ENKRIPSI LINK TRANSMISI UNTUK MENINGKATKAN KEAMANAN DATA PADA SISTEM IR-UWB WBAN

(THE TRANSMISSION LINK ENCRYPTION TO IMPROVE DATA SECURITY IN A IR-UWB WBAN SYSTEM)

Wulan Suryandari[1], Ir, Miftadi Sudjai MSc,Ph.D [2], Danu Dwi Sanjoyo S.T., M.T [3]
[1,2,3] Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**wulansuryandari@telkomuniversity.ac.id**, [2]**mitadisudjai@telkomuniversity.co.id**,
[3]**danudwisanjoyo@telkomuniversity.ac.id**

Abstrak

Wireless Body Area Network (WBAN) adalah sensor yang berada pada tubuh manusia yang bisa langsung berkomunikasi kepada perangkat penerima secara nirkabel. Penggunaan sistem WBAN ini terutama untuk aplikasi di bidang monitoring kesehatan secara nirkabel. Oleh karena itu, diharapkan dapat mempermudah proses memonitoring kondisi pasien, dan dapat menganalisis data dalam jumlah tertentu, dalam periode waktu pengamatan yang lama, sehingga lebih efisien dalam mendapatkan data medis, serta lebih akurat.

Penelitian ini mengunakan metode IR-UWB WBAN dengan modulasi Binary Phase Shift Keying (BPSK), Pulse Posotion Modulation (PPM), serta Gaussian *monocycle* dengan kanal sesuai dengan IEEE 802.15.6. Metode enkripi memiliki beberapa parameter tertentu, yaitu metode enkripsi kriptografi symmetric AES 256 dan DES. Dengan menggunakan metode kriptografi dalam 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), tingkat konsumsi daya yaitu SNR dibandingkan dengan sistem tanpa enkripsi.

Kata kunci : WBAN, IR-UWB, Enkripsi, BER, SNR

Abstract

Wireless Body Area Network (WBAN) is a sensor located in the human body that can communicate directly to the receiving device wirelessly. The use of the WBAN system is mainly for applications in the field of wireless health monitoring. Therefore, it is expected to facilitate the process of monitoring the patient's condition, and can analyze medical record data in a certain amount, in a long period of observation, making it more efficient in obtaining medical data, and more accurate. This research uses IR-UWB WBAN method with Binary Phase Shift Keying (BPSK) modulation, Pulse Posotion Modulation (PPM), and Gaussian monocycle with IEEE 802.15.6 channel. The encryption method has certain parameters, there are symmetric AES 256 and DES and assymmetric Diffie-Hellman encryption methods. By using a cryptography methods in encryption, it is to help simplify system security, and higher energy efficiency. In this final project, will research the encryption method that fulfill these criteria. Meanwhile, the output results obtained from the encryption and decryption system in IR-UWB WBAN fulfilled, which is measured by the performance of the Bit Error Rate (BER), the level of power consumption is Signal Noise Ratio (SNR) compared to the system without encryption.

Keywords: WBAN, IR-UWB, *encryption*, BER, SNR

1. Pendahuluan

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 Posotion Modulation (PPM), serta Gaussian *monocycle* serta kanal CM4 ssssssesuai 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.

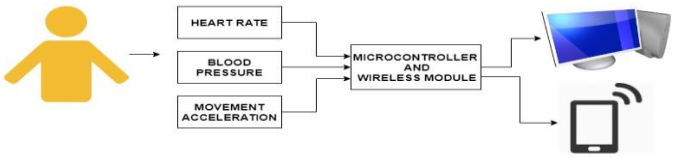
Dalam membuat sistem perlindungan untuk pengiriman sinyal tersebut, penulis merancang sistem enkripsi pada IR-UWB WBAN. Evaluasi sistem kerja tersebut dengan metode link enkripsi dimana melakukan enkripsi dan dekripsi pada data yang akan dikirimkan dan diterima dalam membuat sistem tersebut. Metode enkripi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

