BAB II

2.1 KAJIAN PUSTAKA

Penelitian yang dilakukan oleh Yuli Apriyanti pada tahun 2016 yang berjudul "*Sniffing* sinyal GSM dengan RTL-SDR, GNU Radio, dan wireshark" meneliti tentang percobaan *sniffing* sinyal GSM untuk menentukan lokasi pengguna GSM. Dengan menggunakan teknik *scanning* sinyal terlebih dahulu menggunakan Gqrx untuk melihat *range* frekuensi disekitar penelitian. Dilanjutkan dengan mendecoder sinyal menggunakan GNU Radio dan diteruskan *wireshark* sebagai *analisator* dari sinyal GSM maka menghasilkan *local area identify, cell identify* yang digunakan sebagai penentuan lokasi *user* GSM. Hasil dari penelitian ini lokasi *use*r GSM dibandingkan dengan teknologi GPS lokasinya tidak jauh berbeda. Pada metode penelitian ini tidak mengukur akurasi lokasi *user* sehingga lokasi *user* kurang tepat dan hanya diketahui titik lokasi *user*.[1] Penilitian milik Yuli Apriyanti tidak menjelaskan jarak antara BTS ke MS hanya mengetahui lokasi BTS, sedangkan penelitian milik saya menjelaskan tentang jarak antara BTS ke MS dan penentuan lokasi *user* GSM.

Penelitian yang dilakukan oleh Briyan Rizky Rivaldy pada tahun 2017 yang berjudul " Impelementasi Gr-GSM untuk *decoding* GSM terenskripsi" meneliti tentang *decoding* komunikasi GSM terenskripsi. Dengan menggunakan teknik menangkap sinyal BTS menggunakan RTL-SDR dan aplikasi Gr-GSM untuk proses *decoding* data yang ditangkap dari pancaran frekuensi BTS (*Base Transciver Station*) maka menghasilkan informasi berupa GSM *Frame Number*, IMSI (*International Mobile Subscriber Identifity*), TMSI (*Temporary IMSI*), algoritma yang digunakan pada operator, dan data komunikasi pada keamanan GSM. Metode penelitian ini hanya mendecoding frekuensi yang digunakan, tidak menentukan lokasi *user*. Pada penelitian ini memfokuskan pada keamanan jaringan data operator yang bertujuan untuk meningkatkan keamanan jaringan pada operator yang dipakai.[2] Penelitian milik Briyan Rizky Rivaldy hanya membahas cara *sniffing* sinyal GSM menggunakan RTL-

SDR, sedangkan penelitian milik saya menjelaskan tentang pencarian lokasi user GSM.

Penelitian yang dilakukan oleh Muhammad Hamzah Asy'ari pada tahun 2019 yang berjudul *" Sniffing* sinyal GSM menggunakan RTL-SDR untuk menentukan kordinat pengguna GSM" meneliti tentang percobaan *Sniffing* sinyal GSM untuk mengetahui lokasi pengguna GSM. Penelitian ini menghasilkan beberapa parameter yang digunakan untuk menentukan lokasi pengguna GSM menggunakan RTL-SDR. Pada penelitian ini hanya menggunakan satu area saja yang digunakan sehingga data yang didapat sangatlah kurang dan letak keakurasiannya tidak ditampilkan dibandingkan teknologi lainnya. Pada penelitian ini juga hanya membahas satu pengguna yang dapat di*sniffing* pergerakannya sehingga perlu banyaknya percobaan untuk memastikan keakurasiannya dengan teknologi lainnya.[3] pada penelitian, milik Muhammad Hamzah hanya menggunakan satu area saja, sedangkan penelitian ini menggunakan 30 lokasi yang berbeda, tetapi masuk dalam 3 cakupan BTS.

