ABSTRAK

Jaringan oportunistik (OppNet) adalah jaringan wireless yang bersifat unik dimana setiap node yang ada pada jaringan dapat mengirimkan pesan tanpa adanya proses *encryption/decryption* antara kedua node yang ada di jaringan. Kenyataannya, untuk mengirimkan informasi lewat saluran yang kurang aman kita membutuhkan protokol untuk mengatur otentikasi dari node-node yang ada pada jaringan seperti protokol untuk mengatur distribusi kunci, pembuatan kunci, dan bagaimana cara kerja otentikasi antara kedua node yang sedang berkomunikasi. Di lain hal, node-node pada jaringan oportunistik memiliki sumber daya seperti jumlah buffer dan sumber daya dalam jumlah yang terbatas. Dengan demikian, kita membutuhkan sebuah protokol yang efisien dan bersahabat dengan kekurangan-kekurangan pada node-node di jaringan oportunistik. Pada penilitian ini, penulis menguji efisiensi protokol Diffie – Hellman dengan protokol klasik apabila diterapkan pada jaringan oportunistik. Unjuk kerja yang akan diperhatikan adalah *overhead ratio* dan *delay convergence* dari kunci-kunci yang akan disebarkan.

Hasil pengujian menunjukkan bahwa protokol Diffie – Hellman lebih efektif daripada protokol klasik dalam kasus penyebaran kunci. Hal ini dikarenakan cara kerja dari protokol Diffie – Hellman sendiri yang menggunakan konsep *public* dan *private key*, sedangkan pada protokol klasik menggunakan kunci tanpa menggunakan konsep public dan private key sehingga jumlah kunci yang akan disebarkan berbeda.

Kata kunci : jaringan oportunistik, *overhead ratio*, key convergence, *diffie – hellman protocol*, *public key, private key*.

ABSTRACT

Opportunistic network is a unique wireless network which is every node in the network can deliver a message without encryption/decryption process. In reality, to deliver an information via insecure network needs a protocol that handle the entire authentication of the message such as key distribution, key generation, and how two network authenticate themselves when building a connection. And also in opportunistic network, all nodes have limited buffer, and power. So we need a protocol which is efficient enough and friendly to weaknesses of the nodes. In this research, the writer will analyze the efficiency of Diffie – Hellman protocol and the classic protocol for key exchange . The research will test the *overhead ratio* and *key convergence.*

The result shows Diffie – Hellman protocol more efficient than the classic protocol in opportunistic network in terms of key exchange because Diffie – Hellman protocol use *public* and *private key* to exchange their key. In the other hand, classic protocol not using public and private key. That means the number of key distributed over the network is vary.

Keywords : opportunistic network, overhead ratio, key convergence, diffie – hellman protocol, public key, private key