2. Dasar Teori

2.1 WBAN

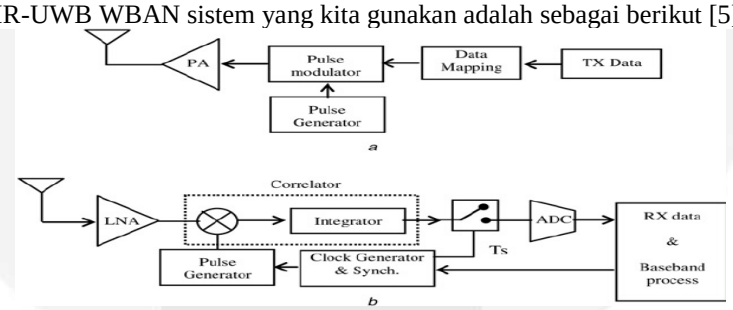
Jaringan area tubuh nirkabel (WBAN) atau disebut juga sebagai jaringan area tubuh (BAN) adalah jaringan nirkabel perangkat komputasi yang dapat dikenakan. Sensor yang ditempatkan di dalam dan di sekitar atau di luar tubuh manusia membentuk jaringan untuk pemantauan sinyal fisiologis kebanyakan WBAN dibangun di sekitar standar IEEE 802.15.6 pada Wireless Body Area Network, yang juga mencakup model saluran berdasarkan pengukuran. Pertukaran informasi yang efisien menjadi komunikasi yang dapat diandalkan, aman, cepat, toleransi kesalahan, dan tahan terhadap gangguan dengan konsumsi daya yang rendah. Tujuan dari WBAN itu sendiri adalah untuk mempermudah proses memonitoring kondisi pasien sehingga dapat lebih efisien dalam mendapatkan data rekam medis dan juga dapat mengefisiensi waktu yang diperlukan.



Gambar 2.1 WBAN Sederhana

2.2 IR-UWB

IR-UWB modern berkomunikasi dengan menggunakan singkat pulsa dalam domain waktu dengan energi mereka tersebar luas bandwidth dalam domain frekuensi. IR-UWB bisa dirancang dengan kekuatan yang relatif rendah, kompleksitas dan rendah konsumsi.Pada kali ini, penulis mmenggunakan teknik IR-UWB pada WBAN yang bertujuan untuk merancang sistem perlindungan dengan link enkripsi yang simple, powerful, serta power efisien. Contoh arsitektur IR-UWB WBAN sistem yang kita gunakan adalah sebagai berikut [5].

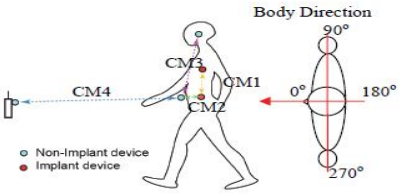


Gambar 2.2 Arsitektur Blok Diagram IR-UWB Sistem [5]

Pada gambar 2.2 Skema modulasi digunakan untuk mengetahui kinerja bentuk pulsa yang dihasilkan di penerima, serta dapat mendukung proses transmisi dengan menilai kinerja bit error rate (BER) yang didapatkan.

2.3 IEEE UWB KANAL

Pemodelan saluran IEEE 802.15.6 mengenai model saluran untuk digunakan dalam tubuh area jaringan. Model saluran bertujuan untuk mengevaluasi kinerja lapisan fisik dari berbagai proposal dan kampanye pengukuran. Kemungkinan hubungan komunikasi antara node dan definisi model saluran, yaitu CM1 - CM4 dapat dilihat pada gambar 2.3.



Gambar 2.3 Pemodelan Kanal IEE WBAN UWB [7]

Setiap kanal memiliki peran tersendiri dengan penjelasan sebagai berikut :

- ✓ Kanal CM1 mendefinisikan sebuah implant-to implant link (S1) yang beroperasi pada frekuensi (402-405 MHz).
- ✓ CM2 menentukan implant-to-body surface (S2) dan hubungan implan-ke-eksternal (S3), beroperasi di frekuensi yang sama dengan CM1.
- ✓ CM3 mendefinisikan body surface-to-body surface untuk LOS (S4) dan NLOS (S5). CM3 diterapkan pada tujuh frekuensi yang berbeda (13.5, 50, 400, 600, 900 MHz 2.4, 3.1-10.6 GHZ).
- ✓ CM4 menentukan body surface-to-eksternal untuk LOS (S6) dan NLOS (S7) diterapkan ke tiga frekuensi yang berbeda (900 MHz 2.4, 3.1-10.6 GHZ). Oleh karena itu, termasuk ke dalam ketentuan frekuensi UWB (3.1 - 10.6 GHz) [7].

