Investigation on Anti-Jamming Techniques for a robust and reliable Communication Electronic Warfare System

M.L.S.N. SWARAJYA LAKSHMI*, D.S RAM KIRAN* , NIRANJAN PRASAD$ AND M.S.G.PRASAD*
*Dept of ECE, K. L. University, Green Fields, Vaddeswaram, Guntur(Dist)522502 , $Scientist-F, DLRL, Hyderabad-500005

Abstract— Jamming-resistant communication is crucial for safety-critical applications such as emergency alert broadcasts or the dissemination of navigation signals in adversarial conditions. Interference due to intentional/unintentional jamming, co-channel and adjacent channel users can cause severe performance degradation to the communication receivers. Several studies on Electronic Attacks (EAs) to the communication network carried out worldwide reveal that the modern communication can have catastrophe effect wherein a wireless security threats can be effectively disrupted using jammers causing the loss of communication signal or unreliable RF communication under wireless network. By emitting noise-like signals arbitrarily on the shared wireless medium, a jammer can easily disturb the network.
Existing Anti-Jam (AJ) and interference mitigation techniques can be applied to reduce the impact of the jammer or interferer to a receiver by determining the characteristics of the interference, then jointly optimizing signal processing to mitigate the characterized jammer or interferer. Depending on the time-frequency nature of the strong interference signal, it may be possible to achieve relatively good anti-jam performance by applying certain signal processing techniques. In this paper, work has been carried out on the application of anti-jamming techniques to QPSK signals.

Index Terms— Anti-Jamming, Robust, Electronic Warfare System, Radio Electronic Combat, Spread Spectrum, Frequency Hoping, Electronic Counter Counter Measures.

1 INTRODUCTION

The main components of Electronic Warfare (EW) comprises of Electronic Support Measures (ESM), Electronic Counter Measures (ECM) and Electronic Counter Counter Measure (ECCM). These components are presently termed as Electronic Support (ES), Electronic attack (EA) and Electronic Protection (EP) respectively. Under the Radio Electronic Combat (REC) situation, the point to point communication can be vulnerable to jamming causing the disruption or loss of voice, data, video etc. To counter the enemy's effective use of REC, suitable EP System can be designed around the Receiver. In EW scenario, as the EA Systems effectiveness became apparent sometimes, weapon systems are required to be protected by means of additional electronic devices that could counter the effect of EA System. EP techniques aim at either making it difficult for the enemy to detect the presence of communication emitters, or make it difficult to jam, or both. Commonly used EP techniques that are effective, yet do not require any sophisticated techniques, are use of directional antennas and transmitter power that is just adequate to operate the communication link in order to avoid detection by the enemy. The method is however, highly dependent on deployment scenario. Sophisticated modem low-probability-of-intercept (LPI) make use of spread-spectrum techniques such as direct-sequence (DS) or frequency hopping (PH) or a hybrid scheme incorporating advantages of both the schemes. These techniques spread the transmitter power over a bandwidth that is significantly larger than the information bandwidth. The subsequent de-spreading operation in the receiver produces a processing gain for the intended signal. This gain is, however, not experienced by the jammer signal thus making the jammer less effective.

2. ROLE OF EP TECHNIQUE

EP Technique is considered to protect the friendly communication system from enemy's deliberate attempts of detection, deception or destruction of RF signals. The first line of defense against REC is a well-trained and alert operator. To combat enemy REC efforts, operators must have selection of appropriate EP techniques while under operational radio signal transmission. EP plans must consider possible up-link and down link jamming. The jamming noise must be defeated by increasing transmitter power or changes in link capacity. Some of the EP measure/actions that can minimize or reduce the vulnerability to an enemy REC effort are as follows:

(a) Prepare backup system-

(b) Prepare to operate with the minimum amount of communications.
(c) Move Communication posts frequently.
(d) Use state-of-the-art equipment
(e) Report all known or suspected REC activities.
(f) Plan and train to counter an REC threat.
(g) Disperse communications equipment over a wide geographical area.

To accomplish the anti-REC missions, the radio signals transmissions should be kept to the minimum as required and the short transmissions duration should be provided. The enemy gains less information from a short transmission and it also limits the enemy's capability to locate the transmitter using Radio DF (RDF)[2].

