

EFFICIENT HYBRID REGION-BASED KEY AGREEMENT PROTOCOL FOR SECURE GROUP COMMUNICATION

K. KUMAR, V. SUMATHY AND J. NAFEESA BEGUM

Abstract

Contributory Group Key Agreement is absolutely a promising solution to achieve access control in collaborative and dynamic group applications, the existing schemes cannot compete the performance lower bound in terms of time, communication and computational cost.

In this paper we propose a Contributory Group Key Agreement which fulfills the efficacious lower bound by utilizing a novel Group Diffie Hellman(GDH) &Tree Group Diffie Hellman(TGDH) protocols for subgroups and for backbone. As the selected protocols are secure Hybrid Region-Based Contributory Key Agreement that establishes subgroups among a group of members in the Group Communication is also secure. The proposed scheme achieves lower rekeying cost than the existing Contributory Group Key Agreement schemes.

Keywords: Group Diffie Hellman(GDH), Tree Group Diffie Hellman(TGDH), Hybrid Region-Based Contributory Key Agreement, Trusted Third Party (TTP).