UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
CURSO DE GRADUAÇÃO EM ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

Murilo Pereira dos Reis

Comparação de Interferências Intencionais sobre Sistemas de Comunicação Digital Convencionais e com Espalhamento Espectral

Patos de Minas – MG
2023

Murilo Pereira dos Reis

Comparação de Interferências Intencionais sobre Sistemas de Comunicação Digital Convencionais e com Espalhamento Espectral

Projeto Final de Curso apresentado à Faculdade de Engenharia Elétrica da Universidade Federal de Uberlândia como requisito parcial para a obtenção do título de Engenheiro Eletrônico e de Telecomunicações.

Orientador: Prof. Dr. André Antônio dos Anjos

Patos de Minas – MG

2023

Murilo Pereira dos Reis

Comparação de Interferências Intencionais sobre Sistemas de Comunicação Digital Convencionais e com Espalhamento Espectral

Este Projeto Final de Curso foi julgado adequado para obtenção do Título de "Engenheiro Eletrônico e de Telecomunicações" e aprovado em sua forma final pelo Curso de Graduação em Engenharia de Eletrônica e de Telecomunicações.

Patos de Minas – MG, 30 de novembro de 2023.

Banca Examinadora:

Prof. Dr. André Antônio dos Anjos
FEELT – UFU

Prof. Dr. Davi Sabbag Roveri
FEELT – UFU

Prof. Dr. Pedro Luiz Lima Bertarini
FEELT – UFU

Agradecimentos

Aos meus pais, Danil e Maria Helena, cujo amor e dedicação durante estes 22 anos são o fundamento de toda esta jornada, minha mais absoluta gratidão.

À minha família, sou extremamente grato, por todo auxílio neste percurso.

Ao meu orientador, Professor André, cuja prestatividade, paciência e conhecimento guiaram e sustentaram este trabalho, o meu mais profundo agradecimento.

Aos professores e técnicos, obrigado por todos os ensinamentos e experiência que se propagarão até o fim da minha trajetória.

Por fim, aos meus amigos por tornarem mais felizes estes anos, que sejam afortunadas suas jornadas.

"Os problemas mais importantes e urgentes da tecnologia de hoje não são mais a satisfação das necessidades primárias ou dos desejos arquetípicos, mas a reparação dos males e danos causados pela tecnologia de ontem." (GABOR, 1970)

RESUMO

A difusão das comunicações digitais traz consigo preocupações sobre o seu possível uso malicioso. Na direção de inibir o mal uso destas tecnologias, contramedidas com interferências intencionais podem ser utilizadas. Este Projeto Final de Curso (PFC) busca comparar a eficiência das seguintes técnicas de bloqueio: (i) tom único, (ii) múltiplos tons, (iii) ruído de banda estreita (*narrow-band noise* - NBN), (iv) pulso com tom, (v) pulso com NBN e (vi) bloqueio por varredura. As técnicas de bloqueio serão avaliadas em um sistema de comunicação BPSK convencional e em um sistema com espalhamento espectral por sequência direta (DSSS), ambos operando em canal AWGN. O objetivo é identificar a técnica de bloqueio mais eficaz para cada cenário avaliado. Para viabilizar as análises, os sistemas de transmissão e recepção BPSK e DSSS BPSK, juntamente com os interferidores, foram simulados no software MATLAB®. Com base nas curvas de BER obtidas por meio da simulação, foram feitas comparações de desempenho dos dois sistemas sob ação de cada técnica de bloqueio avaliada no trabalho. Concluiu-se que o espalhamento espectral traz ganhos significativos de desempenho em cenários de interferência. Além disso, constatou-se que, no cenário apresentado e com os parâmetros de simulação utilizados, o bloqueio por tom único é o mais eficaz contra sistemas de comunicação digital convencionais. Já em relação ao sistema DSSS, a melhor técnica de bloqueio irá depender da relação sinal-ruído-interferência (SINR) sob a qual o receptor interferido estiver submetido.

Palavras-chave: Bloqueadores de RF. Comunicações Digitais. Espalhamento Espectral

ABSTRACT

The spread of digital communications raises concerns about their possible malicious use. In order to inhibit the misuse of these technologies, countermeasures with intentional interference can be used. This Final Course Project seeks to compare the efficiency of the following jamming techniques: (i) single tone, (ii) multiple tones, (iii) narrow-band noise (NBN), (iv) tone pulse, (v) NBN pulse and (vi) swept jamming. The jamming techniques will be evaluated in a conventional BPSK communication system and in a direct sequence spread spectrum (DSSS) system, both operating on AWGN channel. The objective is to identify the most effective jamming technique for each scenario evaluated. To enable the analyses, the BPSK and DSSS BPSK transmission and reception systems, and the jammers were simulated in the MATLAB® software. Based on the BER curves obtained through the simulation, comparisons were made of the performance of the two systems under the action of each jamming technique evaluated in the work. It is concluded that the spread spectrum brings significant performance gains in interference scenarios. Furthermore, it was found that single-tone blocking is the most effective against conventional digital communication systems in the scenario presented and with the simulation parameters used. Regarding the DSSS system, the best jamming technique will depend on the signal-to-noise-interference ratio (SINR) under which the interfered receiver is evaluated.

Keywords: RF Jammer. Digital Communications. Spread Spectrum.