TABLE 1:
3 Elements of Electronic Warfare (EW) System and their roles

Component	Objective	Role
ES	Disclose information about enemy's communication	To Search, Intercept, Identify, Locate
EA	Deny or reduce use of Enemy	To Jam , Deceive
EP	communication Ensure continued effective Use of friendly communications (protect against enemy detection location and identification)	To Anti-Jam, or to protect through Anti-Intercept Techniques

In order to avoid the problems caused by jamming or to avoid interception and exploitation of one's own signals by the enemy, the following are some of the ECCM techniques generally used.

- Spread spectrum techniques Adaptive Techniques
- Burst transmission techniques
- Encryption
- False/dummy data generation
- Directional transmission
- Transmission power control
- FEC techniques

2.1 Description of Spread spectrum

Spread spectrum is a communication technique in which the information signal is spread over a band-width considerably greater than necessary to resist to jamming and other interference. This technique was initially devised for military use. One of the methods of classifying spread spectrum techniques is by modulation. Some of the modulation techniques employed in spread spectrum techniques are Direct Sequence (DS), Frequency Hopping (FH), Chirp etc.

Brief description of DSSS,FHSS, Quadrature Phase Shift Keying (QPSK), QPSK-DSSS and QPSK-FHSS are given below.

2.2 Direct Sequence Spread Spectrum (DSSS)

Direct sequence spread spectrum (DSSS) is a transmission technique in which a pseudorandom (PN) code, independent of the information data, is employed as a modulation waveform to spread the signal energy over a bandwidth much greater than the signal information bandwidth. At the receiver, the signal is despread using a synchronized replica of the pseudo-noise code. The fundamental principle of DSSS is that, in channels with narrowband noise, increasing the transmitted signal bandwidth results is an increased probability that the received information will be correct. This technique sacrifices bandwidth in order to gain signal to interference performance. A frequency domain representation of the spread spectrum concept through Direct Sequence Spread Spectrum (DSSS) is shown in Fig. 1.

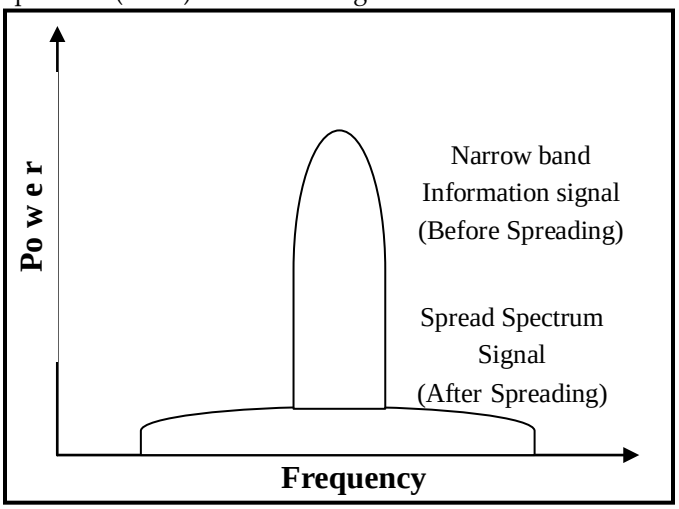


Fig.1: A Typical Sketch of DSSS and its bandwidth spreading

The pseudorandom noise sequence used for spreading the message signal is often a "noise like" signal, which is usually a binary. Digital logic circuitry is typically used to generate a PN sequence and the same circuitry may be used at the transmitter and receiver. one of the important parameters of a spread spectrum technique is the

processing gain (PG). It is defined as the ratio of the bandwidth of the spread signal to the bandwidth of the unspread data signal.

$$PG = \frac{\text{Spread Signal BW}}{\text{Unspread Signal BW}}$$

The basic characteristics of DSSS transmission are:

Much wider bandwidth of the modulated signal than that of transmitted data signal. Use of Pseudo-random sequence Retrieval of actual signal at the receiver through cross correlation technique.

In DSSS the ability to overcome jamming is determined by the processing gain of the system. As the number of bits in the pseudorandom sequence is increased, by increasing the rate of the spreading signal, the processing gain of the system increases and hence so does the bandwidth. However there is limitations to the physical devices that can be generate the PN sequences, this limits the bandwidth in the case of DSSS. This problem is more easily overcome in FHSS, since the instantaneous bandwidth of the FH signal is that of the information bandwidth, and carrier frequency oscillators are available that can hop over a very wideband[3]. In addition, FH is less affected by the near-far effect, because only a small number of frequency hops will be blocked by a nearby transmitter and the remaining hops can be used to recover the original data message. The FHSS is briefly described below.

