FREQUENCY HOPPING-SPREAD SPECTRUM (FHSS) SUATU TEKNIK PENGAMANAN KOMUNIKASI PADA PERANG ELEKTRONIKA (ELECTRONIC WARFARE)

Rustamaji
Staf Pengajar Jurusan Teknik Elektro
Institut Teknologi Nasional
Jln P.H.Mustafa 23, Bandung.Telp.022-727115.
E-mail: Rustamaji@itenas.ac.id

Elan Djaelani
Pusat Penelitian Informatika – LIPI
Jl. Cisitu, Sangkuriang, Bandung 40135
Telp. (022) 2504711, Fax : (022) 2504712, E–mail : elan@informatika.lipi.go.id

ABSTRACT

Frequency hopping is one of spread spectrum, namely a kind of modulation where transmission bandwidth is used more wide then minimum information bandwidth needed to transmission of information.

Spread spectrum is used for meeting charge of communication needs that are reliable, namely communication system which have resistant ability against interference from outside, can operate wih low power spektral bandwidth, can support plural access ability, and high level of security.

Spread spectrum at first time is used for military communication needs, and at next developing time is used for non-military field.

ABSTRAK

Frequency Hopping adalah salah satu teknik spread spectrum, yaitu suatu jenis modulasi dimana lebar bidang transmisi yang digunakan jauh lebih besar dari pada lebar bidang minimum yang dibutuhkan untuk mentransmisikan informasi.

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

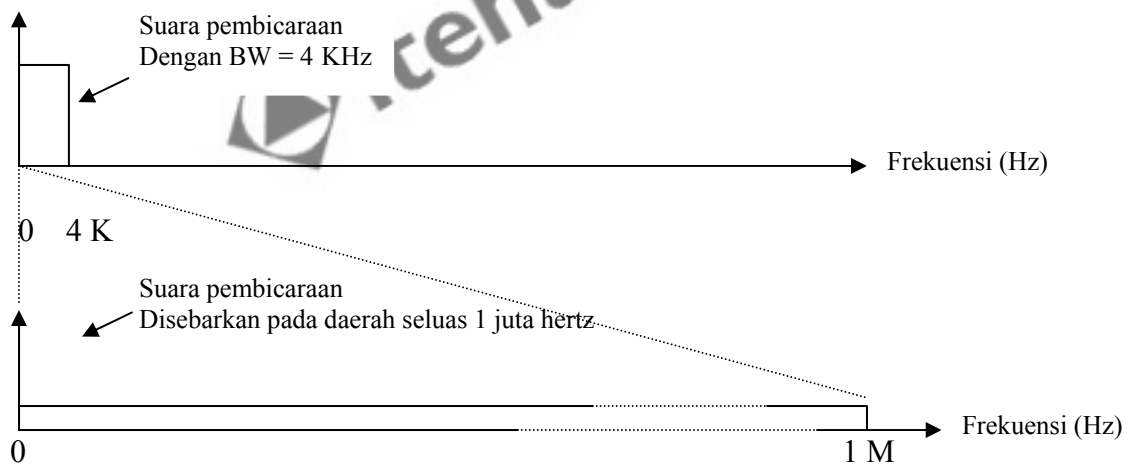
Spread spectrum pada mulanya digunakan untuk kebutuhan komunikasi militer, dan pada perkembangannya dimanfaatkan untuk bidang non-militer.

PENDAHULUAN

Spread spectrum (spektral tersebar) suatu penemuan pada bidang komunikasi yang canggih, karena kelebihannya dimanfaatkan oleh militer untuk mengamankan komunikasi mereka pada situasi peperangan maupun damai, dan akhir-akhir ini mulai dimanfaatkan pada komunikasi seluler.

Dinamakan spread spectrum, karena lebar bidang frekuensi (BW=band width) transimisi yang digunakan jauh lebih besar dari pada lebar bidang frekuensi minimum yang dibutuhkan oleh informasi (pembicaraan).

Sebagai gambaran, misalnya suara pembicaraan manusia mempunyai lebar bidang frekuensi 4 KHz, bila di transmisikan dengan teknik spread spectrum akan dapat menempati (ditebarkan) pada daerah frekuensi selebar 1 MHz tergantung pengaturannya, seperti digambarkan pada (gambar 1).



