SIMULATED ASSESSMENT OF INTERFERENCE EFFECTS IN DIRECT SEQUENCE SPREAD SPECTRUM (DSSS) QPSK RECEIVER

THESIS

Luis S. Rojas, Captain, Chilean Air Force

AFIT-ENG-14-M-64

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-14-M-64

SIMULATED ASSESSMENT OF INTERFERENCE EFFECTS IN DIRECT SEQUENCE SPREAD SPECTRUM (DSSS) QPSK RECEIVER

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Luis S. Rojas, E.E.

Captain, Chilean Air Force

March 2014

AFIT-ENG-14-M-64

SIMULATED ASSESSMENT OF INTERFERENCE EFFECTS IN DIRECT SEQUENCE SPREAD SPECTRUM (DSSS) QPSK RECEIVER

Luis S. Rojas, E.E.
Captain, Chilean Air Force

Approved:

//signed//	11 March 2014
Dr. Richard K. Martin, PhD (Chairman)	Date
//signed//	11 March 2014
Dr. Robert F. Mills, PhD (Member)	Date
//signed//	11 March 2014
Dr. Michael A. Temple, PhD (Member)	Date

AFIT-ENG-14-M-64

Abstract

This research developed and validated a generic simulation for a direct sequence spread spectrum (DSSS), using differential phase shift keying (DPSK) and phase shift keying (PSK) modulations, providing the flexibility for assessing intentional interference effect using DSSS quadrature phase shift keying receiver (QPSK) with matched filtering as a reference. The evaluation compares a comprehensive pool of jamming waveforms at pass-band that include continuous wave (CW) interference, broad-band jamming, partial-band interference and pulsed interference. The methodology for jamming assessment included comparing the bit error rate (BER) versus required jamming to signal ratio (JSR) for different interferers using the Monte Carlo approach. This thesis also analyzes the effect of varying the jammer bandwidth for broad-band jammers including broad-band noise (BBN), frequency hopping interference (FHI), comb-spectrum interference (CSI), multi-tone jamming (MTJ), random frequency modulated interference (RFMI) and linear frequency modulated interference (LFMI). Also, the effect of changing the duty cycle for pulsed CW waveforms is compared with the worst case pulsed jamming equation. After the evaluation of different interferers, the research concludes that pulsed binary phase shift keying (BPSK) jamming is the most effective technique, whereas the CW tone jamming and CW BPSK interference result are least effective. It is also concluded that by finding an optimum bandwidth, FHI and BBN improves the required JSR by approximately 2.1 dB, RFMI and LFMI interference by 0.9 and 1.5 dB respectively. Alternately, MTJ and CSI improves their effectiveness in 4.1 dB and 3.6 dB respectively, matching the performance of the pulsed BPSK jammer.

Dedicated to my beloved wife and my funny little daughter.

Acknowledgments

I would like to express my gratitude to my advisor Dr. Richard K. Martin for the useful comments, remarks and engagement through the learning process here in AFIT. Furthermore, I would like to thank the Chilean Air Force for giving me the opportunity and for trusting in me to follow this master program. My sincere thanks also to the staff of the IMSO for its support and effort for my integration and adaptation since I arrived to AFIT. Also, I would like to thank my friend Nick Rutherford for his support and good time shared during this master program. Finally, I would like to thanks to my classmates Fawwaz Alsubaie, Matthew Crosser, Ethan Hennessey and Richard Rademacher, for interchanging experiences, knowledge and time regardless of language gap.

Luis S. Rojas

Table of Contents

Page

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
AWGN	additive white Gaussian noise
BBN	broad-band noise
BER	bit error rate
BPSK	binary phase shift keying
CDMA	code division multiple access
CSI	comb spectrum interference
CW	continuous wave
DPSK	differential phase shift keying
DBPSK	differential binary phase shift keying
DQPSK	differential quadrature phase shift keying
DRFM	digital radio frequency memory
DSSS	direct sequence spread spectrum
FCC	Federal Communication Commission
FHI	frequency hopped interference
GPS	Global Positioning System
ISI	inter-symbol interference
LFSR	linear feedback shift register
LFMI	linear frequency modulated interference
LPE	low probability of exploitation
LPI	low probability of intercept
JSR	jamming to signal ratio
MTJ	multi-tone jamming
NBN	narrow-band noise

Acronym	Definition
PSD	power spectral density
PSK	phase shift keying
PN	pseudonoise
PBN	partial-band noise
QPSK	quadrature phase shift keying
RFMI	random frequency modulated interference
RF	radio frequency
SNR	signal to noise ratio
SS	spread spectrum

SIMULATED ASSESSMENT OF INTERFERENCE EFFECTS IN DIRECT SEQUENCE SPREAD SPECTRUM (DSSS) QPSK RECEIVER

I. Introduction

1.1 Background

The spread spectrum (SS) technology has been crucial for enabling the coexistence of wireless devices in military and civil applications. According to [1] the origin of SS communication was a natural result of the battle for electronic supremacy after the Second World War.

The first public patent on SS was granted in 1942 and it came from Hedy Lamarr, the Hollywood movie actress, and George Antheil, an avant-garde music composer. Hedy Lamar got the idea from her previous husband who worked on wireless torpedo guidance and its vulnerability to jamming could be avoided by sending messages over multiple radio frequencies in a random pattern. This idea along with the music knowledge of Antheil yielded a solution to provide synchronization based on the 88 piano frequencies, consisting of two rolls perforated with the same pattern where every hole represent a different frequency and a mechanical device to keep the stability in the rotation frequency [2].

The concept of spreading information to avoid interference and increase range resolution was a familiar concept for radar engineers at the end of the Second World War. The SS concept was known and developed during the 1950s and helped by its implementation by the development of information theory contributions made by Claude E. Shannon who in 1947 published a paper revealing that a channel capacity can be maximized by spreading the signal. Shannon showed that the channel capacity was increased by

sending a set of noise-like waveforms and distinguishing them at the receiver via minimum distance criterion of the received signal and a stored waveform copy.

The correlation concept was first published in 1959 by a German scientist, F. H. Lange. It was possible because of the effort of Shannon and Norbert Wiener with his work in filter theory to reduce the noise presence in a signal by comparison with an estimated noiseless signal. However, since the 1960s most of the SS development occurred for military equipment. An important SS milestone was the publication of *Spread Spectrum Systems* by Robert Dixon in 1976 as the first comprehensive book with unclassified and commercial applications. During the 1980s another important milestone occurred with the first authorization for civil use of SS in 1985 by U.S. Federal Communication Commission (FCC) that marked a start point for the development of commercial spread spectrum devices in use today [3].

Nowadays, SS techniques are used broadly from military and civilian prospective with examples such as Wi-Fi, Bluetooth, and Zigbee. Special attention is focused on wireless sensor networks, cellular telephony, wireless tactical military communications due its mobility and flexibility, Global Positioning System (GPS), ranging system and data link systems. One spread spectrum technique with low probability of intercept (LPI), low probability of exploitation (LPE) and good response to unintended and intended interference is direct sequence spread spectrum (DSSS) since the energy of the transmitting signal is distributed across a bandwidth much wider than the message signal itself.

This research motivation consists of simulating a communication receiver that provides flexibility to assess different interference techniques typically studied for DSSS under the variations of jamming parameters. This evaluation gives a good approximation and baseline to evaluate complex communication jamming scenarios at low cost.

1.2 Problem Statement

The interference in communication systems and assessing its effects can be decisive for evaluating existing systems, predicting the quality of data transmission and achieving reliable communication of digital information. A practical way to evaluate the robustness of wireless communication systems is by doing on site testing but it can be costly in regards to availability of the service and resources required. Currently there is a variety of theoretical background on DSSS describing the effect of interference, however few papers in the open literature address simulation of a comprehensive pool of interference techniques or they study particular techniques in isolation. This research focused on developing a DSSS receiver and evaluating its performance in the presence of continuous wave (CW) interference, noise interference and pulse interference with flexibility to vary the jamming signal strength, bandwidth and transmission duty cycle. This simulation can provide a baseline to assess and discriminate the effectiveness of different interfering techniques in a DSSS quadrature phase shift keying (QPSK) communication system at low cost. The simulation is adaptable for adding more complexity and is a good tool for future research.

1.3 Assumptions and Resources

This research considers the interference evaluation of a DSSS receiver for a single user neglecting the environment effects and the angle-of-arrival of the interfering signals. This means that received signals are assumed to arrive in the antenna bore-sight where the desired signal has a constant power simulating a cooperative transmitter with fixed distance to the receiver. Also the interference assessment assumes a coherent receiver with ideal carrier demodulation that neglects phase errors and mixer losses. The despreading mixer considers a Gold sequence that is a perfectly synchronized with the received desired signal while neglecting delays for multi-path using an ideal additive white Gaussian noise (AWGN) channel. The phase shift keying (PSK) DSSS receiver utilized for assessing the

simulated jamming techniques was implemented in MATLAB® and the Communication System Toolbox™, version 2013b.

1.4 Thesis Organization

The thesis has been organized in five chapters. Chapter II provides the basic concept of DSSS and typical implementations, the characteristics of pseudonoise (PN) sequences used in DSSS, the concept and classification of jamming techniques, the properties of interference reduction in DSSS and previous work in DSSS jamming. Chapter III presents the methodology and the receiver model implemented along with the description of the different jamming models simulated. Chapter IV provides evaluation results for different jamming techniques and the effects of varying parameters such bandwidth and duty cycle to optimize the jamming response. Chapter V presents the conclusions, summarizes the thesis and provides future areas of research.

II. Direct Sequence Spread Spectrum Theory

2.1 Introduction

This chapter provides general concepts of spread spectrum theory, the DSSS receiver model, the characteristic of PN sequences implemented in DSSS, a general description of DSSS interference rejection capability along with typical jamming classification schemes. Finally, some references and related DSSS interference work is provided.

2.2 Spread Spectrum Communications

In a communication system the modulated waveform occupies a bandwidth that is dependent on the modulation order (bits per symbol) and the modulation technique. In a SS system the transmission bandwidth is much higher than the minimum bandwidth required to send information. The spreading bandwidth is accomplished by a spreading signal with noise-like characteristics that are independent of the data intended to transmit. The signal recovery or despreading is achieved by correlating the incoming signal with a synchronized replica of the spreading signal used to spread the information.

Spread spectrum can be classified according to the following modulation formats:

- Direct sequence (DSSS): a form of phase-shift keying modulation.
- Frequency hopping (FHSS): a narrow-band frequency-shift keyed signal is hopped over a wide band using pseudo-random carrier frequency selection.
- Time hopping (THSS): similar to frequency hopping but the PN sequence selects a transmission time (slot) within consecutive time frames (a low duty cycle or burst).
- Hybrid: that combines any of the three main types.

This research focused on DSSS modulation implemented as two stages of modulation type: 1) the incoming data sequence is used to modulate a wide-band code, transforming

the narrow-band data sequences into a noise-like signal, 2) a second modulation using a selected phase shift keying technique.

2.3 Direct Sequence Spread Spectrum System Model

Direct sequence spread spectrum modulation can be defined as a means of transmission such as the data sequence is spread by using a code that is independent of the data sequence. The concept of spreading implies a bandwidth expansion far beyond that it is required to transmit the digital data. For instance a requirement to transmit information using a data R_d = 200 Kbits/s occupying a spectrum bandwidth W_{ss} = 200 MHz has a spreading factor of 10^3 as the ratio between the spreading bandwidth and the signal bandwidth.

The unique characteristic and purpose of DSSS modulation is that provides interference suppression, energy density reduction, ranging or time delay measurement [4]. The interference suppression can be a combination of the presence of users with the intention of disrupt the communication (jammers or interferer) or users that independently share a common channel without an external synchronization (multiple access communication). Also multi-path is considered as self interference that is mitigated by spread spectrum techniques, where delayed versions of the signal arrive to the receiver using alternate paths.

The energy density reduction of spread spectrum provides low probability of interception and low probability of exploitation. Those characteristics are important to design a communication system that meets regulations of signal strength, to minimize detectability and to obtain privacy.

With respect to range delay measurement spread spectrum provides low error in successive pulse time delay measurement, since the error is inversely proportional to the spread spectrum signal bandwidth.

A simplified baseline model of DSSS system is depicted in Figure 2.1 [5]. The information signal $x(t)$ represents an antipodal pulse stream with values ± 1, with a given data rate which is modulated by multiplying it with carrier signal $\sqrt{P}\cos\omega_o t$. The resultant

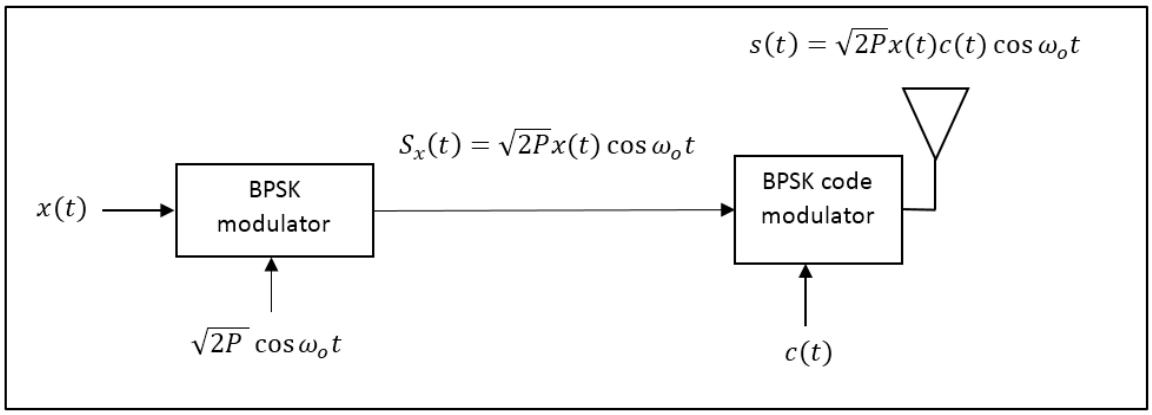

Figure 2.1: DSSS BPSK modulator [5] .

product is a binary phase shift keying (BPSK) signal $S_x(t) = x(t)\sqrt{P}\cos\omega_o t$. The BPSK signal is multiplied by an spreading sequence $c(t)$ with a much higher data rate called chip rate. The effect is a bandwidth expansion given by the convolution of $S_x(t)$ and $c(t)$ in frequency domain. Thus if the signal $S_x(t)$ is narrow-band, then the resulting product $S_x(t)c(t)$ is effectively spread a bandwidth approximately equal to the spreading signal.

At the receiver, as is shown in Figure 2.2 [5], the original signal is recovered ideally by a synchronized replica of the spreading signal. The parameter $\hat{T}_d$ is a delay estimate of the propagation time from the transmitter to receiver. The signal $r(t)$ is considered without interference with constant system gain A and a random phase ϕ in the range from $(0, 2\pi)$. For spread signal $c(t) = \pm 1$, then the product $c(t - T_d)c(t - \hat{T}_d) = 1$ for optimum synchronization with $T_d = \hat{T}_d$. For a synchronized signal, the correlator output is the despread modulated signal (considering a random phase and delay T_d.) Subsequently the signal is filtered in order to remove high frequency components and finally demodulated using a conventional demodulator. Any unwanted signal will be spread by the same bandwidth. The advantage in terms of interference rejection is given by the fact that the

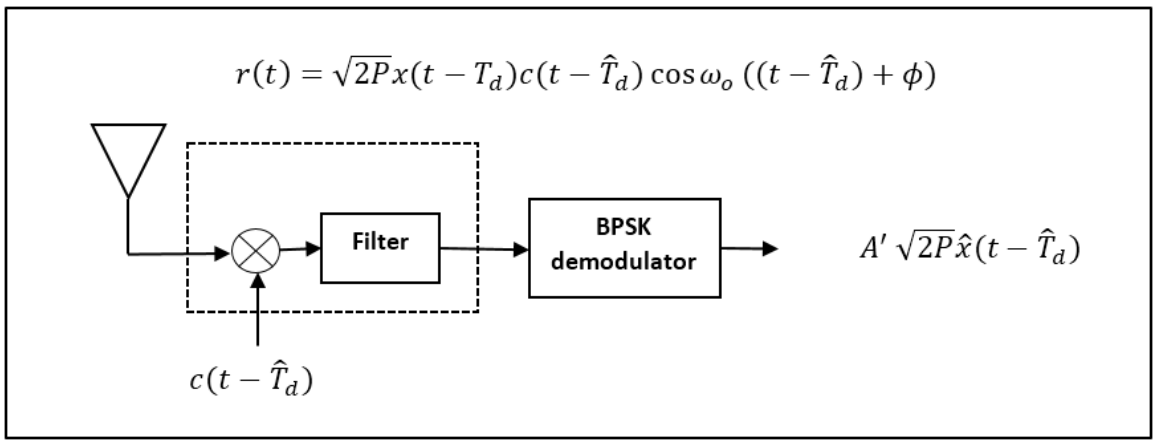

Figure 2.2: DSSS BPSK demodulator [5].

incoming signal is multiplied just one time in the receiver whereas the transmitted signal is multiplied two times in order to recover a good estimate of the original signal $x(t)$.

2.4 Pseudonoise (PN) Sequences

There are two main mechanisms for spreading the signal: transmitted reference (TR) and stored reference (SR).

The first considers two channels, one for transmitting the data and other for the spreading waveform which is randomly generated. The main advantage of TR is that it achieves synchronization easily. However this method has some disadvantages such as the code is available for any unintended users, the performance degrades at lower signal to noise ratio (SNR) and it requires a greater bandwidth and power to transmit.

The SR method requires a single channel to generate a pseudo-random spreading signal which is generated independently by transmitter and receiver. The disadvantage of this technique is that synchronization is more complex to achieve. However depending on the code it cannot easily be predicted or exploited by an unintended receiver.

A PN sequence is defined as a deterministic periodic sequence because it is known by the transmitter and receiver. PN sequence has the main property that statistically is similar to white noise. The main properties of PN sequences are the following:

- Balance property. The number of binary ones differs from the number of binary zeros by at most one digit.
- Run property. A run is defined as a sequence of a single type of binary digits. Among the run of zeros and ones it is desirable that one half of the runs of each type are of length 1, about one fourth of the length 2, one eight of length 3, and so on.
- Correlation property. If a period of the sequence is compared term by term with a cyclic shift of itself, the number of agreements differs from the number of disagreements by no more than one count.

The normalized autocorrelation for a PN coded waveform $x(t)$ with period T can be defined as:

$$R_x(\tau) = \frac{1}{K}\left(\frac{1}{T}\right)\int_{-\frac{T}{2}}^{\frac{T}{2}} x(t)x(t+\tau), \mathrm{d}t \quad \text{for } -\infty < \tau < \infty, \tag{2.1}$$

$$K = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} x(t)^2, \mathrm{d}t \quad \text{where } K \text{ is the energy of the signal.} \tag{2.2}$$

For a PN waveform of unit chip duration and period p chips, the normalized autocorrelation function can be expressed as

$$R_x(\tau) = \frac{1}{p}\left(\left|\frac{agreements - disagreements}{length\ of\ sequence}\right|\right). \tag{2.3}$$

Typically a PN sequence can be generated using a linear feedback shift register (LFSR) whose output is defined by the number of register stages. A maximal length sequence has a period given by $p = 2^{n-1}$, where the each sequence is repeated every p clock pulses.

Figure 2.3 shows a linear shift register [5] example of four stages $X1, \ldots, X4$. A sequence is controlled by a clock pulses (not shown). At each clock pulse the content of

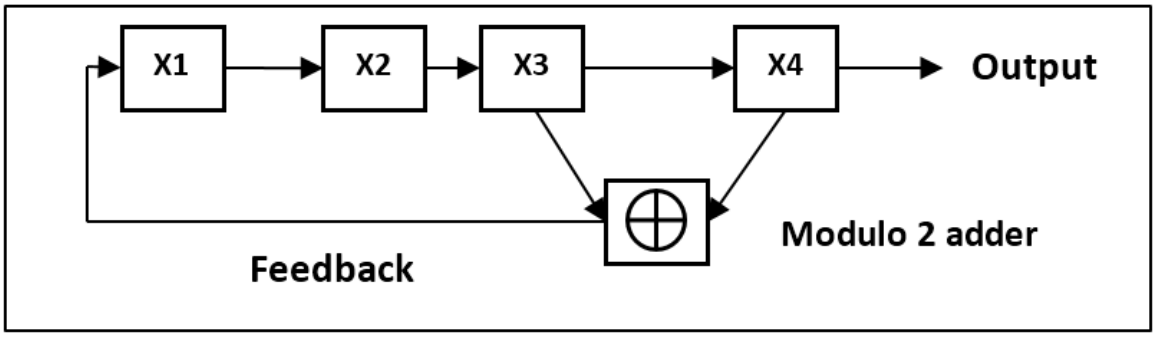

Figure 2.3: Linear feedback shift register [5].

the register is shifted by one stage to the right. Also in each clock the stage $X3$ is modulo 2 added to stage $X4$ and fed back to the stage $X1$.

There are two classes of PN sequences; aperiodic and periodic. An aperiodic sequence does not repeat itself in a periodic way whereas the latter is a sequence that repeats itself exactly with a specific period.