2.4 Pulse Code Modulation (PCM)

PCM adalah pengambilan sampel, kuantisasi, dan pengkodean. Operasi kuantisasi dan pengkodean biasanya dilakukan dalam sirkuit yang sama, yang disebut konverter analog-ke-digital. Operasi dasar dalam penerima adalah regnerasi gangguan sinyal, decoding, dan rekonstruksi sampel terkuantisasi [8].

a. *Non Return to Zero* (NRZ)

Sinyal non return to zero adalah format yang paling mudah untuk dihasilkan karena hampir sama dengan bentuk sinyal masukannya. Sinyal NRZ tidak kembali ke level nol sesuai clock. Pengkodean NRZ biasa digunakan untuk komunikasi dengan kecepatan rendah dengan interface transmisi sinkronus dan asinkronus. Penulis menggunakan Unipolar untuk NRZ kali ini karena unipolar merupakan sinyal yang hanya menggunakan satu level tegangan (bisa positif atau negatif), serta tegangan nol untuk logika "0" [8].

2.5 BinaryPhase Shift Keying (BPSK)

Dalam BPSK, pasangan sinyal $S_1(t)$ dan $S_2(t)$ digunakan untuk mewakili symbol biner 1 dan 0. Penggunaan BPSK dengan meggunakan rumus BPSK adalah sebagai berikut:

3. $S_1(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t)$ (2.1)

4. $S_2(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t + \pi)$ (2.2)

Dimana $0 \leq t \leq T_b$ adalah sinyal yang ditransmisikan menjadi sinyal energi per bit. Untuk membawa setiap bit yang ditransmisikan mengandung jumlah siklus gelombang pembawa yang tidak terpisahkan, frekuensi bebas pembawa f_c dipilih sama dengan n_c / T_b [8].

2.6 Gaussian

Gaussian monocycle pada domain waktu v(t) adalah sbb:

$$Y = \int_0^T g(t)X(t)\ dt \quad (2.3)$$

Disini Y sebagai fungsional linier $X_{(t)}$Perbedaan antara fungsi dan fungsional harus diperhatikan dengan cermat. Misalnya, jumlah $Y = \sum_{i=1}^{N} a_i x_i$ di mana a_i adalah konstanta dan X_i, adalah variabel acak, adalah fungsi linier dari X_i, untuk setiap set nilai yang diamati untuk variabel acak X, penulis memiliki nilai yang sesuai untuk variabel acak Y.

$$v(t) = 6A\sqrt{\frac{e\pi}{3}\frac{t}{\tau_p}}e^{-6\pi(t/\tau_p)^2} \quad (2.4)$$

Dimana A adalah amplituda pulsa, τ_p adalah lebar pulsa, dan t adalah waktu [8].

2.7 Signal-to-Noise Ratio (SNR)

Untuk semua jenis transmisi data, signal to noise ratio (SNR) merupakan parameter yang harus diperhatikan. SNR digunakan untuk menunjukkan seberapa banyak noise mengganggu sinyal yang ditransmisikan. Oleh karena itu, SNR membandingkan daya sinyal yang diinginkan terhadap background noise [9].

$$SNR = 10\log\frac{P_{signal}}{P_{noise}} \quad (2.5)$$

2.8 Random Process

Proses acak memiliki dua sifat. Pertama, adalah fungsi waktu. Kedua, acak dalam arti bahwa sebelum melakukan percobaan, tidak mungkin untuk menentukan bentuk gelombang yang akan diamati.

$$X(t,s),\ -T \leq t \leq T \quad (2.6)$$

Di mana 2T adalah total interval pengamatan. Untuk titik sampel tetap s_i, grafik fungsi X (t, s_i) lawan waktu t disebut fungsi realisasi atau sampel dari proses acak.

Untuk menyederhanakan notasi, dapat dinyatakan fungsi sampel ini sebagai berikut [8]

$$x_i(t) = x(t, s_i) \quad (2.7)$$

1. *Mean*, Auto Korelasi, *Kovarians*

Pertimbangan stasioner acak proses X(t) mendefinisikan rata-rata dari proses X(t) sebagai ekspektasi dari variable acak diperoleh dengan mengamati proses untuk beberapa waktu t, seperti yang ditunjukkan oleh

$$\mu x^{(t)} = E[x(t)] = \int_{-\infty}^{\infty} x f x_{(t)}(x) dx \quad (2.8)$$