Lista de figuras

Lista de abreviaturas e siglas

ANATEL	Agência Nacional de Telecomunicações
AWGN	*Additive white Gaussian noise*
BBN	*Broadband noise*
BER	*Bit error rate*
BPSK	*Binary phase shift keying*
CSS	*Chirp spread spectrum*
DEP	Densidade espectral de potência
DPSK	*Differential phase shift keying*
DSSS	*Direct sequency spread spectrum*
FHSS	*Frequency hopping spread spectrum*
FSK	*Frequency shift keying*
IIR	*Infinite impulse response*
IoT	*Internet of things*
JSR	*Jamming to signal ratio*
Mbps	Megabits por segundo
MPSK	*Multiple phase shift keying*
NBN	*Narrow-band noise*
OFDM	*Orthogonal frequency division multiplexing*
PBN	*Partial band noise*
PFC	Projeto final de curso
PN	Sequência pseudo-aleatório de espalhamento
PSK	*Phase shift keying*
QAM	*Quadrature amplitude modulation*
QPSK	*Quadrature phase shift keying*
SINR	*Signal to interference plus noise ratio*
SNR	*Signal to noise ratio*
SS	*Spread spectrum*
THSS	*Time hopping spread spectrum*
VANT	Veículo aéreo não-tripulado

Lista de símbolos

E_{b}	Energia média de bit
N_0	Densidade espectral de potência do ruído
T	Tempo de símbolo
T_{b}	Tempo de bit
$s_i\,(t)$	Símbolo
f_{c}	Frequência da portadora
n_{c}	Número de ciclos da portadora
$\phi_1\,(t)$	Função base
P_{e}	Probabilidade de erro de símbolo
S_{S}	Densidade espectral de potência do sinal em banda passante
S_{B}	Densidade espectral de potência do sinal em banda base
ρ	Eficiência espectral de potência
R_{b}	Taxa de bits
B	Largura de banda do sinal
R_{c}	Taxa de chips
N	Comprimento da sequência de espalhamento
m	Número de *flip-flops* utilizados na geração da sequência de espalhamento
T_{c}	Tempo de chip
G_{P}	Ganho de processamento
J	Potência do sinal interferente
P	Potência do sinal
M_{J}	Margem de interferência
C	Capacidade de um canal de comunicação
W	Largura média de banda do sinal
N_{T}	Ruído médio total
J_0	Densidade espectral de potência do sinal interferente
ν	Fração do canal sob efeito do bloqueio

Sumário

Capítulo 1

Conceitos Introdutórios

1.1 Introdução

A partir do final do século XX, tecnologias digitais têm se tornado parte integrante do cotidiano da maioria dos seres humanos de forma acelerada (1, 2). O uso cotidiano de celulares (3), o crescente emprego de Internet das coisas (IoT)(4) e a implementação do 5G (5) são alguns exemplos do alcance da expansão tecnológica. Contudo, a difusão destas tecnologias traz consigo desafios não só de natureza técnica, como formas de lidar com ruído e interferências, mas também desperta preocupações no que concerne ética, privacidade, segurança e conformidade legal (6).

O desenvolvimento tecnológico está diretamente relacionado ao seu uso belicoso. Em 2022, logo nos primeiros meses da Guerra na Ucrânia, a ViaSat e a Starlink, dois provedores de comunicações via satélite, registraram ataques e bloqueios por interferência (7). À medida em que a guerra seguiu pelos meses seguintes, o uso de contramedidas eletrônicas se mostrou extremamente bem-sucedido para a Rússia: cerca de 90% dos veículos aéreos não-tripulados (VANTs) ucranianos foram abatidos, segundo estimativas do final de 2022 (8). O uso extensivo destas tecnologias é uma forte evidência de sua relevância na atualidade.

À medida em que os VANTs (conhecidos popularmente como *drones*) evoluíram em tecnologia, o seu uso privado se tornou mais acessível (9). Contudo, em proporção a esta difusão, cresceram também as preocupações a respeito do uso malicioso destes dispositivos, seja por indivíduos ou por grupos (10). Em 2014, o grupo terrorista autointitulado Estado Islâmico adotou o uso de VANTs comerciais e de fabricação própria para ações na Síria e no Iraque (11). Em 2015, ocorreu um notório incidente envolvendo um *drone* fotográfico de uso profissional em Tijuana, cidade no lado mexicano da fronteira com os EUA. O

veículo, que estava carregado com metanfetamina, foi encontrado pelas autoridades após despencar do céu (12). Desde então centenas de incidentes do tipo foram reportados (13). Eventos como estes elevam o nível de cautela da sociedade e das instituições de segurança e levantam debates sobre a necessidade do controle de dispositivos do tipo (14).

No Brasil, um modelo de aparelho bloqueador de drones foi homologado pela Agência Nacional de Telecomunicações (ANATEL) em julho de 2021 (15). Em julho de 2022, este dispositivo foi adquirido pela Secretaria de Administração Penitenciária do estado de São Paulo para uso na penitenciária de Itapetininga (16). O mesmo modelo de aparelho foi também utilizado pela Polícia Federal na posse do presidente Luís Inácio Lula da Silva, em 1º de janeiro de 2023. Na ocasião, um veículo aéreo foi interceptado ao entrar em espaço aéreo não-autorizado (17).

Atualmente, uma série de estudos tem sido feita no âmbito do bloqueio (também chamado de *jamming*) de sinais de VANTs. Um trabalho apresentado em 2022, avaliou as possibilidades do bloqueio de drones comerciais por meio de ruído e pulso eletromagnético (18). Um outro estudo de 2019, propôs um sistema adaptativo para compensar a falta de precisão na localização dos veículos aéreos (19).

Contudo, se em certas situações, a inviabilização de sinais se faz necessária, em aplicações legítimas, se deseja resistência à possíveis interferências. Desta forma, métodos que contornem o problema das interferências se fazem necessários.

Em anos recentes, a necessidade de adicionar robustez na operação dos VANTs elevou o interesse no uso de espalhamento espectral como forma de suprimir interferências. Pesquisadores da Universidade Nacional de Tecnologia de Defesa, da China, apresentaram em 2020 um estudo (20) que avaliou a eficácia destas técnicas contra sinais interferentes de banda-estreita. O algoritmo implementado, teve grande êxito em mitigar os efeitos da interferência.