An aperiodic sequence can be described analytically by a sequence of N plus or n minus ones as follows:

$$a_1, a_2, \ldots, a_n, \quad a_i = \pm 1. \tag{2.4}$$

The aurocorrelation of a PN sequence is defined by:

$$C(k) = \sum_{n=1}^{N-k} a_n a_{n+k} \quad k = 0, 1, \ldots, N-1. \tag{2.5}$$

As an example of autocorrelation in aperiodic sequence, consider a sequence of four digits of plus or minus ones from a_1 through a_4. The autocorrelation for $C(1)$ is obtained by shifting the sequence by one symbol:

$$\begin{array}{cccccc} & a_1 & & a_2 & a_3 & a_4 \\ a_1 & a_2 & & a_3 & a_4 & \\ \hline \mathrm{C}(1) & = & a_1a_2 + a_2a_3 + a_3a_4 & & & \end{array}$$

An ideal aperiodic sequence would have an autocorrelation function given by:

$$C(k) = \begin{cases} N, & k = 0 \\ 0 \quad \text{or} \pm 1, & k \neq 0 \end{cases} \tag{2.6}$$

Such sequences are called Barker sequences and only exist for a few values of N. Specifically they have been found for N=1, 2,3,4,5,7,11 and 13. This kind of sequences is too short as a spreading function and normally is used for synchronization purposes [6].

In a spread spectrum communication system it is important to have sequences where the autocorrelation function is large at zero lag because the synchronization can be accomplished. On the other hand, at non-zero lags it is desirable that the autocorrelation be low in order to avoid false synchronization. Besides, the cross-correlation between the sequences used by two communication systems should be low even at zero lag in order to avoid false correlation between two systems.

A periodic sequence consists of an infinite sequence of plus or minus ones divided into blocks of length N, where each particular block is the same. A periodic sequence can be represented as follows [6]:

$$\ldots, a_{N-1}, a_N, a_1, a_2, \ldots, a_N, a_1, \ldots$$

In every period the number of plus ones differs from the number of minus ones by exactly one. Hence N is odd number. Thus

$$\begin{aligned} N_+ + N_- &= N, \\ |N_+ - N_-| &= 1. \end{aligned} \tag{2.7}$$

In every period half of the runs of the same sign have length 1, one fourth have length 2, one eight have the length 3, and so forth. Also the number of positive runs equals the number of negative runs. The autocorrelation of a periodic sequence is two valued. That

is, it can be described by:

$$C(k) = \sum_{n=1}^{N} a_n a_{n+k} = \begin{cases} N, & k = 0, N, 2N, ... \\ -1, & \text{otherwise} \end{cases} \tag{2.8}$$

where

$$a_{n+N} = a_n. \tag{2.9}$$

In this research the simulation will use a periodic code broadly implemented in code division multiple access (CDMA) and GPS systems which is a Gold code. This code is generated by a modulo-2 operation between two different preferred m-sequences. The preferred m-sequence operation consists of choosing a reference m-sequence with a shifted version or vice-versa. Using two sequences with equal length N, the resultant Gold sequence is N length as well. For a period $N = 2^n - 1$, there are N possible circular shift. Then it is possible to obtain N sequences from two preferred m-sequences. The Gold sequence generated is not an m-sequence with two correlation values instead it has three low correlation values. The autocorrelation r_{xx} and cross-correlation r_{xy} function for this Gold sequence can be represented by [7]:

$$r_{xx}(\tau) = \begin{cases} 1, & \text{for } \tau = 0 \\ \left\{ \frac{-t(n)}{N}, \frac{-1}{N}, \frac{t(n)-2}{N} \right\} & \text{for } \tau \neq 0 \end{cases} \tag{2.10}$$

and

$$r_{xy}(\tau) \in \left\{ \frac{-t(n)}{N}, \frac{-1}{N}, \frac{t(n)-2}{N} \right\}. \tag{2.11}$$

where

$$t(n) = \begin{cases} 1 + 2^{\frac{n+1}{2}} & \text{for } n \text{ odd} \\ 1 + 2^{\frac{n+2}{2}} & \text{for } n \text{ even} \end{cases} \tag{2.12}$$

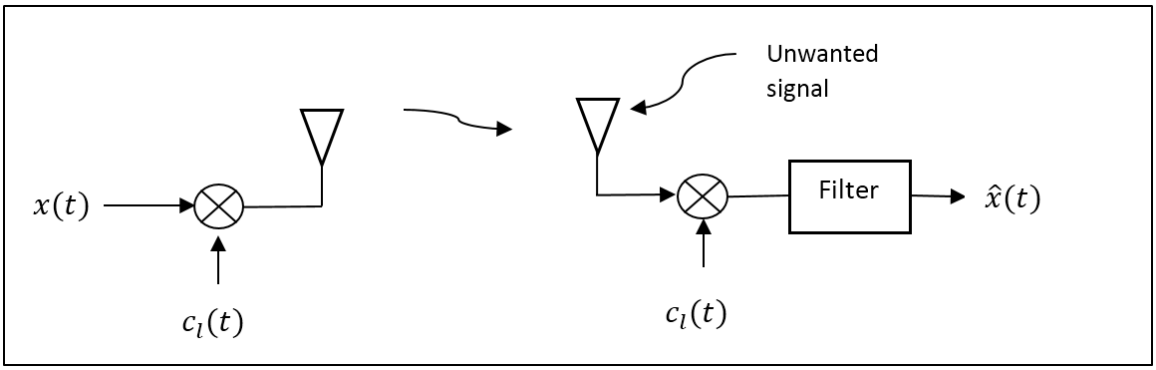

Figure 2.4: Basic DSSS with interference signal [5].

The Gold peak correlation value is $t(n)/N$ and from the above equation less correlation values occur when n is odd. Where n is the stage number or polynomial degree of the two preferred m-sequences.

2.5 Interference in Direct Sequence Spread Spectrum Systems.

The main advantage of spread-spectrum waveforms is their ability to reject interference. The source of interference can be produced by authorized users transmitting simultaneously, or also by a hostile transmitter with the intention of jamming a determined channel [8]. In Figure 2.4 is represented a basic DSSS to illustrate the interference rejection capability: the energy in signal $x(t)$ is spread across a bandwidth given by the multiplication with a PN sequence $c(t)$ and then in the receiver it is multiplied by $c(t)$ again. On the other hand any non-spread interference signal will be multiplied just one time by the spreading replica $c(t)$ when received.

Jamming a communication system implies an intentional and deliberate transmission or retransmission of amplitude, frequency, phase, or otherwise modulated pulsed, CW, or noise-like signals for the purpose of interfering with a receiver [9].

Spread spectrum techniques consider many orthogonal signal coordinates coexisting in a link where only a portion of that signal is present at a given time. The total space of

a signal of bandwidth W and duration T is given by $2WT$ [10]. The intended interference presents a finite power and an ambiguity about the signal coordinates and parameters. Then there are two main possibilities. To jam all space of possible signals present with the power distributed across the bandwidth or to interfere some signal coordinates with different levels of power. The processing gain is an important parameter to measure how the signal spread is resilience to interference. The general expression is given by:

$$G_p = \frac{W_{ss}}{W_{min}} = \frac{R_c}{R_d}, \tag{2.13}$$

where W_{ss} is the spreading signal bandwidth for a chip rate R_c and W_{min} is the minimum required bandwidth of the signal to transmit at data rate R_d.

2.6 Interference Techniques Classification

The main waveforms for generating interference can be divided into the following categories:

- Noise jamming. This waveform consists of injecting interference signal to the receiver with the goal of covering the desired signal by a band limited white Gaussian noise of high power. The main advantage of noise jamming is that it does not require more detailed information about the communication beyond its spread bandwidth [8]. In this technique the jamming carrier signal is modulated with random noise. Depending on the bandwidth available noise jamming technique includes [11]:
  - Broad-band noise. The intended interference energy is distributed through the entire receiver bandwidth. The effect of this technique is to reduce the channel capacity by affecting the SNR at the receiver.
  - Narrow-band noise. The interference energy is distributed over a single channel bandwidth or fraction of that channel bandwidth.

– Partial-band noise. The interference energy is transmitted across multiple channels not necessarily contiguous.

Noise jamming also is related to the communication system channel capacity (C), that is the maximum rate at which the information can be transmitted. It considers a band-limited channel with white noise and with signal power constraints represented by:

$$C = B\log_2\left(1 + \frac{S}{N_o B}\right) \tag{2.14}$$

where:

$$\begin{aligned} C &= \text{Channel capacity in bits/seconds.} \\ B &= \text{Channel bandwidth in Hz.} \\ S &= \text{Average received signal power in the channel bandwidth in Watts.} \end{aligned} \tag{2.15}$$

$N_o B$ =Average noise power in Watts, noise spectral density and bandwidth product.

$\frac{S}{N_o B}$ =Signal to Noise Ratio.

In terms of interference if the average noise power increases by adding intended interference, the channel capacity is affected by SNR reduction in the presence of noise.

- Tone jamming. In this technique one or more carrier frequencies (tones) are transmitted wisely in order to interfere one or more channel simultaneously. Depending on the tones transmitted the technique is called single tone or multi-tone jamming (MTJ). Single tone jamming consists of transmitting an unmodulated carrier with an average power J_p within the spreading bandwidth. In general tone jamming can be effective in DSSS systems if jammer power overcomes the processing gain and if its frequency is centered in the spreading bandwidth. The phase difference between the jammer and target signal has an effect in the power

processed at the receiver, then at more phase difference more power is required to overcome the processing gain. In frequency hopping multi-tone jamming (MTJ) jamming is applicable, however it requires high synchronization and coherency in phase between the jammer signal and target signal, since the energy is distributed in multiple frequencies.

- Pulse jamming. Pulse jamming is similar to the concept of partial-band noise. The transmission is performed over multiple channels by exploiting the concept of duty cycle with the intent of affecting the target signal a fraction of the time the jammer is on. The interferer transmits a pulsed bandlimited white Gaussian noise signal with a power spectral density (PSD) that covers the spread spectrum system bandwidth. The interference duty factor can be denoted by ρ_c representing the ratio of time when the jammer is on relative to the total interval (on and off time). The average interference power J_p with a bandwidth B can be expressed as:

$$J_p = BJ_o\rho_c, \tag{2.16}$$

  where J_o is the constant jamming PSD in Watts/Hz.

- Repeater Jammers. This jamming technique consists of a transceiver that senses and estimates the spread spectrum signal parameters and then amplifies and retransmits the signal with high power. This jamming technique tries to deal with the main strength of spread spectrum which is the generation of a high processing gain on the receiver such that an interferer with no spreading sequence knowledge or spreading sequence estimation requires a high level of power, depending on the spreading sequence length, to induce errors and affect the receiver performance.

From the jammer signal perspective, noise jamming techniques require more power to overcome DSSS the processing gain. If the jammer is able to sense the incoming DSSS signal and replicate it while keeping certain correlation properties, then it is expected to require less power for a given effectiveness.

Under the repeater jammer are jamming techniques that try to disrupt portions of the digital signal required to deny communication. The goal is attack the receiver during the acquisition time of new signals or users. For DSSS signals, this interval consists of detecting the magnitude of a tolerance margin out of phase of the signal. This is a decision circuit that accepts synchronization of a received signal after detecting a certain energy level after cross-correlating to despread the signal. The time of tolerance for synchronization is on the order of $\pm T_c$.

2.7 Related Work

The main sources of open literature that treat interference or jamming in DSSS, presents analytical expressions for noise interference considered as AWGN that increases the receiver noise floor and the receiver performance. For a particular kind of modulation the jamming symbol error probability is derived from their respective symbol error rate or bit error rate expressions. In general this type of interference is described as a Gaussian process and represents the baseline jammer performance. The effectiveness is primarily a function of theDSSS processing gain. However, particular implementations can have different results and 1) there is no particular jamming technique that affects all spread spectrum systems equally and 2) there is no a single spread spectrum that performs best again all jamming waveforms [12]. The analytical results for partial-band noise, single-tone and pulse jamming can be found in [13], [7], [11] and [12]. The theoretical and mathematical analysis for uncoded and coded BPSK DSSS are covered in [13] and [12], including block and convolutional coding.

Other approaches in interference analysis are described as a denial of service in wireless computer sensor network and as radio frequency (RF) layer interference analysis. Authors [14] explore the concept of distributing k interferer nodes to put N nodes out of service. In sensor networks some strategies consist of identifying the jamming area and mapping the network traffic using alternate routes. Managing the power and prioritizing

the traffic are other strategies mentioned to cope with jamming. Authors [15] generalize jamming classes in sensor networks as active jamming and intermittent jamming. The first is based on keeping the channel busy most of the time with a goal to saturate or disrupt communication. The latter considers a trade-off between energy efficiency and interferer effectiveness but requires more knowledge of the network protocols. A general classification for RF intended interference considers the following categories: broad-band noise, partial-band noise, continuous wave jammers, pulse jammers and multi-tone jammers [12], [16].

Other work that describes physical RF interference is [17] that covers the implementation of a real-time reactive jamming (sense and then interfere) on software-defined radio and evaluation of their performance at physical layer on simulated IEEE 802.15.4 in terms of packet reception ratio. The three techniques analyzed include noise jamming (always is present in wireless communication then is the primary source of RF jamming to consider), single tone jamming and modulated jamming. The simulation results in that single-tone (continuous jamming) is the most effective technique in terms of the effectiveness and required jamming gain. The modulated jamming consists of generating the same modulation of the target signal with the idea of breaking synchronization by imitating the preamble and header of transmissions, however to produce similar effects to single-tone jamming significant more jamming power is required. Noise jamming technique also requires more interference power but significantly less than that required for modulated jamming.

The linear frequency modulated interference (LFMI) interference and comb spectrum interference (CSI) are mentioned in [18], [19] as a critical interference source to DSSS, describing mechanism to suppress this interference based on time-frequency representation. Other work that considers simulation of RF jamming techniques was found in [20] where broad-band noise, partial-band noise, multi-tone and frequency, follower jamming are considered on a network users the 802.11p protocol in AWGN and vehicular

channels. This study showed that in orthogonal frequency-division multiplexing (OFDM) signaling under an AWGN channel, partial-band noise and multi-tone jamming (knowing the pilot frequency locations) have more significant effects. Under vehicular channel the study showed that partial and broad-band noise have more significant effects in terms of frame error rate for a given jamming to signal ratio.

Repeater jamming applied to DSSS systems previous works is addressed in [21]. This paper discusses uncorrelated jamming techniques and their respective probability of bit error performance, then it simulates a repeater jamming based on digital radio frequency memory (DRFM) technology to generate correlative jamming technique. DSSS techniques spread the energy of the baseband signal over a wide bandwidth, then they make it difficult to sense the electromagnetic spectrum and then provide an intended interference or jamming. The author shows that non-correlative jamming techniques such as narrow-band noise (NBN), partial-band noise (PBN) and tone jamming applied to DSSS require high power levels to overcome the integration gain due to PN characteristic of coding process. Consequently, the energy which is not synchronized with the PN is spread in the decorrelation process at the receiver. Besides, DSSS receiver could implement adaptive interference mitigation, notch filters and prediction filter. This paper discuses the interference on DSSS acquisition code and obtains the probabilities of bit error for non-fading and Rayleigh fading environment. This research concludes after comparing noise jamming techniques and a correlative jamming technique that the latter is more effective.

Other research related to repeater jamming is described in [22]. This work includes a design and simulation of a jammer technique generated by using a compressive receiver model and adaptive signal extraction. The main task of the jammer is to capture the DSSS transmitted signal that has been corrupted with AWGN. The author proposes a model of compressive receiver that performs a continuous and fast scan over the DSSS frequency band. The output of the compressive filter has the energy at certain times that

correspond to the frequency of the input signal. The signal received is passed through the autocorrelator and then the Levinson-Durbin algorithm is applied. The filter response to a pulse train is dynamically changing (which is an estimate of the shape being transmitted by the DSSS transmitter) and is to be transmitted by the jammer. Then it compares the modem performance without jamming and the modem performance in the presence of jamming.

III. Methodology

This chapter describes the approach and methodology for evaluating different interference techniques in generic DSSS PSK and differential phase shift keying (DPSK) receivers. The chapter includes a description of the evaluation parameters, the PSK/DPSK transmitter and receiver developed and jammer models used for the assessment of different techniques applicable to DSSS.

3.1 Approach

This thesis evaluates the performance of a DSSS QPSK receiver using Gold sequence in terms of BER with different jamming waveforms present. First the research develops and validates synchronized DSSS PSK/DPSK receivers in an AWGN channel. Then this work simulates different jamming waveforms in a DSSS QPSK receiver determining the jamming to signal ratio (JSR) to achieve a frame of reference or jamming margin. Consequently, comparison and analysis are performed including the parameters variations yielding the most effective jamming.

3.2 Evaluation Techniques

The present research methodology evaluates the receiver BER under interference conditions using Monte Carlo performance evaluation. This method is a numeric computation of the BER as the ratio of the number of bits transmitted with error over the total transmitted bits. The errors are produced by the AWGN introduced in the channel which correspond to generating N independent Gaussian random variables with zero mean and variance σ^2 added to an observation vector (information symbols). The errors are counted at every symbol interval by comparing the received symbols and sent symbols and consequently symbols are mapped to bits to compute the BER. This process is repeated K times until a required number of errors are obtained. For interference evaluation the same

methodology is applied in order to estimate the BER when the intended interference signal is added to the channel for a given interference power level.

The probability evaluation consists of:

1. Count the number of times that estimated received bits are different from the transmitted bits. This is the condition for estimating the BER.
2. Estimate the probability as the ratio of the number of times that the condition is satisfied over the number of trials or number of bits required.

The Monte Carlo simulation provides an estimated probability and the number of realizations affect the result [23]. From the simulation perspective it is important to define a tolerance margin or error. The absolute error accounts for the difference between the true probability or ideal BER (P) and the estimated or simulated BER ($\hat{P}$).

$$\epsilon = \frac{\left|P - \hat{P}\right|}{P}. \tag{3.1}$$

Once a desired absolute error is chosen a confidence interval is required to determine a $100(1-\alpha)\%$ of the time the error will be present. Then the number of iterations K should satisfy:

$$K \geq \frac{\left[Q^{-1}(\alpha/2)\right]^2 (1-P)}{\epsilon^2 P}. \tag{3.2}$$

To evaluate system performance, simulated results are compared with analytical expression of receiver performance in terms of BER and the information is presented in plots of BER vs JSR and E_b/N_o.

One of the most important parameters, based on how efficiently in terms of energy a system transmits the information, is the energy per bit to noise power spectral density ratio E_b/N_o because it accounts for the noise in the channel. The E_b/N_o and energy per symbol to noise power spectral density ratio E_s/N_o relation is given by

$$\frac{E_s}{N_o} = \frac{E_b}{N_o} \log_2 M = k \frac{E_b}{N_o}, \tag{3.3}$$

where $\log_2 M$ represent the number of k bits per symbol given modulation index $M = 2^k$. The relation between SNR and E_s/N_o is given by the noise bandwidth and signal bandwidth utilization and the importance of this metric is that it allows evaluation of system performance at specific points in the receiver. The mathematical expression for E_s/N_o:

$$\frac{E_s}{N_0} = \frac{S}{N/B_n} \cdot T_s = \frac{S}{2N} \cdot F_s \cdot T_s, \tag{3.4}$$

where:

- S is the average signal power in Watts.
- N is the average noise power in Watts.
- B_n is the noise bandwidth equivalent to $F_s/2$ for positive frequencies in Hz.
- F_s is the sampling frequency in Hz.
- T_s is the symbol duration in seconds.

The parameter used to evaluate the interference effects on the receiver is the JSR. It is also called the jamming margin of the spread spectrum system, which is the largest JSR considered to satisfy specific BER performance. In the present thesis, this scalar is computed with the goal of determining the JSR required to affect the system BER performance one order-of-magnitude. Therefore the receiver performance at a specific SNR point is considered and then a range of JSR is simulated to determine the JSR value where the BER is degraded by one order-of-magnitude relative to no interference being present. A mathematical expression for JSR and its relation with E_s/J_o can be obtained from:

$$E_s = S \cdot T_s = \frac{S}{R_s}, \tag{3.5}$$

where R_s is the symbol rate in symbols/s. The jamming power spectral density (Watts/Hz) across spreading bandwidth W_{ss} can be expressed as:

$$J_o = \frac{J}{W_{ss}}. \tag{3.6}$$

From Equation (3.5) and Equation (3.6)

$$\frac{E_s}{J_o} = \frac{S/R_s}{J/W_{ss}} = \frac{W_{ss}/R_s}{J/S} = \frac{G_p}{J/S}, \tag{3.7}$$

and

$$G_p = \frac{W_{ss}}{W_{min}} = \frac{R_c}{R_s} = \frac{T_s}{T_c} = N_c. \tag{3.8}$$

G_p is the bandwidth expansion factor, or processing gain, of the DSSS receiver and is equivalent to the number of chips N_c per symbol duration due to $T_s = N_c \cdot T_c$.

