PENGGUNAAN TEKNIK DIRECT SEQUENCE SPREAD SPECTRUM (DSSS) PADA ELECTRONIC WARFARE

Rustamaji
Teknik Elektro Institut Teknologi Nasional (Itenas)
Jl. P.H. H. Mustofa 23 Bandung 40124
e-mail : rustamaji@itenas.ac.id

Elan Djaelani
Puslit Informatika LIPI
Jl. Sangkuriang Bandung
e-mail :elan@informatika.lipi.go.id

ABSTRAK

Perkembangan teknologi pendukung EW = Electronic Warfare dan kebutuhannya dalam lingkungan pertempuran (combat environment).

Spread spectrum yang merupakan suatu bentuk teknik modulasi, digunakan dalam peperangan modern untuk menghadapi gangguan (interferensi) dalam bentuk gelombang elektromagnetik oleh lawan terhadap aliran komunikasi.

Spread spectrum untuk memenuhi tuntutan akan kebutuhan komunikasi yang handal, yaitu tahan terhadap interferensi dari luar, dapat beroperasi dengan rapat spektral daya rendah, menyediakan kemampuan akses jamak, dan tingkat keamanan yang tinggi.

Direct Sequence Spread Spectrum (DSSS) adalah salah satu teknik spread spectrum (spektral tersebar), yaitu suatu jenis modulasi dimana lebar bidang frekuensi (band width) transmisi yang digunakan jauh lebih besar dari pada lebar bidang frekuensi minimum yang dibutuhkan untuk mentransmisikan informasi.

Kata kunci : ***Electronic Warfare*** *, Spread spectrum, Direct Sequence Spread Spectrum*

I. PENDAHULUAN.

Pada saat ini semakin banyak negara-negara di dunia memanfaatkan keunggulan dari **EW = *Electronic Warfare*** dalam lingkungan pertempuran (*combat environment*).

Semakin besar ketergantungan pemanfaatan spektrum elektromagnetik sebagai sarana komunikasi, deteksi sasaran dan pengendalian senjata untuk EW pada masa datang.

Setiap sistem senjata modern yang ada saat ini ataupun yang sedang direncanakan, dimulai dari komunikasi, radar, detektor infra merah, laser, passive multimetre-wave radio metre, kamera televisi dan divais penglihat semuanya menggunakan sebagian dari spektrum elektromagnetik untuk beroperasinya. Konsekuensi dari kondisi tersebut, zona pertempuran modern akan penuh terisi dengan ribuan sinyal (pulsa) elektomagnetik.

Tujuan dari EW untuk mengeksploitasi lingkungan secara penuh ini, dinamakan ***electronic battlefield***. Terdapat dua kategori **EW = *Electronic Warfare***, yaitu *passive EW* dan *active EW*.

Teknik EW pasif (*passive EW*) sering digunakan untuk mendapatkan informasi (*intelligence*) berharga. Memonitor komunikasi lawan dapat memberikan informasi berguna untuk saat itu dan perencanaan aktifitas. Pendeteksian secara pasif radar lawan, emisi laser dan infra merah dapat menyediakan peringatan dini (early warning) dan informasi untuk menyiapkan senjata.

Sedangkan teknik EW aktif (*active EW*) digunakan apabila dipertimbangkan untuk meniadakan atau mencegah lawan menggunakan spectrum elektromagnetik. Maka noise atau *deception jamming* (jamming penyesat) digunakan untuk mengacaukan (*disrupt*) atau mengganggu (interfere) jaringan *C3I (command, control, communication, and information)* dan sistem radar lawan.

Contoh nyata efektifitas penggunaan perangkat EW, terlihat pada perang Malvinas antara agresor Inggris yang tetap ingin menguasai kepulauan Malvinas dengan Argentina yang memilikinya. Dimana rudal Exocet yang diluncurkan oleh pesawat Super Etendard Argentina dibingungkan oleh *chaff* yang ditebarkan dari kapal HMS Hermes milik Inggris. Pada perang Yom Kippur antara Mesir melawan zionis Israel,

dimana pada saat itu digunakan *jamming* oleh kedua belah pihak untuk mengacaukan jalur komunikasi masing-masing. Juga pada perang teluk II, dimana pasukan agresor Amerika menggunakan rudal Patriot dan sistem radarnya untuk menangkis serangan rudal Scud yang diluncurkan pasukan Irak

Tren yang berkembang saat ini dan masa datang adalah rancangan perangkat EW otomatis penuh, dengan mengintegrasikan antara *active EW* dan passive EW yang sesuai melalui interface dengan sensor dan sistem senjata lain.

