ABSTRACT

Penelitian ini mengembangkan sistem manajemen kunci pada arsitektur *publish subscribe* di jaringan *Delay Tolerant Network* (DTN) yang menghadapi tantangan konektivitas tidak stabil. Tantangan utama terletak pada perlindungan konten pesan dan pengelolaan akses bagi subscriber yang berwenang. Untuk mengatasi hal ini, penelitian mengimplementasikan pendekatan *Publish Subscribe Guard* (PSGuard) dengan mekanisme manajemen kunci hierarkis berbasis *Numeric Attribute Key Tree* (NAKT). Sistem ini dirancang untuk mengoptimalkan distribusi kunci enkripsi dan otorisasi melalui *Key Distribution Center* (KDC).

Evaluasi dilakukan menggunakan *The ONE Simulator* dengan membandingkan PSGuard terhadap metode *Subscriber Group*. Hasil penelitian menunjukkan bahwa pendekatan hierarkis PSGuard menawarkan solusi manajemen kunci yang lebih skalabel dan efisien untuk jaringan DTN dinamis. Kestabilan performa PSGuard pada berbagai skala sistem membuktikan efektivitasnya dalam menjaga keamanan data sekaligus mengoptimalkan sumber daya jaringan.

Kata Kunci : Manajemen Kunci, *Publish-Subscribe*, D*elay Tolerant Network*, *PSGuard*, *NAKT*, Skalabilitas.

ABSTRACT

This research develops a key management system within a *publish subscribe* architecture in *Delay Tolerant Networks* (DTNs), which face challenges due to unstable connectivity. The main challenge lies in securing message content and managing access for authorized subscribers. To address this, the study implements the *Publish Subscribe Guard* (PSGuard) approach with a hierarchical key management mechanism based on the *Numeric Attribute Key Tree* (NAKT). The system is designed to optimize the distribution of encryption keys and authorization through a *Key Distribution Center* (KDC).

Evaluation was conducted using *The ONE Simulator* by comparing PSGuard to the *Subscriber Group* method. The results show that the hierarchical PSGuard approach provides a more scalable and efficient key management solution for dynamic DTNs. The stable performance of PSGuard across various system scales demonstrates its effectiveness in ensuring data security while optimizing network resource usage.

Keywords: *Key Management*, *Publish-Subscribe*, *Delay Tolerant Network*, *PSGuard, NAKT, Scalability*.