3.3 Direct Sequence Spread Spectrum Model

The transmitter model for simulation is presented in Figure 3.1 [24], where the digital baseband pulse modulation and pulse shaping filters, were adopted from Communication System Toolbox™, MATLAB® functions, version 2013b. A message source generates a stream of random bits that are grouped according to a modulation index M as k bits per symbol where $k = \log_2(M)$. According to the phase modulator, the symbol representation has M constellation points. Next, the baseband symbol representation is up-sampled and passed through a square root raised cosine filter to reduce the inter-symbol interference (ISI) and adapt the signal to the communication channel. The cascade connection of the up-sampler and the low pass filter is called the interpolator. In this implementation, the up-sampling factor is 403 samples per symbol and the low pass filter (pulse-shaping filer) has gain unity and a filter order in symbols corresponding to 8 symbols. Other design

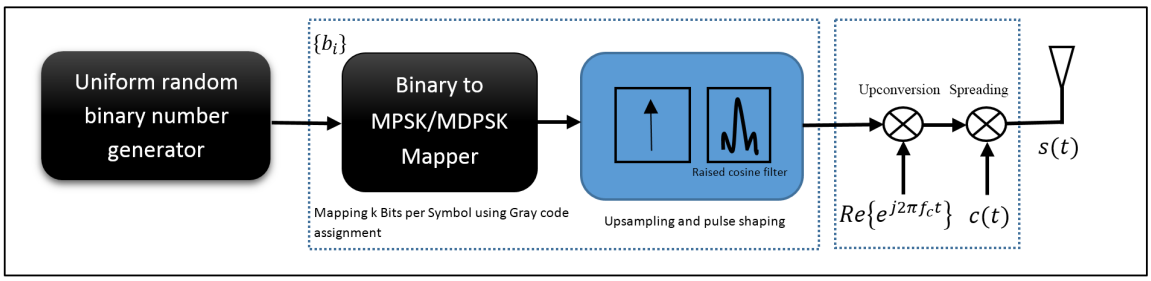

Figure 3.1: DSSS Transmitter Model [24].

parameters include the roll-off factor as a measure of bandwidth occupied over the Nyquist bandwidth $1/2T_s$ where T_s is the symbol duration. Figure 3.2 shows the low-pass root raise cosine filter response implemented using a roll of factor of β=0.2. For a symbol duration T_s=1 ms it implies an excess bandwidth of Δf=100 Hz given by $\beta/(2T_s)$.

Then the baseband signal is modulated by taking the real part of the product of complex carrier signal and complex baseband symbols. Finally the passband signal is spread by using an antipodal Gold coded waveform $c(t)$ of 31 chips. The transmitted spread signal is $S(t)$.

On the receiver side, as is shown in Figure 3.3 [13], [25], the received signal is represented by:

$$r(t) = s(t) + n(t) + J(t), \tag{3.9}$$

where $n(t)$ is a random process with zero mean and variance σ^2 to represent the AWGN channel. $J(t)$ is the interfering signal. The first step is to filter the received signal $r(t)$ in order to eliminate unwanted components out of the spreading bandwidth. The RF filter designed in the first step is a band-pass Butterworth filter of order 16, defined for W_{RF}=62 KHz that corresponds to the spreading bandwidth. However, to minimize phase distortion, the received signal is filtered using a zero-phase filter that doubles the Butterworth filter order. The same process is used for the despreading filter but for a bandwidth W_{DS}=2 KHz.

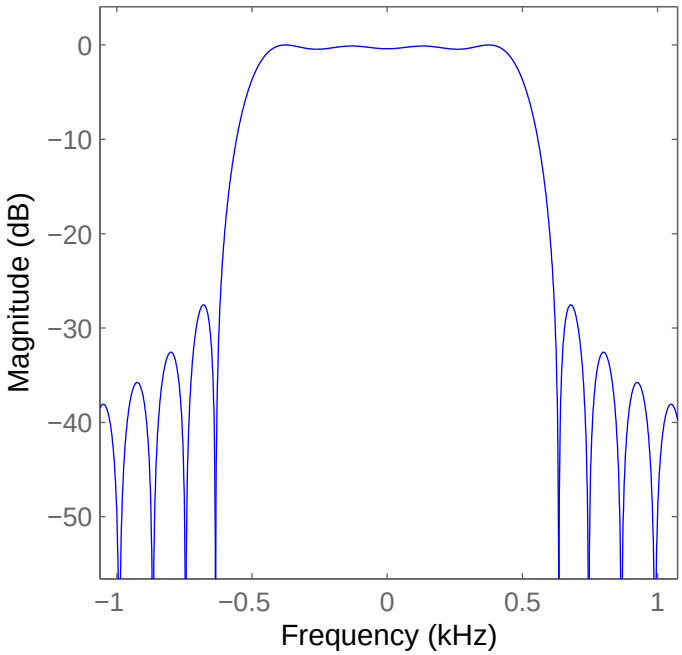

Figure 3.2: The square root raised cosine filter frequency response.

Figure 3.4 presents the frequency response for the RF and despreading filters. The bandpass W_{RF} and W_{DS} filtering implementation ares used in this thesis not only to allow improving the SNR by attenuating noise and unwanted signal components, but also to analyze the bandpass DSSS interference reduction on the receiver prior and after despreading the received signal [13].

As a second step, the filtered signal is despread by using a known sequence $c(t)$ and filtered according to the signal bandwidth. As a third step the despread filtered signal is down-converted to a baseband and passed through the received matched filter [24], consequently the resultant signal is down-sampled to obtain the received baseband symbols representation. The received matched filter presents the same design specification as the transmit pulse shaping filter, however the cascade of the down-sampler and low-pass filtering the signal is called decimation. In this case the decimation is performed by

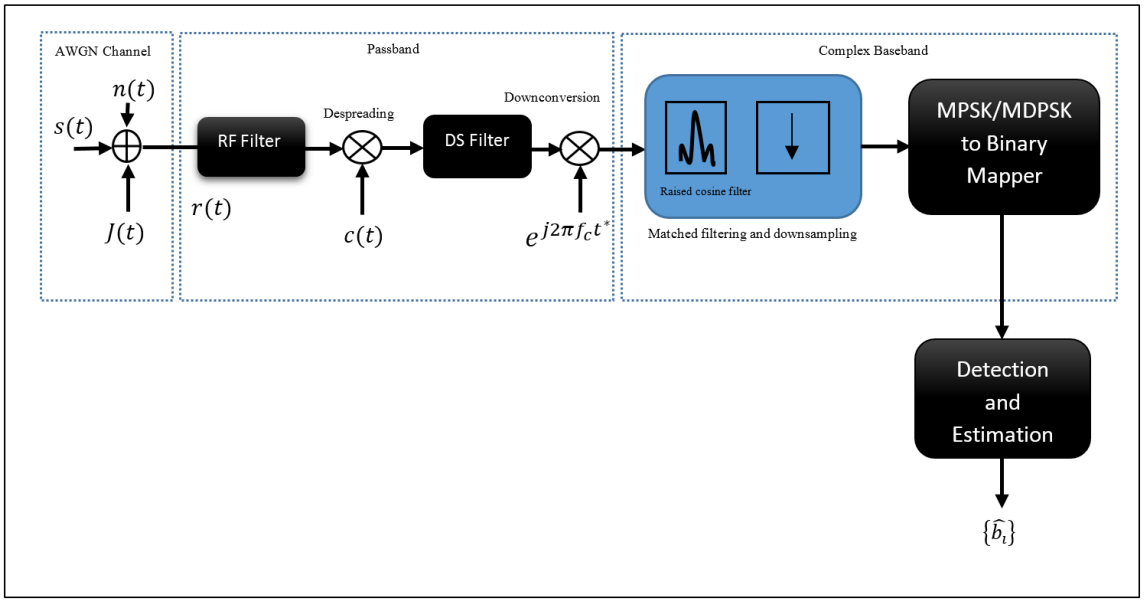

Figure 3.3: DSSS Receiver Model [13], [25].

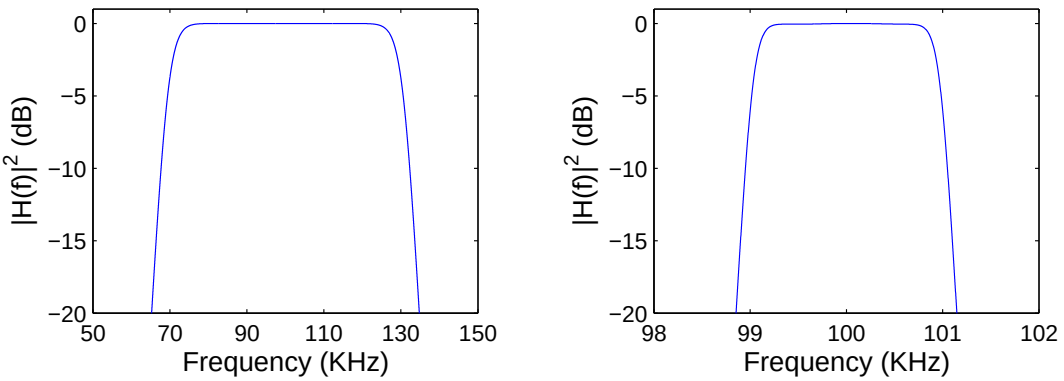

Figure 3.4: Normalized frequency response of the RF filter (left) and despreading filter (right).

a factor of 403 samples per symbol to recover the original symbol transmitted. Finally the bit estimation $\hat{b}$ process is performed by mapping from symbols to bits and then comparing the estimated bits with transmitted bits in order to compute BER.

3.3.1 Phase Shift Keying Modulation.

For M-ary digital phase modulation the modulated signal can be represented by the product of a pulse shape $g(t)$ and the carrier signal:

$$\begin{aligned} S_m(t) &= \mathrm{Re}\left[g(t)e^{(j2\pi\theta_m)}e^{(j2\pi f_c t)}\right], \quad 1 \leqslant m \leqslant M, \quad 0 \leqslant t \leqslant T \\ &= g(t)\cos\left[2\pi f_c t + \theta_m\right] \\ , &= g(t)\cos(\theta_m)\cos(2\pi f_c t) - g(t)\sin(\theta_m)\sin(2\pi f_c t). \end{aligned} \tag{3.10}$$

where

$$\theta_m = \frac{2\pi(m-1)}{M}; \quad m \in 1, 2, \ldots, M \tag{3.11}$$

The vector representation in terms of orthogonal signal basis is given by [26]:

$$\mathbf{S}_m = \left[\ \sqrt{E_s}\cos(\theta_m) \quad \sqrt{E_s}\sin(\theta_m)\right] \tag{3.12}$$

where E_s is the symbol energy. Since the signal waveforms have equal energy, the optimum detector for AWGN channel is given by the correlation of the received signal vector $\mathbf{r}$ and the vector representation of reference signals. This operation represents the projection of $\mathbf{r}$ vector in the direction of reference signals $\mathbf{S}_m$.

$$C(\mathbf{r}, \mathbf{S}_m) = \mathbf{r} \cdot \mathbf{S}_m; \quad m = 1, 2, \ldots, M. \tag{3.13}$$

For the binary case M=2, from Equation (3.12), $s_1(t)$ and $s_2(t)$ are antipodal signals with equal energy and the bit error probability expression is given by [26]:

$$P_b = Q\left(\sqrt{\left(\frac{2E_b}{N_o}\right)}\right). \tag{3.14}$$

For $M = 4$, from the receiver's perspective the effect is like having two binary phase-modulation signals in quadrature and it implies that there is no interference to each other. Thus the Equation (3.14) is also applicable for QPSK.

For $M > 4$ the analytical expression for the symbol error probability using Gray code assignment is given by the following expression [26]:

$$P_s \approx 2Q\left(\sqrt{\frac{2E_s}{N_o}}\sin\left(\frac{\pi}{M}\right)\right), \tag{3.15}$$
$$\approx 2Q\left(\sqrt{\frac{2kE_b}{N_o}}\sin\left(\frac{\pi}{M}\right)\right).$$

As implementing in this research the Gray code assignment produces a constellation scheme where from consecutive symbol representation the distance between each other is one bit. Under this code assignment the relation between bit error probability (P_b) and symbol error probability (P_s) with k bits per symbol yields:

$$P_b \approx \frac{1}{k}P_s. \tag{3.16}$$

3.3.2 Differential Phase Shift Keying Modulation.

For DPSK modulation the received phase symbol at a given symbol interval is compared to the phase of the received symbol at previous signaling interval. The information transmitted is conveyed in θ_k where every symbol m to transmit defines:

$$\Delta\theta_k = \frac{2\pi(m-1)}{M}; \quad m \in 1, 2, \ldots, M. \tag{3.17}$$

The modulator differentially phase encodes the transmitted symbols from a set of M symbols. Consequently for transmitting $\Delta\theta_k$ at kth transmission interval the transmitter computes $\theta_k = \theta_{k-1} + \Delta\theta_k$ modulo 2π and then modulate θ_k on the carrier [27]. For the first symbol it can be assumed $\theta_{k-1} = 0$.

To demodulate a differentially encoded phase signal the received signal is projected onto basis functions $\cos(2\pi f_c t)$ and $\sin(2\pi f_c t)$ over the interval T_s. At the k_{th} signaling interval, the demodulator output is [26]:

$$r_k = \left[\sqrt{E_s}\cos(\theta_k - \phi) + n_{k1} \quad \sqrt{E_s}\sin(\theta_k - \phi) + n_{k2}\right], \tag{3.18}$$

$$r_k = \sqrt{E_s}\exp(j\theta_k - \phi) + n_k. \tag{3.19}$$

where θ_k is the phase angle of the transmitted signal at the k_{th} signaling interval, ϕ is the carrier phase and $n_k = n_{k1} + n_{k2}$ is the noise vector. Similarly, the received signal vector at previous interval yields:

$$r_{k-1} = \sqrt{E_s}\exp(j\theta_{k-1} - \phi) + n_{k-1}. \tag{3.20}$$

The projection of r_k onto r_{k-1} for the complex received signal representation yields:

$$r_k r_{k-1}^* = E_s \exp(j\theta_k - \theta_{k-1}) + \sqrt{E_s}\exp(j\theta_k - \phi)n_{k-1}^* + \sqrt{E_s}\exp(j\theta_{k-1} - \phi)n_k + n_k n_{k-1}^*. \tag{3.21}$$

The previous expression in absence of noise can be considered as the phase difference $\theta_k - \theta_{k-1}$. Therefore, the mean value of $r_k r_{k-1}^*$ is independent of the carrier phase. Assuming that phase difference $\theta_k - \theta_{k-1}$ is zero, the exponential factors $\exp(j\theta_{k-1} - \phi)$ and $\exp(j\theta_k - \phi)$ can be absorbed into the Gaussian noise component without changing their statistical properties and $r_k r_{k-1}^*$ can be expressed as [26]:

$$r_k r_{k-1}^* = E_s + \sqrt{E_s}(n_k + n_k^*) + n_k n_{k-1}^*. \tag{3.22}$$

For high SNR the term $n_k n_{k-1}^*$ is small than $\sqrt{E_s}(n_k + n_k^*)$ and it can be neglected. Normalizing Equation (3.22) by $\sqrt{E_s}$, the decisions components are [26]:

$$x = \sqrt{E_s} + \mathrm{Re}(n_k + n_{k-1}^*). \tag{3.23}$$

$$y = \mathrm{Im}(n_k + n_{k-1}^*). \tag{3.24}$$

The variables x and y are uncorrelated Gaussian random variables with identical variances $\sigma_n^2 = N_o$. The received phase is:

$$\theta_r = \arctan\left(\frac{y}{x}\right). \tag{3.25}$$

The phase decision can be made by comparing the correct received phase with previous phase θ_{r-1}. For an AWGN channel the probability of bit error for binary DPSK is given by:

$$P_b = \frac{1}{2}e^{-\frac{E_b}{N_o}}. \tag{3.26}$$

The P_b for binary DPSK comparatively yields poorer performance than binary PSK, with approximately less than 3 dB for a higher SNR required for a given BER [26].

When $M > 2$ the DPSK symbol error probability with k bits per symbol in an AWGN channel and for a large E_s/N_o tends to [5]:

$$\begin{aligned} P_s &\approx 2Q\left(\sqrt{\frac{2E_s}{N_o}}\sin\left(\frac{\pi}{\sqrt{2}M}\right)\right), \\ &\approx 2Q\left(\sqrt{\frac{2kE_b}{N_o}}\sin\left(\frac{\pi}{\sqrt{2}M}\right)\right). \end{aligned} \tag{3.27}$$

According to [28] the bit error probability P_b for $M > 2$ with k bits per symbol can be approximated by:

$$P_b = \frac{1}{k}\left[\sum_{i=1}^{M/2}(\overline{w}_i)A_i\right] \tag{3.28}$$

where $\overline{w}_i = w_i + w_{M-i}$, $\overline{w}_{M/2} = w_{M/2}$, w_i is the Hamming distance of bits assigned to symbol i and:

$$A_i = F\left[\frac{(2i+1)\pi}{M}\right] - F\left[\frac{(2i-1)\pi}{M}\right], \tag{3.29}$$

$$F(\psi) = -\frac{\sin\psi}{4\pi}\int_{\pi/2}^{-\pi/2}\frac{\exp\left[-kE_b/N_o\,(1-\cos\psi\cos t)\right]}{1-\cos\psi\cos t}\,dt. \tag{3.30}$$

Particularly for M=4, using Gray code assignment, the BER from Equation (3.28) and Equation (3.29) can be obtained evaluating the integral presented in Equation (3.30):

$$P_b = F\left[\frac{5\pi}{4}\right] - F\left[\frac{\pi}{4}\right]. \tag{3.31}$$

3.4 Jamming Models

This research considers the following jamming categories: simulated noise interference, continuous wave jammers, pulse jammers and multi-tone jammers. The main as-

sumption for DSSS is that is essentially not frequency agile system, therefore the most applicable strategies are noise, tone and pulsed interference schemes. The latter interference approach searches for generating spectral components within the RF filter that can approximately cover the RF bandwidth or equivalently transmit high power intermittent signals over portion of the RF bandwidth. The receiver model corrupted with noise and interference can be represented by:

$$r(t) = S(t) + J(t) + n(t), \tag{3.32}$$

where $J(t)$ denotes the interference signal and $n(t)$ is a zero mean AWGN.

Noise interference can be modeled as a broad-band interferer that tries to cover the entire channel bandwidth or as a narrow-band (partial band) jamming by filtering an assumed AWGN signal for the required bandwidth and controlling the average power to achieve a required jamming margin. The resultant signal after the filtering process is a colored version of Gaussian noise due to spectral changes in the original noise signal. Similarly tone jamming techniques consider a function to control the power for a required jamming margin considering a tone either with a random phase or tone with random frequency within the RF bandwidth. For the tone jamming the phase variation generates a PSD approximately centered at the RF filter depending on the knowledge of the receiver frequency. For the random frequency interference it is desirable to get a PSD distributed over the RF bandwidth.

The simulated interference waveforms are categorized as a continuous jammer when the jamming signal is present during the symbol interval and for all symbols generated in the message transmitted interval. On the other hand pulse jamming is an intermittent interference signal with a given pulse duration and pulse repetition interval to determine a duty cycle as a ratio between on transmission and pulse repetition interval. In this research all pulsed waveforms generated were derived from continuous waves as a product of the waveform and a pulse train with a determined duty cycle. The MTJ is considered as a

finite number of frequencies within the signal duration either as tones using the same waveform and transmitted at different frequencies or waveforms that generate different frequencies describing some spectrum pattern as a frequency hopped interference (FHI) or comb spectrum interference (CSI).

3.4.1 Broad-band Interference.

The broadband interference for DSSS can be any waveform that occupies a bandwidth equal to or greater than the spreading bandwidth. In this research the spreading bandwidth W_{ss} is defined as a function of the chip rate R_c in chips per seconds. For a DSSS passband signal this bandwidth can be expressed as:

$$W_{ss} = 2R_c = 2\frac{1}{T_c}, \tag{3.33}$$

and the symbol interval $T_s = N_c T_c$, where N_c is the number of chips per symbol and T_c is the chip interval in seconds. Then the spreading bandwidth measured in Herz in terms of the symbol rate R_S, yields :

$$W_{ss} = 2\frac{N_c}{T_s} = 2N_c R_s. \tag{3.34}$$

Therefore within the category of broadband interference can be considered multi-tone interference, noise interference or any random modulated waveform that exceeds W_{ss}. In this research the waveforms considered include: broad-band noise (BBN), random frequency modulated interference (RFMI), LFMI, FHI, CSI and MTJ.

3.4.1.1 Broad-band Noise.

In BBN the spectral components are affected equally and similarly for different frequencies. This interference technique is the simplest to generate because it only requires knowledge of the spreading bandwidth. This can be simulated as an AWGN with average jamming power J_p over the simulated receiver bandwidth ($F_s/2$) or using the spreading bandwidth W_{ss}:

$$J_p = 2W_{ss}\frac{J_o}{2} = W_{ss}J_o, \tag{3.35}$$

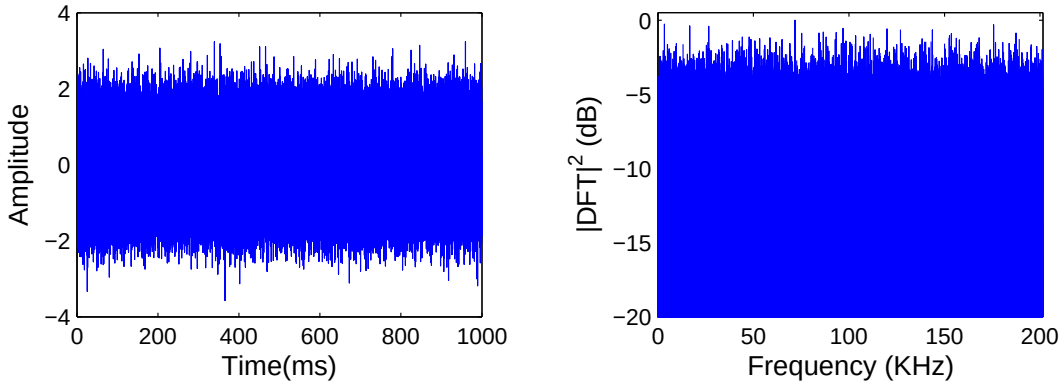

Figure 3.5: Time domain response (left) for 1000, T_s=1 ms, symbols and normalized PSD (right) for BBN using a bandwidth W_J=201.5 KHz.

where J_o is the jamming PSD in units of Watts per Hz.