Apesar de o uso da técnica de espalhamento espectral ser antigo (21), o interesse em sua aplicação como forma de aprimorar a segurança de diversos tipos de comunicação permanece atual. Uma série de publicações recentes tem como foco o estudo de espalhamento espectral por sequência direta (DSSS), em especial na sua aplicação anti-interferência. O trabalho de Munir e Maud (22) publicado em 2019 avaliou o uso de sequências de espalhamento variáveis como forma de adicionar segurança à comunicação. A técnica se mostrou promissora neste quesito, mas sob o ônus de dificultar a sincronização entre transmissor e receptor.

As técnicas de espalhamento espectral não se restringem à comunicação por ondas eletromagnéticas. Um estudo (23) de 2018 avaliou três técnicas de bloqueio (monotônico, por banda estreita e bloqueio correlacionado baseado em modulação PSK por pseudocódigo) atuando sobre comunicações acústicas subaquáticas por DSSS. O artigo concluiu que, na situação avaliada, onde o agente interferente conhece perfeitamente as características

do sinal alvo, o bloqueio correlacionado foi ligeiramente mais eficaz que o monotônico, enquanto o bloqueio por banda estreita operou pior que ambos. O experimento também demonstrou que um aumento da sequência de espalhamento está correlacionado com uma maior robustez à interferência. O uso de DSSS em meios pouco usuais para as comunicações digitais são um forte indício de sua versatilidade.

Apesar de que, em muitos dos casos, interferências sejam elementos indesejados, o seu uso como método de segurança tem sido explorado em grande escala. Os chamados bloqueios cooperativos consistem na transmissão de ruído artificial que imerge a mensagem, visando evitar que ela seja interceptada por um intruso (24). Técnicas deste tipo podem ser aplicadas, por exemplo, mas não exclusivamente, a VANTs (25), IoT (26), ou outros tipos de redes de comunicação (27). Aplicações como estas apoiam o paradigma do uso de interferências intencionais como forma de proteção contra agentes maliciosos.

1.2 Problematização

A difusão das telecomunicações traz consigo preocupações sobre o seu possível uso ilegal (11, 12, 13, 14). De forma a suprimir o mal uso destas tecnologias, instituições de segurança têm interesse na aquisição de instrumentos e técnicas de contramedida (16, 17). Uma abordagem usual para estas contramedidas é o uso de *jammers*.

Ao visar o desenvolvimento de *jammers* cada vez mais eficazes contra sinais maliciosos, torna-se indispensável tanto a pesquisa de novas soluções quanto o estudo de técnicas de bloqueio já existentes atuando sobre diferentes sistemas de transmissão digital em diversas configurações.

Estudos prévios já analisaram o desempenho de sistemas DSSS atuando sob interferência de diversos tipos, como a técnica por tom único e por ruído de banda estreita. Estes estudos demostraram que o sistema DSSS é altamente robusto contra este tipo de degradação (20, 22, 23). No entanto, para um entendimento mais aprofundado das várias técnicas disponíveis e para selecionar a técnica de bloqueio mais eficiente para cada caso específico, novos testes em diferentes sistemas de comunicação digital e cenários de recepção ainda são necessários, sendo este o principal foco deste trabalho.

1.3 Tema do Projeto

Este Projeto Final de Curso (PFC) tem como tema a aplicação de interferências intencionais de vários tipos sobre dois sistemas de comunicação digital: um que usa a técnica de espalhamento espectral por sequência direta (DSSS) e outro sistema convencional operando com modulação binária por chaveamento de fase (BPSK).

1.4 Objetivos

1.4.1 Objetivos Gerais

Este PFC tem como objetivos tanto avaliar a eficiência de diversas técnicas de interferência intencional em inviabilizar comunicações com modulações digitais, quanto comparar a robustez às interferências de sistemas operando com DSSS em relação a sistemas com modulação digital convencionais.

1.4.2 Objetivos Específicos

As atividades necessárias para alcançar os objetivos gerais deste trabalho, foram divididas conforme a descrição que segue.

Na parte I do PFC foram realizadas as seguintes atividades:

a) Estudo dos conceitos básicos sobre sistemas de comunicação com modulações digitais convencionais;

b) Estudo do funcionamento e as principais características de sistemas de comunicação digital com espalhamento espectral;

c) Compreensão do conceito e das diferentes técnicas de interferência intencional.

A parte II do PFC, por sua vez, compreende as seguintes atividades:

a) Implementação, no software de simulação computacional MATLAB®, de um sistema de transmissão e recepção BPSK (*binary phase shift keying*), representando as modulações digitais convencionais;

b) Implementação, também em MATLAB®, de um sistema de transmissão e recepção BPSK DSSS;

c) Implementação de diversas técnicas de bloqueio — sendo elas: por tom único, por tons múltiplos, por ruído em banda estreita (NBN), por pulso tonal, por pulso NBN e por varredura — operando contra ambos os sistemas de comunicação digital;

d) Análise, em termos de taxa de erro de bit (BER), do desempenho de cada um dos sistemas de comunicação em um cenário sem interferência e com ruído Gaussiano branco aditivo (AWGN) para diferentes valores de relação sinal–ruído (SNR);

e) Análise, em termos de BER, do desempenho dos sistemas sob ação simultânea de ruído e interferência para diferentes valores de relação sinal–ruído-mais-interferência (SINR);

f) Exame comparativo da performance dos dois sistemas (convencional e com espalhamento espectral) e avaliação de qual deles operou melhor em cada cenário.

