Performance Analysis of Sponsor Selection Algorithms in Group Key Agreement

Network Security and Cryptography

© 2011 by IJCA Journal

NSC - Number 5

Year of Publication: 2011

Authors:

Shital Supase
Rajesh Ingle

10.5120/4350-050

Abstract

Many of the emerging group oriented, collaborative and distributed application are based on the secure group communication. The various group key agreement protocols are proposed for the same. The performance of all these group key agreement protocols depends on their performance metrics like communication cost and computation cost. In this work we present the performance analysis of STR protocol based on two different sponsor selection algorithms. These two algorithms are implemented by extending the Adaptive Middleware APIs for text conferencing application. Here we present the comparative analysis communication cost and computation cost for both algorithms.

Reference
- Yongdae Kim, Adrian Perrig, and Gene Tsudik, “Tree-based Group Key Agreement”.
- Yongdae Kim, Adrian Perrig, and Gene Tsudik, “Communication-Efficient Group Key Agreement”

Index Terms

Computer Science Security

Key words

Security

Secure group communication

Group key agreement

sponsor selection