Gambar 1. Suara pembicaraan 4 KHz ditebarkan pada daerah frekuensi selebar 1 MHz

Dari gambar 1, dapat dibayangkan bagaimana sukarnya untuk melacak (menyadap) suatu informasi pembicaraan selebar 4 KHz yang ditebarkan pada daerah frekuensi selebar 1 MHz dengan teknik spread spectrum (mempunyai perbandingan penebaran 1000/ 4 kali). Untuk lebih menjamin keamanan informasi pembicaraan, dalam proses penebarannya dilakukan pengacakan dengan kode-kode tertentu.

Gambaran diatas adalah salah satu keunggulan teknik spread spectrum untuk mengamankan informasi pembicaraan, disamping keunggulan lainnya seperti : kemampuan melawan jamming, mampu menekan gangguan sinyal dari luar, mampu melawan perlemahan sinyal akibat propagasi, dll.

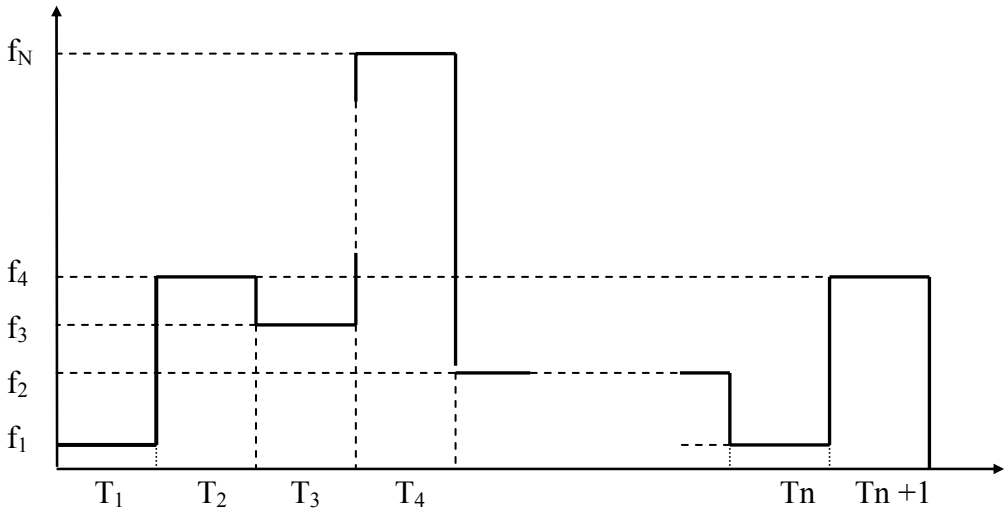
Beberapa teknik spread spectrum yang dikenal antara lain :

- Direct sequence spread spectrum
- Frequency hopping spread spectrum
- Time hopping spread spectrum
- Chirp spread spectrum
- Hybrid method

Dari keempat teknik spread spectrum ini, frequency hopping spread spectrum (FHSS) mempunyai keandalan yang paling tinggi untuk mengamankan informasi pembicaraan, disamping dimanfaatkan pada komunikasi seluler.

FREQUENCY HOPPING SPREAD SPECTRUM (FHSS)

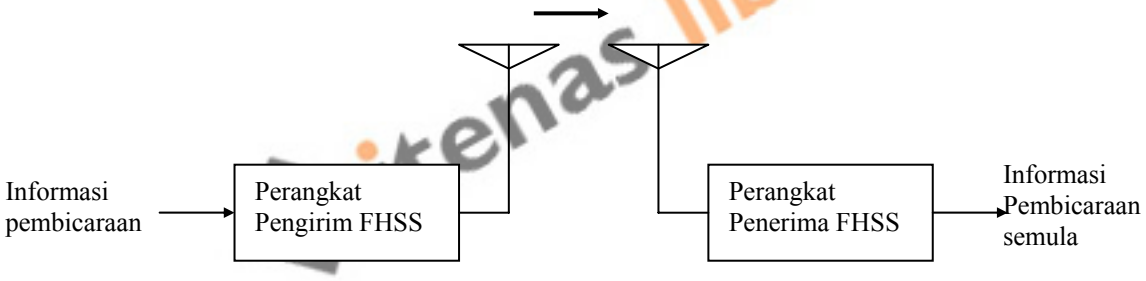
Pada FHSS proses penebaran informasi pembicaraan pada suatu daerah frekuensi dengan lebar tertentu, dilakukan dengan cara mengubah-ubah frekuensi sinyal pembawa setiap saat seperti contoh pada (gambar 2). Dimana frekuensi sinyal pembawa ini mengandung (membawa) informasi pembicaraan.