1.5 Justificativas

Como mostrado em (20), comunicações operando com DSSS apresentam grande robustez a interferências em comparação a modulações convencionais. De forma a mensurar o quão grande é este ganho de desempenho, sistemas operando com ambas as técnicas serão submetidos às mesmas condições. A técnica DSSS também é conveniente para avaliar diferentes tipos de interferência. Se uma técnica específica de bloqueio for capaz de interromper a comunicação desse sistema robusto, isso é um forte indicativo de sua eficácia contra qualquer sistema de comunicação digital.

A escolha da modulação BPSK para representar as modulações digitais convencionais se deve ao fato de que, em quesito de BER e sob ruído, ela apresentar o melhor desempenho dentre as modulações digitais. Ou seja, se o sistema operando com DSSS tiver melhor desempenho (menor BER) que o sistema BPSK, ele performará melhor que qualquer outra modulação digital operando sob os mesmos parâmetros de SINR. A modulação QPSK (*quadrature phase shift keying*) apresenta desempenho igual à BPSK sob mesmas condições (28), mas uma vez que aquela tem implementação mais complexa, optou-se pela contraparte mais simples.

Com as análises realizadas neste trabalho, espera-se contribuir para o melhor entendimento das diferentes técnicas de bloqueio, além de auxiliar na seleção da técnica mais eficiente para inviabilização de comunicação em diversos cenários de aplicação prática.

Capítulo 2

Referencial Teórico

Este capítulo aborda os aspectos teóricos cuja compreensão é necessária para o desenvolvimento deste PFC. Conforme foi mencionado na seção 1.4.2, os assuntos aqui tratados são: sistemas de comunicação digital convencionais (com foco em modulação BPSK), sistemas com espalhamento espectral (com foco em DSSS) e interferências intencionais em sistemas de comunicação.

2.1 Sistemas de Comunicação Digital Convencionais

Há várias modulações utilizadas em comunicações digitais, dentre as quais se pode citar: BPSK, QPSK, sua generalização MPSK, entre outras. Conforme justificado na seção 1.5 foi escolhida a modulação BPSK para a análise do sistema convencional.

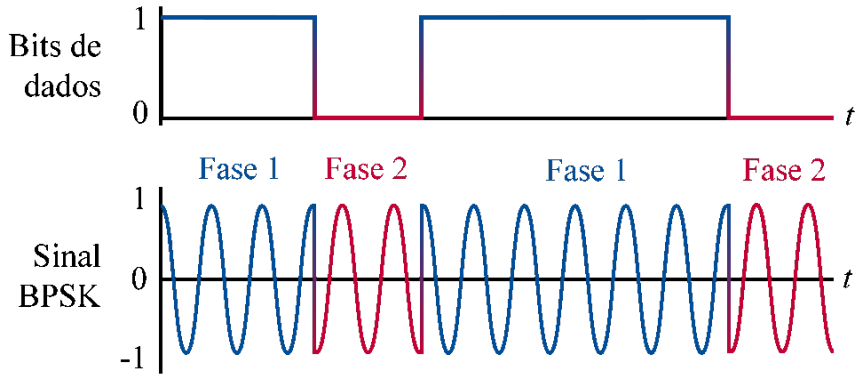
2.1.1 Modulação BPSK

Nas modulações por chaveamento de fase (PSK), a informação é contida na fase da onda portadora. A figura 2.1 mostra um exemplo de sinal modulado para a sinalização PSK binária.

A modulação BPSK é composta por dois símbolos, portanto, a duração de um símbolo (T) é precisamente o tempo de um único bit (T_b). As suas formas de onda são

$$s_i(t) = \begin{cases} s_1(t) = \sqrt{\dfrac{2E_\mathrm{b}}{T_\mathrm{b}}} \cos 2\pi f_\mathrm{c} t \\ s_2(t) = -\sqrt{\dfrac{2E_\mathrm{b}}{T_\mathrm{b}}} \cos 2\pi f_\mathrm{c} t \end{cases}, \tag{2.1}$$

Figura 2.1 – Sinal BPSK, no domínio do tempo.



Fonte: O autor.

onde E_b é a energia média de bit e f_c (frequência de portadora) é tal que

$$f_\mathrm{c} = n_\mathrm{c}\frac{1}{T_\mathrm{b}}, \tag{2.2}$$

sendo n_c um número inteiro. Ou seja, no intervalo do tempo de bit T_b, ocorrem n_c ciclos da portadora.

A sinalização da modulação BPSK é antipodal, o que implica que um símbolo tem módulo igual ao outro, mas a fase invertida.

2.1.1.1 Função-base da modulação BPSK

Uma vez que a modulação é uma sinalização antipodal, ela possui uma única função base, de energia unitária, tal que

$$\phi_1(t) = \frac{s_i(t)}{\sqrt{E_\mathrm{b}}} = \sqrt{\frac{2}{T_\mathrm{b}}}\cos 2\pi f_\mathrm{c} t\,, \quad 0 \leq t < T_\mathrm{b}. \tag{2.3}$$

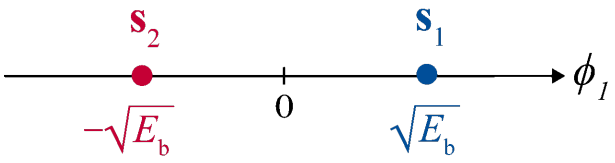
Para representar geometricamente os símbolos $s_1(t)$ e $s_2(t)$, os coeficientes devem ser respectivamente $s_{11} = \sqrt{E_\mathrm{b}}$ e $s_{21} = -\sqrt{E_\mathrm{b}}$. Assim os dois símbolos do sistema poderão ser sintetizados de acordo com

$$s_i(t) = \begin{cases} s_1(t) = s_{11}\phi_1(t) = \sqrt{E_\mathrm{b}}\phi_1(t) \\ s_2(t) = s_{21}\phi_1(t) = -\sqrt{E_\mathrm{b}}\phi_1(t) \end{cases} \quad 0 \leq t < T_\mathrm{b}. \tag{2.4}$$

2.1.1.2 Constelação da modulação BPSK

O espaço de sinais, ou constelação, desta modulação pode ser construído a partir dos resultados da equação (2.4) e é mostrado na figura 2.2

Figura 2.2 – Constelação de um sinal BPSK.