Dimana $f_{x(t)}(x)$ adalah fungsi probabilitas urutan pertama dari prosess. Dari Persamaan (1.4) menyimpulkan bahwa untuk proses acak stasioner $fx_{(t)}(x)$ tidak tergantung pada waktu t. Akibatnya, rata-rata dari proses stasioner adalah konstan, seperti yang ditunjukkan oleh

$$\mu_x(t) = \mu_x \text{ for all } t \quad (2.9)$$

Mendefinisikan fungsi autokorelasi dari proses X(t) sebagai ekspektasi produk dari dua variabel acak , X (t_1) dan X (t_2), diperoleh dengan mengamati proses X(t) pada waktu t_1 dan t_2, masing-masing. Secara khusus, dapat ditulis sbb :

$$Rx(t_1, t_2) = E[X(t_1)\, X(t_2)]$$

$$= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x_1 x_2 fx(t_1), x(t_2)\,(x_1, x_2) dx_1 dx_2 \quad (2,10)$$

Dimana $fx(t_1)$, $x(t_2)$ (x_1,x_2) adalah orde kedua fungsi kepadatan probabilitas darith.proses e Dari Persamaan (1.5), disimpulkan stasioner sebuah random process, $fx(t_1)$,$x(t_2)$ (x_1, x_2) hanya bergantung pada perbedaan antara pengamatan kali $t_1$dan t_2. Ini, pada gilirannya, menunjukkan bahwa fungsi autokorelasi proses ketat stasioner hanya bergantung pada perbedaan waktu t_2- t_1, seperti yang ditunjukkan oleh

$$Rx(t_1, t_2) = Rx(t_2,- t_1) \quad \text{untuk semua } t_1, \text{ dan } t_2 \quad (2.11)$$

Demikian pula, fungsi auto kovarian dari proses stasioner ketat X(t) ditulis sebagai berikut [8]

$$Cx(t_1, t_2) = E[(X(t_1) - \mu_x)(X(t_2) - \mu_x)]$$

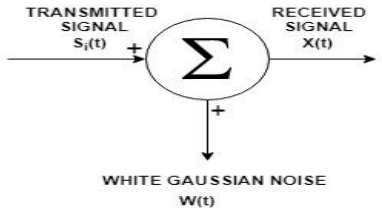
$$= Rx(t_2 - t_1) - \mu^2{}_x \quad (2.11)$$

2.8 *Additive White Gaussian Noise* (AWGN)

Saluran kanal gangguan adalah fungsi sampel dari Gaussian putih rata-rata nol proses. Alasan untuk asumsi ini adalah karena membuat sinyal dapat dihitung secara kuantitatif. Saluran tersebut dapat disebut sebagai saluran *Additive White Gaussian Noise* (AWGN). Dengan cepat, maka dapat menyatakan sinyal yang diterima x (t) sebagai berikut :

$$x(t) = s_i(t) + w(t), \quad \begin{cases} 0 \le t \le T \\ i = 1,2,\ldots,M \end{cases} \quad (2.12)$$

Model dasar ini dapat memberikan desain penerima yang optimal, karena akan menggunakan representasi geometris dari set transmisi yang diketahuisinyal, $\{(S_i),(t)\}$. Metode ini, memberikan banyak wawasan, dengan penyederhanaan detail yang cukup besar [8].



Gambar 2.4 Model saluran *Additive White Gaussian Noise* (AWGN) [8]

2.9 Advanced Encryption Standard (AES)

Sebelum mengaplikasikan metode AES, kita harus menentukan block data (Nb) dan key (Nr). AES mengizinkan block data ukuran : 128 , 168 , 192 , 224 dan 256 bit. Untuk key memiliki varian : 128 , 192 dan 256 bit. Perlu diketahui bahwa standar block data dan key pada metode AES adalah 128 bit.

Berikut adalah algoritma dari AES yang secara umum akan kita gunakan adalah sebagai berikut [11] :

1. SubBytes, sebagai transformasi substitusi.
2. ShiftRows, sebagai transformasi permutasi.
3. MixColumns, sebagai transformasi pengacakan.
4. AddRoundKey, sebagai transformasi penambahan kunci.

2.10 *Data Encryption Standard* (DES)

DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok yang mengenkripsi data 64 bit. Panjang kunci ekternal = 64 bit (sesuai ukuran blok), tetapi hanya 56 bit yang dipakai (8 bit tidak digunakan). Setiap blok (plainteks atau cipherteks) dienkripsi dalam 16 putaran. Setiap putaran menggunakan kunci internal berbeda.

Pengertian dari skema global algoritma DES adalah sebagai berikut :

1. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).

2. Hasil permutasi awal kemudian di-*enciphering*- sebanyak 16 kali (16 putaran). Setiap putaran dapat menggunakan kunci internal yang berbeda.
3. Hasil *enciphering* yang didapatkan lalu dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP^{-1}) menjadi blok cipherteks [12].

