

ABSTRAK

Sifat dinamis keanggotaan dalam komunikasi grup menyebabkan adanya kebutuhan akan pembaruan kunci (*rekeying*) untuk menjaga keamanan komunikasi. Dalam grup yang sering mengalami perubahan anggota, proses *rekeying* dapat menyebabkan peningkatan biaya komputasi dan komunikasi. *Tree-Based Group Diffie-Hellman* (TGDH) menyediakan mekanisme pengelolaan kunci berbasis struktur pohon yang mendukung pengelolaan kunci grup secara terdistribusi. Untuk meningkatkan efisiensi *rekeying*, digunakan algoritma *batch* yang memproses beberapa permintaan perubahan anggota (bergabung dan keluar) secara bersamaan dalam interval waktu tertentu. Penelitian ini menganalisis kinerja algoritma Batch dalam protokol TGDH melalui simulasi dengan probabilitas yang bervariasi terkait anggota yang bergabung dan keluar. Evaluasi ini menggunakan metrik *exponentiation* dan *renewed nodes* untuk mengukur biaya komputasi dan komunikasi yang dihasilkan selama proses *rekeying*. Analisis ini bertujuan untuk memberikan pemahaman mengenai karakteristik algoritma *batch* dalam menangani perubahan keanggotaan pada kelompok dinamis.

Kata kunci : *Tree-Based Group Diffie-Hellman, rekeying, Batch, Exponentiaion, Renewed Nodes.*

ABSTRACT

The dynamic nature of group membership in group communication necessitates key rekeying to maintain communication security. In groups that frequently experience changes in membership, the rekeying process can lead to increased computational and communication costs. Tree-Based Group Diffie-Hellman (TGDH) provides a tree-structured key management mechanism that supports distributed group key management. To improve rekeying efficiency, a batch algorithm is used that processes multiple membership change requests (joins and leaves) simultaneously within a specific time interval. This study analyzes the performance of the batch algorithm in the TGDH protocol through simulations with varying probabilities of members joining and leaving. This evaluation uses the metrics of exponentiation and renewed nodes to measure the computational and communication costs incurred during the rekeying process. This analysis aims to provide an understanding of the characteristics of the batch algorithm in handling membership changes in dynamic groups.

Keywords: Tree-Based Group Diffie-Hellman, rekeying, Batch, Exponentiation, Renewed Nodes.