Fonte: O autor.

2.1.1.3 Probabilidade de erro modulação BPSK

Para sinalizações antipodais, ambas as probabilidades de erro (de símbolo e de bit) são iguais e, em um canal AWGN, são dadas por

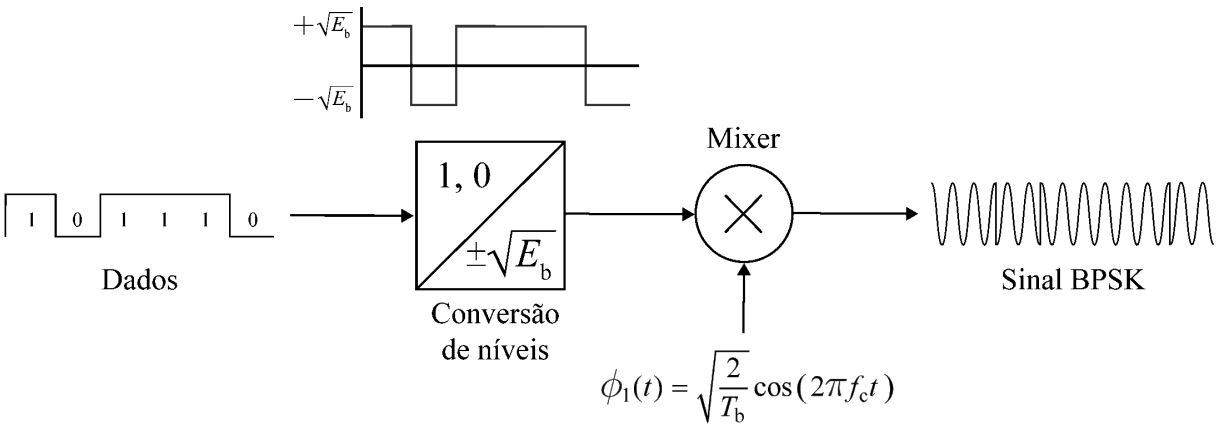
$$P_{\mathrm{e}} = \mathrm{BER} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{E_{\mathrm{b}}}{N_0}}\right), \tag{2.5}$$

onde P_{e} é a probabilidade de erro de símbolo, BER é a taxa de erro de bits, N_0 é a densidade espectral de potência do ruído e "erfc" denota a função de erro complementar (29).

2.1.1.4 Geração e demodulação com detecção coerente de um sinal BPSK

O modulador de sinais BPSK consiste em dois elementos: um conversor recebe os bits de informação 0 ou 1 e retorna os respectivos níveis $-\sqrt{E_{\mathrm{b}}}$ e $\sqrt{E_{\mathrm{b}}}$, a seguir o resultado é multiplicado pela função base $\phi_1(t)$ em um *mixer*. A saída deste último bloco é o sinal BPSK, como mostra o esquema da figura 2.3.

Figura 2.3 – Diagrama de blocos de um modulador BPSK.

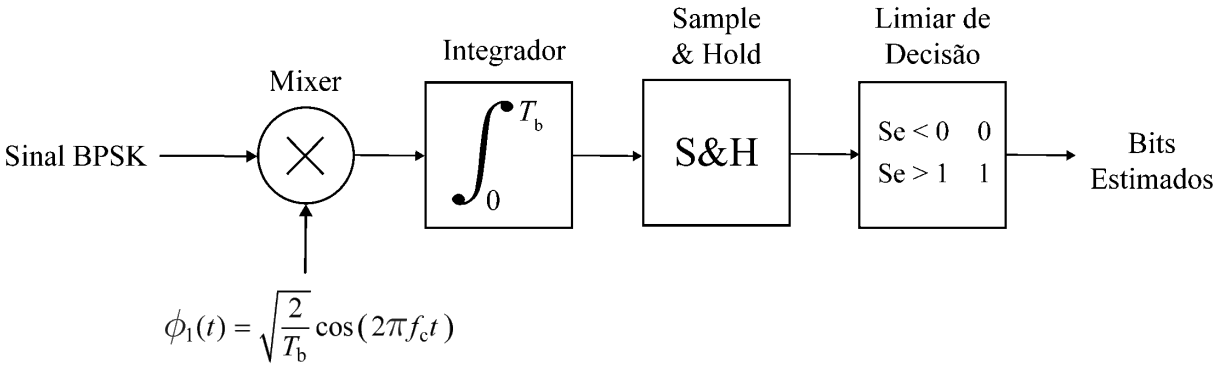


Fonte: Adaptado de (30).

Uma vez transmitido, o sinal é recebido por um detector, cujo esquema é mostrado na figura 2.4. A fim de ter uma detecção coerente, é necessário que haja no receptor

a própria função-base e em fase com a função-base da transmissão. Como mostrado anteriormente, a modulação BPSK tem somente uma dimensão (ver figura 2.2); portanto, é possível simplificar o receptor, sendo necessário um único correlator. A seguir, é feita a integração em tempo de bit e a amostragem com retenção (*sample and hold*). Então um bloco responsável pela decisão verifica se o resultado é positivo ou negativo e estima qual foi o bit enviado.

Figura 2.4 – Diagrama de blocos de um demodulador BPSK.



Fonte: Adaptado de (30).