Secara matematis, satu putaran DES dinyatakan sebagai berikut :

$$L_i = R_i - 1 \quad (2.2)$$

$$R_i = L_i - 1 \oplus f(R_i - 1, K_i) \quad (2.3)$$

Pada proses *enciphering*, blok plainteks menjadi dua bagian, kiri (L) dan kanan (R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES.

2.11 DIFFIE- HELLMAN

Algoritma pertukaran kunci Diffie-Hellman (protokol Diffie-Hellman) berguna untuk mempertukarkan kunci rahasia untuk komunikasi menggunakan kriptografi simetris. Langkah-langkahnya adalah sebagai berikut,

1. Misalkan Alice dan Bob merupakan pihak-pihak yang berkomunikasi. Alice dan Bob menyepakati 2 buah bilangan yang besar (sebaiknya prima) D dan E, sedemikian sehingga D < E. Nilai D dan E tidak perlu rahasia, bahkan Alice dan Bob dapat membicarakannya melalui saluran yang tidak aman sekalipun.
2. Alice membangkitkan bilangan bulat acak x yang besar dan mengirim hasil perhitungan berikut kepada Bob :
   X = D^y mod E.
3. Bob membangkitkan bilangan bulat acak y yang besar dan mengirim hasil perhitungan berikut kepada Alice:
   Y = D^y mod E.
4. Alice menghitung
   K = Y^x mod E.
5. Bob menghitung
   K' = X^y mod E.

Jika perhitungan dilakukan dengan benar, maka *K= K'.* Baik *K* dan *K*' sama dengan *gxy* mod *n*. Eve yang menyadap pembicaraan antara Alice dan Bob tidak dapat menghitung *K*. Ia hanya memiliki informasi *n*, *g*, *X* dan *Y*, tetapi ia tidak mempunyai informasi nilai *x* dan *y*. Untuk mengetahui *x* atau *y*, perlu melakukan perhitungan logaritma diskrit, yang mana sangat sulit dikerjakan [13].

2.13 BER

Bit Error Rate (BER) adalah cara untuk mengetahui bit yang error dengan menghitung jumlah bit dibagi dengan membagi sejumlah bit yang diterima atau dikirim selama beberapa periode yang ditetapkan. BER 10^{-3}, artinya dalam 1000 bit sinyal yang dikirimkan maka maksimum jumlah bit yang boleh salah adalah 3 bit.

3. Perancangan Sistem

3.1. Desain Sistem

Pada desain sistem kali ini adalah perancangan yang dilakukan dengan menggunakan frekuensi 3,1 GHz - 10,6 GHz sesuai standar IEEE 802.15.6 untuk perlindungan data yang akan dikirimkan dienkripsi dengan kriptografi terhadap sistem IR-UWB WBAN.

Gambar 3.1 Sistem WBAN [4]

Perancangan enkripsi kriptografi terhadap sistem IR-UWB WBAN ini dilakukan dengan menggunakan simulasi software. Dengan metode kriptografi Symmetric yaitu mengggunakan AES 256, DES, dan Assymmetric Diffie Hellman. Enkripsi dilakukan terhadap transmitter dan receiver sistem. Dengan metode ini diharapkan dapat membuat enkripsi yang sederhana, dan power efisien.

3.2. Kanal

Pada sistem IR-UWB WBAN kali ini, penulis menggunakan kanal CM4 yang telah sesuai dengan standar oleh IEEE 802.15.6. CM4 menentukan body surface-to-eksternal diterapkan ke tiga frekuensi yang berbeda (900 MHz 2.4, 3.1-10.6 GHZ). Model CM4 didasarkan pada pengukuran di mana antena TX tetap dekat dengan dinding, sedangkan antena Rx ditempatkan pada tubuh dan bervariasi untuk posisi yang berbeda. Power Delay Profile adalah kekuatan rata-rata dari sinyal sebagai fungsi dari keterlambatan sehubungan dengan jalur kedatangan pertama. Karakteristik respons kanal dari Power Delay Profile (PDP) adalah sebagai berikut [6] :

$$h(t) = \sum_{m=0}^{L-1} a_m \delta(t - \tau_m) \quad (3.1)$$

dimana

$$|a_m|^2 = \Omega_0 e^{\frac{\tau_m}{\mathbb{T}} k[1-\delta(m)]} \beta \quad (3.2)$$