Penelitan yang dilakukan oleh Fahrudin Mukti Wibowo pada tahun 2018 yang berjudul "Penerapan kalman *filter* pada metode trilaterasi untuk peningkatan akurasi estimasi perhitungan jarak di dalam ruang" meneliti tentang menghitung tingkat akurasi menggunakan metode trilaterasi yang dilakukan di dalam ruangan. Media yang digunakan dalam penelitian ini adalah frekuensi wifi yang diterima oleh handphone. Dalam penelitian ini juga menjelaskan perhitungan jarak wifi ke *handphone* menggunakan metode BLE (*Bluetooth Low Energy*) dan metode trilaterasi. Perbedaan dengan penelitian saya adalah penelitian saya hanya menggunakan metode trilaterasi dan penelitian saya dilakukan di luar ruangan dan di dalam ruangan menggunakan media frekuensi yang dipancarkan oleh BTS[4].

2.2 DASAR TEORI

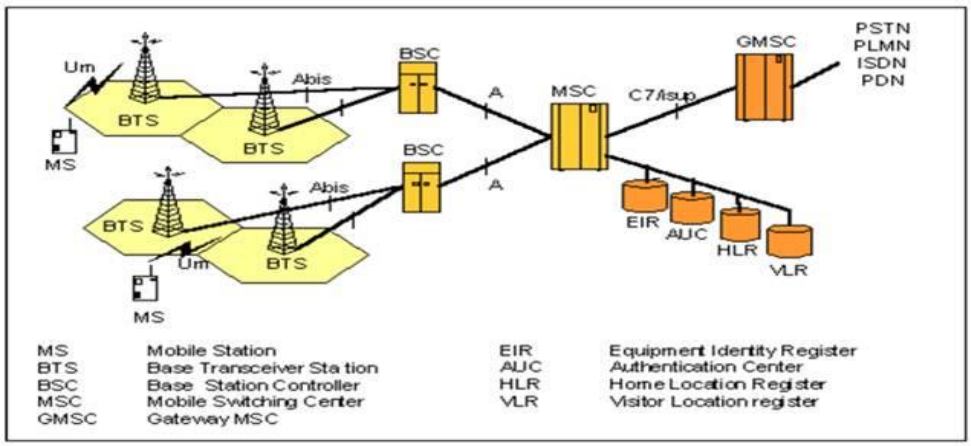
2.2.1 *Global System Mobile* (GSM)

GSM (*Global System Mobile*) merupakan standar global untuk *system* seluler.[4] Teknologi GSM menggunakan teknologi TDMA

dengan alokasi kurang lebih sekitar delapan pengguna didalam satu *channel* frekuensi sebesar 200 khz per satuan waktu. Teknologi ini memanfaatkan gelombang mikro dan pengiriman sinyal yang dibagi berdasarkan waktu, sehingga sinyal informasi yang dikirim akan sampai ke tujuan. GSM kemudian dijadikan sistem standar yang digunakan oleh sebagian besar jaringan telepon di seluruh dunia. Sistem yang menggunakan jaringan seluler berbasis di sekitar stasiun siaran atau teknologi satelit yang terhubung ke sinyal dari orbit bisa menjadi bagian dari jaringan sistem. Telepon yang menggunakan jaringan jenis ini akan disertai dengan *Subscriber Identity Module* (SIM) *card,* sedangkan pada CDMA (*Code Division Multiple Access*).[2]

GSM merupakan teknologi yang diciptakan untuk kepentingan jaringan nirkabel menggunakan mobile. GSM sendiri pada awalnya hanya bekerja difrekuensi 900 Mhz yang kemudiaan menjadi sistem komunikasi generasi kedua atau biasa disebut 2G. GSM dijadikan standar global untuk komunikasi selular sekaligus sebagai teknologi seluler yang paling banyak digunakan orang diseluruh dunia. Teknologi jaringan GSM perlahan terus melakukan perkembangan yang segnifikan, bahkan pada saat itu operator GSM telah memasuki masa jaringan 3G.

