ABSTRAK

Wireless Sensor Network (WSN) atau Jaringan Sensor Nirkabel (JSN) merupakan teknologi yang sedang hangatnya digunakan baik untuk riset maupun untuk mempermudah kehidupan sehari-hari. Sistem keamanan adalah salah satu hal penting yang harus diperhatikan baik dalam *wireless network* maupun *wireline network*. Jaringan sensor nirkabel semakin berkembang yang mengakibatkan mudah diserang dan sebab itu membutuhkan mekanisme keamanan yang efektif. Jaringan sensor nirkabel memiliki beberapa kendala seperti memori terbatas, energi dan kemampuan komputasi yang menimbulkan kendala bila ditambah dengan keamanan di *node* sensor.

Untuk menyelesaikan masalah diatas, tugas akhir ini mengimplementasikan dan menganalisa sistem keamanan di jaringan sensor nirkabel mengacu pada standar ZigBee. Skema ZigBee dapat disetarakan dengan protokol baru yang ditargetkan pada *low rate*, perangkat dengan daya kecil, dan *node* sensor. ZigBee membutuhkan kriptografi yang diharapkan bisa menghemat daya, kemampuan komputasi, dan sumber penyimpanan. Untuk itu, sistem keamanan yang dipilih adalah menggunakan algoritma enkripsi AES128 (*Advanced Encryption Standard*) yang diimplementasikan langsung pada ZigBee.

Pada tugas akhir ini berhasil mengimplementasikan algoritma enkripsi dekripsi AES128 pada jaringan sensor nirkabel. Pengujian yang digunakan adalah passive attacks yang hanya bisa melihat dan meng-*capture* paket saja. Pada analisa performansi keamanan, parameter *confidentiality* tidak terpenuhi jika tidak menggunakan keamanan. Parameter *integrity* terpenuhi menggunakan atau tanpa menggunakan keamanan. Nilai *throughput* terbesar adalah 1122 *byte*s/s pada jarak 21 meter. Dan nilai *delay* terbesar pada jarak 49,5 meter dengan nilai 4,1483 s.

Kata Kunci : WSN, ZigBee, AES128