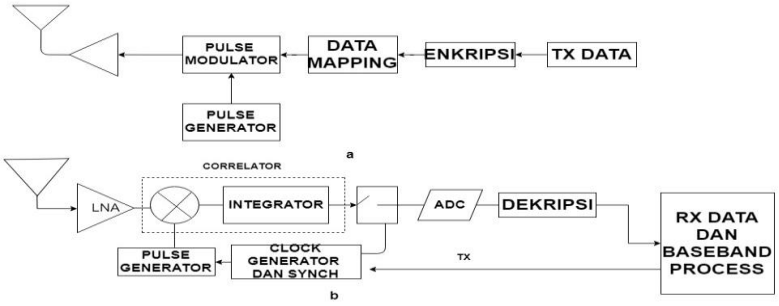
$$k = \Delta k\left(\frac{ln10}{10}\right);\ \tau_0 = {}^{d}/_{c}\ ; and\ \beta \sim \log norma\ (0, \sigma) \qquad (3.3)$$

Tabel 3.1 Tabel Parameter CM4 [6]

Direction of Body	Γ[ns]	k (Δk[dB])	σ[dB]
0	44.6346	5.111 (22.2)	7.30
90	54.2868	4.348 (18.8)	7.08
180	53.4186	3.638 (15.8)	7.03
270	83.9635	3.983 (17.3)	7.19

Pada tabel 3.1 mengenai parameter CM4 telah didapatkan data mengenai parameter CM4 juga bergantung pada arah tubuh ke arah antena TX.

3.3 Blok Diagram Sistem IR-UWB WBAN dengan Enkripsi dan Dekripsi



Gambar 3.2 Struktur Transmitter dan Reveiver IR-UWB WBAN [5]

3.3.1 Transmitter dan Receiver Sistematis

Pada transceiver penulis menggunakan NRZ pada data dikarenakan tidak terlalu kompleks dan dapat menghemat energi. Dengan permisalan jika ada tegangan, maka dinyatakan dengan logika "1" dan jika tidak ada tegangan, maka dinyatakan dengan logika "0".

A. Sistematis Keseluruhan

Data dari transmitter yang diperoleh adalah sebagai berikut :

$$g(t) = d(t)\ x\ enkripsi \qquad (3.5)$$

Dimana

$$x(t) = g(t)\ x\ s(t)\ x\ h(t)$$
$$x(t) = g(t)\ x\ \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t)\ x\ 6A\sqrt{\frac{e\pi}{3}\frac{t}{\tau_p}}e^{-6\pi({}^{t}/_{\tau_p})^2} \qquad (3.6)$$

Data pada receiver adalah sebagai berikut :

$$y(t) = x(t) * h(t)\ + w(t)$$
$$y(t) = x(t) * \sum_{m=0}^{L-1} a_m \delta\ (t - \tau_m)\ + w(t) \qquad (3.7)$$

dimana

$$y(t)\ x\ 6A\sqrt{\frac{e\pi}{3}\frac{t}{\tau_p}}e^{-6\pi({}^{t}/_{\tau_p})^2}\ x\ 6A\sqrt{\frac{e\pi}{3}\frac{t}{\tau_p}}e^{-6\pi({}^{t}/_{\tau_p})^2} \rightarrow g'(t) \qquad (3.8)$$

maka

$$g'(t) x\ dekripsi\ \rightarrow \hat{d}(t) \qquad (3.9)$$

Keterangan :

$d(t) =$ Data
$g(t) =$ Data + Enkripsi
$s(t) =$ *Binary Phase Shift Keying* (BPSK)
$w(t) =$ *Additive White Gaussian Noise* (AWGN)
$y(t) =$ Receiver
$g'(t) =$ Hasil dari Trasnmitter x gaussian x BPSK
$\hat{d}(t) =$ Hasil keseluruhan setelah proses dekripsi/data awal.

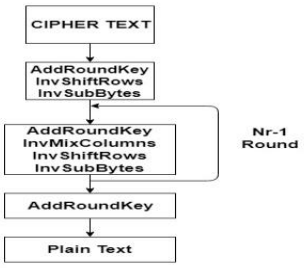
1. Advanced Encryption Standard (AES)

Setelah itu, ada proses enkripsi yang akan dilakukan. Pertama adalah metode AES 256 bit, pada proses enkripsi awalnya teks asli dibentuk sebagai sebuah state. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut AddRoundKey). Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde. Proses AES yang dilakukan adalah sebagai berikut :

a. AddRoundKey: melakukan XOR antara state awal (plainteks) dengan cipher key. Tahap ini disebut juga initial round.
b. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a) SubBytes: Substitusi byte dengan menggunakan table substitusi (S-box).
   b) ShiftRows: Pergeseran baris-baris array state secara wrapping.
   c) MixColumns: Mengacak data di masing-masing kolom array state.
   d) AddRoundKey: Melakukan XOR antara state sekarang dengan round key.