Jaringan 3G ini memungkinkan pengguna untuk berkomunikasi yang lebih baik lagi, bahkan secara *realtime.* Namun sampai sekarang GSM semakin berkembang meninggalkan generasi ke 3G dan memasuki generasi 4G, dimana jarin gan tersebut membuat komunikasi semakin baik dari generasi sebelumnya. Bahkan sampai saat ini jaringan GSM semakin berkembang dan mengembangkan generasi yang terbaru yakni generasi 5g.[3]

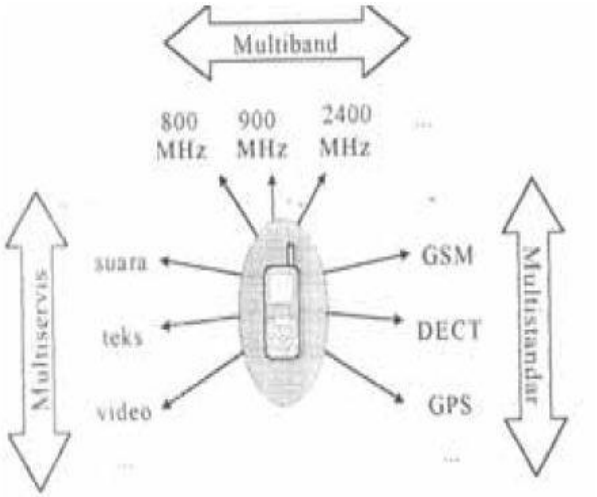


Gambar 2 8 Arsitektur GSM[5]

2.2.2. SDR (*Software Defined Radio*)

Software Defined Radio (SDR) ada yang menyebutnya *Software Radio* diperkenalkan pertama kali pada tahun 1991 oleh joseph miltola. *Software-defined radio* (SDR) adalah sistem komunikasi radio dimana komponen yang telah biasanya diimplementasikan dalam perangkat keras (misalnya *mixer, filter, amplifier,* modulator / demodulator, detektor, dll)[6]. Diimplementasikan dengan menggunakan perangkat lunak pada komputer pribadi atau sistem tertanam.[7]

Teknologi SDR yang muncul untuk membangun sistem radio yang sangat *fleksibelity*, multiservice, multiband, *reconfigurable* dan *reprogamabbel* dengan menggunakan *software*[8]



Gambar 2 *9 Software radio*[8]

Fleksibility : Merupakan perangkat radio yang dapat diubah atau dimodifikasi karakteristiknya sesuai dengan sistem radio yang dikehendakinya.

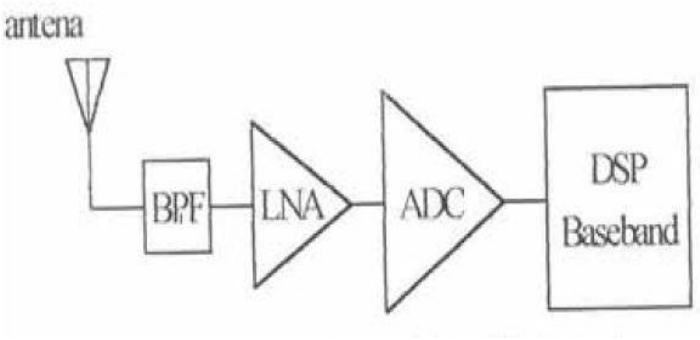
Multiservice : Merupakan suatu radio yang dapat mengaplikasikan berbagai pelayanan atau *service* berupa suara, data, dan teks[8]

Multistandart : Merupakan suatu perangkat radio yang dapat dioprasikan atau diaktifkan dalam standar radio yang berbeda-beda seperti GSM, AMPS, DECT dan lain sebagainya.[8]

Multiband : merupakan suatu sinyal radio yang dapat digunakan pada frekuensi yang berlainan seperti 800 MHz, 900 MHz, 2400 VHF dan lain sebagainya.[8]

Reconfigurable : Perangkat radio bisa diubah-ubah konfigurasinya sesuai dengan standar yang sudah ada.[8]

Reprogrammable : Perangkat radio dapat diprogram ulang sehingga memungkinkan untuk *mendownload software* yang baru, seperti untuk penambahan *servis*, daerah frekuensi, pengkodean dan lain sebagainya.[8]



Gambar 2 10. simulasi penerima SDR Ideal[8]

BPF : *Bandpass Filter*

DSP : *Digital Signal Processor*

LNA : *Low Noise Amplifier*

ADC : *Analog To Digital Converter*

Gambar diatas merupakan simulasi dari penerima *Software Defiend Radio* yang Ideal. Pada ilustrasi diatas tingkat sinyal analog telah dikurangi. Komponen data yang analog berada diantena, *bandpass filter*, dan *Low Noise Amplifier*. Konversi analog ke digital dilakukan oleh ADC. Pengolahan sinyal digital dilakukan dari hasil *output* konverter A/D. Pengolahan tersebut dilakukan oleh *software* yang diprogram dalam DSP yang mere*progamable*.[8]

