Bab I

Pendahuluan

1.1 Latar Belakang

Keamanan dalam pengiriman suatu informasi maupun data mempunyai peranan yang penting untuk menjaga kerahasiaan serta integritas informasi pada jaringan sensorik nirkabel. Setiap jaringan nirkabel maupun bukan nirkabel mempunyai potensi untuk tidak bekerja secara optimal serta memenuhi ekspektasi dikarenakan berbagai kendala yang muncul pada jaringan tersebut baik dimana kendala tersebut muncul secara internal mapun eksternal. Kendala tersebut dapat menimbulkan dampak merugikan seperti hilangnya kemampuan untuk mengirimkan informasi, pencurian data sampai kondisi jaringan secara keseluruhan berada dalam kondisi tidak aktif.

Protokol keamanan dibuat untuk memberikan penanganan terhadap segala efek yang merugikan kepada jaringan nirkabel maupun non-nirkabel. Protokol keamanan tersebut mempunyai tujuan untuk mempertahankan originalitas informasi serta memastikan informasi tersebut tetap dapat dikirimkan untuk dapat memberikan analisa secara mendalam dan akurat. Jaringan sensor nirkabel menggunakan sensor yang mempunyai keterbatasan pada sumber daya, kemampuan komputasi serta kemampuan untuk mengirimkan informasi dan sensor tersebut ditempatkan pada kondisi lingkungan yang tidak kondisif [1], sehingga menimbulkan kemungkinan terjadinya berbagai kendala pada jaringan sensorik nirkabel.

Berdasarkan hal diatas, dapat dirangkum bahwa terdapat beberapa faktor untuk membuat menentukan titik tumpu[13] dalam menentukan protokol terbaik yang dapat digunakan dalam jaringan sensorik nirkabel, yaitu dalam segi key management, pengamanan jalur routing dan pencegahan serangan pada jaringan nirkabel[13].

Dalam tugas akhir ini, penulis melakukan perbandingan protokol keamanan jaringan MiniSec [16] dan Sensor Network Encryption Protocol (SNEP) [18] pada jaringan sensorik nirkabel, MiniSec merupakan protokol keamanan yang

menggunakan *block cipher* yang dapat menjamin kerahasiaan dan autentikasi data pada pesan yang akan dikirimkan [16] dan SNEP merupakan protokol keamanan yang menjamin kerahasiaan dan autentikasi pada pesan dengan *overhead* yang rendah [18]. Perbandingan dilakukan untuk mengetahui protokol keamanan yang lebih baik antara MiniSec dan SNEP dikarenakan kedua protokol tersebut menjamin bahwa pesan yang dikirimkan tidak dapat mengalami perubahan dan dibaca oleh *attacker*. Parameter utama dalam melakukan perbandingan protokol keamanan pada jaringan sensor nirkabel merupakan kerahasisaan data, integritas informasi, originalitas dan penggunaan energi serta simulasi serangan [1] pada jaringan sensorik nirkabel. Protokol keamanan MiniSec dan *Sensor Network Encryption Protocol* mempunyai kelemahan dimana protokol keamanan MiniSec mempunyai kelemahan pada penanganan serangan *Denial-of-Service* [21] dan pada *Sensor Network Encryption Protocol* (SNEP) mempunyai kelemahan pada keamanan data dikarenakan apabila SNEP bergantung hanya dengan menggunakan enkripsi tidak akan cukup serta lemahnya originalitas informasi yang dikirimkan [18] seiring berjalannya waktu dalam pengumpulan informasi oleh sensor pada saat menggunakan protokol keamanan tersebut. Protokol keamanan SNEP mempunyai performa yang lebih rendah dikarenakan SNEP tidak mempunyai mekanisme pendeteksian pemalsuan master key [1] dibandingkan dengan protokol keamanan MiniSec. Proses perbandingan protokol keamanan dilakukan dengan menggunakan metoda studi literatur dan Simulasi protokol keamanan menggunakan aplikasi NS-3.

1.2 Perumusan Masalah

Adapun permasalahan yang akan diselesaikan dalam pembuatan tugas akhir ini, diantaranya adalah sebagai berikut:

1. Bagaimana menerapkan protokol keamanan MiniSec dan *Sensor Network Encryption Protocol* (SNEP) untuk menentukan protokol manakah yang berkerja lebih baik dalam jaringan sensorik nirkabel?
2. Bagaimana performasi protokol keamanan MiniSec dan *Sensor Network Encryption Protocol* (SNEP) dengan menggunakan parameter yang telah ditetapkan dalam jaringan sensorik nirkabel?