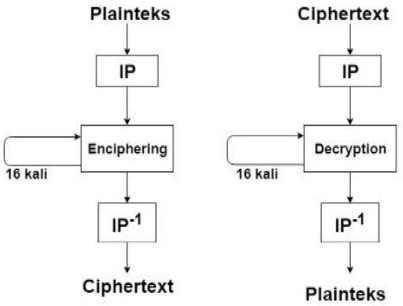
c. Final round: proses untuk putaran terakhir:
   a) SubBytes
   b) ShiftRows
   c) AddRoundKey

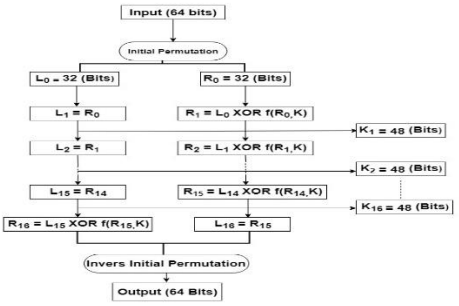
Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns. Berikut adalah gambar proses dari dekripsi AES.



Gambar 3.2 Proses Dekripsi AES

2. Data Encryption Standard (DES)





Gambar 3.3 Skema Global DES Gambar 3.4 DES

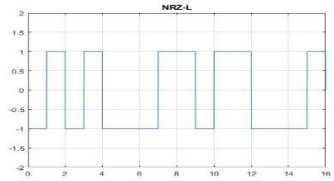
Secara matematis, satu putaran DES dinyatakan sebagai berikut :

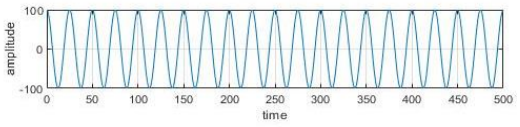
$$L_i = R_i - 1 \quad (2.2)$$

$$R_i = L_i - 1 \oplus f(R_i - 1, K_i) \quad (2.3)$$

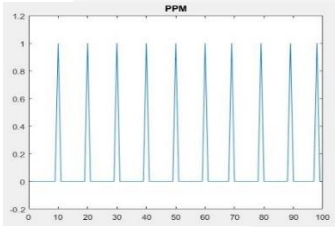
Pada proses *enciphering*, blok plainteks menjadi dua bagian, kiri (L) dan kanan (R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES.

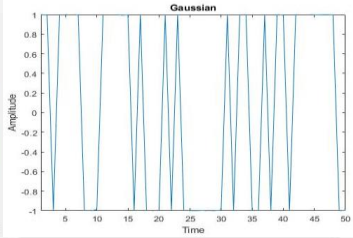
4. Hasil dan Analisis





Gambar 4.1 Analisis NRZ Gambar 4.2 Analisis BPSK



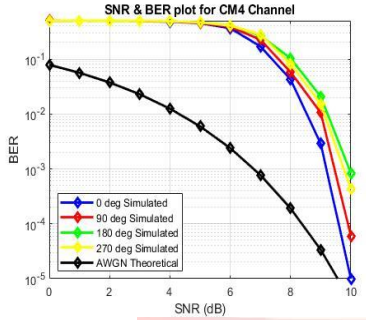


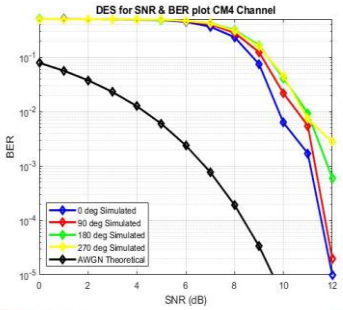
Gambar 4.3 PPM Gambar 4.4 Gaussian

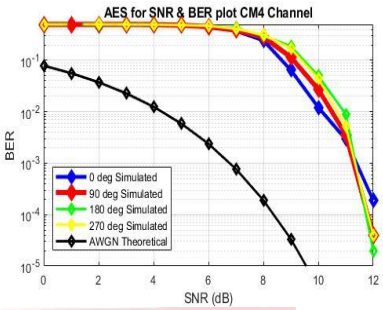
a. Analisis Hasil IR-UWB Pengukuran BER

Pengukuran ini dilakukan untsk mengetahui hasil BER yang dihasilkan sebelum dilakukan proses enkripsi untuk mendapatkan perbandingan data yang telah dihasilkan pada gambar 4.5.

