{tag} {/tag}

IJCA Proceedings on International Seminar on Computer Vision 2013
IJCA Journal

ISCV

Year of Publication: 2014

Authors:
S. Devakani

P. Chanthiya

K. Kumar

{bibtex}iscv1310.bib{/bibtex}

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

- Ingemar Ingemarsson, Donald T. Tang, and C. K. Wong,1982, "A conference key distribution system," IEEE Transactions on Information Theory, vol. IT-28, no. 5, pp. 714–720. Mike Burmester and Yvo Desmedt,1994, "A secure and efficient conference key distribution system," in Advances in Cryptology – EUROCRYPT '94, pp. 275–286.

- Klaus Becker and Uta Wille,1998, "Communication complexity of group key distribution," in 5th ACM conference on Computer and Communication Security.
- Michael Steiner, Gene Tsudik, and Michael Waidner,2000, "Key agreement in dynamic peer groups," IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769– 780.
- Y. Kim, A. Perrig, and G. Tsudik, 2004, "Tree-based group key agreement," ACM Transactions on Information and System Security, vol. 7, no. 1, pp. 60–96.
- Hua-yi lin , Tzu-chiangchiang, 2011, "Efficient key agreements in dynamic multicast height balanced tree for secure multicast communications in ad hoc networks", EURASIP journal on wireless communication and networking. ArticleID 382701.
- S. Maria Celestin Vigila ,K. Muneeswaran,2011, "ECC based contributory group key computation scheme using one time pad", Journal of computing,volume 3,issue 6.
- William stallings,2005," cryptography and network security": principles and practices", fourth edition, prentice hall.
- Eric Ricardo Anton, Otto Carlos Muniz Bandeira Duarte,2002," Group Key Establishment in Wireless Ad Hoc Networks", Workshop em Qualidade de Serviço e Mobilidade, Brazil.

Index Terms

Computer Science Networks

Keywords