Figure 3.5 shows the time domain response of noise for 1000, T_s=1 ms, symbols (left subplot) and the normalized PSD response (right subplot) using a bandwidth W_J=201.5 KHz that corresponds to the simulated bandwidth $F_s/2$. Figure 3.6 show the time-frequency representation of BBN jammers using two different bandwidths W_J=$F_s/2$ and a filtered noise (colored noise) using the spreading bandwidth W_J= W_{ss} implemented with a Butterworth filter of order 8 to illustrate the frequency distribution differences across time.

3.4.1.2 Random Frequency Modulated Interference (RFMI).

This jamming technique generates random frequencies from the center carrier frequency and within the W_{ss} bandwidth, controlled with the frequency deviation factor Δf. The frequency randomness is generated by a random instantaneous phase of $\pm\pi$ over T_s. A RFMI can be represented by [29]:

$$J(t) = \sqrt{2J_p}\cos(2\pi f_c t + \theta(t) + \phi), \tag{3.36}$$

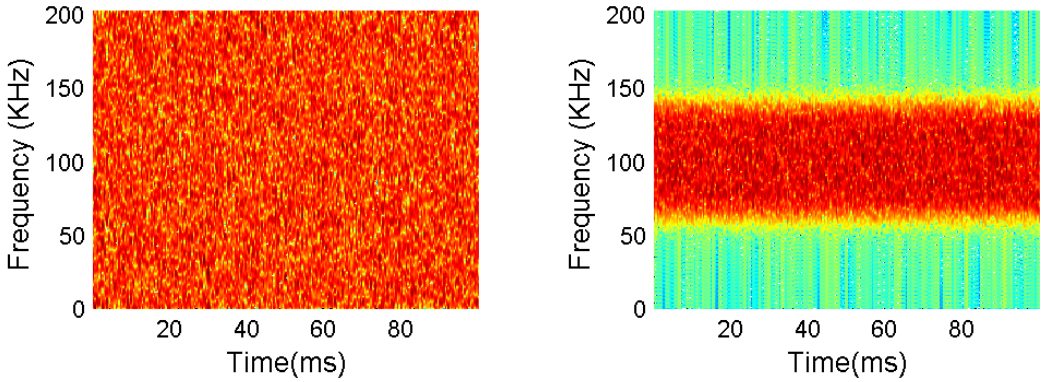

Figure 3.6: BBN spectrograms showing 100, T_s=1 ms, symbols and W_J=201.5 KHz (left) and W_J=62 KHz (right) bandwidths.

with

$$\theta(t) = \phi + \Delta f \int_0^{T_s} f(\alpha)\mathrm{d}\alpha, \tag{3.37}$$

where

ϕ is the initial phase.

$\theta(t)$ is a random process characterizing the signal's instantaneous phase.

$f(\alpha)$ is the instantaneous random frequency modulated signal in Hz.

Δf is the frequency deviation from the central frequency in Hz.

T_s is the symbol duration in seconds.

As an example of RFMI Figure 3.7 shows the time domain signal (the left subplot) and the normalized PSD for two symbols (right subplot) with T_s=1 ms. The RFMI waveform generation was adopted from the MATLAB® simulation introduced by Temple [30]. Figure 3.8presents the corresponding time-frequency plot to illustrate how the random frequency is varying with respect to the time. Random frequency modulated signals are used in wide-band radar for intra-pulse modulation due to its properties of low side-lobe

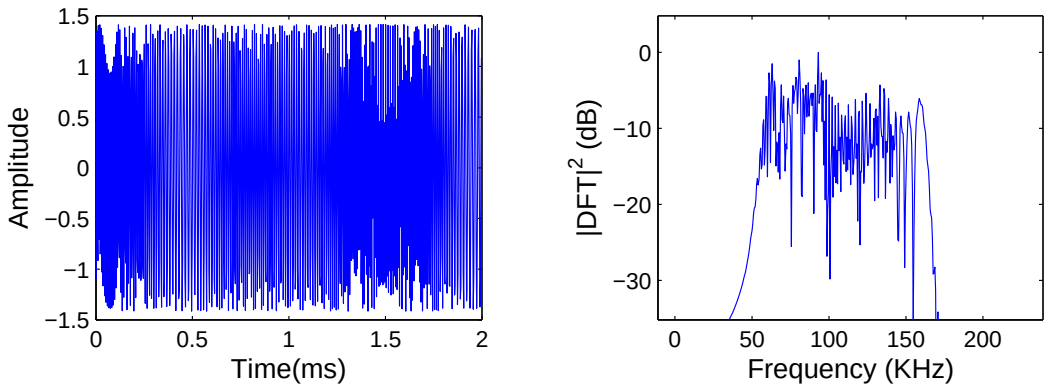

Figure 3.7: The RFMI time domain response (left) and normalized PSD (right) for two, T_s=1 ms, symbols.

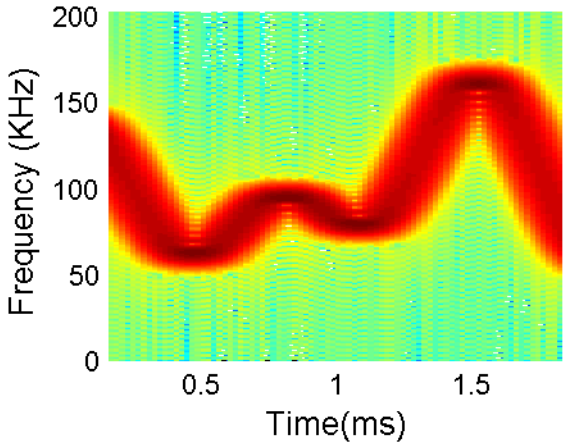

Figure 3.8: The RFMI spectrogram showing three, T_s=1 ms, symbols.

autocorrelation, good range resolution and interference suppression. The RFMI can achieve lower side-lobes than conventional intra-pulse modulation in radar used to increase the range resolution [31].

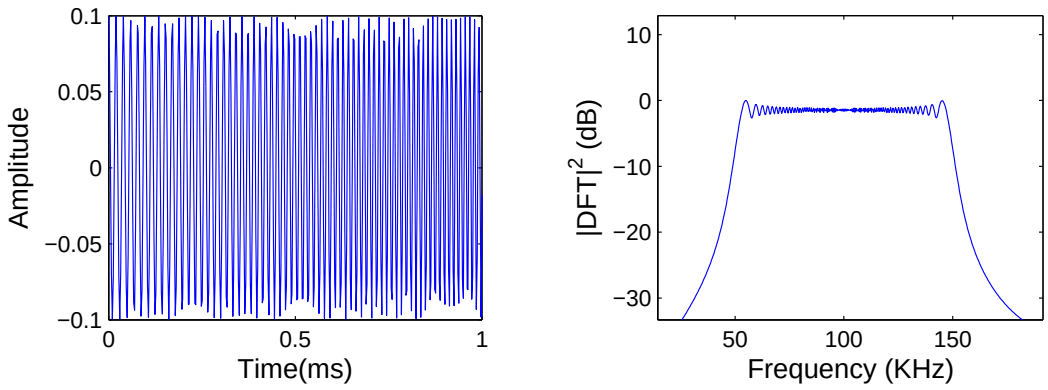

Figure 3.9: Time domain response (left) for one, T_s=1 ms, symbol and normalized PSD (right) for CW LFMI for three symbols.

3.4.1.3 Linear Frequency Modulated Interference (LFMI).

A LFMI signal is broadly used in radar and spread spectrum communications also called chirp spread spectrum signaling. The LFMI signal a waveform whose frequency varies linearly within the signal duration to generate a high bandwidth maintaining the pulse duration. The resultant signal can achieve a time-bandwidth product much greater than the non-modulated pulsed signal where this factor is not greater than 2, due to the passband bandwidth for non-modulated pulsed signal is typically defined as $2/\tau$. Mathematically LFMI can be modeled as having an average power J_p and initial phase ϕ:

$$J(t) = \sqrt{2J_p}\exp\left\{j2\pi f_c t + j\pi\mu_o t^2 + j\phi\right\}, \tag{3.38}$$

where $\mu_0 = B/\tau$ is the is linear frequency slope factor from the initial frequency f_c and B in Hz is the frequency deviation over signal duration τ in seconds. The units of μ_0 are S^{-2} [32]. Figure 3.9 shows the time domain (left subplot) and the normalized PSD (right subplot) for a generated LFMI signal considering three symbols with T_s=1 ms. Figure 3.10 illustrate a LFMI plot of frequency versus time to observe the linear frequency variation.

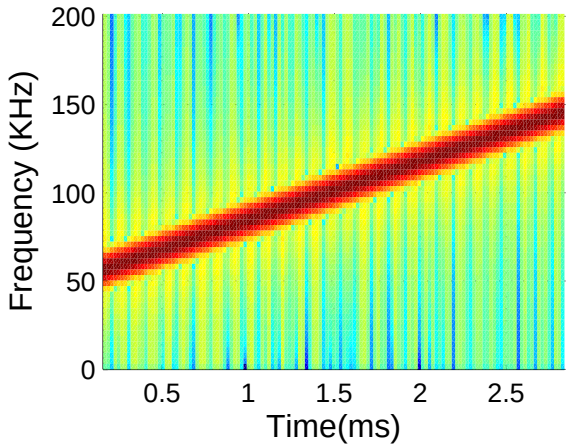

Figure 3.10: The LFMI spectrogram showing three, T_s=1 ms, symbols.

3.4.1.4 Frequency Hopped Interference (FHI).

Another model of simulated interference to evaluate the DSSS receiver performance is presented by [18]. The FHI consist of a signal with power J_p as a product of a rectangular window shifted by a time hopping interval TH and different frequency tones f_k chosen randomly within a jamming bandwidth W_j and initial phase ϕ_o. The mathematical model is:

$$J(t) = \sqrt{2J_p} \sum_{k=1}^{N} \sqcap_{T_H}(t - kT_H) \times \exp\left[j2\pi f_k(t - kT_H) + j\phi_o\right], \tag{3.39}$$

where

$$\sqcap_{T_H} = \begin{cases} 1, & |t| < \frac{T_H}{2} \\ 0, & |t| > \frac{T_H}{2} \end{cases} \tag{3.40}$$

The simulated FHI is shown in Figure 3.11 for five $T_s = 1$ ms symbols using a TH with the same duration as the symbol duration, including time domain (left subplot) and the normalized PSD (right subplot) responses, showing five frequencies in a bandwidth

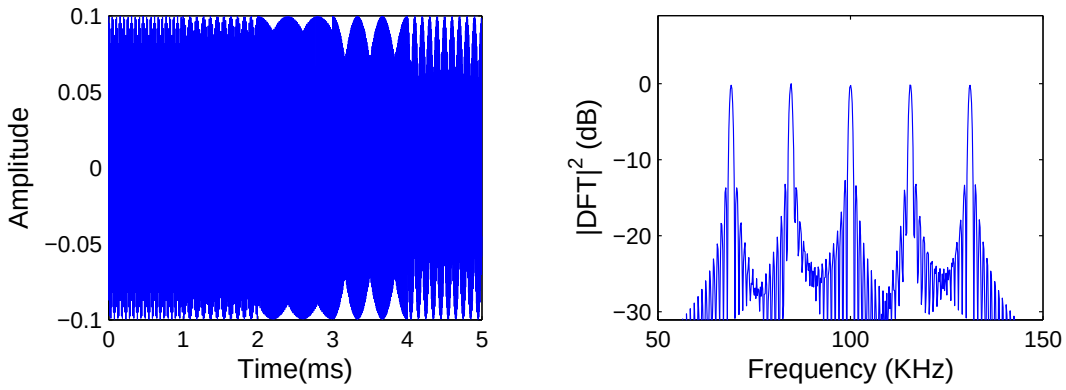

Figure 3.11: Time domain (left) and normalized PSD (right) for the FHI showing five, T_s=1 ms, symbols and bandwidth W_j=62 KHz.

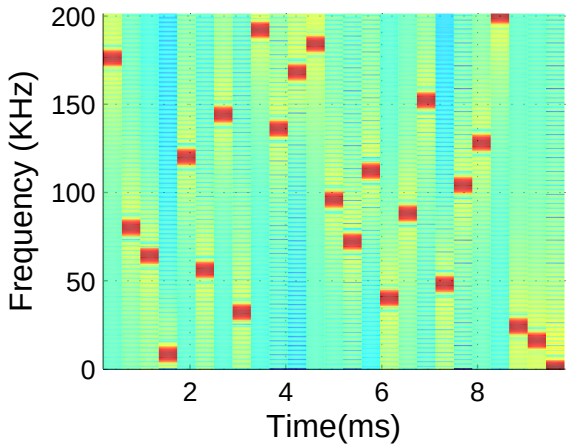

Figure 3.12: The FHI spectrogram for 10, T_s=1 ms, symbols and bandwidth W_j=200 KHz.

W_j=62 KHz. The time-frequency plot in Figure 3.12 shows a FHI for 10, T_s = 1 ms, symbols, using a TH=0.4 ms, resulting in 26 frequencies random uniformly distributed in a bandwidth W_J=200 KHz.

3.4.1.5 *Comb-Spectrum Interference (CSI).*

The CSI model consists of generating a series of narrow-band signals modulated by a series of tones distributed over the W_{ss} bandwidth [18].

$$J(t) = \sqrt{2P_k} \sum_{k=1}^{N} \exp\{j2\pi f_k t + 0.01\Delta f \sin(2\pi\Delta f)\} \tag{3.41}$$

$J(t)$ is generated by a group of frequency modulated signals, where f_k is the central frequency for each component with a frequency deviation of $\pm\Delta f$ in Hz from the center frequency such that $\Delta f \ll f_k$. Figure 3.13 shows the temporal CSI response (left) for one T_s=1 ms symbol and the normalized PSD for 1000, T_s=1 ms, symbols, five frequencies and a frequency deviation Δf=0.5 Hz. Figure 3.14 presents the corresponding time-frequency plot to illustrate that the comb-like spectrum across the time, showing five frequencies for a total of 50, T_s=1 ms, symbols and Δf=0.5 Hz.

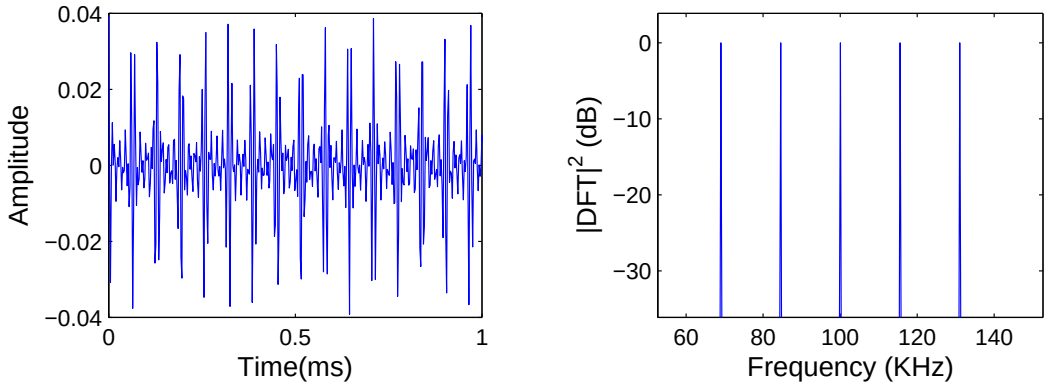

Figure 3.13: The time domain CSI response (left) for one, T_s=1 ms, symbol and normalized PSD (right) response for five frequencies, 1000 symbols and Δf=0.5 Hz.

3.4.1.6 *Multi-Tone Jamming (MTJ).*

This jammer can be describes as a summation of several tones each of frequency f_k and random phase which is uniformly distributed in the interval $[0, 2\pi]$ and average power J_p.

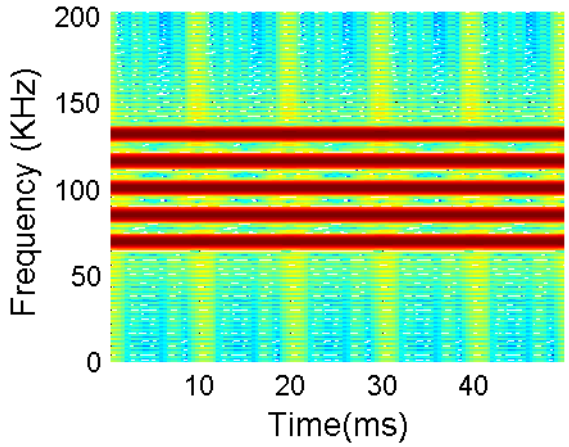

Figure 3.14: The CSI spectrogram for 50, T_s=1 ms, symbols and bandwidth $W_j \approx$ 62 KHz.

Under this technique, also called multiple CW tone interference, the total received jamming power is divided in N_t different random phase CW tones. The tones are usually distributed over the spreading bandwidth. The MTJ can be modeled by the following expression:

$$\sum_{k=1}^{N_t} \sqrt{2\frac{J_p}{N_t}} \cos(2\pi f_k t + \phi) \quad \text{where} \quad \phi \sim U[0, 2\pi]. \tag{3.42}$$

In Figure 3.15 can be observed the time domain representation of a multi-tone signal for one, T_s=1 ms, symbol interval (left subplot) and the normalized PSD (right subplot) for 1000 symbols using 10 random phase tones. Figure 3.16 presents the corresponding time-frequency plot to illustrate that MTJ generates multiple tones with constant frequency as the time varies.

3.4.2 Narrow-Band Interference (NBI).

In this research NBI is considered a waveform that occupies passband bandwidth that is much less than the RF bandwidth of the DSSS. Within this category are considered 1) CW interference signals that occupy a smaller band-pass bandwidth compared to the W_{ss} bandwidth and 2) partial-band jammers.

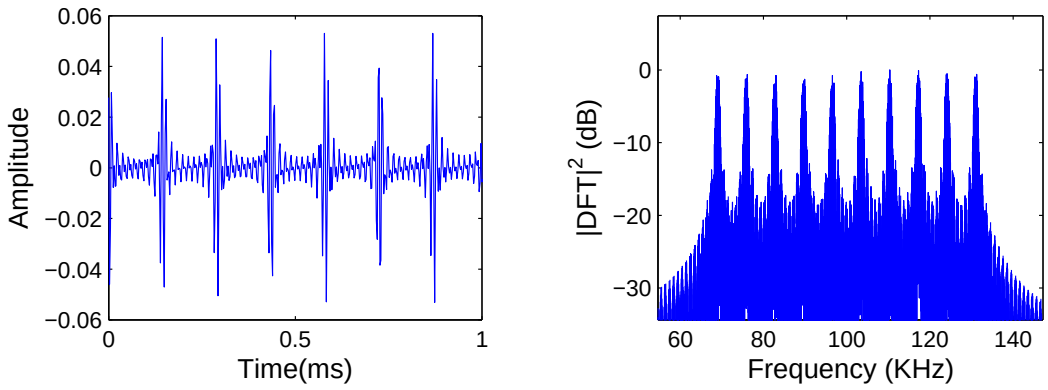

Figure 3.15: Time domain MTJ response (left) for one, T_s=1 ms, symbol interval and normalized PSD for 10 random phase tones and 1000 symbols.

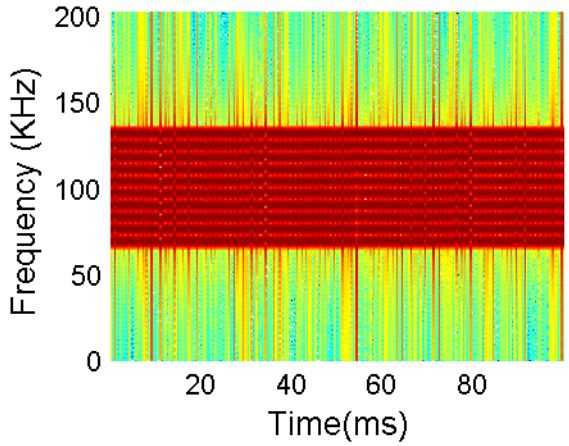

Figure 3.16: The MTJ spectrogram for 100, T_s = 1 ms, symbols and bandwidth W_J≈62 KHz.

3.4.2.1 Tone Jammer.

The tone jammer considered in this research assumes that carrier frequency is known and the phase is a random variable uniformly distributed over the interval $[0, 2\pi]$. The phase varies in a symbol by symbol basis and $J(t)$ has an average power J_p. The mathematical

representation is:

$$J(t) = \sqrt{2J_p}\cos(2\pi f_c t + \phi) \quad \text{where} \quad \phi \sim U[0, 2\pi]. \tag{3.43}$$

In Figure 3.17 is presented the tone jammer time domain response (left subplot) illustrating a random symbol transition from the first to the second symbol and normalized PSD (right subplot) response for tone jammer with random phase for 1000 T_s =1 ms symbols. Figure 3.18 presents the corresponding time-frequency plot to illustrate the tone jammer with constant frequency across time variation.