Spread spectrum yang merupakan suatu bentuk teknik modulasi, digunakan dalam peperangan modern untuk menghadapi gangguan (interferensi) dalam bentuk gelombang elektromagnetik oleh lawan terhadap aliran komunikasi.

Terdapat beberapa teknik *Spread spectrum* yang dikenal, antara lain :

- Direct sequence spread spectrum (DSSS)
- Frequency hopping spread spectrum (FHSS),
- Time hopping spread spectrum (THSS)
- Chirp spread spectrum (CSS)
- Hybrid method

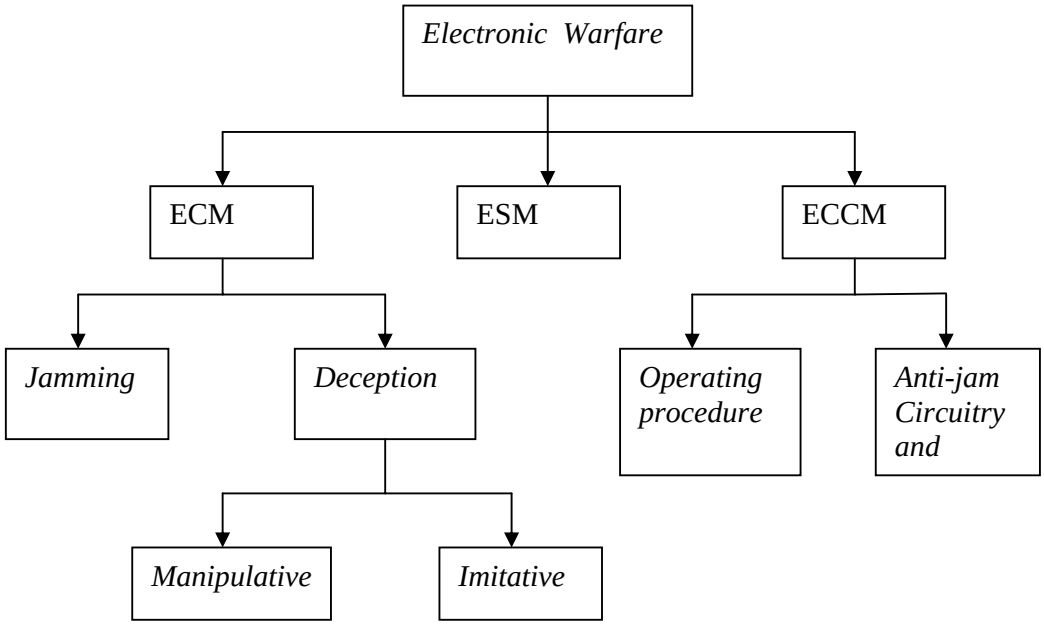
Suatu system komunikasi diklasifikasikan sebagai "*Spread Spectrum*", apabila :

- energi sinyal hasil modulasi spread spectrum tersebar pada lebar pita yang jauh lebih besar dari Laju Bit Informasi.
- proses demodulasi dilakukan dengan mengunakan proses korelasi antara sinyal masuk dengan replika sinyal penebar.

II. PEPERANGAN ELEKTRONIKA (EW *: ELECTRONIC WARFARE*).

Electronic Warfare (EW) umumnya disebut pula *Radio Electronic Combat* (REC) atau *Maskirovka* dalam istilah Rusia, merupakan elemen penting pada konsep peperangan modern (*modern warfare*)

Electronic Warfare (EW) dibagi menjadi tiga bagian yaitu, *Electronic counter measures* (ECM), *Electronic counter-counter measures* (ECCM), dan *Electronic-warfare support measures* (ESM) seperti terlihat pada gambar 1.



Gambar 1. Struktur EW (EW *tree*)