2.3 Frequency Hopping Spread Spectrum (FHSS)

FHSS is a spread spectrum technique in which the data bits are transmitted in a different frequency slots at different times. The total bandwidth of the output signal is equal to the sum of all the frequency slots, also called hops. Frequency hopping is usually pseudorandom and the sequence of hops is only known to the desired transmitter and the receiver. Unwanted receivers have to cover the complete output bandwidth to receive the frequency hopped signal. Thus in FHSS the carrier frequency hops randomly from one frequency to another. Frequency hopping allows communicators to hop out of frequency channels with interference. To exploit this capability, error-correcting codes, appropriate interleaving, and disjoint frequency channels are nearly used. FHSS may be classified as fast or slow. Fast frequency hopping occurs if there is a frequency hop for each transmitted symbol. Thus, fast frequency hopping implies that the hopping rate equals or exceeds the information symbol rate. Slow frequency hopping occurs if two or more symbols are transmitted in the time interval between frequency hops.

3. QUADRATURE PHASE SHIFT KEYING (QPSK)

QPSK is a method for transmitting digital information across an analog channel in which both a cosine and sine carrier wave are varied in phase, keeping amplitude and frequency constant. In this modulation technique two bits are transmitted in a single modulation symbol, resulting in four different symbols. The phase of carrier takes one of the four possible values such as 0,π/2,π,3π/2.where each phase corresponds to a unique symbol. The block diagram of a typical QPSK transmitter is shown in Fig. 2.

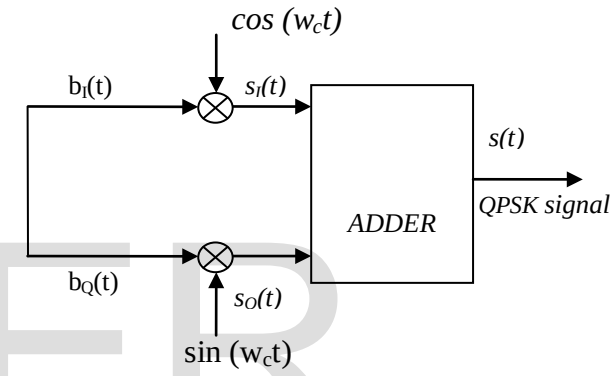


Fig.2: QPSK Transmitter

The input bit stream $d_b(t)$ is split into In-phase and Quadrature bit-streams which are then separately modulated by two carrier signals (in phase and Quadrature carriers). Each modulated BPSK signal is summed up to produce QPSK signal. At the receiver, a band-pass filter is used to remove the in-band noise and reduce the effect of adjacent channel interference. The filtered signal is then splitted into two parts, and each part is coherently demodulated using the in-phase and quadrature carriers. The demodulator outputs are passed through a decision-making circuit that generates estimates of the in-phase and quadrature binary streams. These two streams are then multiplexed to reproduce the original message binary sequence. The modeled results for In-phase (I) and Quadrature phase (Q) signals are shown in Fig.3 below:

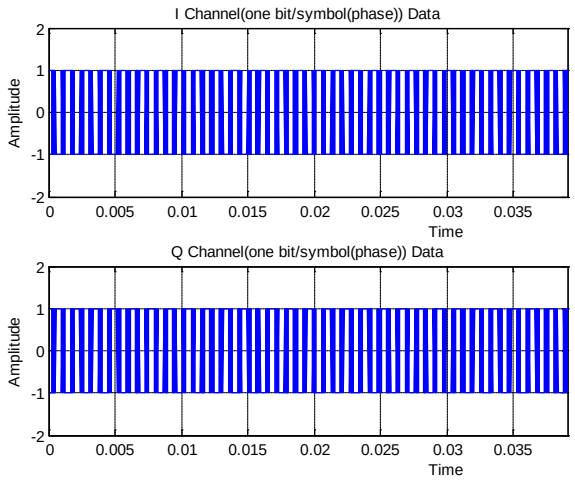


Fig.3: Results for QPSK (I) and (Q) Phase Signals

In QPSK, two bits are transmitted in a single modulation symbol instead of one of one bit as for BPSK. Thus the bandwidth efficiency of QPSK is twice as that of BPSK. This is because the main -lobe of the power spectral density of a QPSK signal i.e., the null-to null bandwidth is equal to twice the symbol rate, which is half that of BPSK signal. Furthermore, the bit error probability of QPSK is nearly identical to BPSK, while twice as much data can be sent in the same bandwidth. When there is no crosstalk interference between the two Quadrature channels for coherent detection, the bit-error probability is given as