1.3 Tujuan

Tujuan dari pengerjaan Tugas Akhir ini adalah sebagai berikut:

1. Menerapkan protokol keamanan MiniSec dan *Sensor Network Encryption Protocol* (SNEP) untuk penentuan protokol terbaik dalam jaringan

sensorik nirkabel.

2. Mengetahui performasi protokol keamanan MiniSec dan *Sensor Network Encryption Protocol* (SNEP) dengan menggunakan parameter yang telah ditetapkan dalam jaringan sensorik nirkabel.

1.4 Hipotesis

Protokol keamanan *Sensor Network Encryption Protocol* (SNEP) kemungkinan mempunyai performa yang lebih rendah dikarenakan SNEP tidak mempunyai mekanisme pendeteksian terhadap pemalsuan master key serta dapat terjadinya counter synchronization [1] pada jaringan sensorik nirkabel yang menggunakan protokol keamanan SNEP, dimana protokol keamanan MiniSec mempunyai dua format packet untuk melakukan pengiriman yaitu *Minisec-U* untuk melakukan transmisi secara unicast dan *MiniSec-B* untuk melakukan transimis secara broadcast [16] pada jaringan sensorik nirkabel. Penelitian menunjukan bahwa MiniSec menggunakan energi sebesar 0.0368 dengan total ukuran 39 B sedangkan SNEP menggunakan energy sebesar 0.0415 dengan ukuran 44 B [21]. Berdasarkan hal tersebut protokol keamanan MiniSec diharapkan dapat memberikan pengamanan yang lebih baik dalam aspek message integrity, authenticity, encryption, availability, freshness dan energy consumption dalam pengiriman informasi dalam jaringan sensorik nirkabel dibandingkan dengan protokol keamanan SNEP.

1.5 Metodologi Penyelesaian Masalah

Metodologi yang digunakan dalam menyelesaikan Tugas Akhir ini adalah sebagai berikut:

1. Studi Literatur

   Studi literature dilakukan dengan cara mengumpulkan dan memahami referensi yang berkaitan dengan protokol keamanan jaringan sensorik nirkabel dimana sumber referensi didapat dari berbagai media, seperti paper, jurnal, internet dan buku. Paper acuan yang diambil penulis adalah paper yang dibuat oleh Abu Shohel Ahmed dengan judul "An Evaluation of Security Protocol on Wireless Sensor Network", paper yang dibuat oleh Mark Luk, Ghita Mezzour, Adrian Perrig dan Virgil Gligor dengan judul "MiniSec: A Secure Sensor Network Communication Architecture" dan paper yang dibuat oleh Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen dan David E. Culler dengan judul "SPINS: Security Protocol for Sensor Networks".

2. Konsultasi

   Melakukan bimbingan dengan dosen pembimbing dan dosesn lainnya yang terkait dengan permasalahan yang dikerjakana pada Tugas Akhir ini.

3. Pengumpulan Data

   Pengumpulan data dilakukan dengan cara mengambil parameter utama dari paper yang berhubungan dengan evaluasi protokol keamanan pada jaringan sensorik nirkabel, dimana parameter utama yang ditentukan untuk Tugas Akhir ini merupakan *message integrity*, *authenticity*, *encryption*, dan *energy consumption* serta berbagai informasi lainnya terkait implementasi untuk simulasi jaringan sensorik nirkabel dengen menggunan protokol keamanan MiniSec dan Sensor Network Encryption Protocol (SNEP) terhadap penyerangan pada Wireless Sensor Network.

4. Perancangan Model

   Tahap ini merupakan tahapan dalam perancangan model simulasi terhadap protokol keamanan MiniSec dan Sensor Network Encryption Protocol (SNEP) untuk simulasi jaringan sensorik nirkabel.

5. Implementasi Simulasi

   Pada tahapan implementasi simulasi akan dilakukan pengkodingan terkait protokol keamanan MiniSec dan Sensor Network Encryption Protocol (SNEP) pada aplikasi NS-3.

6. Testing dan Analisis Hasil Simulasi

   Pengujian dilakukan dengan menggunakan aplikasi NS-3 dengan mengimplementasikan protokol keamanan MiniSec dan Sensor Network Encryption Protocol (SNEP) terhadap penanganan serangan pada jaringan sensorik nirkabel.

7. Penyusunan Buku Tugas Akhir

   Pada tahapan ini, buku Tugas Akhir akan dibuat berdasarkan proses dan hasil dokumentasi dari penelitian hasil simulasi terhadap protokol keamanan yang dibandingkan.