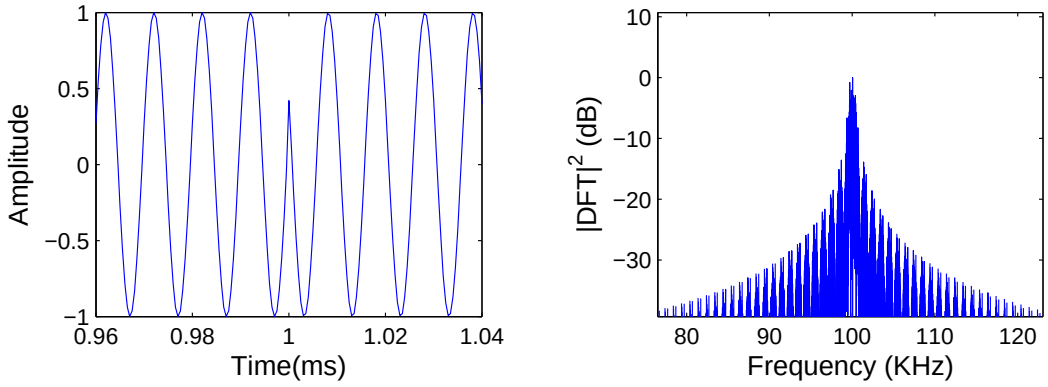

Figure 3.17: Time domain response showing one, T_s=1 ms, symbol phase transition (left) and normalized PSD (right) for tone jammer for 1000, T_s =1ms, symbols.

3.4.2.2 Binay Phase Shift Keying (BPSK) Interference.

The BPSK interference model consists of a source of random binary data that is mapped according to:

$$\theta_m = \pi(m-1); \quad m \in 1, 2. \tag{3.44}$$

Then the jamming signal yields:

$$J = \sqrt{2J_p}\cos(2\pi f_c t + \theta_m). \tag{3.45}$$

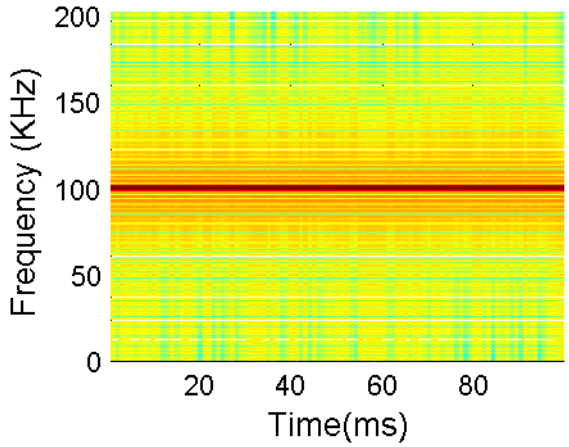

Figure 3.18: The tone jammer spectrogram for 100, T_s=1 ms, symbols.

From the above equation θ_m takes values either 0 or π. This is another waveform that is similar to the target signal with no knowledge of the spreading sequence and it also can be used to generate a pulse jamming interference.

3.4.2.3 Partial-Band Noise.

As it was explained noise interference is a function of the signal bandwidth. However, the noise power can be distributed over a desired bandwidth instead of the total spreading bandwidth. In this research the partial-band noise or narrow-band noise is simulated using filtered (colored) AWGN noise signal. The average jamming power J_p can be expressed as a function of ρ_n that represents a fraction of the spreading bandwidth W_{ss}:

$$\rho_n = \frac{W_J}{W_{ss}} \leq 1, \tag{3.46}$$

where W_J is the jamming bandwidth. The jammer PSD S_j can be represented by [11]:

$$S_j = \frac{J_p}{W_J} = \frac{J_p}{W_{ss}} \cdot \frac{W_{ss}}{W_J},$$
$$S_j = \frac{J_o}{\rho_n}. \tag{3.47}$$

J_o is equivalent to the noise power spectral density as if the jammer power were spread over W_{ss}.

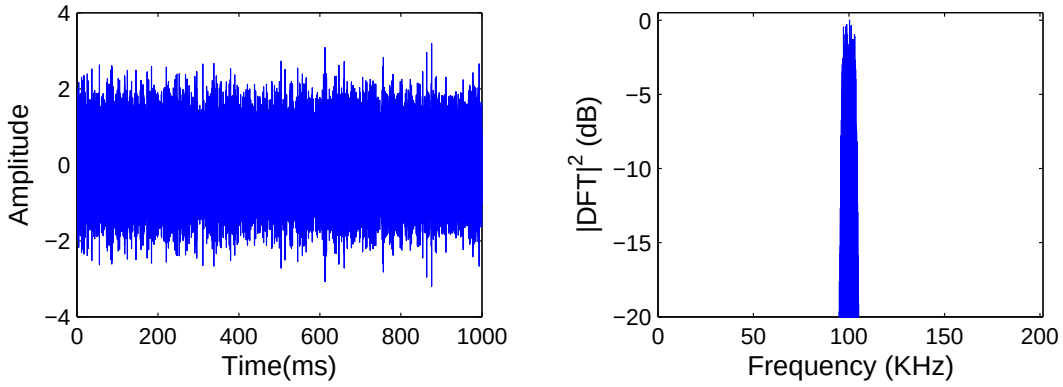

Figure 3.19: Time domain response for 1000, T_s=1 ms, symbols (left) and normalized PSD (right) for NBN using a bandwidth W_J≈8 KHz.

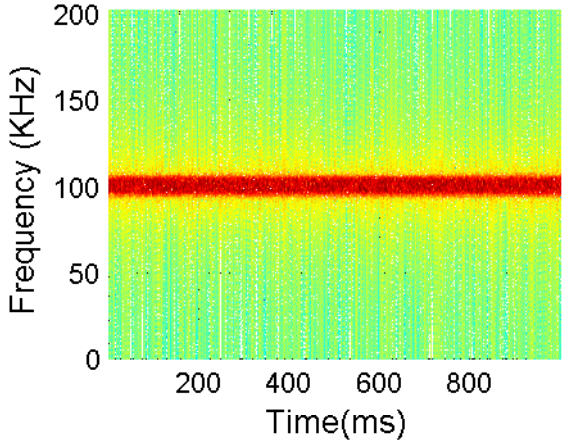

Figure 3.20: NBN spectrograms showing 100, T_s=1 ms, symbols for W_J≈8 KHz.

Figure 3.19 shows the time domain response for1000, T_s=1 ms, symbols (left subplot) and the normalized PSD for NBN using a W_J≈8 Khz (right subplot). Figure 3.20 illustrate the time-frequency plot for NBN for 100, T_s=1 ms, symbols and bandwidth W_J≈8 KHz.

3.4.3 Pulse Jamming.

Pulse jamming is a kind of interference that occurs sporadically for short durations, periodic or aperiodic [7]. At baseband the pulse burst model can be represented by:

$$X_p(t) = \sum_{m=0}^{M-1} \sqcap(t - mT_p) \tag{3.48}$$

where

$X_p(t)$ is the baseband train of pulses.

M is the number of pulses in the burst.

T_p is the pulse repetition interval in seconds.

$\sqcap(t)$ is the rectangular function with a duration of τ seconds.

and

$$\sqcap(t) = \text{rect}\left(\frac{t}{\tau}\right) = \begin{cases} 1, & \text{if } |t| \leq \frac{\tau}{2}, \\ 0, & \text{if } |t| > \frac{\tau}{2}. \end{cases} \tag{3.49}$$

Any interfering pulsed waveform can be simulated as a product of the pulse train in Equation (3.48) and a continuous waveform $f(t)$ as follows:

$$J(t) = \sqrt{2\frac{J_p}{\rho}} X_p(t) \cdot f(t), \tag{3.50}$$

where J_p is the average jamming power and ρ is the duty cycle.

In Figure 3.21 are shown the pulsed BPSK time domain response for one Ts=1 ms symbol (right subplot) with pulse duration τ=100 usec and a duty cycle ρ=0.3 and the pulsed BPSK

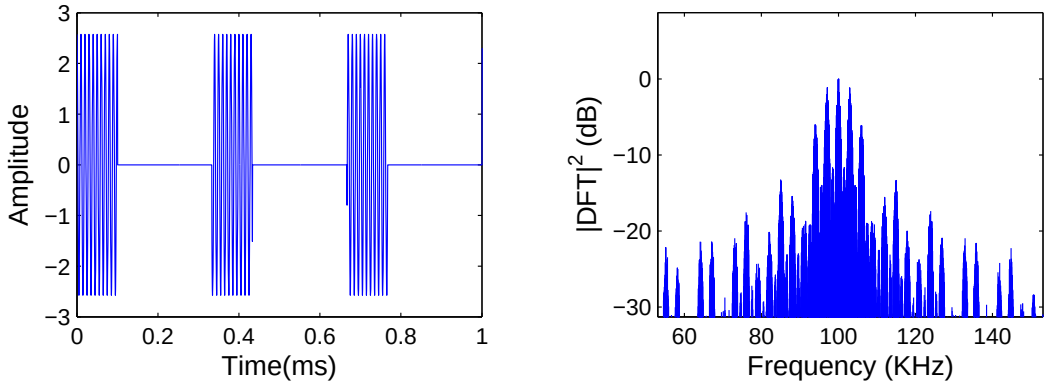

Figure 3.21: Time domain response for 1000, T_s =1 ms, symbols and normalized PSD for pulsed BPSK.

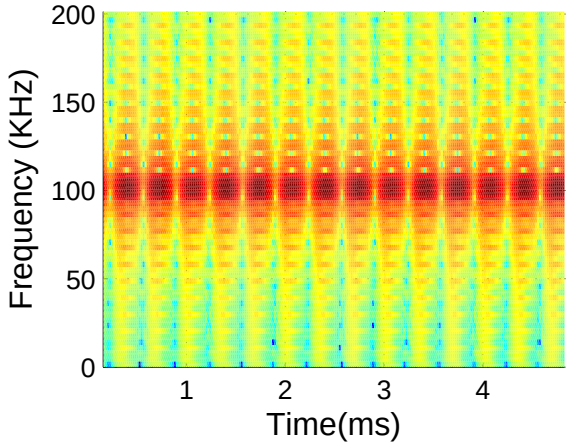

Figure 3.22: Pulse BPSK spectrograms showing 5, T_s=1 ms, symbols.

normalized PSD response for 1000, Ts=1 ms, symbols (right subplot). Figure 3.22 shows the pulsed BPSK time-frequency response illustrating the how the spectrum is varying across time, considering 5, T_s=1 ms, symbols.

3.5 Jamming Performance Evaluation

The process involved in the interference evaluation consists of the receiver validation, receiver performance with implemented filters and JSR computation requirements for the different interference techniques described in Section 3.4.

3.5.1 Receiver Validation.

First the receiver performance is compared with the theoretical expression under an AWGN channel with ideal conditions. It means that the RF and despreading filters are not considered and therefore the received signal PSD is not altered by filter coloration. It is important to contrast results with the analytical expressions in an AWGN channel presented in Section 3.3. The spread spectrum model presented in Figure 3.3 can be used either for PSK or DPSK modulation that are the most representative signaling schemes in a DSSS communication system.

The parameters considered as a baseline for BER receiver simulations are presented in Table 3.1. In the present research the simulation considered a total of 1000 symbols for $E_b/N_o \in [0, 8]$ dB in 0.5 dB increments. For each E_b/N_o level the symbols are generated until 500 bit errors are found by comparing the symbols received with respect to the effective symbols transmitted. The average simulation error is less than 30 percent for a 95 percent confident interval as a trade-off between error and number of bits required, according to the criteria described in Section 3.2.

In Figure 3.23 is presented the performance of a QPSK DSSS receiver implemented with a sequence N_c=31 chips that follows the Gold code properties as explained in Section 2.4. The signal power considered is fixed to1 Watt while varying the noise power to obtain the required E_b/N_o levels. It is observed that simulated QPSK performance is the same as BPSK but efficiently allows doubling of the data rate. The results presented validates the simulated performance compared with analytical expression since

Table 3.1: Signal parameters considered for the simulated receiver.

	DSSS Modulation		
	QPSK	DBPSK	DQPSK
Carrier Frequency (KHz)	1	1	1
Symbol Rate R_s (Sym/s)	1000	1000	1000
Data Rate R_d (KBits/s)	2	1	2
Code Rate R_c (KBits/s)	62	31	62
Spread Sequence(Chips)	Gold(31)	Gold(31)	Gold(31)
RF Bandwidth W_{RF} (KHz)	62	62	62
Despreading Filter Bandwidth W_{DS} (KHz)	2	1	2

the simulated results closely approach the analytical curves. The blue curve was computed using Equation (3.14).

In Figure 3.24 is presented the performance of DPSK for a modulation index M=2 and M=4. It is observed that simulated results approach closely to the analytical results. For E_b/N_o ratios greater than 4 dB in order to obtain similar performance differential quadrature phase shift keying (DQPSK) requires an E_b/N_o of approximately 1 dB more with respect to differential binary phase shift keying (DBPSK) performance. Comparing QPSK with binary DPSK, the first modulation type performs 1.5 dB better. For QPSK compared with DQPSK, it is observed than the latter is approximately 2.5 dB poorer. In Table 3.2 are presented simulated BER for PSK and DPSK for E_b/N_o ratios from 5 to 8 dB showing the approximate differences discussed previously.

3.5.2 Receiver Performance with Bandpass Filters.

Once the receiver has been validated under ideal conditions, a second step considered is the receiver performance simulated using the bandpass RF and the bandpass despreading

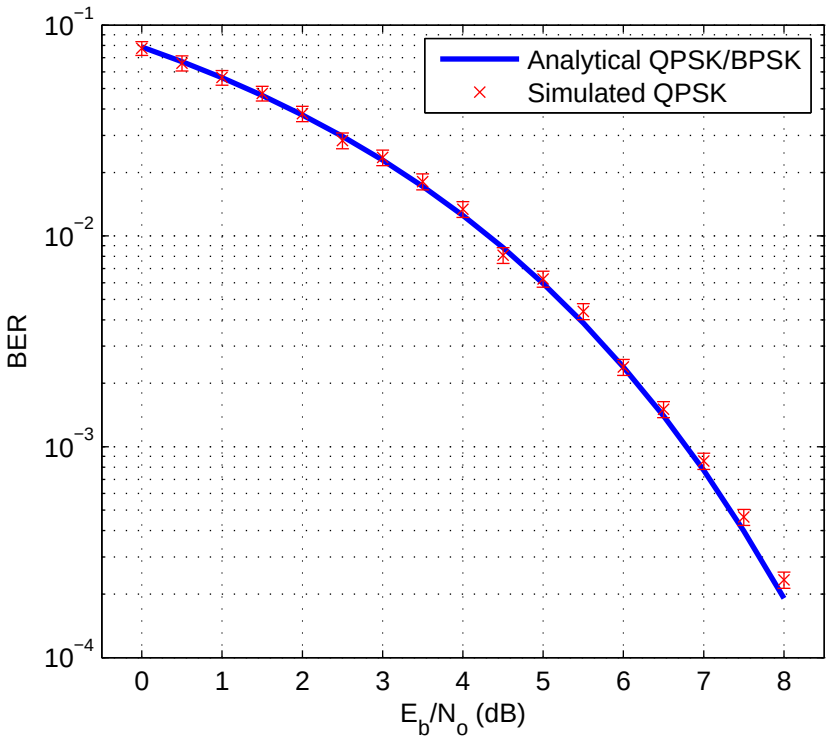

Figure 3.23: BER performance for QPSK in AWGN channel.

Table 3.2: PSK and DPSK BER performance comparison.

	BER $\times 10^{-3}$						
QPSK	6.3	4.4	2.4	1.5	0.9	0.5	0.2
DBPSK	20.8	16	9.7	6.1	3.5	2.1	1
DQPSK	31.7	25	18.1	12.4	9.3	6.2	4
E_b/N_o (dB)	5	5.5	6	6.5	7	7.5	8

filters to simulate a real receiver implementation where the signal is filtered previous to down-conversion in order to remove the unwanted spectral components and to improve the SNR and also to estimate the interference reduction after the despreading mixer. In

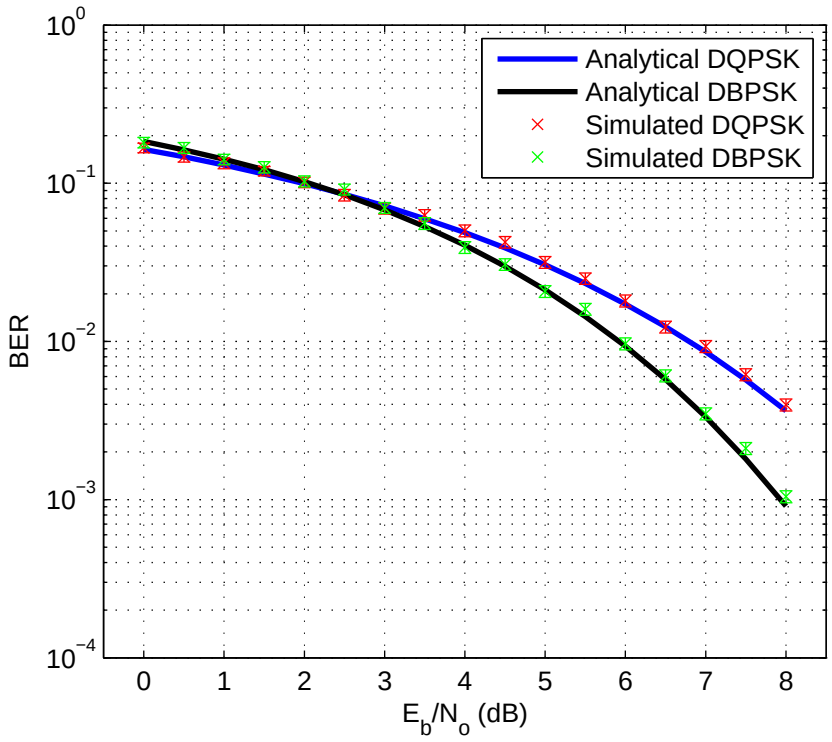

Figure 3.24: BER performance for DQPSK and DBPSK in AWGN channel.

this research and for the purpose of interference analysis the modulation scheme that will be considered is QPSK because it presents the best performance in PSK modulation and bandwidth efficiency in terms of data rate, that is, for equal symbol rate it doubles the data rate compared with BPSK with the same BER performance. Figure 3.25 shows results of an ideal DSSS QPSK receiver along with the performance using filters as BER versus E_b/N_o. From the figure it is possible to observe that the filtered signal is degraded such that approximately each BER point of the receiver requires 0.5 dB higher E_b/N_o to obtain the ideal receiver's performance neglecting the filter in an AWGN ideal condition that performs closely to the theoretical curve as was observed in the receiver validation.

The performance degradation is the result of RF and despreading filtering generating an approximately constant error for the E_b/N_o levels simulated. However there is an

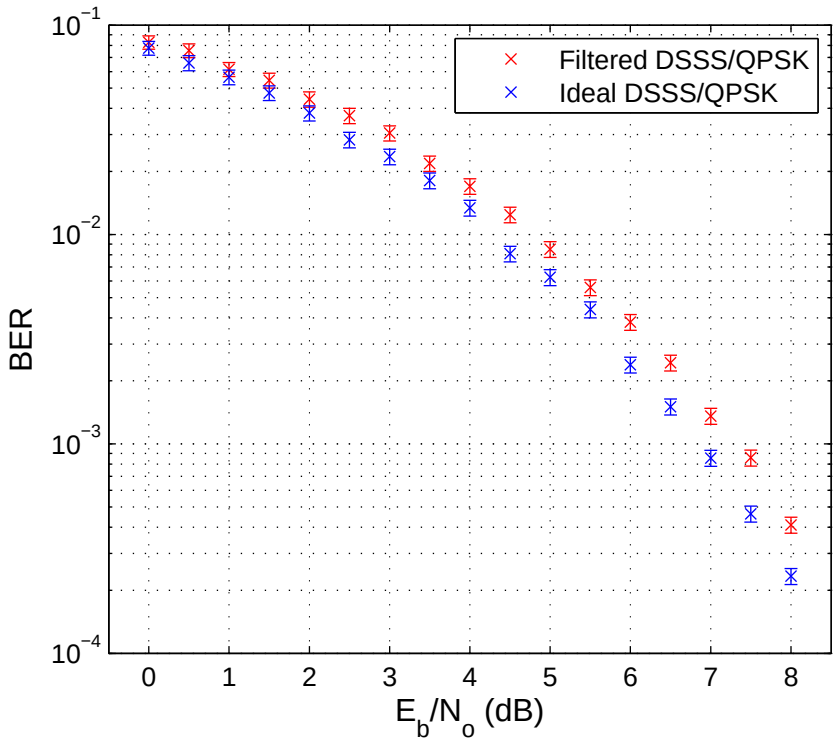

Figure 3.25: Simulated BER performance for DSSS QPSK receiver in AWGN channel illustrating the effect of band-pass filtering.

improvement in the SNR after each filter where the noise is filtered and attenuated in greater proportion compared with the signal. In Figure 3.26 are presented the linear relation of SNR_{RF} prior despreading the received filtered signal and SNR_{DS} after despreading and filtering the signal ($W_{Sim} \approx 201.5$ KHz $> W_{RF} \approx 62$ KHz $> W_{DS} \approx 2$ KHz). The plot shows the relation in respect to the input SNR_{Sim} that numerically represents an average increment of approximately 4.9 dB after W_{RF} filtering and 14.87 dB from W_{RF} to W_{DS} filtering. The latter result is tightly close to the theoretical processing gain using a Gold sequence of 31 chips length, i.e., $10\log_{10}(31) \approx 14.91$ dB.