$$P_b = Q[\sqrt{2\frac{E_b}{N_o}}]\ldots\ldots \quad \text{(eq(1)]}$$

where, E_b is the bit energy, N_0 is the one-sided noise spectral density and

Q(x) is defined as

$$Q(x) = \frac{1}{2} erfc\left(\sqrt{\frac{x}{2}}\right) and\ erfc(u) = \frac{1}{\sqrt{2\pi}}\int_0^u e^{-z^2/2}\, dz \quad \text{(eq(2)]}$$

3.1 EP Techniques for Communication:

3.1.1 QPSK DSSS

QPSK modulation one may transmit 2 different signals on the in phase / quadrature components of the same carrier, within the same bandwidth they are using the same frequency spectrum, one being reflected in the real part and one on the imaginary part the bandwidth occupied is

$B_{QPSK}=\max\{B^1_{BPSK}, B^2_{BPSK}\}$ eq (3)

Where B^2_{BPSK} represents the frequency bands occupied by the two BPSK signals apparent to the channels. The error probability for each channel is the same each of them can be seen as a separate BPSK signal; if the same signal is transmitted on both in phase /quadrature components the error probability decrease since the transmission redundancy increases coherent demodulation (carrier phase and frequency) must be known exactly at the receiver); In the case of spread spectrum signals the bandwidth is not anymore a restrictive parameter this type of modulation is used due to the fact that the quadrature transmission are harder to detect and less sensitive to several types of noises[4].

The general form for a QPSK narrowband signal is:

$s_d(t)=\sqrt{2}S[m_1(t)\cos w_0 t + m_2(t)\sin w_0 t]$

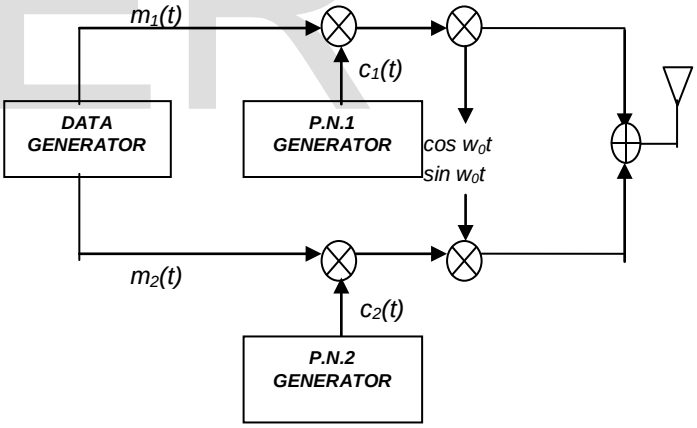
eq (4)

where $m_1(t)$, $m_2(t)$ represents binary data signals.

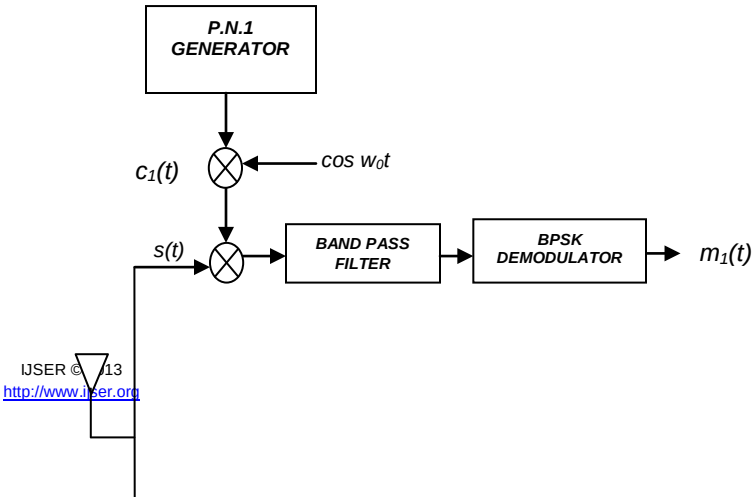
The QPSK DS-SS signal is obtained by multiplication of the two components, respectively in quadrature, with two pseudorandom codes c1(t), c2(t) respectively. In the general case c1(t) and c2(t) are complete independents, with the bit rate Rc1=1/Tc1respectively Rc2=1/Tc2, Rc1, Rc2 >> Rb. The mathematical expression of QPSK DS-SS signal is[3]:

$s_T(t)=\sqrt{2}S[m_1(t)\, c_1(t)\cos w_0 t + m_2(t)\, c_2(t)\sin w_0 t$ eq(5)]

The block diagram of a QPSK DS-SS transmission & reception system is represented in Fig4.



(a) Transmitter



→ $m_2(t)$

(b)Receiver

Fig 4. The block scheme of (a) QPSK DS-SS transmitter-(b) receiver system.

The received signal will be affected by the channel noise, interference and a t delay, if the estimation of both codes is correct, then

$c_1(t-\tau)\, c_1(t-\tau')=1$; $c_1(t-\tau)\, c_2(t-\tau')=0$

$c_2(t-\tau)\, c_2(t-\tau')=1$; $c_2(t-\tau)\, c_1(t-\tau')=0$

and the output signal of the band pass filters are:

$x(t)=\sqrt{S}m_1(t)\,(t-\tau)\, c_1(t-\tau)\, c_1(t-\tau')+\,)=\sqrt{S}m_2(t)\,(t-\tau)\, c_2(t-\tau)\, c_2(t-\tau')=\,)=\sqrt{S}m_1(t)$

$y(t)=\sqrt{S}m_1(t)\,(t-\tau)\, c_1(t-\tau)\, c_1(t-\tau')+\,)=\sqrt{S}m_2(t)\,(t-\tau)\, c_2(t-\tau)\, c_2(t-\tau')=\,)=\sqrt{S}m_1(t)$

so the two informational signal are recovered. In general this type of transmission, with two independent codes, it is used for the connection between satellites (TDRSS), with the mention that the in phase and quadrature, don't have equal powers. A simpler situation is the one that uses the same spreading code for both phase and quadrature signal. This system is balanced QPSK DS-SS (or 2 channel QPSK).

$s_T(t)=\sqrt{2}Sd(t)[m_1(t)\, c_1(t)\cos w_0 t+ m_2(t)\, c_2(t)\sin w_0 t$

eq(6)]

The transmitter and receiver scheme are almost identical with those presented in the figure.1. The only difference being that the correlation output data from the two channels are summed. The band pass filtering and QPSK detection is made after this summation[5].

Simulation is also carried out to compare the spectral response of spread and un-spread version of QPSK is shown in Fig.5.

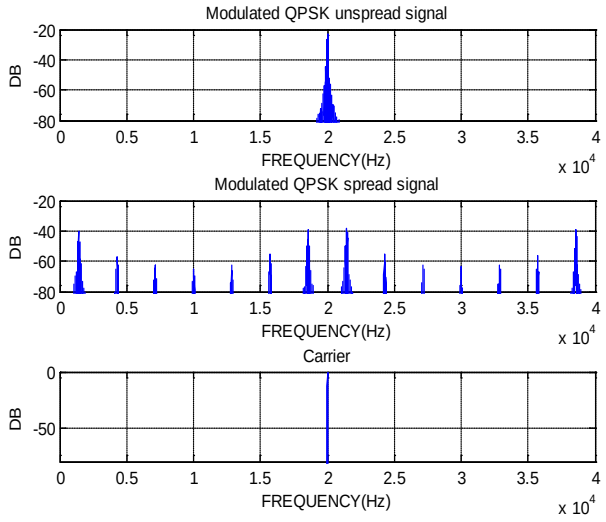


Fig.5: QPSK signal spectrum (spread and unspread conditon)

The DSSS signal under unspread condition is much below the noise threshold of the receiver.in such case a noise jammer signal with white Gaussian characteristics can resemble to DSSS signals under noise. The time and frequency domain representation of noise signals is shown in Fig. 6.