2.1.1.5 Densidade espectral de potência para BPSK

A densidade espectral de potência (DEP) para um sinal BPSK é dado pela seguinte expressão (30):

$$\begin{aligned} S_{\mathrm{S}} &= \frac{1}{4}\left[S_{\mathrm{B}}\left(f - f_{\mathrm{c}}\right) + S_{\mathrm{B}}\left(f + f_{\mathrm{c}}\right)\right] \\ &= \frac{E_{\mathrm{b}}}{2}\mathrm{sinc}^2\left[\left(f - f_{\mathrm{c}}\right)T_{\mathrm{b}}\right] + \frac{E_{\mathrm{b}}}{2}\mathrm{sinc}^2\left[\left(f + f_{\mathrm{c}}\right)T_{\mathrm{b}}\right], \end{aligned} \tag{2.6}$$

onde S_{B} representa a densidade espectral do sinal BPSK em banda base.

O esboço desta DEP é mostrado na figura 2.5, destacando a largura dos lóbulos principal e secundários.

2.1.1.6 Eficiência espectral da modulação BPSK

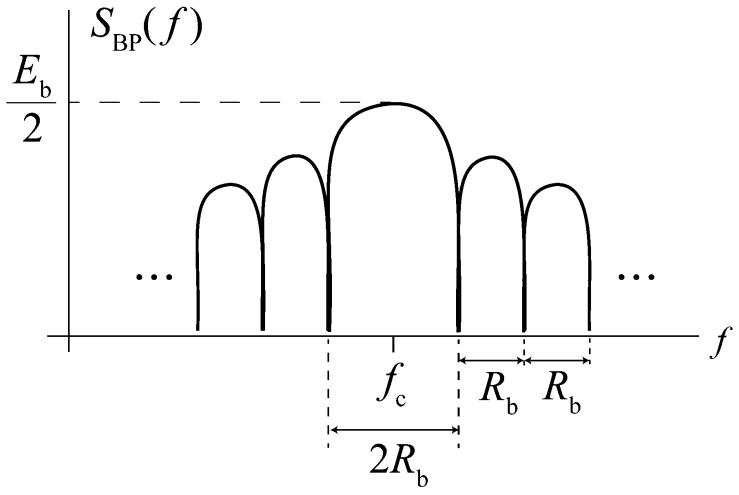
A eficiência espectral de um sinal qualquer é definida matematicamente como

$$\rho = \frac{R_{\mathrm{b}}}{B}, \tag{2.7}$$

em que $R_{\mathrm{b}} = 1/T_{\mathrm{b}}$ é a taxa de bits e B representa a banda ocupada pelo sinal transmitido.

Desconsiderando os lóbulos laterais, e considerando que a banda de um sinal BPSK seja somente a largura de seu lóbulo principal — $B = 2/T_{\mathrm{b}}$ —, a eficiência espectral de

Figura 2.5 – DEP teórica para um sinal BPSK.



Fonte: O autor.

um sinal BPSK é

$$\rho = \frac{R_\mathrm{b}}{2/T_\mathrm{b}} = \frac{R_\mathrm{b}}{2R_\mathrm{b}} = \frac{1}{2}\frac{\mathrm{bit/s}}{\mathrm{Hz}}. \tag{2.8}$$

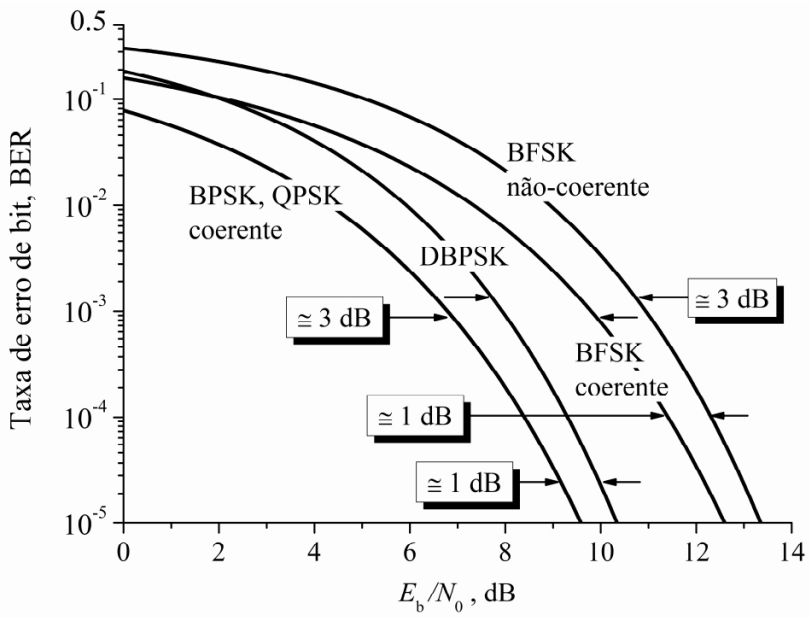
2.1.2 Outras modulações digitais

O foco deste trabalho, no que diz respeito a sistemas de comunicação digital convencionais, é a modulação BPSK. Ressalta-se, porém, a existência de outros tipos de modulação digital, com vantagens e desvantagens distintas.

Outro tipo de modulação de uso comum são os sistemas MPSK (*Multiple phase shift keying*), uma generalização das modulações PSK. DPSK (o "D" significa "diferencial") é uma variante das modulações PSK, aplicável para casos sem detecção coerente. Neste tipo de modulação, um bit de informação é determinado pela diferença de fase entre dois símbolos consecutivos. Sistemas DPSK podem ser binários (DBPSK) ou de ordem mais elevada (31). Outros tipos de modulações incluem aquelas por chaveamento de frequência (FSK, do inglês: *frequency shift keying*) e por amplitude em quadratura (QAM, *quadrature amplitude modulation*).