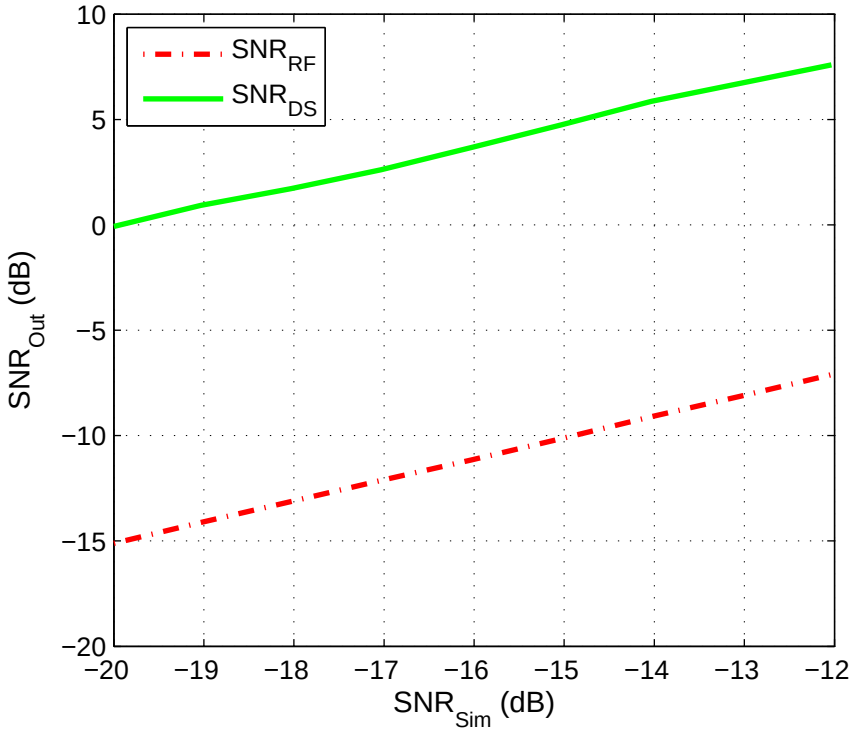

Figure 3.26: Comparison of input SNR_{Sim} and SNR_{Out} of the band-pass RF filter (SNR_{RF}) and despreading filter (SNR_{DS}).

3.5.3 Simulation to Determine the Jamming to Signal Ratio (JSR).

The JSR is a parameter that depends on jamming waveform and it is measured at the receiver. This research develop a simulation of the receiver to contrast the effect of different interference signals described in Section 3.4. It implies to vary the jamming signal increasingly in order to overcome the processing gain. For this purpose it is necessary select as a baseline the receiver performance in terms of BER at a specific E_b/N_o ratio in dB. It simulates a receiver static in respect to the jammer, also the simulated scenario assumes maximum antenna directivity in the jammer direction, neglecting the antenna pattern and assuming that the desired signal is received with constant power. From the DSSS receiver perspective it allows to observe a specific BER performance for a given energy per bit

and noise power spectral density that remain constant while the interference average power varies with respect to the average signal power.

Under the assumption considered previously the performance comparison is based on the jamming margin required to degrade the receiver performance chosen by one order of magnitude. From that point it has been considered that the interference overcomes the processing gain of the DSSS receiver. Chapter IV provides results using the jammer models presented in Section 3.4 in plots of BER versus JSR after the RF filter in order to evaluate the performance of a QPSK for different interference waveforms. Finally all jammers are compared in respect to the JSR and processing gain required to degrade the DSSS BER by one order-of-magnitude relative to a BER of E_b/N_o =7 dB with no interference present. The variation of the jamming bandwidth is explored for the broadband jammers and the duty cycle for the pulsed jammers with the goal of determining their optimum responses. Finally the most effective jammers are evaluated on the receiver for the JSR found by changing the input E_b/N_o.

IV. Results and Analysis

This chapter presents the results and analysis of different jammers' performance in a simulated DSSS QPSK receiver. The parameters considered in the simulation follow Table 3.1. The sampling frequency for all simulated jammer was 403 KHz to avoid aliasing based on passband spreading bandwidth W_J=62 KHz and using an oversampling factor of 1.5. The simulation was performed considering a DSSS QPSK receiver due to its performance and bandwidth efficiency compared with binary PSK or DPSK. The conditions for the simulation assume that the receiver is perfectly synchronized with the carrier frequency ignoring mixing losses or errors due to phase variation. Also the despreading process considers a perfectly synchronized sequence. The results presented were obtained by generating a message of 1000 symbols length for a fixed E_b/N_o=7 dB that corresponds to BER=1.4×10^{-3}. The input JSR $\in [-15, 15]$ dB in increments of 2 dB with the goal of determining a BER degradation of one order-of-magnitude. The E_b/N_o point chosen and the JSR range is a trade-off between simulation time and interference assessment accuracy, however the constraints considered allow to compare between different jamming techniques.

4.1 Simulation of Broad-band Jammers

Figure 4.1 shows the performance of broad-band jammers that include BBN with a bandwidth greater than the spreading bandwidth W_{ss}, FHI, CSI, MTJ and RFMI with a bandwidth that covers exactly W_{ss} and centered at carrier frequency. The horizontal axis represents the JSR at the output of the RF filter (JSR_{RF}) denoting that for BBN using the simulation bandwidth $F_s/2$ the jamming power is decreased considerably because the filter eliminates the spectral component out of the band W_{ss}. The red line represent the BER=1.4×10^{-2} at which the receiver performance is degraded in one order-of-magnitude

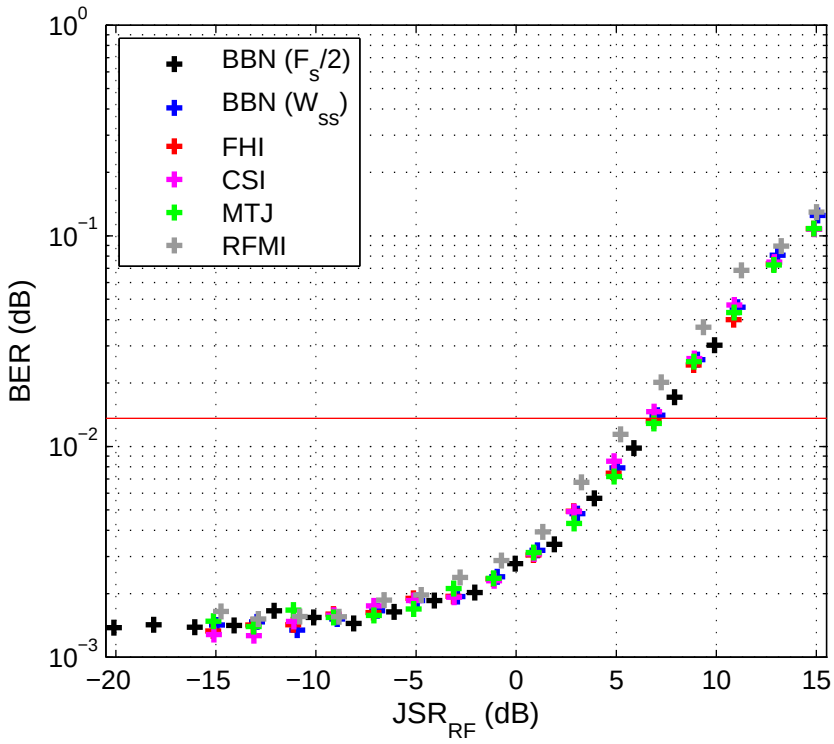

Figure 4.1: Broad-band jammer BER performance versus JSR_{RF} for E_b/N_o=7 dB.

from the baseline at E_b/N_o= 7 dB. In general all broad-band jammers behave similarly for the JSR range simulated with the exception of RFMI that produces slightly more degradation and also requires slightly less JSR_{RF} signal to pass the BER reference point (red line). The BBN ($F_s/2$) results in the least effect due to its PSD being distributed uniformly over the simulated channel bandwidth and consequently its average power is attenuated more by the RF filtering.

4.2 Simulation of Continuous Wave and Narrow-band Noise Jammers

The Figure 4.2 present the JSR curves for CW interferers and for narrow-band jammers. The CW jammers include LFMI, tone jammer and BPSK. Narrow-band jammers include filtered noise for two different jammer bandwidths (W_J), including W_J=7.75

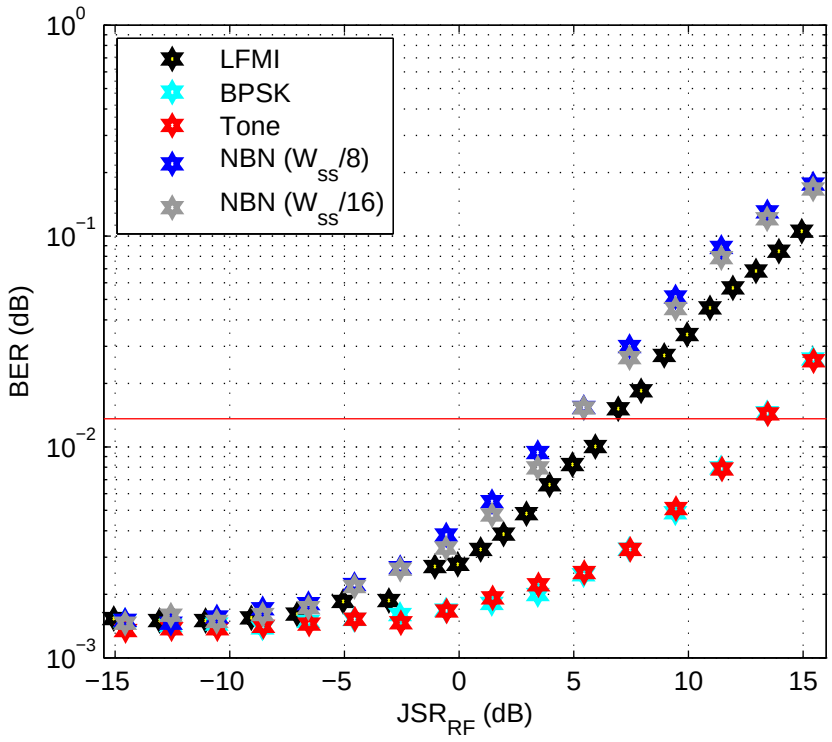

Figure 4.2: CW and NBN BER performance versus JSR_{RF} for E_b/N_o=7 dB.

KHz ($W_{ss}/8$) and W_J=3.875 KHz ($W_{ss}/16$). Results denote that for tone and BPSK the performance is similar requiring more JSR_{RF} to reach the jamming margin, i.e. the point where the curve passes the red line. LFMI interference presents a considerably better jamming performance than BPSK and tone jammers occupying the spreading bandwidth W_{ss}. On the other hand colored noise perform better than CW interference occupying fraction of the spreading bandwidth with slight performance improvement when the bandwidth is $1/8$ of W_{ss} compared to $1/16$ of W_{ss}. The colored noise interference using a narrow bandwidth requires approximately 1.63 dB less JSR_{RF} than LFMI and approximately 8.3 dB and 8.4 dB less JSR_{RF} for BPSK and tone jamming respectively.

4.3 Simulation of Pulsed Jammers

For pulse interference the average jamming power spectral density can be expressed as the ratio between the jammer PSD and the duty cycle ρ as J_o/ρ and the equivalent noise PSD at the receiver is N_{oe} [7]:

$$N_{oe} = N_o + J_o/\rho, \tag{4.1}$$

and the symbol error probability P_s for pulse jammer is

$$P_s \cong \rho Q\left(\sqrt{2E_sN_o + J_o/\rho}\right) + (1-\rho)Q\left(\sqrt{2E_sN_o}\right), \qquad 0 \le \rho \le 1. \tag{4.2}$$

When ρ is treated as a continuous variable over $[0, 1]$ and $J_o \gg N_o$, the value that maximizes P_s is:

$$\rho_o \cong \begin{cases} 0.7\left(\frac{E_s}{J_o}\right)^{-1}, & \frac{E_s}{J_o} > 0.7 \\ 1, & \frac{E_s}{J_o} \le 0.7 \end{cases} \tag{4.3}$$

The worst-case pulse interference from the receiver perspective is more effective than continuous interference if $E_s/J_o > 0.7$. Substituting $\rho = \rho_o$ into Equation (4.2), P_s when $J_o \gg N_o$ is:

$$P_s \cong \begin{cases} 0.083\left(\frac{E_s}{J_o}\right)^{-1}, & \frac{E_s}{J_o} > 0.7 \\ Q\sqrt{\left(\frac{2E_s}{J_o}\right)}, & \frac{E_s}{J_o} \le 0.7 \end{cases} \tag{4.4}$$

According to the preceding expression the bit error probability performance is a function of pulse duty cycle ρ and the optimum ρ decreases as E_s/J_o ratio increases. It is the worst jamming case scenario that maximize the jamming effectiveness. In Figure 4.3 are presented simulated results for pulsed jamming waveform as BER versus JSR after the RF filter. Plots are considered for a variable duty cycle as a function of the JSR and for a

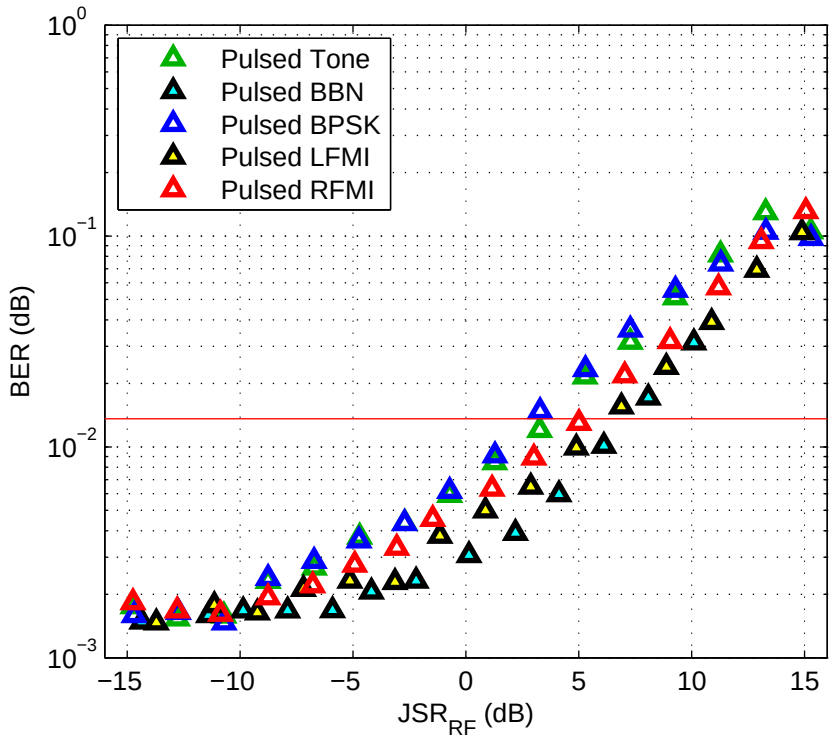

Figure 4.3: Pulsed jamming BER performance versus JSR_{RF} for E_b/N_o=7 dB and ρ varying according to Equation (4.3).

fixed pulse-width of 0.1 milliseconds, that is equivalent to a bandwidth $W_J \approx 20$ KHz. This computation was concluded after plotting JSR for different duty cycles and due to analysis of theoretical P_s in Equation (4.4) described in [13], [7], [11] and that show the worst jamming scenario is obtained when the duty cycle decreases as the JSR increases. Clearly results show that pulse BPSK presents the best performance with a required $JSR_{RF} \approx 3.05$ dB. Pulse tone requires approximately 0.74 dB more of JSR_{RF} to reach the jamming margin, whereas the pulse LFMI requires 3.38 dB, pulsed RFMI requires 2.25 dB and pulsed BBN requires 4.28 dB of additional JSR_{RF} to produce the same degradation, being the least effective of the pulsed jammers simulated.

Table 4.1: JSR_{RF} in dB required for broad-band jammers to degrade BER by one order-of-magnitude.

Jammer	BBN($F_s/2$)	BBN(W_{ss})	FHI	CSI	MTJ	RFMI	LFMI
JSR_{RF}	7.18	7.03	7.05	6.74	7.12	6.05	6.67
JSR_{DS}	-8.22	-8.04	-8.26	-8.57	-8.17	-7.98	-8.62
Imp. fact.	-15.40	-15.08	-15.32	-15.31	-15.29	-14.04	-15.29

4.4 Jammer Comparison

The JSR performance curves have been grouped all together in order to observe the general behavior once the signal has been received after the RF filter. The main objective of this measurement is to compare the effects of simulated partial-band interference, narrow-band interference, broad-band interference, CW and pulsed jammers. In Figure 4.4 is presented the BER performance of a total of 15 simulated jammers. It is possible to confirm that CW interference, single tone frequency, has the poorest effectiveness denoting slight difference between BPSK and single tone jamming. The BPSK jammer performs slightly better than tone jamming for different symbols generated randomly at the carrier frequency. The tone jammer is centered at the carrier frequency but the phase varies randomly in symbol by symbol basis within the interval between 0 and 2π. Also from this plot it is possible to conclude that pulsed BPSK presents the best performance followed closely by pulsed tone jamming. The narrow-band noise jammers require approximately 2 dB more of JSR_{RF} than pulsed BPSK. The broad-band jammer's performance is similar to pulsed LFMI and pulsed noise waveforms.

The summary of the numerical JSR_{RF}, expressed in dB, required to degrade the receiver performance to a BER=1.4×10^{-2} for 15 of the jammers simulated are shown

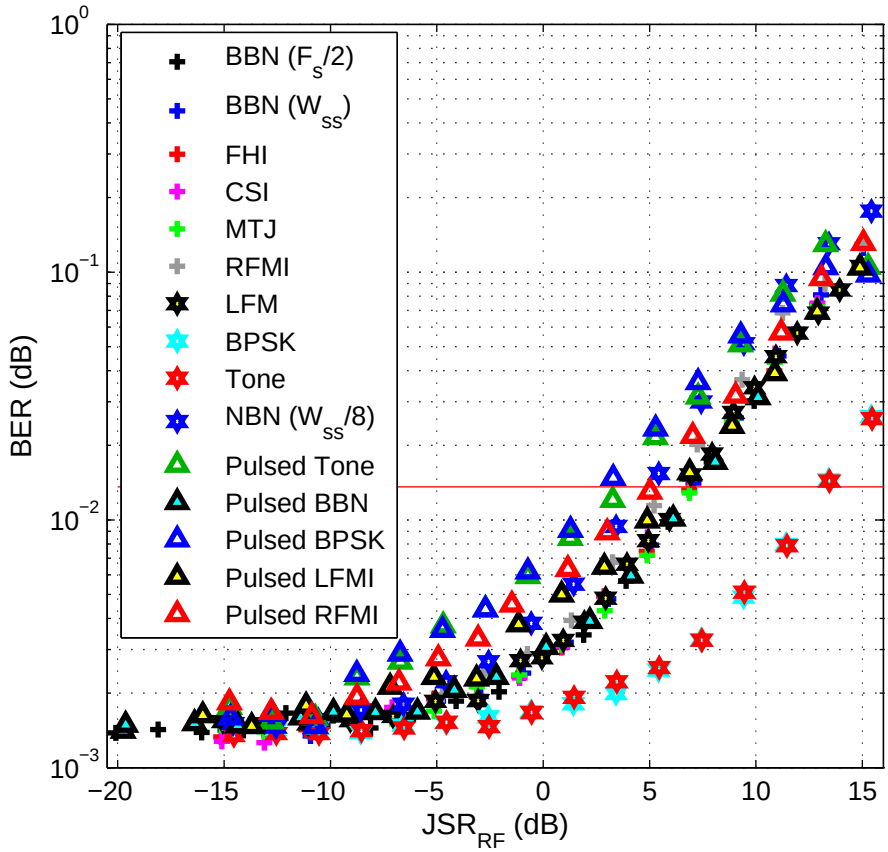

Figure 4.4: BER versus for JSR_{RF} comparing all jammer signals.

Table 4.2: JSR_{RF} in dB required for CW, Narrow-band noise and pulsed jammers to degrade BER by one order-of-magnitude.

Jammer	BPSK	Tone	NBN	P. BPSK	P. Tone	P. BBN	P. LFMI	P. RFMI
JSR_{RF}	13.30	13.48	5.04	3.05	3.80	7.33	6.43	5.30
JSR_{DS}	-2.39	-2.66	-7.72	-9.61	-8.68	-7.83	-8.58	-8.33
Imp. fact.	-15.69	-16.15	-12.77	-12.67	-12.49	-15.16	-15.02	-13.91

in Table 4.1 and Table 4.2 respectively. The NBN jammer correspond to the colored noise with a simulated bandwidth of $1/8$ of the spreading bandwidth (W_{ss}).

In presence of jamming, the processing gain also can be expressed as an improvement in the JSR at the despreading filter output (JSR_{DS}) compared to the JSR at after the RF filter. From data presented in Table 4.1 broad-band noise jamming present less JSR improvement compared to broad-band jammers, that is, the jamming power decreases in more proportion in comparison to the signal power. From Table 4.2 and consistent with Figure 4.4, tone and CW BPSK jamming present the least JSR improvement factor agreeing with its performance. Similarly pulsed BBN and pulse LFMI present improvement factors close to the improvement achieved for broad-band jammers with the exception of pulsed RFMI that performs approximately 1 dB better.