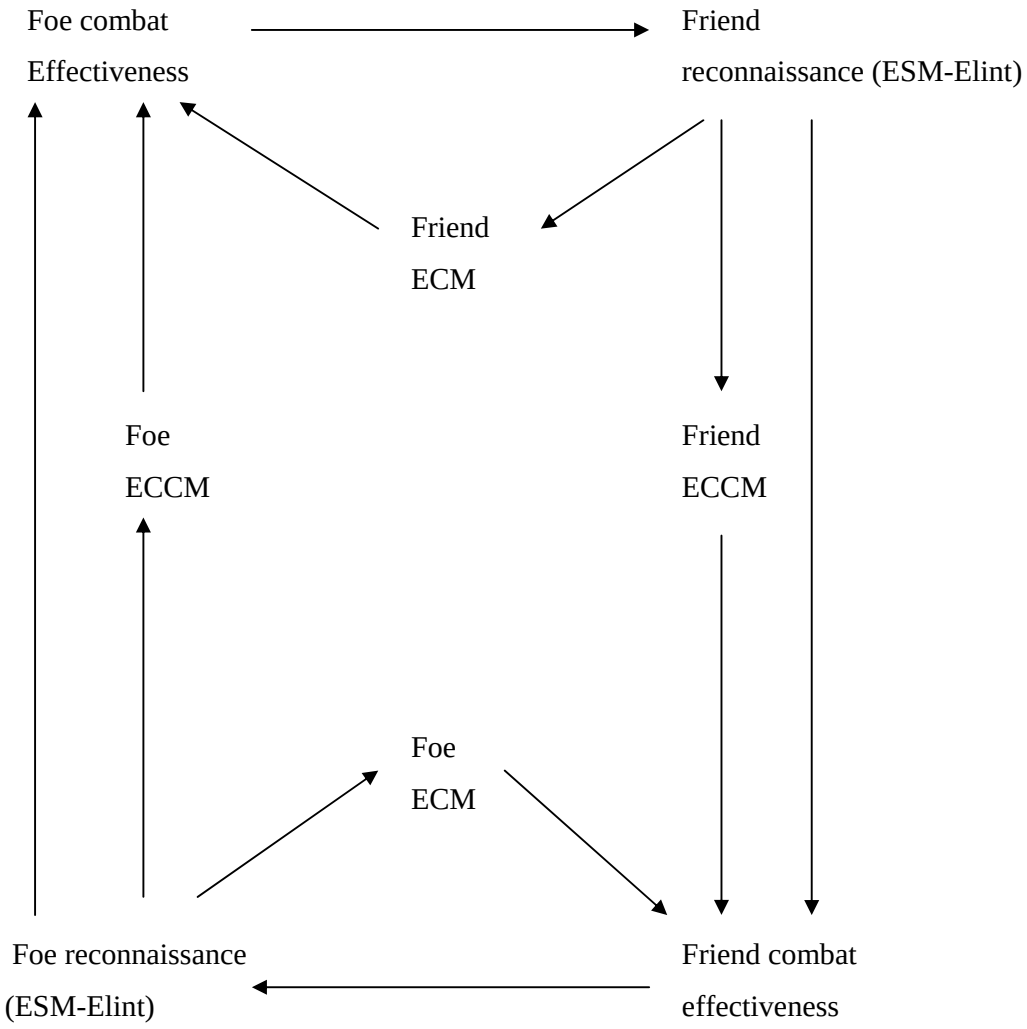
Di Amerika serikat, *electronic, communication and signal intelligence* (ELINT / COMINT / SIGINT) dan *electromagnetic compatibility* (EMC) tidak dimasukkan kedalam struktur EW.

III. PENGERTIAN *ELECTRONIC WARFARE* (EW).

Electronic Warfare (EW) adalah pekerjaan militer pada energi elektromagnetik yang meliputi : Aksi yang diambil untuk menekan (*reduce*) atau mencegah (*prevent*) musuh (*foe*) menggunakan spektrum elektromagnetik; menjamin teman (*friend*) menggunakan spektrum elektromagnetik; dan menyergap (*intercept*), mengenali (*identify*), menganalisis (*analyze*), dan menemukan (*locate*) pancaran elektromagnetik musuh untuk mendukung ECM dan ECCM.

Electronic Warfare (EW) modern, dimulai pada perang dunia ke-2, dengan digunakannya secara intensif peralatan komunikasi elektronika dan Radar dari fihak sekutu maupun poros pada peperangan.

Skenario *Electronic Warfare* (EW), ditunjukkan pada gambar 2 berupa diagram Interaksi antara elemen *Electronic Warfare* (EW) .



Gambar 2. Interaksi antara elemen ***Electronic Warfare.***

Skenario melibatkan *friend* (teman) dan *foe* (lawan). *Friend* membangun jaringan komunikasi dan menjaganya tetap operasional. Dalam operasinya *friend*

menghadapi *electronic warfare* : dimana *foe* akan berusaha membangun *a set of measure* (langkah tindakan) untuk (*deny*) menyangkal atau meniadakan tujuan *friend*, atau akan menyadap (*tap*) saluran komunikasi dan membawa informasi dari *friend* ke dalam jaringannya.

Dalam situasi yang dinamis, diasumsikan kedua jaringan komunikasi *friend* dan *foe* bekerja dalam kondisi terbaik.