Cada uma das modulações apresentam expressões próprias de BER e de probabilidade de erro de símbolo, podendo ser diferentes daquela apresentada na equação (2.5) para a modulação BPSK. A figura 2.6 apresenta curvas teóricas de BER para diversas modulações em função da relação sinal–ruído E_b/N_0. Verifica-se uma melhor eficiência de potência nas modulações BPSK e QPSK coerentes, ou seja, estas modulações apresentam menor BER para uma mesma relação E_b/N_0 se comparadas às demais.

Figura 2.6 – BER de algumas modulações em função de E_b/N_0.



Fonte: (30).

2.2 Sistemas de Comunicação Digital com espalhamento espectral

A técnica de espalhamento espectral (SS) consiste em alargar a banda de um sinal para um valor muito superior à largura de faixa normalmente necessária para transmiti-lo. É importante esclarecer que nem todo sinal com banda larga tem espalhamento espectral, assim como um sinal SS pode ter banda relativamente estreita. A afirmação a respeito da grande largura de faixa do sinal após o espalhamento é feita em relação ao sinal original, sem espalhamento.

As principais técnicas de espalhamento consistem em: espalhamento espectral por sequência direta (DSSS), espalhamento espectral por salto de frequência (FHSS), espalhamento espectral por salto de tempo (THSS) e espalhamento espectral *chirp* (CSS). Uma combinação destas técnicas também é possível (32).

Neste trabalho foi utilizada a técnica DSSS para representar um sistema com espalhamento espectral.

2.2.1 Espalhamento Espectral por Sequência Direta

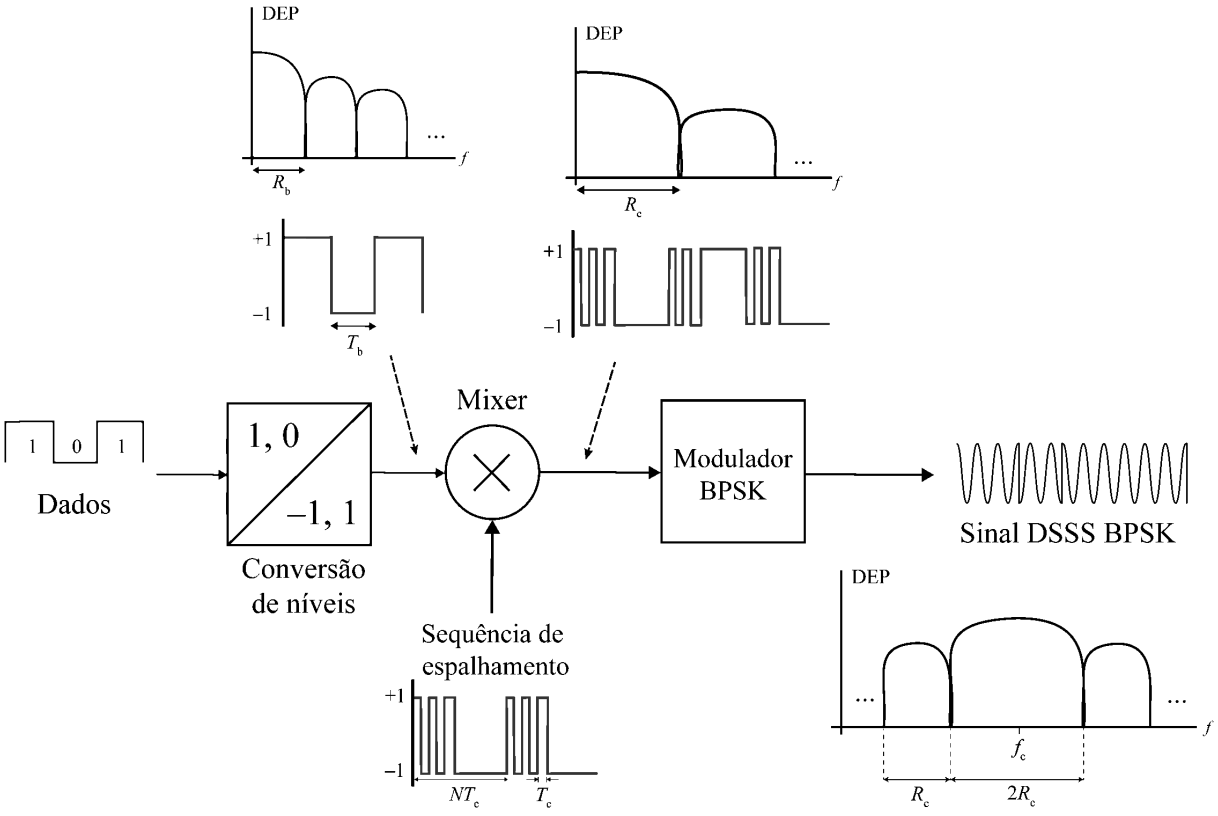
Na técnica DSSS, o sinal espalhado espectralmente é obtido multiplicando os bits de informação (convertidos para a forma bipolar) por uma sequência com taxa muito maior que a taxa dos bits de informação. A taxa da sequência de espalhamento é denominada "taxa de chips" (R_c), sendo "chip" um bit desta sequência.

A sequência de espalhamento é periódica, se repetindo a cada $N = 2^m - 1$, em que m representa o número de *flip-flops* utilizados pelo seu gerador. Dentro de um período NT_c, a sequência é aproximadamente aleatória, sendo comumente denominada pseudoaleatória.

2.2.1.1 Geração e transmissão de um sinal DSSS

A figura 2.7 mostra uma representação de um transmissor DSSS. A transmissão de um sinal DSSS começa com a conversão dos bits de informação (forma unipolar) para uma forma bipolar. O resultado desta conversão é um espectro cuja potência está concentrada em um lóbulo central de largura R_b. Adiante, este sinal resultante é multiplicado pela sequência pseudoaleatória de espalhamento de taxa R_c.