Software Defined Radio memiliki beberapa keunggulan diantaranya adalah sebagai berikut :

1. Mampu beradaptasi : SDR mampu beradaptasi ke setiap jenis sistem radio yang ada dengan pemakaian multiband dan multistandart.
2. Tidak memerlukan penambahan *hardware* : untuk pembuatan sistem radio yang baru tidak diperkukannya menambah atau mengganti *hardware*, cukup dengan penambahan *software* yang diprogram dalam DSP.
3. Mudah dan Sederhana : pemilihan sistem radio yang dikehendaki dapat dilakukan dengan perubahan yang mudah dan sederhana yaitu cukup dengan mengaktifkan sistem radio yang dikehendaki.
4. Mendukung pengembangan : Sistem SDR mampu mengembangkan sistem komunikasi radio yang lebih maju.

2.2.3 RTL-SDR

RTL-SDR merupakan *software defined radio* yang murah serta menggunakan DVD-TV Tuner Dongle berbasis chipse*t* RTL2832U yang menghasilkan sinyal data I/Q dapat diakses secara langsung. RTL kepanjangan dari Register Transfer Level dalam rancangan hardware rangkaian digital adalah suatu rancangan abstrak model synchronous digital circuit yang mengalirkan sinyal data digital antara hardware register dan operasi logika yang di tampilkan dalam bentuk sinyal[9].

RTL-SDR bisa digunakan untuk scanner radio pita lebar, mendengar percakapan yang tidak tereskripsi yaitu ambulance/ pemadam kebakaran, scanner radio pita lebar, dan menerima citra satelit cuaca NOAA dan lain sabagainya[5]

Gambar 2 11 RTL-SDR Dongle[1]

2.2.4 GNU Radio

GNU Radio merupakan sebuah perangkat lunak yang menyediakan teknik pemrosesan sinyal untuk mengimplentasikan software radio[10]. Aplikasi GNU Radio sebagian besar ditulis menggunakan bahasa pemrograman *Python*, sedangkan bagian pemrosesan sinyal diimplementasikan menggunakan bahasa C++ menggunakan prosesor ekstensi *floatig-point.* GNU Radio mendukung pengembangan algoritma pemprosesan sinyal menggunakan pra-pemrosesan atau pasca pemrosesan utnuk menghindari kebutuhan memiliki perangkat keras radio frekuensi yang sebenarnya.[5]

Gambar 2 12 GNU Radio[5]

2.2.5 Wireshark

Wireshark merupakan penganalisa jaringan yang popular saat ini, program ini bukan dikenal sesuai dengan fungsi utamanya melainkan dikenal karena digunakan untuk keperluan hacking untuk para pemula[11]. Kinerja dari wireshark dapat melingkupi proses penangkapan paket-paket data atau informasi yang berlalu-lalang dalam sebuah jaringan, sampai digunakan untuk *sniffing* atau memperoleh informasi penting seperti email, dan lain sebagainya. Wireshark juga digunakan untuk membaca data secara langsung dari ethernet, token ring, FDDI, serial (PPP dan SLIP), 802.11 wireless LAN dan koneksi ATM, dan mengetahui IP seseorang melalui *Typingan room*. *Software* wireshark juga digunakan untuk menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi antar *computer*.[12]

Gambar 2 13 Simbol Wireshark

2.2.6 Decoding

Decoding adalah proses konversi data yang telah dikirimkan oleh sumber pesan menjadi informasi yang dimengerti oleh penerima[13].