Friend mempunyai jaringan komunikasi dengan tujuan :

1. untuk membangun dan memelihara jaringan komunikasi
2. untuk melawan (*counteract*) setiap usaha *foe* untuk menghalangi atau memanfaatkan (*detect* : mendeteksi, *eavesdrop on* : mencuri dengar) aliran komunikasi

sedangkan terhadap *friend.*

Foe mempunyai kesempatan :

1. untuk *detect* dan atau *localize* (menentukan lokasi) keberadaan link komunikasi , dengan
2. to *eavesdrop on* aliran informasi
3. *to block* aliran informasi dengan (*jamming* : pemacetan)
4. *to insert* (menyusupkan) informasi salah (*spoofing*)
5. memilih strategi baru, apabila apabila ada kontra tindakan (*countermeasures*) oleh pemilik jaringan.

Apabila interaksi kedua cenar *friend* dan *foe* semakin meningkat : komunikasi atau tindakan elektronik (EM : *electronic measure*) akan diikuti kontra tindakan elektronik (ECM : *electronic countermeasure*), ini akan memicu kontra kontra tindakan elektronik (ECCM : *electronic counter countermeasure*), dan seterusnya seperti digambarkan berikut :

Action by friend	*Action by foe*
EM	
	ECM
ECCM	
	EC $^{n-1}$M
EC ^{n}M	
	EC $^{n+1}$M

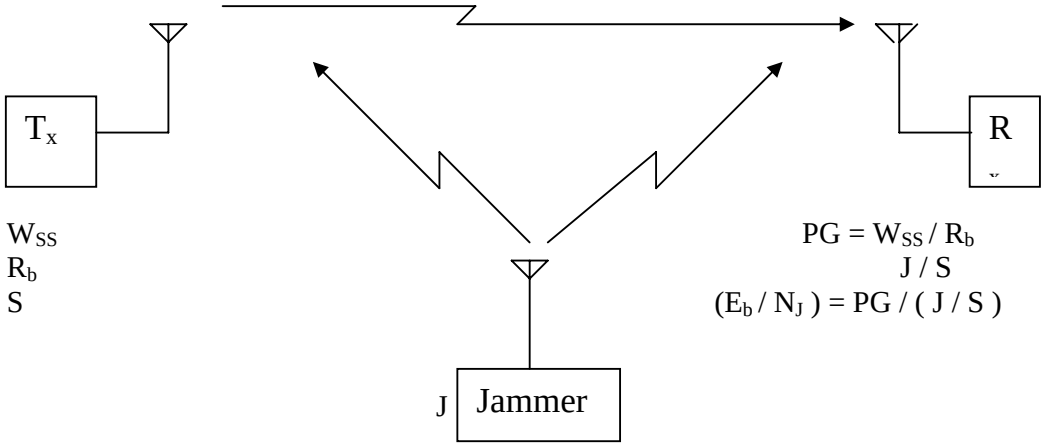
Faktor yang membatasi dalam proses ini adalah waktu dan biaya, dalam hal ini adalah teknologi.

Terlihat dari skenario diatas, fihak yang menguasai teknologi akan lebih unggul dalam peperangan elektronika.

IV. SPREAD SPECTRUM PADA ELECTRONIC WARFARE.

Tujuan komunikasi adalah menyalurkan informasi (dalam bentuk digital) dari satu titik ke titik lainnya dalam lingkungan yang diganggu oleh AWGN (additive white gaussian noise). Selain kanal AWGN tersebut di atas, ada jenis kanal lain yang sifat gangguannya tidak bersifat AWGN, misalnya gangguan "jammer", propagasi multipath fading dan interferensi. Dengan mengunakan teknik spread spectrum, maka gangguan-gangguan non-AWGN dapat diatasi.

Gambaran gangguan oleh *Jammer* pada sistem komunikasi yang menggunakan teknik *spread spectrum* dapat dilihat pada gambar 3 :



Gambar 3. *Jammer* pada sistem komunikasi

Dimana W_{SS} : bandwith sinyal spread spectrum (Hz)
R_b : bit rate sinyal informasi (bps)
S : daya sinyal (W)
J : daya jamming (W)

Dari gambar 3, terlihat sistem komunikasi yang menggunakan teknik *spread spectrum* diganggu oleh *jammer* yang mempunyai daya sebesar J.

Pemancar Tx mempunyai bit rate masukan $R_{b,}$ bandwitdh transmisi W_{SS} dan daya sinyal S. Dengan menggunakan teknik *spread spectrum* maka Tx mempunyai processing gain (PG) sebesar :

$PG = W_{SS} / R_b$.