4.4.1 Effects of Jamming under Bandwidth and Duty Cycle Variation.

Considering the comparison of all simulated jammers and the close results of pulsed jamming and narrow-band jamming, this section analyzes the effect of varying the bandwidth for the broad-band interferers and the duty cycle for pulsed jammers in order to find the optimal responses for those jammer with better results in term of effectiveness in the simulated DSSS QPSK receiver. From the analysis of broad-band and narrow-band jamming it was observed from Figure 4.1 and Figure 4.2 that changing the bandwidth of noise jamming varies the effectiveness in terms of JSR_{RF} required and BER degradation. In order to analyze the effect of bandwidth variation for broad-band interference a simulation for the baseline E_b/N_o=7 dB and a JSR=5 dB were run. Figure 4.5 shows BER versus jammer bandwidth for $[0, 62]$ KHz where W_{ss}=62 KHz and $W_J \approx 0$ represents the single tone jamming frequency. This simulation denotes that approximately from 10 to 40 KHz of bandwidth, the average response is optimal with a maximum BER degradation depending on the jamming waveform. The CSI and MTJ were simulated for a total of 100 frequencies in the spreading bandwidth but the number of frequencies vary according to the bandwidth.

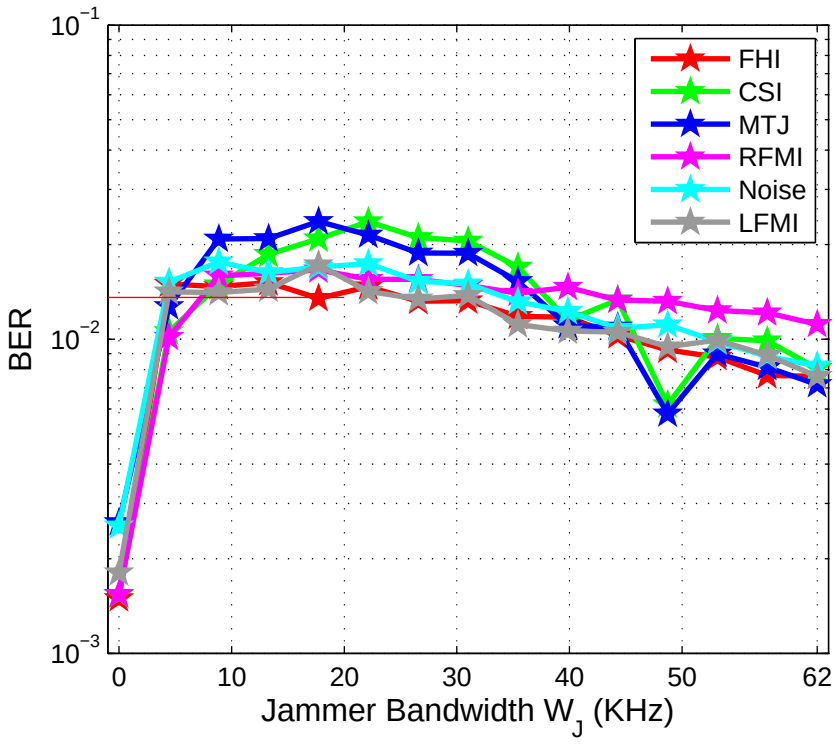

Figure 4.5: BER performance versus bandwidth variation for broad-band jammers for JSR= 5 dB and E_b/N_o=7 dB, where $W_J \approx 0$ represents single tone jamming frequency.

FHI differs in respect to the total of frequencies generated. For a given time hopping less than the symbol interval and considering 1000 symbols a total of 2600 frequencies were generated from random permutations considering the spreading bandwidth centered at the carrier frequency. The Figure 4.5 shows that CSI and MTJ generate more degradation with a BER=2.3×10^{-2} using $W_J \approx 22.1$ KHz and $W_J \approx 17.71$ KHz of bandwidth respectively. The minimum BER performance was obtained for a $W_J \approx 48.7$ KHz. These were CSI and MTJ cases, due to the tones separation varies with the bandwidth for a fixed number of tones N_t=100, resulting in a jammer PSD with frequency components distributed farther from the jamming central frequency f_j that are significantly spread after convolving with the spreading waveform and consequently filtered out the signal bandwidth W_{DS}=2 KHz.

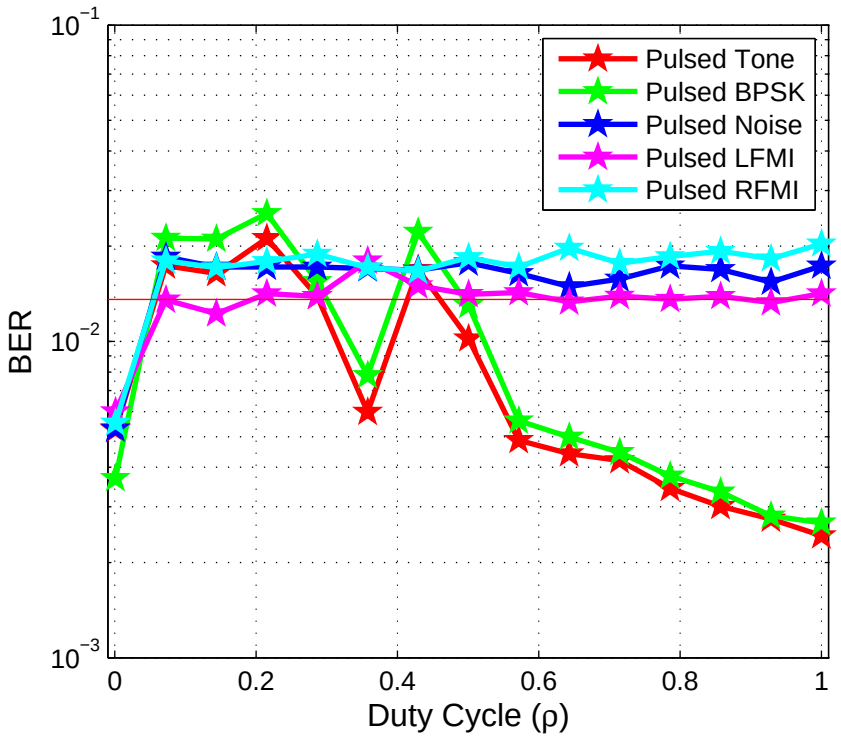

Figure 4.6: BER performance effect for duty cycle variation $\rho \in [10^{-3}, 1]$ for pulsed jamming.

Figure 4.6 shows BER performance for different pulse jammers when the duty cycle $\rho \in [10^{-3}, 1]$ that confirms that pulsed BPSK is the most effective pulsed jamming technique between other pulsed waveforms simulated. The simulation was run for the JSR required to degrade the performance to a BER=1.4×10^{-2} and for an $E_b/N_o = 7$ dB. Pulsed tone and pulsed BPSK jammers show the best performance with a duty cycle ρ=0.21 using a JSR=5 dB. Pulsed noise simulation was run for a JSR=13 dB with the maximum BER corresponding to a duty cycle ρ=0.07, pulsed LFMI and pulsed RFMI were simulated with a JSR of 7 dB with maximum BER at ρ=0.36 and ρ=0.64 respectively. The JSR requirement and maximum ρ value was the result of convolving the pulsed windows and broad-band waveforms in the frequency domain. The duty cycle variation ρ for a

pulse duration τ=100 useg implies that pulse repetition period T_p varies inversely. For pulsed BPSK and pulsed tone jammers with ρ=0.36 the simulattion showed that the BER performance changed abruptly independent of the number of required bit for that particular performance. In this case, the convolution of pulsed window is performed with a narrow-band CW signal with $W_J \approx$ 2 KHz. Consequently, as ρ increases the T_P decreases but the spectral separation of frequency components for multiples of $1/T_p$ increase, resulting in an abrupt jammer energy reduction after despread and filter the signal in the bandwidth W_{DS}=2 KHz. However, the duty cycle relevant for pulsed jammer analysis considered was ρ=0.21.

4.4.2 Narrow-band and Pulsed Jamming Comparison.

According to Figure 4.4 pulsed tone, pulsed BPSK jammers and the narrow-band noise jammers were the most effective. However the effect of varying the bandwidth also denoted that for certain values of bandwidth the BER versus JSR_{RF} curves perform better requiring less JSR_{RF} to degrade the receiver's performance in comparison to the broad-band jammers previously simulated. Based on BER versus bandwidth the jamming's BER performance for each jammer at the optimum bandwidth are presented in Figure 4.7. The results show that both MTJ and CSI perform similar requiring the minimum JSR_{RF} to degrade the BER performance in one order-of-magnitude with respect to the other jammer presented. MTJ requires approximately a $JSR_{RF}\approx$3.03 dB to degrade the BER to a P_b=1.4×10^{-2}, followed by CSI that requires a $JSR_{RF}\approx$3.09 dB. In contrast, FHI, LFMI, NBN and RFMI require at least a $JSR_{RF}\approx$4.9 dB to degrade the BER to the same level. Also it is observed that for JSR_{RF}>10 dB MTJ and CSI achieve less degradation compared with the rest of the jammers simulated.

In Table 4.3 are summarized the JSR_{RF}, JSR_{DS} and the improvement factor for broad-band jammers simulated with an optimum bandwidth at the BER=1.4×10^{-2}. The results denote that both MTJ and CSI jammers present the best performance. Also from Table 4.3

Table 4.3: The JSR_{RF} in dB for broad-band jammers.

Jammer	FHI	MTJ	RFMI	NBN	CSI	LFM
JSR_{RF}	4.92	3.03	5.12	4.92	3.09	5.08
JSR_{DS}	-7.58	-9.29	-7.50	-7.73	-9.57	-7.42
W_J	13.3	17.71	17.71	8.86	22.1	17.71
Imp. fact.	-12.50	-12.33	-12.63	-12.66	-12.66	-12.51

it is observed that the effect of finding an optimum bandwidth results in greater JSR improvement and consequently more effectiveness in favor of narrow-band jamming using an optimum bandwidth in comparison to the improvement factors presented in Table 4.1 for broad-band jammers. The improvement factors presented in Table 4.3 are close to the improvement factors for pulsed BPSK and pulsed tone jammers consistent with the required JSR_{RF}.

Also the effect of duty cycle variations are presented in Figure 4.8 for the two most effective pulsed jammers presented in Section 4.4.1, pulsed BPSK and pulsed tone jammers, curves in blue and green respectively. These results were simulated with a duty cycle variation according to Equation (4.4), that is, every JSR point has a duty cycle that is in inverse proportion to the E_s/J_o ratio. On the other hand, curves in red and gray represent the performance when the optimum value of duty cycle is chosen from Figure 4.6 that corresponds to ρ=0.21 for pulsed BPSK and pulsed tone respectively. This result confirms that Equation (4.4) corresponds to the worst case pulsed jamming scenario showing that both pulsed BPSK and pulse tone require less JSR to degrade the BER to a P_b=1.4×10^{-2} in comparison to the simulation with an optimum duty cycle ρ=0.21, although the differences are on the order of hundredths of a decibel. Also it is observed that over a JSR_{RF}=10 dB, pulsed tone jammer with a duty cycle ρ=0.21, achieves slightly more BER degradation than pulsed BPSK.

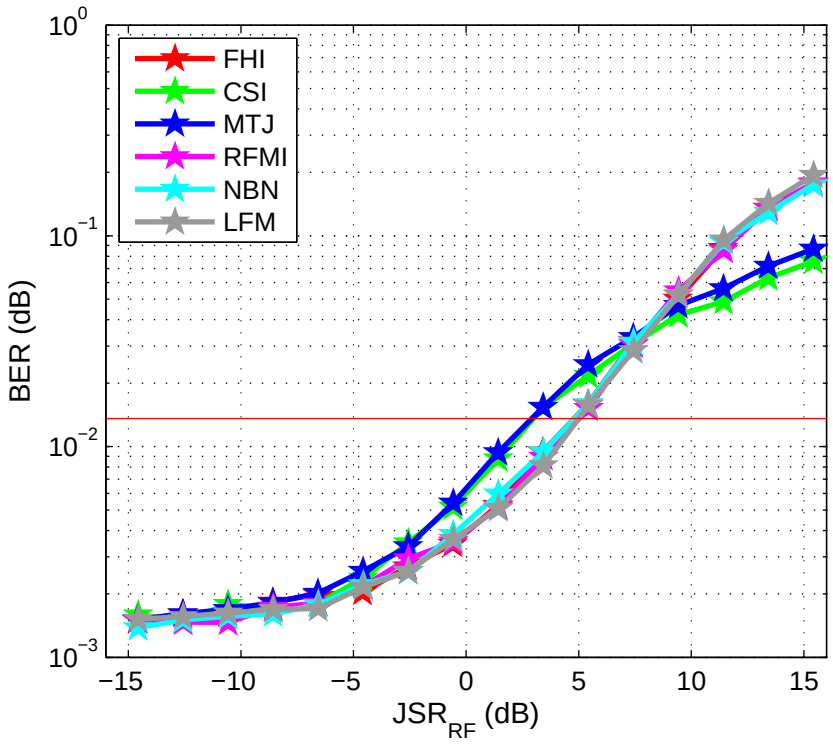

Figure 4.7: BER performance with optimum bandwidth for broad-band jammers for an E_b/N_o=7 dB.

4.4.3 Optimum Bandwidth for Pulsed Broad-band Jammers.

Another important point derived from bandwidth's and duty cycle's analysis is the BER performance for pulse jamming implemented using a pulsed window and a broad-band waveforms (waveforms with a bandwidth equal or greater than the spreading bandwidth W_{ss}) compared to pulse jamming using waveform with optimum bandwidth. Previously pulsed BBN, pulsed RFMI and pulsed LFMI jammers required JSR_{RF} values of approximately 2.2 dB to 4.3 dB more than the pulsed BPSK jammer. Based on this results and the optimized bandwidth analyzed in Section 4.4.1. Figure 4.9 show simulations for pulsed jammers with optimized bandwidth along with pulsed broad-band jammers with non-optimal bandwidth. The pulsed window applied on broad-band waveforms

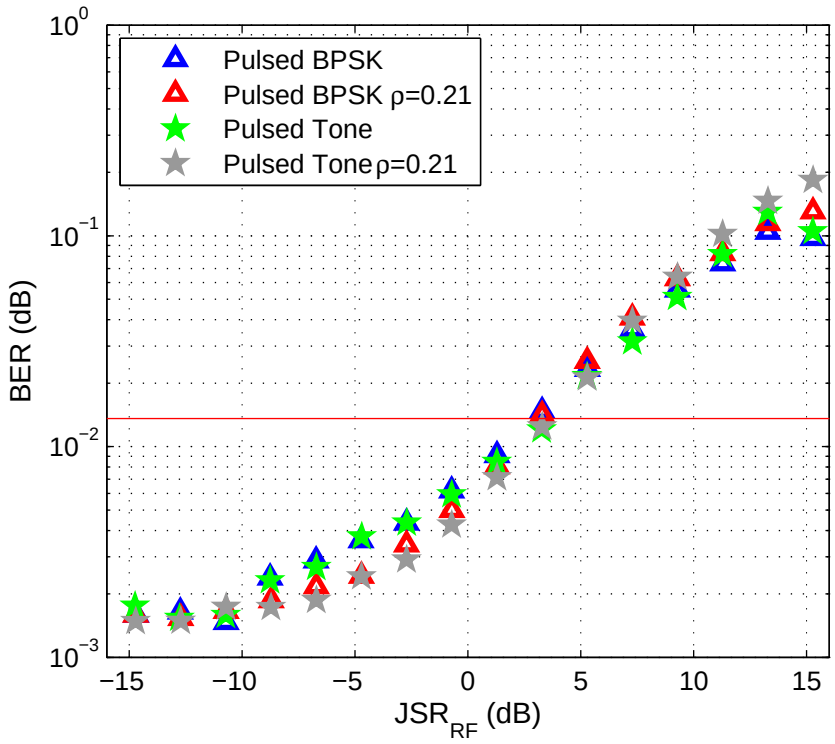

Figure 4.8: Comparison of BER performance for pulsed BPSK and pulsed tone for changing the duty cycle and E_b/N_o=7 dB.

did not improve the JSR_{RF} as it did when it was applied on CW BPSK and CW tone, where the JSR_{RF} was between 9 dB to 10 dB approximately. However the combination of the optimum bandwidth for broad-band waveforms and pulsed window improve the jamming effectiveness. The pulsed broad-band jammers, using the optimum bandwidth $W_J \approx 17.71$ KHz found previously, resulted in a required $JSR_{RF} \approx 3.92$ dB for pulsed RFMI, $JSR_{RF} \approx 3.98$ dB for pulsed LFMI and $JSR_{RF} \approx 3.81$ dB for pulsed noise with an optimum bandwidth $W_J \approx 8.86$ KHz, denoting a JSR_{RF} improvement of approximately 2.44 dB, 1.36 dB and 3.51 dB respectively in respect to the pulsed jammers generated from broad-band waveform presented in Table 4.2. After using the optimum bandwidth for pulsed broad-band jammers, the results approach to the pulsed BPSK performance with approximately 1

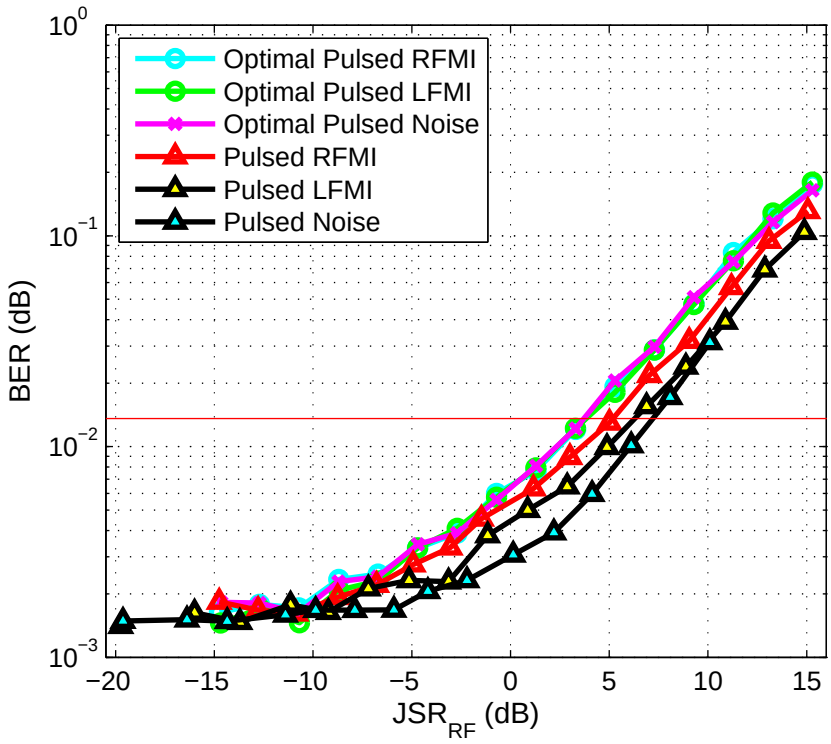

Figure 4.9: BER performance comparison for optimal bandwidth pulsed jammers and non-optimal bandwidth pulsed jammers.

dB of difference in the required JSR_{RF}. Also the simulations show that pulsed broad-band jammers with optimum bandwidth produce more degradation above JSR_{RF}=13 dB.

4.5 Analysis for Optimum Jammers

Considering the different jamming techniques compared and the effect of bandwidth and duty cycle variation, it is possible to conclude that MTJ, pulsed BPSK and CSI present the optimum performance in terms of requiring a JSR_{RF} range from 3.03-3.09 to degrade the DSSS QPSK receiver. The Figure 4.10 shows the optimum jammers denoting that MTJ requires $JSR_{RF}\approx$3.03 dB followed by pulsed BPSK that requires JSR_{RF}=3.05 dB and CSI requires $JSR_{RF}\approx$3.09 dB.

