BAB I
PENDAHULUAN

1.1 Latar Belakang

Wireless Sensor Network (WSN) atau Jaringan Sensor Nirkabel (JSN) merupakan teknologi yang sedang hangatnya digunakan baik untuk riset maupun untuk mempermudah kehidupan sehari-hari. WSN adalah jaringan dengan infrastruktur yang bisa mendeteksi, menghitung dan mempunyai elemen komunikasi yang dapat mengirimkan data kepada administrator untuk mengukur, mengobservasi, dan memberikan perintah jika ada suatu kondisi tertentu. Salah satu tujuan dari *wireless sensor network* adalah untuk membawa informasi yang dapat dipercaya dari satu *node* ke *node* yang lain dalam jaringan tersebut [1]. *Wireless sensor setwork* adalah aspek krusial yang ada dalam pengimplementasian IoT karena sensor merupakan perangkat kecil, portable, dan bisa diimplementasikan di banyak aplikasi [2].

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 [1]. Pengguna WSN seharusnya percaya bahwa informasi yang mereka terima dari jaringan dapat dipercaya, akurat, dan tidak dirusak oleh pihak yang tidak bertanggung jawab. Contohnya jika seorang petani menggunakan WSN untuk sistem irigasi otomatis harus percaya bahwa sensor tidak rusak yang dapat mengakibatkan tanah akan kering atau tanaman kering sebelum memperingatkan petani [2]. Jaringan sensor nirkabel memiliki beberapa kendala seperti memori terbatas, energi dan kemampuan komputasi yang menimbulkan kendala bila ditambah dengan keamanan di *node* sensor. Untuk mengirimkan informasi yang telah dibaca oleh *node* sensor membutuhkan ZigBee untuk mengirim sehingga informasi tersebut sampai kepada pengguna WSN tersebut. ZigBee merupakan standar yang diatur dalam IEEE

802.15.4, yang terdiri dari *physical layer*, *medium access control* (MAC) *layer*, *network layer*, dan *application layer* [3].

Untuk menyelesaikan masalah diatas, tugas akhir ini akan mengimplementasikan dan menganalisa sistem keamanan di jaringan sensor nirkabel mengacu pada standar ZigBee. ZigBee seperti standar yang mana sepanjang konfigurasi sensor mikro dari ZigBee yang dapat saling berhubungan satu sama lain dari Adhoc [3]. ZigBee adalah standar yang muncul untuk *low power*, *low rate* komunikasi nirkabel dimana dengan tujuan dua sistem dapat bekerjasama dan dapat mencakup seluruh perangkat dalam cakupan WSN walaupun daya pada *node* sensor rendah [4]. ZigBee membutuhkan kriptografi yang diharapkan bisa menghemat daya, kemampuan komputasi, dan sumber penyimpanan. Algoritma enkripsi AES pernah dilakukan pada standar IEEE 802.15.4 tetapi menggunakan perangkat TelosB [5]. Untuk itu, sistem keamanan yang dipilih adalah menggunakan algoritma enkripsi AES (*Advanced Encryption Standard*) yang diimplementasikan langsung pada ZigBee.

1.2 Tujuan Penelitian

Tujuan dari pembuatan tugas akhir ini adalah sebagai berikut:

1. Memodelkan jaringan sensor nirkabel menggunakan standar ZigBee
2. Algoritma enkripsi AES128 dapat diimplementasikan langsung pada standar ZigBee dan dapat menyediakan mutu keamanan yang cukup untuk melindungi kerahasiaan data pada jaringan sensor network.
3. Mengetahui kualitas jaringan ketika terdapat sistem keamanan dengan dan tanpa menggunakan algoritma enkripsi AES128
4. Mengetahui kemampuan Raven USB Stick dalam *sniffing* jaringan sensor nirkabel.

1.3 Rumusan Masalah

Bedasarkan deskripsi latar belakang, maka dapat dirumuskan beberapa masalah di tugas akhir ini yaitu :

1. Bagaimana memodelkan sistem jaringan sensor nirkabel menggunakan algortima enkripsi AES128
2. Bagaimana meng-aktifkan kunci enkripsi pada perangkat XBee S2
3. Bagaimana mengimplementasikan sistem jaringan sensor nirkabel menggunakan algoritma enkripsi AES128 pada Arduino Uno
4. Bagaimana menganalisis hasil *sniffing* oleh Raven USB Stick

1.4 Batasan Masalah

Batasan masalah dalam penelitian tugas akhir ini adalah :

1. Komunikasi jaringan sensor nirkabel menggunakan standar ZigBee
2. Tidak menampilkan hasil sensor secara *online*
3. Jumlah perangkat yang digunakan 2 *node* sensor dan 1 *node* koordinator
4. Sistem minimun mikrokontroler yang digunakan adalah Arduino Uno R3
5. WiFi *module* yang digunakan adalah XBee Series 2 *Wire Antenna*
6. Algoritma enkripsi yang digunakan adalah AES128
7. Hanya menggunakan *passive attacks*

1.5 Metodologi Penelitian

Pengerjaan tugas akhir ini menggunakan beberapa metodologi, antara lain:

1. Studi Literatur

   Tahap pertama yang dilakukan adalah pencarian referensi dan materi yang berhubungan dengan WSN, standar ZigBee, keamanan pada WSN, dan algoritma enkripsi AES. Serta, mempelajari konsep dan teori pendukung yang berkaitan dengan tugas akhir ini. Sumber yang digunakan berasal dari buku, jurnal ilmiah dan *website*.

2. Perencanaan dan Perangcangan Sistem

   Dilakukan perencanaan dan perancangan sistem keamanan mengggunakan algoritma enkrispi AES pada standar ZigBee.

3. Implementasi

   Pada tahap ini mengintegrasikan perangkat yang digunakan dengan algoritma enkripsi AES

4. Pengujian Sistem

   Pada tahap ini akan dilakukan pengamatan dan pengujian kinerja dari sistem yang telah dirancang serta akurasi sistem terhadap beberapa kondisi yang telah ditentukan.

5. Analisa

   Dilakukan analisis terhadap paramenter-parameter kinerja sistem dari berbagai kondisi yang diimplementasikan.

6. Penyimpulan Hasil

   Dilakukan penarikan kesimpulan terhadap beberapa parameter kinerja sistem dari berbagai kondisi yang diimplementasikan.

1.6 Sistematika Penulisan

Secara umum penulisan Tugas Akhir ini terbagi menjadi lima bab yang disusun dengan sistematika sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini dijelaskan mengenai latar belakang, tujuan, perumusan masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan dari Tugas Akhir.

BAB II DASAR TEORI

Pada bab ini berisi dasar teori mengenai jaringan sensor nirkabel, IEEE 802.15.4 (standar ZigBee), algoritma enkrispsi AES, dan teori lain yang berhubungan dengan Tugas Akhir ini.

BAB III PERANCANGAN MODEL JARINGAN

Pada bab ini dibahas tentang perencanaan dan perancangan algoritma enkripsi AES dalam jaringan sensor nirkabel dan bagaimana scenario penyerangan jaringan sensor nirkabel.

BAB IV PENGUJIAN DAN ANALISIS HASIL

Pada bab ini akan membahas tentang hasil pengujian dari algoritma enkripsi AES pada jaringan sensor nirkabel menggunakan standar ZigBee.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dan saran dari pengujian dan analisa yang didapatkan dari tugas akhir ini.