Gambar 2. Proses penebaran informasi dengan FHSS

Dari (gambar 2) terlihat bahwa informasi pembicaraan ditebarkan pada daerah frekuensi f_1 s/d f_N yang jauh sangat lebar bila dibandingkan dengan lebar bidang frekuensi informasi pembicaran. Dengan kode-kode tertentu yang dapat diacak maka seolah-olah informasi pembicaraan akan menempati daerah frekuensi yang berubah-ubah secara acak pula, atau dengan kata lain informasi pembicaraan akan melompat (hopping) dari satu lokasi frekuensi ke frekuensi lainnya antara f_1 s/d f_N secara acak sesuai dengan kode-kode yang sudah ditentukan.

Karena daerah frekuensi yang ditempati oleh informasi pembicaraan akan selalu berpindah-pindah (hopping) secara acak dari waktu ke waktu dengan kecepatan perpindahan yang sangat tinggi, maka sangat sukar untuk dilakukan jamming (pemacetan) oleh pihak lain yang tidak mengetahui atau tidak mampu menguraikan kode-kode yang digunakan untuk mengubah-ubah frekuensi. Karena kemampuan FHSS untuk menghindari penyadapan dan pemacetan oleh pihak yang tidak diinginkan inilah, maka FHSS sangat tepat apabila digunakan untuk teknik pengamanan informasi pembicaraan, sesuai dengan (gambar 3).



Gambar 3. Diagram blok komunikasi dengan perangkat FHSS

SKENARIO PERANG ELEKTRONIKA (*ELECTRONIC WARFARE*)

Dalam skenario ini dapat digambarkan pentingnya penggunaan teknik pengamanan sinyal informasi. 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 (*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 sistem *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.

Dari skenario diatas terlihat jelas pentingnya penggunaan teknik tertentu untuk mengatasi kemungkinan gangguan komunikasi yang dilakukan oleh *foe* (lawan). Dimana FHSS adalah salah satu teknik yang dapat digunakan untuk mengatasi ganggguan tersebut.

Ketangguhan FHSS untuk pengamanan informasi pembicaraan (dan data) sudah dibuktikan oleh militer Israel dalam peperangan didaratan tinggi Golan tahun 1980 an, dimana kendaraan lapis baja (tank) milik AD Israel yang dilengkapi peralatan komunikasi dengan FHSS mampu menghindari penyadapan dan pemacetan pihak lawan sehingga selalu berhasil dalam setiap operasinya.

Kemampuan FHSS juga dimanfaatkan untuk komunikasi akses jamak (multiple acces) pada komunikasi seluler, yang dikenal sebagai FHMA (Frequency Hopping Multiple Acces) untuk menghasilkan multiple acces rangking environment kapasitas tinggi. Apabila pada FHSS untuk pengubahan frekuensi pembawa dilakukan secara acak dengan mengunakan kode-kode tertentu yang dirahasiakan, maka pada FHMA pengubahan frekuensi dilakukan secara teratur mengunakan kode-kode yang unik. Pengunaan kode-kode yang unik pada FHMA inilah yang merupakan dasar komunikasi seluler dengan teknologi CDMA (Code division multiple acces), dan W-CDMA (wide band – CDMA).

HASIL PENELITIAN

- Penelitian yang telah dilakukan antara lain, perancangan model perangkat frequency hopping.
- Penelitian perancangan dan relaisasi pengirim dan penerima frequency hopping

PENUTUP

Dengan mengunakan teknik frequency hopping spreas spectrum, sinyal informasi baik analog maupun digital 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

Cooper, G.R. and Mc Gilem, C.D. (1988), "*Modern Communication and Spread Spectrum*". McGraw Hill.

Hyuck, M.Kwon. (1990), "Capacity and Cut-off Rate of Coded FH/ MFSK Communication with Imperfect Side Information Generator". *IEEE Journal on Selected Areas in Communication, vol 8 no 5*, June.

Kaplan, E. (1993), “Frequency Hopping Takes the Leap”, *Radio Resource*, vol 7 no 2.

Kimo, J.J. and Liu, Shyh-Chang. (1990), ”Maximal Length Sequences for Frequency Hopping*”, IEEE Journal on Selected Areas in Communication*, vol 8 no 5, June.

Rustamaji. (1998), “Perancangan Model Perangkat Frekuensi Hopping”, *Tesis Magister*.

Simon, M.K; Scholtz, R.A. and Levitt, B.K. (1985), “Spread Spectrum”, Computer Science Press,.

Small, M. “HF Amateur Band Frequency Synthesizer”.,*Electronic Word*, vol 85 No. 1519.

Ziemer, R.E. and Peterson, R.L. (1985), “Digital Communication and Spread Spectrum System”.