In Figure 4.11 are shown the BER versus E_b/N_o results for the best jammers found: MTJ, BPSK, CSI. The NBN jammer for an optimum bandwidth $W_J \approx 8.86$ KHz is presented as a reference due to it presents similar performance to the optimized FHI, RFMI and LFMI jammer. The receiver's performance with no jamming is shown to compare results with the jamming's degradation as the E_b/N_o varies. The simulations consider a fixed JSR_{RF}=3.1 dB to reach a BER's degradation to P_b=1.4 $\times$ 10^{-2} which is approximately equivalent to the receiver's performance in absence of jamming for an E_b/N_o=4.5 dB. The plot shows that, for an E_b/N_o=7 dB (SNR_{RF}=-8.1 dB) and JSR_{RF}=3.1 dB, indicated with a segmented vertical red line, the receiver under the incidence of the most effective jammers degrades its performance to a BER=1.4 $\times$ 10^{-2} or one order-of-magnitude in respect to the BER for E_b/N_o= 7 dB with no jamming. It is observed that NBN jammer does not achieve the BER degradation, due to it requires JSR_{RF}=4.9 db consistent with previous results. However, for the best jammers as the $E_b/N_o > 7$ dB there is a slight reduction of BER due to average noise power decreases. However, above E_b/N_o=9 dB, as the noise decreases considerably, its impact on BER becomes negligible in comparison to the errors caused by the jamming power, generating a fixed BER that trends to a P_b=10^{-2}. This result is because at high E_b/N_o and a fixed JSR the average noise power N trends to zero and the JSR becomes dominant. Considering the theoretical BER for DSSS QPSK receiver according to Equation (3.14) with equivalent noise power spectral density $N_{oe} = N_o + J_o$ yields :

$$P_b \approx Q\left(\sqrt{\left(\frac{2E_b}{N_o + J_o}\right)}\right), \tag{4.5}$$

as the average noise power N trend to zero, the P_b for high E_b/N_o, the P_b goes asymptotically to:

$$\lim_{N\to 0} \implies P_b \approx Q\left(\sqrt{\frac{2E_b}{J_o}}\right) = Q\left(\sqrt{\frac{E_s}{J_o}}\right) = Q\left(\sqrt{\left(\frac{S \cdot T_s}{J/W_{ss}}\right)}\right). \tag{4.6}$$

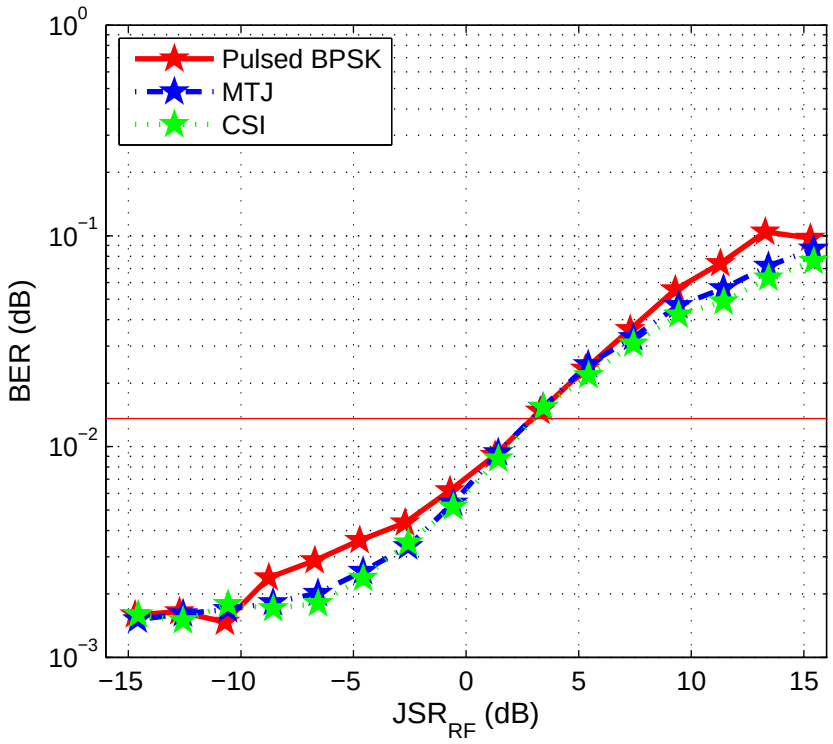

Figure 4.10: Pulsed BPSK, MTJ and CSI, the most effective jammers for E_b/N_o=7 dB.

As a general analysis, the JSR_{DS} values result in a variable reduction with respect to the input JSR_{RF}, depending on the jamming waveform, due to desired signal is despread conserving its average energy with typical power losses after filtering that approximate to 10% comparing to the average energy before the bandpass filter, that normally in PSK modulation corresponds approximately to 90% of the average power for the null-null bandwidth [33]. On the other hand, the jamming signal is spread across the sequence bandwidth limiting its average power not only because the processing gain but also because of the despreading filter effect. This characteristic of DSSS explain that JSR decreases reducing the jammings energy in favor of signal's energy. As the JSR improvement factor decreases it suggest the jamming waveform is more effective. The simulations with optimum bandwidth for broad-band jammers in Table 4.3 denoted that the jamming

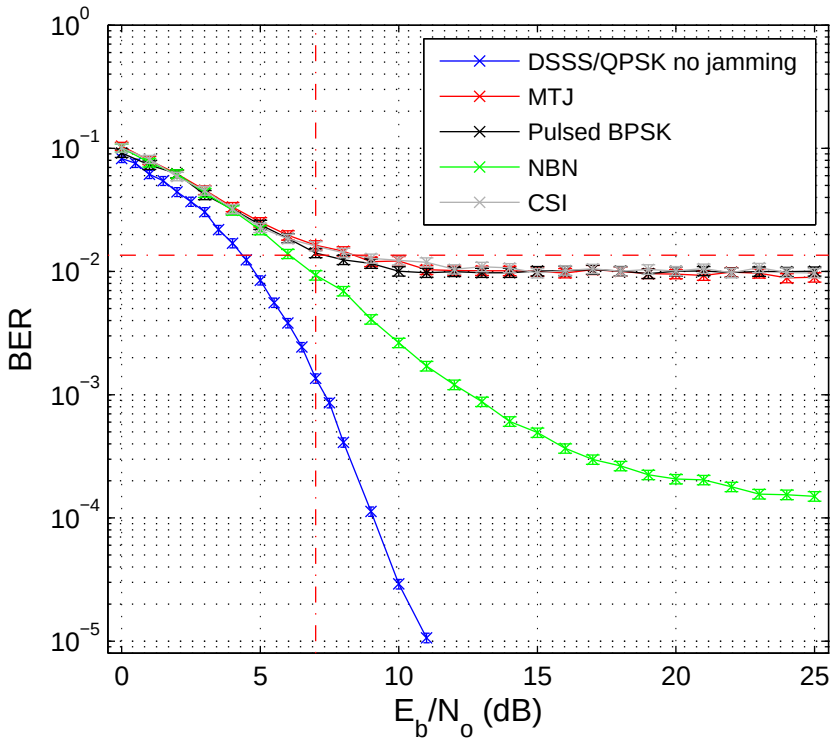

Figure 4.11: BER performance for the optimized jammers at JSR_{RF}=3.1 dB.

improvement factor resulted in approximately 3 dB better than the values presented in Table 4.1 for the non optimized jammers. Besides, the jamming improvement factors are consistent with the most effective jammers found.

The bandwidth consideration is key to affect the performance of the simulated DSSS QPSK receiver with matched filtering implementation. However there is not a specific optimum bandwidth for each waveform and it requires simulations and comparisons. Under this perspective the pulsed BPSK required less parameter variations to affect the receiver performance, considering a variable duty cycle in function of the JSR.

V. Conclusions

5.1 Research Contributions

This research provides a comprehensive characterization of intentional interference and the evaluation of the effects in a DSSS QPSK receiver as a function of the JSR degrading reference BER (P_b) by one order-of-magnitude. Also jamming parameter variation such as bandwidth and duty cycle of pulsed interferers was explored. Results delivered give a reference for required simulated JSR to degrade a DSSS QPSK receiver considering traditional jamming techniques available in open literature. Also this research gives a simulated perspective of varying jamming waveform parameters and how the jamming in DSSS can be optimized. The receiver model utilized for jamming assessment was developed with the idea of implementing and varying parameters such as spreading sequences or testing M-ary PSK and DPSK modulations with low complexity and good flexibility. The receiver model has been validated with respective analytical P_b expressions for binary and 4-ary DPSK and PSK cases.

5.2 Results Found

The DSSS QPSK simulated receiver result in a degraded performance of approximately 0.5 dB as a consequence of the RF and despreading filter incorporated to analyze the bandwidth effects on the receiver before and after despreading the received signal. This effect is due to filter coloration and signal attenuation. The SNR improvement from the input (SNR_{sim}) to the output of the spreading filter (SNR_{DS}) was approximately 19.8 dB and the processing gain measured from after the RF filter(SNR_{RF}) to the despreading filter output (SNR_{DS}) was 14.87 dB, very close to the analytical processing gain for Gold code of N_c=31 chips which is $10\log 10(31) \approx 14.91 dB$.

The tone jamming and the BPSK jammer were the least effective techniques with a required $JSR_{RF} \approx$ 13.3 and $JSR_{RF} \approx$13.48 dB respectively.

Broadband jammers resulted in a better performance in comparison with the tone jammers with slight variations, depending on the waveform simulated, because they required JSR_{RF} varied between 6-7.18 dB to degrade the BER to $P_b = 1.4 \times 10^{-2}$ reference. That is the case of LFMI, FHI, MTJ, RFMI and CSI. Regarding to noise jamming, the effect of taking a smaller fraction of the noise bandwidth such as $W_J = W_{ss}/8$ and $W_J = W_{ss}/16$ reduce the required JSR_{RF} by approximately 2 dB.

The pulsed BPSK jammer obtained the best performance between the jammers analyzed with a required $JSR_{RF} \approx 3.05$ dB. However pulsed BBN required $JSR_{RF} \approx 7.33$ dB to reach the threshold that is even more than the broadband interferers discussed with maximum values around $JSR_{RF} \approx 7.1$ dB. Generating pulsed jamming waveforms using tone jamming significantly improved the jamming performance by approximately 9.6 dB, whereas for pulsed LFMI improvement was just 0.24 dB. Regarding to pulsed noise the simulation resulted in a poorer performance compared with NBN with a required JSR_{RF} close to 7.33 dB that is approximate 2.1 dB more.

Considering the differences between broad-band jammers and the best case of pulsed jammers which was near to $JSR_{RF} \approx 3$ dB, the improvements achieved for noise jammers by reducing the bandwidth and also the high JSR required for tone jamming, the effect of bandwidth variation for broad-band jammers was explored. The analysis showed that for $W_J \approx 10$ KHz to $W_J \approx 40$ KHz it was possible to optimize the jamming performance and the jammers that generated more degradation were MTJ using a bandwidth $W_J \approx 17.7$ KHz and CSI with a bandwidth $W_J \approx 22.1$ KHz obtaining a required $JSR_{RF} \approx 3.03$ dB and $JSR_{RF} \approx 3.09$ dB respectively. In regard to LFMI, RFMI the optimum bandwidth found was $W_J \approx 17.7$ KHz with similar required $JSR_{RF} \approx 5.08$ dB and $JSR_{RF} \approx 5.12$ dB respectively.

With respect to FHI and NBN the optimum bandwidths required were $W_J \approx 13.3$ KHz and $W_J \approx 8.86$ KHz respectively for a required $JSR_{RF} \approx 4.9$ dB for both jammers.

The effect of varying the duty cycle ρ for the pulsed jammers showed that $\rho = 0.21$ was the optimum duty cycle. However in terms of JSR_{RF} the results do not vary significantly in respect to the worst case pulsed jamming which has a duty cycle that changes as the inverse of the E_s/J_o ratio.

As a general conclusion the most effective jamming technique between those analyzed in this research was pulsed BPSK. The jamming effectiveness from the baseline AWGN interference denoted that broadband jamming waveforms can increase the degradation when the bandwidth is chosen wisely.Using optimum bandwidth allowed decreasing the required JSR by approximately 2 dB for BBN, RFMI, LFMI and FHI relative to the same jammers with sub-optimal bandwidth. But also it was demonstrated, in a simulated environment, that MTJ and CSI with optimum bandwidth result in a reduction in the required JSR of approximately 4.1 dB and 3.6 dB respectively matching the best jammer found, that is, pulsed BPSK with a variable duty cycle that follows the worst case analytical expression in Equation (4.4) for pulsed jamming. Also in this research was demonstrated that the processing gain expressed as a comparison between the JSR at the despreading filter with respect to the JSR at the output of the RF filter increases when the jammer are optimized, agreeing with the most effective jammers and it is approximately 3 dB lower for the least effective jammers.

Finally it can be concluded that jammer bandwidth choice is the most important parameter to degrade the performance of the DSSS QPSK with matched filtering implementation. However the optimum bandwidth depends on the waveform chosen. The optimum results implemented with Gold sequence $N_c = 31$ chips require at least $JSR_{RF} \approx 3$ dB to degrade the receiver's BER by one order-of-magnitude; this was the case for pulsed BPSK, MTJ and CSI jammer with optimum bandwidths.

5.3 Recommendations for Future Research.

In this research several jamming waveform have been analyzed considering a DSSS QPSK receiver using Gold code spreading. Besides, the interference assessment was performed under the assumption of a perfect channel, synchronized receiver and supposing a case where the receiver is stationary and the interferer approaches the receiver to induce increased jamming power. Future research areas that can be considered are:

1. Analysis of the effect of comparing different spreading sequences for the jammers evaluated in this research and the extension for long sequence to explore if the optimum bandwidth and jamming improvement factor for broad-band jammers keeps similar proportion for large sequences in respect to shorter sequences.
2. Analysis of the effect of error correction and interleaving over the most effective jammers assessed in this research and what codes are more effective for particular waveforms.
3. Study of repeater jammers and the effects on synchronization [21], assuming that the jammer represent a delay copy of the desired signal. This topic involves developing code and carrier acquisition and tracking module in order to estimate code delay and frequency shit of interference signals.
4. Another area of research could include interference assessment under flat fading or selective fading. It implies channel estimation under the cases that the channel phase response is linear or when the channel gain and phase response varies with time and frequency. This area of research requires adding channel estimation and additional techniques for interference due to multipath such as channel equalization or rake receiver implementation. In [34] is explored the performance of DSSS over flat Rayleigh fading channels in single-tone interference further research could include other jamming waveforms analyzed in this thesis. Another reference for performance evaluation of PSK system in selective fading is studied in [35].

Bibliography

[1] R.A. Scholtz, "The Origins of Spread-Spectrum Communications," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 822–854, 1982.

[2] R. Price, "Further Notes and Anecdotes on Spread-Spectrum Origins," *IEEE Transactions on Communications*, vol. 31, no. 1, pp. 85–97, 1983.

[3] M. J. Marcus, "Early Civil Spread Spectrum History," [Online]. Available: http://www.marcus-spectrum.com/page4/SSHist.html, 2011.

[4] A. Viterbi, "Spread Spectrum Communications - Myths and Realities," *IEEE Communications Magazine*, vol. 17, no. 3, pp. 11–18, 1979.

[5] B. Sklar, *Digital Communications: Fundamentals and Applications*, Prentice Hall Communications Engineering and Emerging Technologies Series. Prentice-Hall PTR, 2001.

[6] G.R. Cooper and C.D. McGillem, *Modern Communications and Spread Spectrum*, Series in Electrical Engineering: Communications and Signal Processing. McGraw-Hill, 1986.

[7] D.J. Torrieri, *Principles of Spread-Spectrum Communication Systems*, Springer, 2005.

[8] S.S. Haykin, *Communication systems*, Wiley, 2001.

[9] M. Skolnik, *Radar Handbook, Third Edition*, Electronics Electrical Engineering. McGraw-Hill Education, 2008.

[10] C.E. Shannon, "Communication in the Presence of Noise," *Proceedings of the IRE*, vol. 37, no. 1, pp. 10–21, 1949.

[11] R. Poisel, *Modern Communications Jamming: Principles and Techniques*, Communications engineering. Artech House, Incorporated, 2004.

[12] M.K. Simon, *Spread Spectrum Communications*, Number v. 1 in Electrical engineering communications and signal processing series. Computer Science Press, 1985.

[13] R. L. Peterson, R.E. Ziemer, and D.E. Borth, *Introduction to Spread Spectrum Communications*, Prentice Hall International, 1995.

[14] A. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[15] Wenyuan Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, New York, NY, USA, 2005, MobiHoc '05, pp. 46–57, ACM.

[16] Yao Liu, Peng Ning, Huaiyu Dai, and An Liu, "Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication," in *Proceedings IEEE INFOCOM*, 2010, pp. 1–9.

[17] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short Paper: Reactive Jamming in Wireless Networks: How Realistic is the Threat?," in *Proceedings of the Fourth ACM Conference on Wireless Network Security*, New York, NY, USA, 2011, WiSec '11, pp. 47–52, ACM.

[18] Y. Bo, Sh. Gao-ping, and S. Hong-sheng, "An Automatic Interference Recognition Method in DSSS Communication System Based on SVM," in *2nd International Conference on Computer Engineering and Technology (ICCET)*, 2010, vol. 3, pp. V3–4–V3–8.

[19] Kewu Huang and Ran Tao, "Interference Suppression in Spread Spectrum Systems Using the CR-Fractional Fourier Transform," in *First International Conference on Pervasive Computing Signal Processing and Applications (PCSPA)*, 2010, pp. 560–563.

[20] M. Tilal and R. Minhas, *Effects of Jamming on IEEE 802.11p Systems*, M.S. Thesis, Chalmers Univ. of Technology, Gothenburg, Sweden, November 2010.

[21] J. Guo H.Wang and Z. Wang, "Evaluation of Security for DSSS Under Repeater Jamming," in *IEEE International Conference on Communications, ICC '07.*, 2007, pp. 5525–5530.

[22] A. Yousaf and A. Loan, "Effect of Jamming Technique on the Performance of Direct Sequence Spread Spectrum Modem," in *13th International Conference on Advanced Communication Technology (ICACT)*, 2011, pp. 874–877.

[23] S.M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, Prentice Hall Signal Processing Series. Prentice-Hall PTR, 1998.

[24] The MathWorks Inc., "Communications System Toolbox Documentation, R2013b," [Online]. Available: http://www.mathworks.com/help/comm/ug/digital-modulation.html, 2013.

[25] M. Temple, "Class Project, Synchronous DSSS Interference Suppression , EENG673 Spread Spectrum Communications," School of Engineering and Management, Air Force Institute of Technology, Wright-Patterson AFB OH, Sumer Quarter 2013.

[26] J.G. Proakis, *Digital Communications*, McGraw-Hill Series in Electrical and Computer Engineering. McGraw-Hill Education, 2001.

[27] M. K. Simon and M.S. Alouini, "A Unified Approach to the Probability of Error for Noncoherent and Differentially Coherent Modulations over Generalized Fading Channels," *IEEE Transactions on Communications*, vol. 46, no. 12, pp. 1625–1638, 1998.

[28] M.K. Simon and M.S. Alouini, *Digital Communication over Fading Channels: a Unified Approach to Performance Analysis*, Wiley series in telecommunications and signal processing. John Wiley & Sons, 2000.

[29] L. Pralon, B. Pompeo, G. Beltrao, H. Cioqueta, B. Cosenza, and J.M. Fortes, "Random Phase/Frequency Modulated Waveforms for Noise Radar Systems Considering Phase Shift," in *9th European Radar Conference (EuRAD)*, Oct 2012, pp. 314–317.

[30] M. Temple and S. Stone, "Class handout, EENG673 Spread Spectrum Communications," School of Engineering and Management, Air Force Institute of Technology, Wright-Patterson AFB OH, Sumer Quarter 2013.

[31] Sune R J Axelsson, "Noise Radar Using Random Phase and Frequency Modulation," *IEEE Transactions on Geoscience and Remote Sensing,*, vol. 42, no. 11, pp. 2370–2384, Nov 2004.

[32] N. Levanon and E. Mozeson, *Radar Signals*, Wiley, 2004.

[33] D.A. Guimaraes, *Digital Transmission: A Simulation-Aided Introduction with VisSim/Comm*, Signals and Communication Technology. Springer, 2010.

[34] Z. Guo-zhen, G. Yuan-Yuan, and M. Jing, "Performance Analysis of the Cooperative DS/SS Systems in Single-tone Interference Over Flat Rayleigh Fading Channels," in *International Conference on Communications, Circuits and Systems (ICCCAS)*, July 2010, pp. 126–130.

[35] T.L. Staley, R.C. North, Jianxia Luo, W.H. Ku, and J.R. Zeidler, "Performance Evaluation for Multichannel Reception of Coherent MPSK over Frequency Selective Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 4, pp. 877–894, Jul 2001.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
27–03–2014	Master's Thesis	Oct 2013–Mar 2014

4. TITLE AND SUBTITLE

Simulated Assessment of Interference Effects in Direct Sequence Spread Spectrum (DSSS) QPSK Receiver

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Rojas, Luis S., Captain, Chilean Air Force

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-14-M-64

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Intentionally Left Blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
This work is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
This research developed and validated a generic simulation for a direct sequence spread spectrum (DSSS), using differential phase shift keying (DPSK) and phase shift keying (PSK) modulations, providing the flexibility for assessing intentional interference effect using DSSS quadrature phase shift keying receiver (QPSK) with matched filtering as a reference. The evaluation compares a comprehensive pool of jamming waveforms at pass-band that include continuous wave (CW) interference, broad-band jamming, partial-band interference and pulsed interference. The methodology for jamming assessment included comparing the bit error rate (BER) versus required jamming to signal ratio (JSR) for different interferers using the Monte Carlo approach. This thesis also analyzes the effect of varying the jammer bandwidth for broad-band jammers including broad-band noise (BBN), frequency hopping interference (FHI), comb-spectrum interference (CSI), multi-tone jamming (MTJ), random frequency modulated interference (RFMI) and linear frequency modulated interference (LFMI). Also, the effect of changing the duty cycle for pulsed CW waveforms is compared with the worst case pulsed jamming equation. After the evaluation of different interferers, the research concludes that pulsed binary phase shift keying (BPSK) jamming is the most effective technique, whereas the CW tone jamming and CW BPSK interference result are least effective. It is also concluded that by finding an optimum bandwidth, FHI and BBN improves the required JSR by approximately 2.1 dB, RFMI and LFMI interference by 0.9 and 1.5 dB respectively. Alternately, MTJ and CSI improves their effectiveness in 4.1 dB and 3.6 dB respectively, matching the performance of the pulsed BPSK jammer.

15. SUBJECT TERMS
DSSS, QPSK, Jamming, Interference assessment, BBN, FHI, CSI, LFM, RFMI.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Richard K. Martin (ENG)
U	U	U	UU	95	19b. TELEPHONE NUMBER *(include area code)* (937)785-3636 xx4625 Richard.Martin@afit.edu