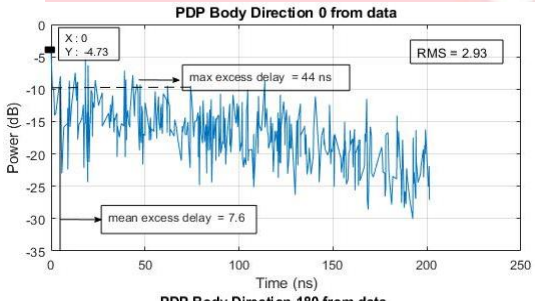
Dengan menggunakan kanal CM4 untuk *Wireless Body Area Network* (WBAN) penulis mengambil data dari sudut yang berbeda yaitu pada 0^o, 90^o, 180^o, dan 270^o. Penulis menggunakan teknik pengulangan yang dilakukan untuk mendapatkan hasil minimum dari BER agar sesuai dengan yang diharapkan.

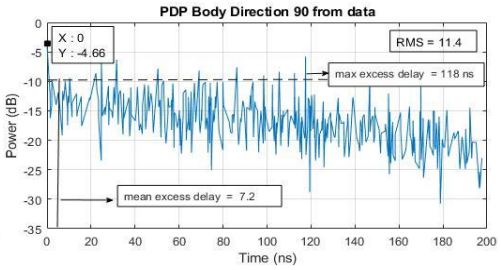


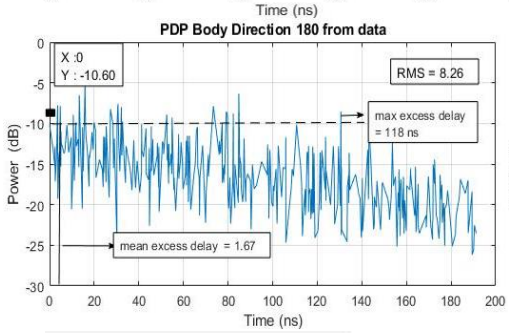


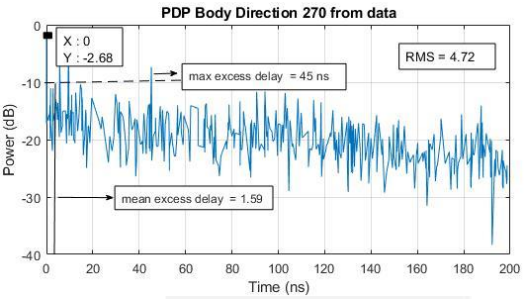


Gambar 4.4 Simulasi IR-UWB BER Gambar 4.5 Hasil simulasi BER dengan metode AES
Gambar 4.6 Hasil simulasi BER dan SNR pada DES









Gambar 4.7 PDP Body Direction 0-270 deg

Metode	SNR	BER
Non Enkripsi	9.91 dB	10^{-5}
AES	12dB	10^{-4}
DES	12dB	10^{-5}

1. Non Enkripsi

   Max Excess Delay Total = $51.5 + 59 + 74.8 + 98 = 283\ ns$

   Mean Excess Delay Total = $71.8 + 74 + 70.80 + 87.9 = 304.5\ ns$

   RMS = $70.8 + 72.16 + 69.2 + 86.5 = 298.66\ ns$

2. AES

   Max Excess Delay Total = $53 + 88 + 104 + 131 = 376\ \mu s$

   Mean Excess Delay Total = $83.9 + 83.5 + 85.8 + 78 = 331.2\ ns$

   RMS = $82.26 + 81.8 + 84.41 + 76.2 = 324.67\ ns$

3. DES

   Max Excess Delay Total = $44 + 118 + 118 + 45 = 325\ ns$

   Mean Excess Delay Total = $76 + 72 + 81.6 + 89.7 = 319.3\ ns$

   RMS = $75.2 + 71.27 + 79.9 + 88.3 = 314.67\ ns$

Berikut adalah hasil perbandingan dari Non Enkripsi, AES dan DES dari data yang diperoleh bahwa AES dan DES membutuhkan waktu delay dan daya yang lebih besar daripada Non Enkripsi.