Document details - Enhanced Group Key Distribution Protocol for Intra Group and Inter Group Communication Using Access Control Polynomial

Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

Volume 13119 LNAI, 2022, Pages 225-232

9th International Conference on Mining Intelligence and Knowledge Exploration, MIKE 2021; Virtual, Online; ; 1 November 2021 through 3 November 2021; Code 287859

Enhanced Group Key Distribution Protocol for Intra Group and Inter Group Communication Using Access Control Polynomial(Conference Paper)

Ragunathan, M., Kathirvalavakumar, T., Prasath, R.

[a]Department of Information Technology, V.H.N. Senthikumara Nadar College, Tamil Nadu, Virudhunagar, 626001, India
[b]Research Centre in Computer Science, V.H.N. Senthikumara Nadar College, Tamil Nadu, Virudhunagar, 626001, India
[c]Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, Andhra Pradesh, Chittoor, India

Abstract

In today's Internet world, group communications have become very crucial for several applications. It is essential to maintain confidentiality during communication hence it is very important to efficiently and securely distribute the common keys to the group members and target group members for encrypting and decrypting the message. This paper proposes an access control polynomial based on Chinese remainder theorem (CRT) for group key distribution (ACPGKD). Also proposes an authentication protocol for dynamic members to join or leave the group using the polynomial to keep backward and forward secrecy in inter-group and intra-group communications. It has been shown that the proposed work is secure and computationally efficient. © 2022, Springer Nature Switzerland AG.

Author keywords

Chinese remainder theorem | Group key distribution | Polynomial based key communication | Rekeying | Secure group communication

Indexed keywords

Engineering controlled terms: Access control

Engineering uncontrolled terms: Chinese remainder theorem | Group communications | Group key distribution | Group key distribution protocols | Group members | Inter-group communication | Intra-group | Polynomial based key communication | Re-keying | Secure group communications

Engineering main heading: Polynomials

ISSN: 03029743
ISBN: 978-303121516-2
Source Type: Book Series
Original language: English

DOI: 10.1007/978-3-031-21517-9_23
Document Type: Conference Paper
Volume Editors: Chbeir R.,Manolopoulos Y.,Prasath R.
Publisher: Springer Science and Business Media Deutschland GmbH