Abstract

Secure group communication is an active area of research and its popularity is fuelled by the growing importance of group oriented internet applications such as voice & video conferences, pay per view, etc. Several groupware applications like video conferences, distributed computations, etc requires secure transmission while communicating over the Internet. For secure communication, the integrity of the messages, member authentication, and confidentiality are must be provided among group members. To provide message integrity all group members must be agreed up on a common group key to encrypt and decrypt the messages. This paper proposes an efficient and contributory group key agreement protocol and also support dynamic operations like join, leave, merge, etc. by using ECC based Diffie Hellman key exchange. This protocol employs ternary tree like structure instead of binary tree in the process of group key generation. The performance of the proposed scheme is compared with that of several others existing schemes in literature and it is found that the proposed one is performs well in terms of communication and computation cost. In addition, the formal security validation is done using AVISPA tool that demonstrated that the proposed protocol is safe against passive and active attacks.
References

- Alves-Foss, J. An efficient secure authenticated group key exchange algorithm for large and dynamic groups. In IN PROC. 23 RD NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE (2000), pp. 254-266.
- Ching Chan, K., and h. Gary Chan, S. Key management approaches to offer data confidentiality for secure multicast. IEEE Netw (2003), 30-39.
- Peyravian, M., Matyas, S., and Zunic, N. Decentralized group key management for
- S. Maria Celestín Vigila, K. M.  Ecc based contributory group key computation scheme using one time pad. JOURNAL OF COMPUTING.

**Index Terms**

Computer Science  
Security

**Keywords**

ECC  group key agreement  ternary tree  ECC based Diffie-Hellman  AVISPA.