ABSTRAKSI

Di zaman sekarang, jaringan sensor nirkabel atau *Wireless Sensor Network (WSN)* sudah mulai banyak diterapkan di berbagai bidang kehidupan, seperti kesehatan, lingkungan, dll. Dan salah satu bentuk aplikatif yang mulai banyak diterapkan saat ini adalah untuk monitoring, misal seperti *environmental control* yang dapat memantau keadaan sebuah lingkungan. WSN terbentuk dari beberapa perangkat sensor, atau sensor *node*, yang saling terhubung melalui jaringan nirkabel (*wireless*) dan dapat saling bertukar data secara *real-time*. Ukurannya yang kecil mengakibatkan perangkat sensor memiliki keterbatasan sumber daya, terutama dalam menjamin aspek keamanan seperti *confidentiality*, *integrity* dan *authenticity*. Karena itulah dibutuhkan sebuah protokol keamanan yang tidak hanya dapat menjamin aspek-aspek keamanan tersebut namun juga dapat meminimalkan *overhead* dari perangkat sensor. Untuk menjamin aspek-aspek keamanan yang ada, digunakan metode pengamanan *Cipher Block Chaining (CBC) Message Authentication Code (MAC).* Pada penelitian tugas akhir ini akan digunakan dua buah protokol keamanan, yaitu TinySec dan *Link-Layer Security Protocol (LLSP)*. Akan dilakukan uji coba terhadap kedua protokol ini melalui sebuah simulasi menggunakan aplikasi NS-3. Kemudian akan ditunjukkan dan dibandingkan tingkat performansi antara kedua protokol tersebut. Parameter performansi yang menjadi tolak ukur adalah konsumsi energi, *confidentiality*, *integrity* dan *authentication*. Dari hasil pengujian yang dilakukan, disimpulkan bahwa protokol LLSP dapat menghemat konsumsi energi hingga 15% dari protokol TinySec, karena adanya perbedaaan panjang *byte* untuk melakukan operasi keamanan yang dibutuhkan.

Kata kunci: *Wireless sensor network (WSN)*, *Security protocol*, TinySec, *Link-Layer Security Protocol (LLSP)*.