Akibat adanya *jammer*, maka pada penerima Rx selain diterima sinyal S juga diterima sinyal *jammer* J, sehingga dihasilkan *bit energy to jammer noise ratio* :

$(E_b / N_J) = PG / (J / S)$

$= W_{SS} .S / R_b . J$

dimana J / S adalah *jammer to signal power ratio.*

Terlihat dari persamaan, dengan adanya sinyal *jammer* J maka nilai E_b / N_J akan turun.

Maka untuk mempertahankan atau memperbesar nilai E_b / N_J , maka W_{SS} harus diperbesar.

Sesuai formulasi Shannon (*Shannon limit for information capacity*) :

$$C = BW \ ^2\log (1 + S/N)$$

dimana C : Kapasitas kanal (bps)

BW : lebar bidang frekuensi (Hz)

S/N : perbandingan daya sinyal terhadap daya noise

terlihat dari formulasi Shannon, untuk mempertahankan besarnya C (kapasitas kanal) pada kondisi kinerja komunikasi (S/N) yang rendah, maka BW (lebar bidang frekuensi) harus diperbesar. Salah satu teknik untuk memperbesar lebar bidang frekuensi digunakan teknik *Spread Spectrum*

Kinerja dari suatu sistem komunikasi dengan teknik *Spread Spectrum*, dinyatakan oleh *processing gain* (PG). PG didefinisikan sebagai perbandingan antara lebar bidang frekuensi transmisi setelah ditebar dengan lebar bidang frekuensi informasi sebelum ditebar.

$$PG = \text{BW transmisi / BW informasi}$$
$$= W_{SS} / R_b$$

V. *DIRECT SEQUENCE SPREAD SPECTRUM*.

Direct Sequence Spread Spectrum (DSSS) adalah salah satu teknik spread spectrum (spektral tersebar), yaitu suatu jenis modulasi dimana lebar bidang frekuensi (*band width*) transmisi yang digunakan jauh lebih besar dari pada lebar bidang frekuensi minimum yang dibutuhkan untuk mentransmisikan informasi, sementara tidak ada kaitan langsung antara lebar bidang frekuensi keluaran dengan modulasi oleh sinyal informasinya.

Dengan adanya pemodulasian secara *Direct Sequence Spread Spectrum*, sinyal informasi (termodulasi digital) yang mempunyai lebar bidang frekuensi terbatas akan ditebarkan pada daerah frekuensi yang jauh lebih lebar, serta akan dapat bekerja pada rapat spektral daya yang rendah.

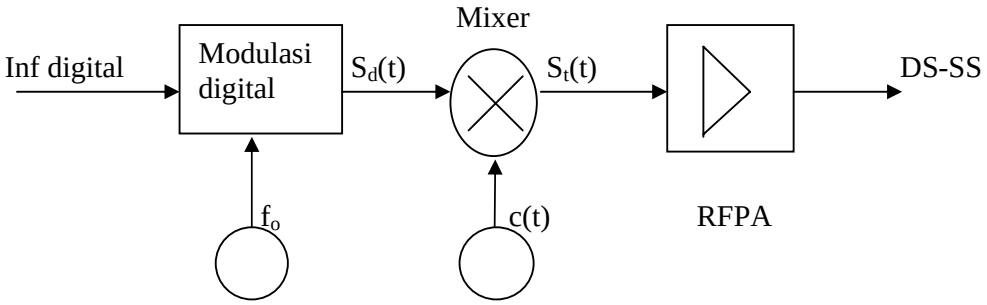
Pada *Direct Sequence Spread Spectrum*, proses penebaran dilakukan dengan melakukan perkalian langsung (*direct*) antara sinyal informasi (yang dimodulasikan secara digital) dengan suatu urutan spreading code (kode penebar). Lebar bidang frekuensi daerah sinyal informasi ditebarkan tergantung pada *chip rate* (laju chip) dari kode penebar, dimana kode penebar ini dihasilkan oleh suatu PN (*pseudo noise*) *generator* dengan panjang urutan tertentu yang dapat diprogram.

Proses demodulasi (*despreading*) sinyal *Direct Sequence Spread Spectrum* di penerima, dilakukan menggunakan proses korelasi antara sinyal *Direct Sequence Spread Spectrum* diterima dengan replika kode penebar yang dibangkitkan di penerima dengan bantuan rangkaian akuisisi dan tracking.

Karena sinyal informasi ditebarkan pada daerah frekuensi yang cukup lebar dengan teknik *Direct Sequence Spread Spectrum*, sinyal informasi akan tahan terhadap sinyal interferensi (gangguan) dari luar dan sinyal *jamming* (pemacetan) yang sengaja dilakukan oleh perangkat komunikasi lain.