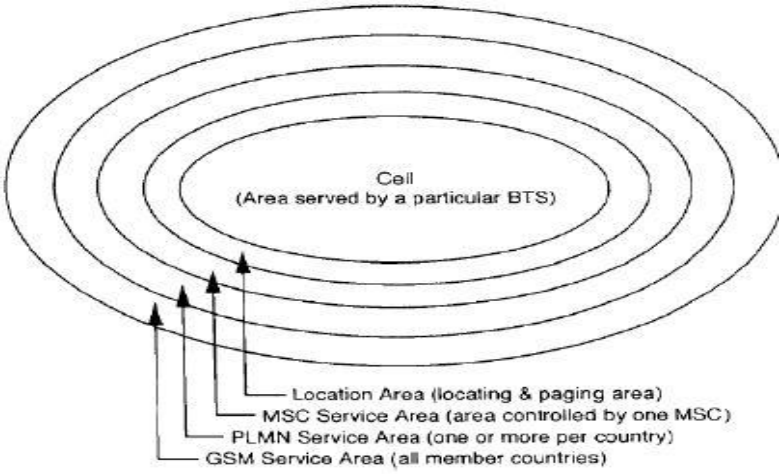
Dalam proses ini sinyal dikonversikan terlebih dahulu sehingga penerima dapat membaca informasi yang dikirimkan dari transmiter[14]

2.2.7 LAI (*Local Area Identifity*)

LAI atau *Local Area Identify* merupakan sebuah data yang didapatkan dari hasil *sniffing* sinyal menggunakan GNU radio dan wireshark. Data-data ini berupa MCC,MNC, LAC, dan *cell identify*. Data ini yang akan digunakan untuk melakukan sebuah pelacakan pada sebuah jaringan GSM. Pada sebuah LAI ini merupakan sebuah data penting dalam bidang telekomunikasi khususnya pada jaringan GSM.

2.2.8 Cell ID

Cell ID adalah cakupan area terkecil dari sebuah jaringan seluler. Dimulai dari GSM dengan cakupan wilayah seluruh dunia diwakili dengan code MCC, *Public Land Mobile Network* (PLMN) yang merupakan operator seluler hingga *Local area* dan *Cell* yang diwakili dengan *Cell ID*. Setiap Cell ID memiliki data spasifik *Cell*. Jangkauan *Cell ID* di perkotaan dan di pedesaan berbeda, hal ini dikarenakan di daerah perkotaan cakupan wilayahnya lebih sempit dibandingkan dengan dipedesaan. Berikut ini adalah gambar dari letak Cell ID[15]



Gambar 2 14 letak Cell ID[15]

2.2.9 MCC (*Mobile Country Code*)

MCC atau *Mobile county code* merupakan sebuah kode area dalam bidang telekomunikasi. Setiap negara mempunyai MCC yang berbeda-beda, hal ini dikarenakan untuk menunjukan letak operator telekomunikasi berada disuatu negara.

TABEL 2 3 Kode MCC di Indonesia[3]

No	Nama Operator	MCC
1	Telkomsel	510
2	XL axiata	510
3	Indosat Ooredoo	510
4	3 Tri Indonesia	510
5	Smartfren	510
6	Bolt Super 4G	510

2.2.10 MNC (*Mobile network code)*

MNC atau *Mobile network code* merupakan sebuah kode operator telekomunikasi. Kode-kode MNC ini berbeda-beda dikarenakan untuk menunjukan operator-operator telekomunikasi. Kode ini bisa digunakan untuk menentukan sebuah kordinat user yang dipakainya melalui berbagai proses tertentu.

TABEL 2 4 Kode MNC[3]

No	Nama Operator	MNC
1	Telkomsel	10
2	XL axiata	11
3	Indosat Ooredoo	01

4	3 Tri Indonesia	89
5	Smartfren	09
6	Bolt Super 4G	88

2.2.11 Pybombs

Pyboms (*Python Build Oberlay Managed Bundle System)* adalah sebuah sistem managemen baru digunakan untuk instalasi GNU Radio agar berjalan dengan baik. Pada dasarnya GNU Radio berada di dalam bahasa pemrograman *Python* dan C++. Fungsi di buatnya Pybombs adalah menggabungkan beberapa aplikasi yang di gunakan untuk menyelesaikan suatu proyek dengan menggunakan bahasa pemrograman *Pyhton*. Maka dari itu pybombs menjadi dasar yang harus ada sebelum aplikasi GNU Radio yang dimana aplikasi tersebut terdiri dari beberapa aplikasi pengolah sinyal Radio.[5]

2.2.12 Paket *Sniffing*

Paket *sniffing* adalah teknik pemantauan setiap paket yang melintasi jaringan. Paket sniffing merupakan bagian dari paket lunak atau perangkat keras yang memonitoring semua lalu lintas jaringan. Ancaman keamanan yang digunakan oleh penyadap adalah kemampuan mereka untuk menangkap semua lalu lintas data yang keluar masuk, tidak terkecuali username dan password atau bahan sensitif lainnya[12].