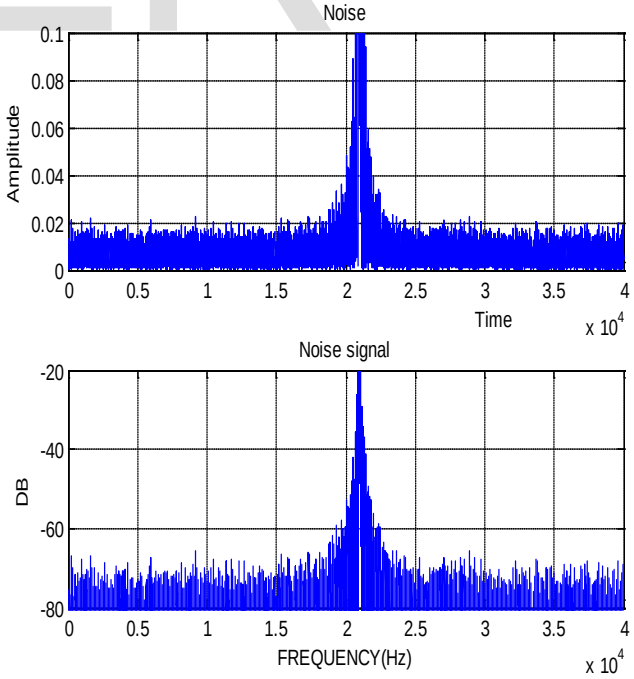


Fig.6 : Noise signals in (a) Time domain and (b) Frequency domain

T.1he demodulated response of I channel and Q channel of QPSK signals are shown in Fig 7.

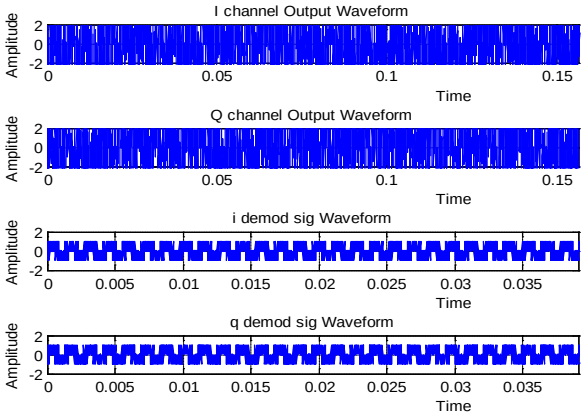
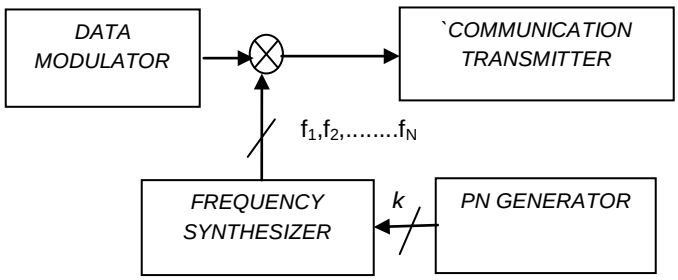


Fig. 7: After spreading demodulator output of QPSK

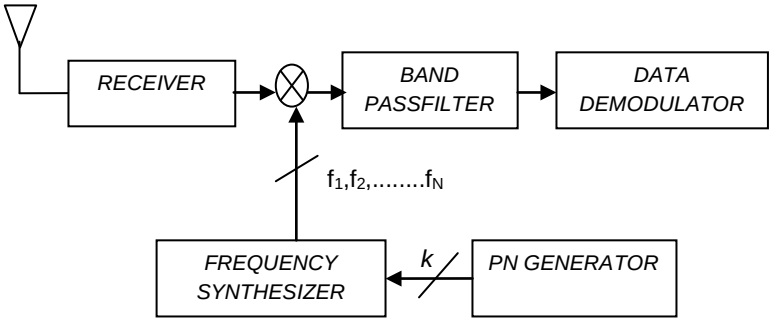
3.1.2 QPSK Frequency Hopping Spread Spectrum Signals (FH-SS):

In the case of Frequency Hopping Spread Spectrum signals – FH-SS the pseudorandom code is not used for a direct modulation of the data signal; hence, it is used to control the frequency synthesizer which chooses the carrier frequency that will be used in the next hopping interval. The spectrum spreading must be removed from reception the local frequency synthesizer (the same with the transmission one!!) is coordinated by a code signal which is synchronous with the one used at the transmitter[6]. If the code period Tc is greater than the data's one Ts the system is called with "slow frequency hopping"($T_c > T_s$), and if is smaller - "fast frequency hopping" ($T_c < T_s$),.

