

ABSTRAK

Sistem publish-subscribe berbasis konten merupakan paradigma yang sedang berkembang untuk membangun berbagai aplikasi terdistribusi khususnya di jaringan Delay Tolerant Network (DTN). Masalah khusus dalam system berbasis konten adalah pendistribusian event secara aman kepada klien yang berlangganan pada event tersebut. Dalam sistem berbasis konten, setiap event dapat memiliki kumpulan subscriber yang berbeda-beda. Untuk memberikan jaminan kerahasiaan, Subscriber Group dapat mengenkripsi pesan sehingga hanya subscriber yang tertarik yang dapat membaca pesan tersebut.

Untuk melakukan evaluasi, The ONE Simulator digunakan untuk membandingkan Subscriber Group dengan metode PSGuard. Hasilnya akan menunjukkan perbandingan antara Siplisitas dan efisiensi untuk jaringan DTN dinamis. Bahasan ini akan menyajikan analisis analitis mengenai algoritma begitu juga simulasi cara bekerjanya.

Kata Kunci : Publish-subscribe, Keamanan pesan, Manajemen kunci

ABSTRACT

A content-based publish-subscribe system is an emerging paradigm for building various distributed applications, particularly within Delay Tolerant Network (DTN) environments. A specific challenge in content-based systems is the secure distribution of events to clients subscribed to those events. In such systems, each event may have a different set of subscribers. To ensure confidentiality, the Subscriber Group can encrypt messages so that only interested subscribers are able to read them.

For evaluation purposes, The ONE Simulator is used to compare the Subscriber Group approach with the PSGuard method. The results will highlight the trade-offs between simplicity and efficiency in dynamic DTN environments. This discussion presents both an analytical analysis of the algorithms and a simulation of their operational behavior.

Keywords : Publish-subscribe, Message Security, Key Management