Potensi bahayanya dari *packet sniffing* adalah hilangnya prifasi, dan tercurinya informasi penting dan rahasia yang dimiliki oleh seorang user. Agar dapat membaca dan menganalisa setiap aktifitas data yang melintas dalam sebuah jaringan maka diperlukan program-program untuk bisa membelokan paket dari komputer ke attacker.[12]

2.2.13 Metode Trilaterasi

Trilateration atau trilaterasi merupakan metode untuk menentukan posisi objek (*smartphone*) berdasarkan pengukuran jarak secara simultan

dari tiga buah titik *access point* (BTS) yang berada di sekitar lokasi. Metode trilaterasi sama dengan teknik trigonometri dimana suatu objek bergerak dan diamati, koordinat dari sebuah objek tersebut mampu di hitung walaupun objek tersebut bergerak tidak aturan. Dalam metode ini posisi objek dapat diibaratkan koordinat (x,y) dapat terdeteksi dengan cara pengukuran jarak objek dari tiga buah access point (BTS) tersebut. [1]

Pada algoritma trilaterasi ini jika (x,y) belum di ketahui maka formulasi berdasarkan rumus pythagoras adalah sebagai berikut

$$(\boldsymbol{x - x_1})^2 + (\boldsymbol{y - y_1})^2 = \boldsymbol{r_1} \quad (1)$$

$$(\boldsymbol{x - x_2})^2 + (\boldsymbol{y - y_2})^2 = \boldsymbol{r_2} \quad (2)$$

$$(\boldsymbol{x - x_3})^2 + (\boldsymbol{y - y_3})^2 = \boldsymbol{r_3} \quad (3)$$

Dimana dengan $n = \{1,2,3\}$

x = Titik koordinat longtitude user GSM (°)

x_n = Titik koordinat longtitude dari BTS ke-n (°)

y = Titik koordinat latitude user GSM (°)

y_n = Titik koordinat dari Latitude BTS ke-n (°)

r_n = Jarak antara User GSM – BTS ke-n (°)

Formulasi di atas kemudian akan diturunkan menjadi beberapa formulasi untuk mencari titik koordinat yang di cari yakni titik x dan y. Untuk itu formulasi diturunkan sebagai berikut ini:

$$(-\boldsymbol{2x_1 + 2x_2})\boldsymbol{x} + (-\boldsymbol{2y_1 + 2y_2})\boldsymbol{y} = \boldsymbol{r_1}^2 - \boldsymbol{r_2}^2 + \boldsymbol{x_1}^2 + \boldsymbol{x_2}^2 - \boldsymbol{y_1}^2 + \boldsymbol{y_2}^2 \quad (4)$$

$$(-\boldsymbol{2x_2 + 2x_3})\boldsymbol{x} + (-\boldsymbol{2y_2 + 2y_3})\boldsymbol{y} = \boldsymbol{r_2}^2 - \boldsymbol{r_3}^2 + \boldsymbol{x_2}^2 + \boldsymbol{x_3}^2 - \boldsymbol{y_2}^2 + \boldsymbol{y_3}^2 \quad (5)$$

Dari persamaan 4 dan 5 kita dapatkan:

$$A = 2(x_2 - x_1) \quad (6)$$

$$B = 2(y_2 - y_1) \quad (7)$$

$$C = r_1^2 - r_2^2 + x_1^2 + x_2^2 - y_1^2 + y_2^2 \quad (8)$$

$$D = 2(x_3 - x_2) \quad (9)$$

$$E = 2(y_3 - y_2) \quad (10)$$

$$F = r_2{}^2 - r_3{}^2 + x_2{}^2 + x_3{}^2 - y_2{}^2 + y_3{}^2 \quad (11)$$

Sehingga Selanjutnya formulasi tersebut bisa dimasukkan ke dalam *matriks* persamaan linier seperti di bawah ini:

$$\begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{D} & \boldsymbol{E} \end{bmatrix} \begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{bmatrix} = \begin{bmatrix} \boldsymbol{C} \\ \boldsymbol{F} \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{bmatrix} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{D} & \boldsymbol{E} \end{bmatrix}^{-1} \begin{bmatrix} \boldsymbol{C} \\ \boldsymbol{F} \end{bmatrix} \quad (12)$$