A block diagram of a transmission-receiver system with frequency hopping is represented in the figure 1.14. Note that, unlike the DS-SS signals, where every bit was used independently to modulate the data signal, in the case of FH-SS signals, k bytes of code are used at a given moment to choose one of the N=2k possible frequencies to be generated by the frequency synthesizer.



(a) Transmitter



(b) Receiver

Fig 8. Block scheme of a FH-SS transmitter-receiver system

Because of the major difficulties that rise from the hardware implementation of a coherent frequency hopping system, the frequency hopping systems use a non-coherent or partial coherent modulation for data. In this case, at the receiver is not necessary to rebuild the carrier phase. For frequency hopping system which uses a QPSK data signal, The data modulator will generate at the output one of the M= 4 possible tones on a duration of 2T seconds, where T=Tb represents the bit period. To ensure the orthogonality of QPSK modulated signal, the 2 hopping frequencies must be separated between them with at least 1/2T Hz, so the bandwidth occupied by QPSK signal is approximately 2/T. The simulated QPSK signal with frequency hop spreading spectrum and its FFT plot of FHSS are shown in Figs. 9 and 10 respectively.

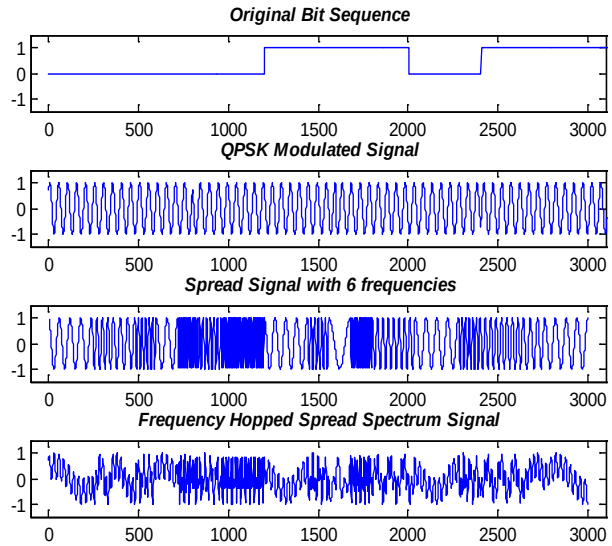


Fig.9 QPSK signal under frequncy hop spreading

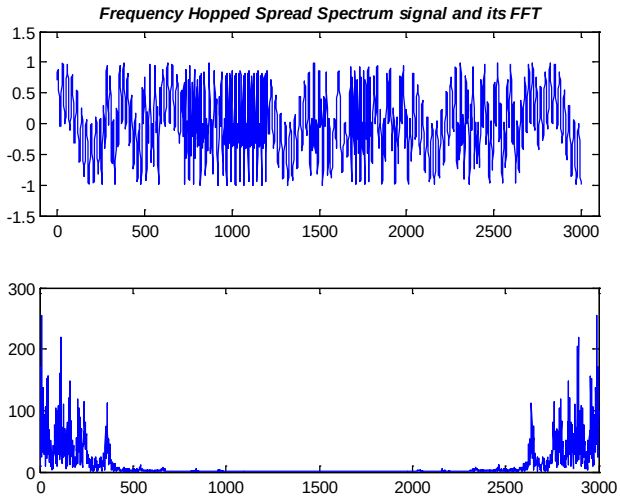


Fig.10:FFT of Frequency Hop Spreading

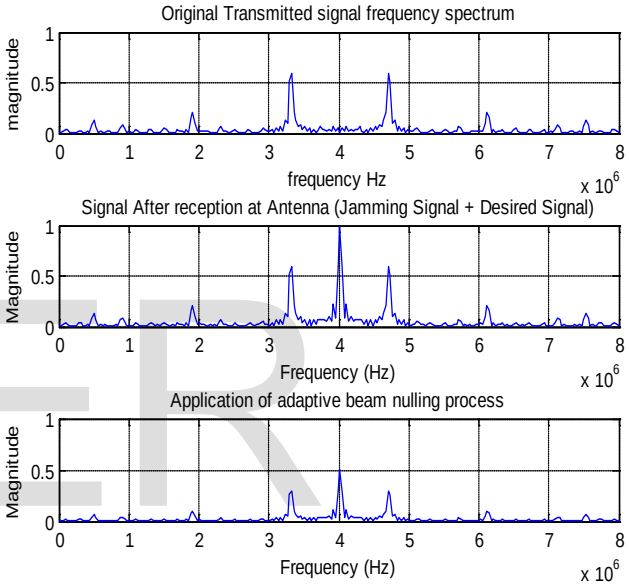
4 ADAPTIVE ARRAY ANTENNAS

This system uses the variety of new digital signal processing algorithms that have been developed to effectively locate and track various types of signals and dynamically reduce the interference due to jamming. These algorithms are used continuously to distinguish between desired signals, multipath, and jamming signals. They can also calculate direction of arrival because of the lobe formation.

This method of continuously updating the environment in which is communicating in is desired because it enables the system the ability to track the corresponding transmitter it is communicating with, smoothly using the main lobes. Since the main lobe is directly pointed to the desired transmitter, side-lobes are naturally formed so that null areas are formed that create minimal gain in directions that are not in the direction of the communicating receiver. This reduces the jamming performance in the system. The interference rejection capability of the system provides larger coverage than the other traditional or switched beam.