Dengan kemampuan mengatasi *jamming* serta kinerja yang baik inilah, *Direct Sequence Spread Spectrum* pada awalnya digunakan pada komunikasi militer dan pada saat sekarang teknik *Direct Sequence Spread Spectrum* mulai banyak digunakan untuk kebutuhan non-militer seperti GPS, telemetri, dan komunikasi seluler yang dikenal sebagai teknologi CDMA (*code division multiple access*)

Prinsip dasar *Direct Sequence Spread Spectrum*



Gambar 4. Prinsip dasar *Direct Sequence Spread Spectrum* :

Dalam sistem ini digunakan kode penebar (*spreading code*) sedemikian rupa sehingga proses deteksinya mudah dilakukan, tanpa gangguan yang berarti dari sinyal-sinyal lain yang menempati pita frekuensi yang sama.

Sinyal keluaran modulator digital dapat dituliskan sebagai berikut :

$$S_d(t) = \sqrt{2P}\ \cos [\omega_O t + \theta_d(t)]$$

dimana $\theta_d(t)$ berharga 0 atau π karena mengunakan modulasi BPSK.

Perubahan fasa $\theta_d(t)$ dapat terjadi setiap perioda bit = T_b = 1/(laju bit).

Untuk menebarkan sinyal tersebut diatas, maka $S_d(t)$ dikalikan dengan kode penebar c(t), yang dalam realisasinya merupakan sinyal NRZ-polar dengan amplitude = 1 dan mempunyai lebar satuan = T_C lebar "chip".

Laju "chip" atau "chip rate" adalah jumlah chip perdetik atau = 1/ T_C .

Format c(t) dibuat sedemikian rupa sehingga dapat disebut sebagai "sinyal acak semu".

Dengan demikian, sinyal keluaran $S_t(t)$ dapat dituliskan sebagai :

$$S_t(t) = \sqrt{2P} \cdot c(t).\cos [\omega_O t + \theta_d(t)]$$

Sinyal $S_t(t)$ inilah yang dinamakan *Direct Sequence Spread Spectrum*, selanjutnya dapat oleh RFPA (*radio frequency power amplifier*) diperkuat sebelum dikirimkan ke penerima.

Rapat daya sinyal DS-SS.

Rapat Spektral Daya Sinyal BPSK $S_d(t)$:

$$S_d(f) = \tfrac{1}{2} PT_S \{ \text{sinc}^2 [(f - f_0) T_S] + \text{sinc}^2 [(f + f_0) T_S] \}$$

Rapat Spektral Daya kode penebar c(t) :

Rapat daya dari kode penebar c(t) adalah transformasi Fourier dari fungsi otokorelasinya :

$$F\left(R_c(\tau)\right) = S_c(f) = \int_{\infty}^{\infty} R_c(\tau)\, e^{-j2\pi f\tau}\, d\tau$$

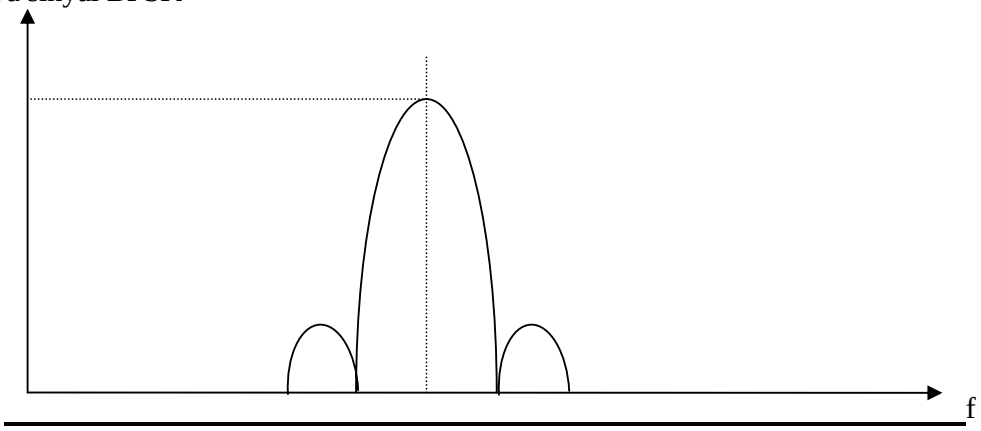
$$S_c(f) = T_c \,\text{sinc}^2 (Ft_c)$$

Rapat daya sinyal DS-SS $S_t(t)$:

$$S_t(f) = \frac{PT_c}{2}\left|\frac{\sin\pi(f - f_o)T_c}{\pi(f - f_o)T_c}\right|^2 + \frac{PT_c}{2}\left|\frac{\sin\pi(f + f_o)T_c}{\pi(f + f_o)T_c}\right|^2$$

Berikut adalah gambaran penebaran sinyal BPSK dengan teknik DSSS, dimana besarnya perbandingan nilai Tc = Tb/2, atau nilai chip rate Rc dua kali nilai bit rate Rb.

