction of the members are the main criteria to change the group key and to give them more assurance of a secret communication, which is known as re-keying. Since it is a frequently performed activity during a communication, the group key updating need to be done in a scalable and efficient manner. Earlier, client-server paradigm is the most predominantly used technique for applications like conferencing, chat groups, interactive video gaming, etc which use the concept of unicast for the transmission of data. Present day advancements in the Internet technologies, especially the increase of bandwidth are definitely encouraging environment for new developments. Unlike the old communication models, where the delivery of the packets are to be carried out in an unicast model, multicasting technique provides an efficient delivery service to larger user-community with effective and efficient network resource utilization.
In the earlier schemes proposed for rekeying mechanism like LKH [4], FDLKH [7], DLPKH [9], the entire group will be disturbed with change in the membership. This paper proposes two new ideas: one with an objective of efficient re-keying and the other with an objective of disturbing only a subset of the group. Both the ideas don't need the secure channel for the distribution of the key material like [4],[7] and also does not reveal the private keys like [9]. The number of keys maintained at each member in this scheme, number of messages sent, size of the messages and number of encryption and decryptions are always constant unlike the other schemes which typically depends on the height of the tree.

Reference


Index Terms

Computer Science

Security
Key words

- Multicast group
- re-keying
- group communication
- secure channel