The switched beam antennas will suppress the interference in the environment and direct it away from the current center of the active beam in use. Switched beam solutions work with low interference, and may not be well suited for a high power jammer. A problem might araise that by jamming the antenna near the center of the active beam, the jamming signal can actually gain power than any of the actual desired signals in the system[7]. therefore adaptive arrays offer better jamming protection than switched beam and traditional antennas ,the main reason behind this enhancement is the improvement of making the elements in the array dynamic so that there can be an infinite number of combinations so that it can handle multiple jamming scenarios.

Simulation is carried out using Adaptive Beam Nulling algorithm. The desired signal is received through "**n**" element adaptive array removing the jammer signal by creating null along the jammer signal direction. The corresponding results is shown in Fig. 11.



Conclusion:

Modern communications systems are complex digital systems are operating under a number of frequency bands. Due to the technological innovation jammers are also developed to disrupt the operation of communication system by adversary. To counter the jamming some of EP techniques namely FHSS, DSSS and adaptive beam nulling are presented in this paper. Further work on anti-jamming can be carried out to counter the effect of different jamming scenario.

REFERENCES

[1] Moeness G. Amin, Senior Member, *IEEE."* Interference Mitigation in Spread Spectrum Communication Systems

Using Time-Frequency Distributions" IEEE transactions on signal processing, vol. 45, no. 1, January 2009.

[2] Bradley P. Badke, "Global Positioning System Anti-Jamming Techniques", *Ph.D Dissertation*, Arizona State University, 2002. Laurence B. Milstein, "Interference Rejection Techniques in Spread Spectrum Communications", Proceedings of the IEEE, Vol. 76,No. 6, June 2005.

[3] W.W. Jones, K.R. Jones, "Narrowband Interference Suppression Using Filter-Bank Analysis/Synthesis Techniques," IEEE MILCOMConference, San Diego, California, Paper 38.1.1, 2003.

[4] Laurence B. Milstein, "Interference Rejection Techniques in Spread Spectrum Communications", Proceedings of the IEEE, Vol. 76,No. 6, June 2002.

[5] Liang Zhao, Moeness G. Amin, and Alan R. Lindsey, "Subspace Projection Techniques for Anti-FM Jamming GPS Receivers",Proceedings of the Tenth IEEE Workshop on Statistical Signal and Array Processing, 2000.

[6] A. Vadhri, and "Rejection of Narrow-Band Interferences in PN Spread Spectrum Systems Using an Eigen analysis Approach",IEEE Seventh SP Workshop on Statistical Signal and Array Processing, pp.383-386, 2004.

[7] Paine, Andrew S. "An Adaptive Beam forming Technique For Countering Synthetic Aperture Radar (SAR) Jamming Threats "Radar Conference, 2007 IEEE Page(s): 630 - 634 2007