2.2.14 GQRX

GQRX adalah sebuah *software open source* SDR yang dibuat untuk mendukung hadware SDR dalam hal ini yakni RTL-SDR GQRX berfungsi untuk men*scaaning* frekuensi dan memastikan apakah ada frekuensi GSM yang dipancarkan dalam area lokasi perangkat RTL-SDR.

2.2 15 PATHLOSS

Dalam dunia telekomunikasi untuk membuat *link budget* dan analisis *menggunakan* pathloss. *Pathloss* merupakan pengurangan kepadatan daya atau atenuasi suatu gelombang elektromagnetik karena memenuhi suatu ruangan[16]. *Pathloss* adalah unsur utama dalam desain *link budget* serta analisis dari suatu *system* telekomunikasi. *Pathloss* juga merupakan komponen utama dalam perencanaan *link* radio, yang termasuk elemen path loss yaitu rugi-rugi atmosfer, *free space loss*, pengendapan, penyerapan uap air, *multipath*, *fading*, serta efek lainnya berdasarkan lingkungan dan frekuensinya[17]. Apabila jalur utama propagansi adalah ruangan bebas maka *free space loss* dapat dihitung menggunakan persamaan Friis, yaitu:

$$\boldsymbol{L} = \frac{\boldsymbol{4\pi d}}{\boldsymbol{\lambda}} \quad (13)$$

$$\boldsymbol{P_{RX}} = \frac{\boldsymbol{P_{TX}}}{\boldsymbol{L}} = \boldsymbol{P_{TX}} \left(\frac{\boldsymbol{\lambda}}{\boldsymbol{4\pi d}}\right)^{\boldsymbol{\gamma}} \quad (14)$$

Dimana

$L =$ Path loss

$P_{TX} =$ Daya yang dipancarkan pancar sinyal frekuensi radio (Tx)

P_{RX} = Daya yang diterima (Rx)

d = Jarak antara perangkat Tx dan Rx

$\lambda = \frac{c}{f}$ = Panjang gelombang

f = frekuensi kerja

γ = *Pathloss exponent*

Faktor yang mempengaruhi pathloss ialah kontur medan, dan lingkungan seperti bangunan, pepohonan, medium propagasi (tingkat kelembaban lingkungan), jarak antara antenna pemancar dan penerima, serta tingkat ketinggian dan tempat dari suatu antenna. Kerugian propagasi didalam pathloss yang ditimbulkan dari sebuah gelombah radio bebas, penyerepan kerugian atau kerugian penetrasi, dan kerugian yang ditimbulkan oleh penyebab lainnya[17].

Pathloss memiliki sebuah tabel PLE untuk setiap keadaan yang berbeda. Tabel tersebut adalah sebagai berikut

Tabel 2.2. 15. 1 Tabel path loss exponent

Environment	Path loss exponent
Free space	2
Urban area cellular radio	3 to 5
In building line of sight	1.6-1.8
Obstructed in building	4 -6
Obstructed in factories	2 – 3

2.2.17 *Mean Square Error* (MSE)

MSE atau *mean square error* adalah sebuah metode statistik untuk mengukur besar selisih antara target dan keluaran perhitungan[18]. Formulasi matematis dari MSE adalah sebagai berikut

$$\boldsymbol{W = E[(X - Y)^2] = \frac{\sum_{n=1}^{N}(X_n - Y_n)^2}{N}} \quad (15)$$

Dimana

W = *Mean Square Error* atau galat kuadrat rata-rata

X dan Y = dua himpunan data yang akan dibandingkan

$E[...] =$ Operator ekspektasi atau rata-rata atau *mean*