

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Adanya perkembangan teknologi yang sangat cepat dan efisien saat ini terutama pada bidang kesehatan, dibutuhkan sarana teknologi telekomunikasi yang mampu memenuhi kebutuhan tersebut dengan lebih baik. Salah satu contohnya adalah Wireless Body Area Network (WBAN) yang umumnya digunakan untuk aplikasi di bidang monitoring kesehatan jarak jauh. WBAN merupakan jaringan nirkabel komunikasi, yang dapat mempermudah proses memonitoring kondisi pasien sehingga dapat lebih efisien dalam mendapatkan data medis dan juga dapat mengefisiensi waktu yang diperlukan.

Dalam sistem WBAN itu sendiri terdapat beberapa metode, akan tetapi penulis menggunakan metode IR-UWB. Metode IR-UWB ini menggunakan standard sesuai IEEE 802.15.6 [1], dan memiliki singkat pulsa dalam domain waktu dengan energi bandwidth mereka yang tersebar luas dalam domain frekuensi. Secara umum suatu sistem dapat dikategorikan sebagai komunikasi IR-UWB jika memiliki kriteria bandwidth fraksional lebih besar daripada 20%. Sistem komunikasi IR-UWB sendiri telah diajukan oleh Federal Communication Commission (FCC) pada tahun 2002 untuk beroperasi pada spektrum frekuensi 3,1 - 10,6 GHz [2]. Sistem komunikasi IR-UWB adalah sistem komunikasi jarak pendek yang memiliki bandwidth yang sangat lebar, untuk itu suatu sistem dapat dikategorikan sebagai komunikasi IR-UWB maka syaratnya adalah lebar bandwidthnya lebih besar dari 500 MHz [3].

Dengan menggunakan metode IR-UWB WBAN dengan NRZ dan modulasi Binary Phase Shift Keying (BPSK), Pulse Position Modulation (PPM), serta Gaussian *monocycle* serta kanal CM4 sesuai dengan IEEE 802.15.6. Salah satu hal yang paling penting yaitu keamanan pada saat pengiriman serta penerimaan sinyal informasi atau data yang telah didapatkan dari metode IR-UWB itu sendiri. Perlu dilakukan metode pengamanan data dengan metode enkripsi kriptografi pada sinyal informasi yang akan

dikirimkan untuk mencegah adanya pengambilan atau pemalsuan data pada saat pengiriman atau penerimaan data.

Dalam membuat sistem perlindungan untuk pengiriman sinyal tersebut, penulis merancang sistem enkripsi pada IR-UWB WBAN. Evaluasi sistem kerja tersebut dengan melakukan enkripsi dan dekripsi pada data yang akan dikirimkan dan diterima dalam membuat sistem tersebut. Metode enkripsi memiliki beberapa parameter tertentu, yaitu metode enkripsi kriptografi symmetric AES 256, DES. Dengan menggunakan metode enkripsi bertujuan untuk membantu keamanan sistem lebih sederhana, dan efisiensi daya tinggi (*power efficient*).

Dalam tugas akhir ini, penulis akan meneliti metode enkripsi yang paling memenuhi kriteria tersebut. Sedangkan, hasil output yang didapatkan dari sistem enkripsi dan dekripsi dalam IR-UWB WBAN yang memenuhi, yakni diukur dari kinerja *Bit Error Rate* (BER) enkripsi dan dekripsi, daya yang dihasilkan lalu dibandingkan dengan sistem tanpa enkripsi.

1.2 Tujuan dan Manfaat

1.2.1 Tujuan

Permasalahan pada sistem WBAN dengan metode IR-UWB itu sendiri adalah kurangnya perlindungan sistem saat mengirimkan ataupun menerima data yang bersifat rahasia untuk pihak tertentu agar data atau informasi tidak jatuh ke pihak lain. Oleh sebab itu tujuan dari penelitin tugas akhir ini adalah sebagai berikut :

1. Pembuatan sistem perlindungan dengan keamanan data enkripsi yang sederhana, dan efisiensi daya tinggi (*power efficient*).
2. Menganalisis enkripsi dan dekripsi yang digunakan serta sinyal yang digunakan dengan outputnya.
3. Evaluasi kinerja enkripsi dengan metode simulasi pada sistem yang digunakan dan analisis data dari hasil simulasi yang didapatkan.