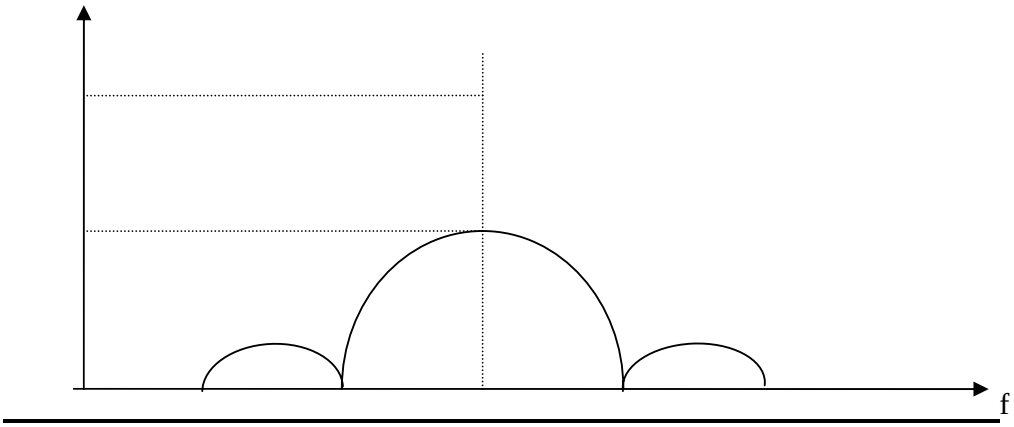
Daya sinyal BPSK



Gambar 5a. Spektrum sinyal informasi (BPSK) sebelum ditebarkan

Dari gambar 5a, terlihat sinyal informasi (BPSK) sebelum ditebarkan mempunyai amplitudo sebesar A watt dan bandwidth selebar B hertz..

Daya sinyal DS-SS

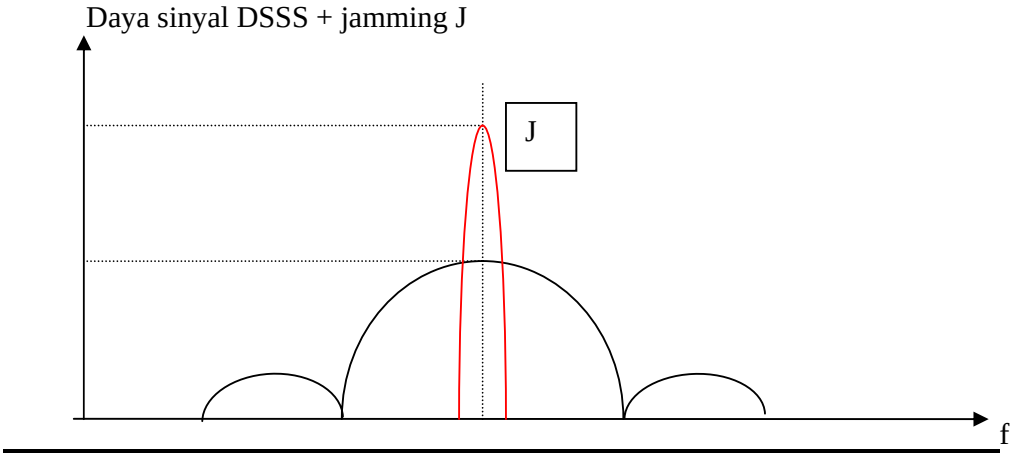


Gambar 5b. Spektrum sinyal informasi (BPSK) setelah ditebarkan

Dari gambar 5b, terlihat sinyal informasi (BPSK) setelah ditebarkan mempunyai amplitudo sebesar ½ A watt dan bandwidth selebar 2B hertz..

Dari gambar 5a dan 5b terlihat bahwa dengan perbandingan nilai Tc = Tb/2 maka bandwidth sinyal BPSK setelah ditebarkan akan menjadi dua kalinya, sedangkan amplitudo (energi) akan menjadi setengahnya dari semula.

