Bab I
Pendahuluan

1.1 Latar Belakang

Jaringan sensor nirkabel merupakan kumpulan sensor yang tersusun menjadi sebuah jaringan yang dapat merasakan dan mengontrol lingkungannya sehingga dapat dilakukannya interaksi antara manusia atau komputer dengan lingkungan sekitarnya. Pada awalnya jaringan sensor nirkabel digunakan hanya untuk kepentingan militer, sekarang jaringan sensor nirkabel sudah mulai dikembangkan untuk berbagai bidang lainnya, seperti pertanian, kesehatan, dan lain-lain.

Node sensor tidak dapat selalu diawasi satu persatu oleh manusia. Oleh karena itu, keamanan node sensor pada jaringan sensor nirkabel sangat dibutuhkan, terutama saat pengiriman data dan informasi. Data dan informasi yang dikirimkan node sensor bersifat rahasia, karena isi data dan informasi yang dikirimkan node sensor adalah hal penting yang merupakan keadaan sebenarnya dari lingkungan. Apabila kerahasiaan data dan informasi tidak ada atau rusak, sehingga data dan informasi dapat dilihat dan diubah oleh pihak ketiga yang dapat mengakibatkan penyusupan kedalam jaringan, kebocoran informasi, bahkan pemalsuan informasi yang dapat merusak jalur informasi pada jaringan.

Terbatasnya memori dan energi yang dapat disimpan oleh node sensor mengakibatkan komputasi yang dilakukan node sensor haruslah lebih sederhana dibandingkan komputasi yang dilakukan oleh komputer yang biasa digunakan sehari-hari. Begitu pula dengan protokol keamanan yang digunakan untuk jaringan sensor nirkabel, tidak hanya harus memenuhi kebutuhan keamanan tapi juga harus sesuai dengan sumber daya dan kemampuan yang dimiliki oleh node sensor, sehingga tidak sembarang protokol keamanan dapat diaplikasikan pada jaringan sensor nirkabel.

Dalam penelitian ini, akan dilakukan analisis terhadap perbandingan performa antara dua protokol keamanan, yaitu LEAP dan RKP dimana kedua protokol keamanan tersebut bertipe manajemen kunci. Walaupun keduanya bertipe manajemen kunci, tapi kedua protokol keamanan tersebut memiliki cara manajemen kunci yang berbeda. Protokol keamanan LEAP menggunakan empat jenis kunci yang digunakan berdasarkan node yang dituju untuk berkomunikasi. RKP menggunakan *key ring* yang berisi kunci-kunci yang nantinya digunakan untuk membangun jalur komunikasi. Selain itu, LEAP dan RKP mendukung aspek *confidentiality* dan *authentication*. Perbandingan protokol keamanan LEAP dan RKP dilakukan menggunakan NS3.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan sebelumnya, rumusan masalah dari penelitian ini adalah:

1. Bagaimana mensimulasikan protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP) pada NS-3?
2. Bagaimana perbandingan performasi dari protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP)?

1.3 Tujuan

Mengaju pada rumusan masalah yang sudah dijelaskan sebelumnya, tujuan dari penelitian ini adalah:

1. Mensimulasikan protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP) pada NS-3.
2. Mengetahui perbandingan performasi dari protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP).

1.4 Batasan Masalah

Batasan masalah yang ada selama pelaksananaan penelitian ini adalah:

1. Simulasi menggunakan NS-3.
2. Eksternal library crypto++ digunakan untuk implementasi enskripsi pesan.
3. Parameter pengujian yang digunakan adalah confidentiality, authentication, dan *energy consumption*.

1.5 Metode Penelitian

Metodologi yang digunakan adalah sebagai berikut:

1. Studi Literatur
   Mengumpulakan dan melakukan pencarian teknik dan metode yang terkait dengan penelitian ini dan informasi yang berhubungan dari berbagai sumber, seperti jurnal ilmiah, buku teks, dan internet sebagai

acuan dari protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP).

2. Pengumpulan Data
   Pengumpulan data dilakukan dengan memanfaatkan paper untuk mendapatkan parameter yang dapat diterapkan pada protokol keamanan pada jaringan sensor nirkabel, yaitu confidentiality, authentication, dan energy consumption agar simulasi protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP) dapat dilakukan.
3. Perancangan Model
   Melakukan perancangan model protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP) untuk simulasi pada jaringan sensor nirkabel.
4. Simulasi
   Mensimulasikan protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP) pada NS-3.
5. Pengujian dan Analisis
   Pengujian dilakukan terhadap protokol keamanan *Localized Encryption and Authentication Protocol* (LEAP) dan *Random Key Pre-distribution* (RKP) dan analisis dilakukan terhadap hasil pengujian.
6. Pembuatan Laporan
   Melakukan pembuatan laporan akhir berdasarkan proses dan hasil dari simulasi terhadap protokol keamanan yang dibandingkan