1.2.2 Manfaat

Dalam penelitian ini sinyal WBAN yang dikirimkan memiliki data yang penting yaitu mengenai data kesehatan. Data yang telah didapatkan dari hasil analisis akan dikirimkan untuk dapat diproses. Oleh karena itu, dengan metode IR-UWB pada data yang dikirimkan dalam proses pengiriman dan penerimaan dapat terjaga kerahasiaannya menggunakan link enkripsi sehingga informasi atau data yang didapat tidak jatuh ke pihak lain yang tidak diinginkan. Serta mencegah hacking atau peretasan data yang dapat mengganggu pengiriman data tersebut.

1.3 Rumusan Masalah

Permasalahan yang dijadikan pada pengembangan dan penelitian dalam tugas akhir ini adalah sebagai berikut:

1. Bagaimana membuat sistem enkripsi yang sederhana, dan power efisien pada perlindungan sistem WBAN dengan metode IR-UWB dalam pengiriman dan penerimaan data atau informasi?
2. Bagaimana analisis sistem enkripsi kriptografi pada IR-UWB WBAN?
3. Bagaimana evaluasi kinerja dari enkripsi untuk perlindungan sistem WBAN dengan metode IR-UWB dalam mengirimkan data?

1.4 Batasan Masalah

Agar tugas akhir ini menjadi lebih terarah maka diperlukan beberapa batasan masalah sebagai berikut :

1. Sistem enkripsi untuk meningkatkan keamanan data informasi untuk sistem IR-UWB WBAN.
2. Menggunakan frekuensi dari 3,1 GHz sampai dengan 10,6 GHz sesuai standar IEEE 802.15.6.
3. Metode enkripsi dan dekripsi dengan AES, DES.
4. Simulasi sistem menggunakan software matlab.
5. Hasil simulasi yang diperoleh dari parameter yang ditentukan dan output berupa BER, dan efisiensi konsumsi daya.

1.5 Metode Penelitian

a. Studi Literatur

Kegiatan pembelajaran dapat melalui sumber pustaka, baik berupa buku, artikel maupun jurnal ilmiah. Akan tetapi, dosen pembimbing juga sangat membantu dalam penelitian tersebut.

b. Pemodelan Sistem

Berdasarkan parameter – parameter dan studi literatur yang telah didapat, sistem dapat dimodelkan dengan enkripsi dan dekripsi yang simple, kuat atau tahan terhadap gangguan (powerfull), dan efisiensi daya rendah (power efficient). Metode enkripsi dan dekripsi yang digunakan berupa kriptografi symmetric dengan AES 256 dan DES.

c. Simulasi Sistem

Simulasi sistem menggunakan software dengan metode Monte Carlo. Simulasi sistem juga menggunakan link enkripsi dengan enkripsi dan dekripsi sebagai metodenya. Metode enkripsi dan dekripsi yang digunakan adalah kriptografi Symmteric.

d. Analisis hasil simulasi

Pada simulasi dilakukan perubahan parameter yang telah ditentukan untuk mendapatkan berbagai macam kondisi untuk dianalisis pengaruhnya terhadap keamanan pengiriman dan penerimaan data dengan link enkripsi pada metode IR-UWB.

e. Kesimpulan

Untuk mendapatkan gagasan dari hasil analisis kinerja yang didapatkan dan menjelaskan dengan singkat secara keseluruhan mengenai permasalahan yang ada beserta jawabannya berdasarkan hasil data dari penelitian.

1.6 Sistematika Penelitian

Untuk pembahasan yang lebih detail, laporan tugas akhir ini disusun dengan sistematika sebagai berikut :

BAB I Pendahuluan

Bab ini membahas tentang latar belakang dari pembuatan tugas akhir ini, penelitian terkait, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penelitian.

BAB II Tinjauan Pustaka

Bab ini membahas tentang konsep, teori dan cara kerja Enkripsi Link Transmisi Untuk Meningkatkan Keamanan Data Pada Sistem IR-UWB WBAN dan komponen-komponen apa saja yang dibutuhkan untuk merancanginya.

BAB III Perancangan Sistem

Bab ini membahas tentang perancangan dan desain Enkripsi Link Transmisi pada Sistem IR-UWB WBAN, selain itu bab ini juga membahas skema dan hasil dari desain Enkripsi Link Transmisi pada Sistem IR-UWB WBAN.

BAB IV Analisis Simulasi Sistem

Bab ini membahas tentang skema pengujian dan sistem yang telah dibuat, setelah itu data-data pengujian yang telah terkumpul akan diolah dan dianalisis agar mendapatkan hasil yang sesuai dengan tujuan penelitian tugas akhir ini.

BAB V Kesimpulan dan Saran

Bab ini membahas kesimpulan tentang data-data hasil simulasi dan analisis, lalu menghasilkan saran untuk penelitian selanjutnya.