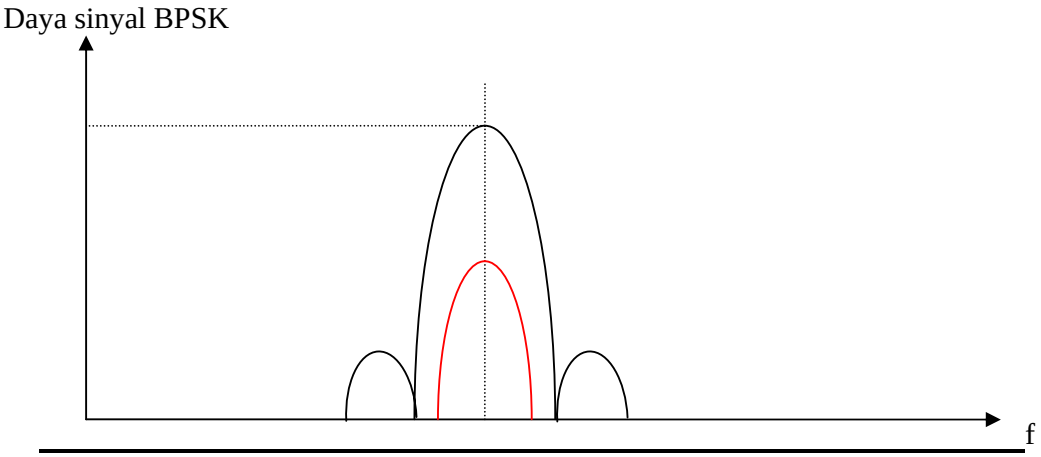
Contoh kasus, apabila sinyal DSSS terkena sinyal jamming J, maka gambarannya adalah seperti gambar 6 :



Gambar 6a. Spektrum sinyal DSSS + sinyal jamming J (warna merah)

Terlihat dari gambar 6a, sinyal DSSS terkena sinyal jamming (single tone) dengan amplitudo sebesar J watt, yang nilainya lebih besar dari amplitudo sinyal DSSS.

Dengan digunakannya teknik DSSS, maka di penerima akan terjadi proses despreading, sehingga amplitudo (energi) dan bandwidth sinyal BPSK kembali seperti semula. Amplitudo (energi) menjadi A watt dan bandwidth menjadi B hertz. Sedangkan amplitudo (energi) sinyal jamming menjadi 1/2J dan bandwidth-nya menjadi ½ nya, seperti gambar 6b.



Gambar 6a. Spektrum sinyal informasi (BPSK) + jamming setelah despreading

Dengan amplitudo (energi) sinyal jamming ditekan menjadi 1/2J dan bandwidth-nya menjadi 2 kalinya, maka tidak akan mengganggu sinyal informasi BPSK. Semakin besar perbandingan antara Tb dan Tc, maka amplitudo (energi) sinyal jamming akan semakin kecil, sehingga tingkat efektivitas gangguan sinyal jamming pada sinyal informasi BPSK semakin rendah, atau dikatakan rasio perbandingan sinyal terhadap noise (S/N) di penerima membesar.

VI. PENUTUP.

- Pengusaan teknologi elektronika komunikasi sangat diperlukan untuk memenangkan pertempuran (***electronic battlefield*** **)**
- Dari pembahasan dapat dilihat pentingnya penggunaan teknik spread spectrum pada electronic warfare
- Dengan mengunakan teknik direct sequence spread spectrum, sinyal informasi yang mempunyai BW terbatas dapat ditebarkan (spread) pada daerah frekuensi (BW)

transmisi yang jauh lebih besar. Sehingga sangat sulit untuk dapat dideteksi dan diganggu oleh penerima yang tidak dikehendaki (lawan)

DAFTAR PUSTAKA

1. International Defense Review - Electronic Warfare
2. Military Technology - Electronic in Defence
3. Defences Electronic - The Electronic Navy
4. R, Skaug, J.F. Hjelmstad – Spread Spectrum In Communication
5. Marvin K. Simon etc – Spread Spectrum Communication
6. Rustamaji; Elan Djaelani, 'Pemancar Frequency Hopping Spead Spectrum Untuk Pengamanan Sinyal Informasi", Jurnal Teknologi Informasi LIPI, Vol 3 no 1, 2002.
7. Rustamaji; Elan Djaelani, 'Frequency Hopping Spead Spectrum Suatu Teknik Pengamanan Komunikasi Pada Perang Elektronika (Electronic Warfare)", Prosiding, Pemaparan Hasil Litbang 2003 LIPI, 2003
8. Plessey Semiconductor, "Frequency Dividers and Synthesyzers IC Handbook".
9. Ulrich L, Rohde; T T N Bucher,"Communication Receiver : Principles and Design",McGraw Hill