Figura 2.7 – Diagrama de blocos de um transmissor DSSS BPSK com esboço dos respectivos espectros.



Fonte: Adaptado de (30).

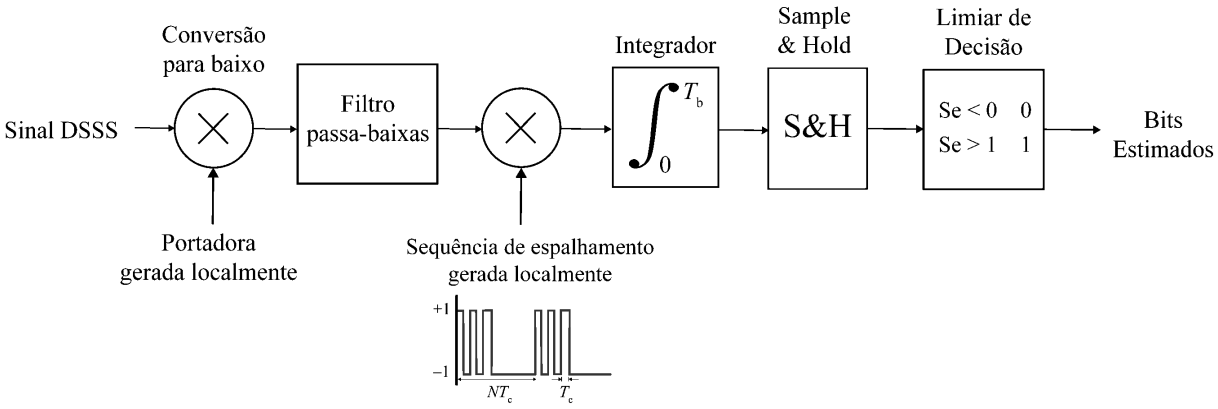
Devido à periodicidade da sequência de espalhamento, o resultado, em termos espectrais, é discreto e com raias de distância igual à taxa de repetição da sequência; ou seja, ocorrem a cada $1/NT_c$. Como resultado da multiplicação entre a sequência de bits bipolar e a sequência PN de taxa R_c, tem-se um sinal DSSS em banda base com banda igual a $1/T_c = R_c$, se considerada somente a banda do lóbulo principal.

Uma vez completado o processo de espalhamento, o sinal é transladado para banda passante — em geral utilizando moduladores que entreguem boa eficiência de potência, como é o caso da modulação BPSK, da figura 2.7 — e é transmitido pelo canal de comunicação. Vale notar que o sinal transmitido tem banda igual a $2R_{\mathrm{c}} \gg 2R_{\mathrm{b}}$.

2.2.1.2 Recepção de um sinal DSSS

A figura 2.8 mostra o diagrama de blocos de um receptor para o sinal transmitido anteriormente. A recepção do sinal DSSS se inicia pela translação para banda-base. Esta operação de multiplicação de sinais gera sinais residuais que devem ser atenuados por um filtro passa-baixas. A seguir, o sinal em banda-base passa por um processo de desespalhamento por meio da correlação com uma sequência de espalhamento idêntica à da transmissão. A saída do correlator é amostrada para geração de uma variável de decisão que, comparada com o limiar, resulta nos bits estimados.

Figura 2.8 – Esquema de um sistema de recepção DSSS BPSK.



Fonte: Adaptado de (30).

2.2.1.3 Ganho de Processamento

O ganho de processamento (G_{P}) se refere a um ganho de SINR proporcionado pelo uso da técnica DSSS em relação a outro sistema que não a utiliza. Por definição este ganho calculado como sendo a razão entre a SINR após e antes de processo de desespalhamento no receptor:

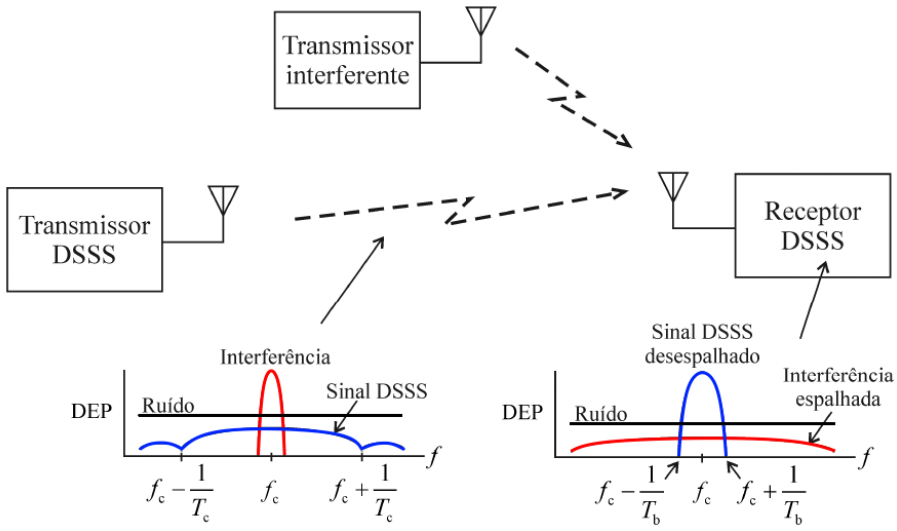
$$G_{\mathrm{P}} = \frac{\mathrm{SINR}_{\mathrm{após}}}{\mathrm{SINR}_{\mathrm{antes}}}. \tag{2.9}$$

Especificamente para os sistemas DSSS BPSK, o ganho de processamento é dado pela relação entre as taxas de chip e de bit:

$$G_{\mathrm{P}} = \frac{T_{\mathrm{b}}}{T_{\mathrm{c}}} = \frac{R_{\mathrm{c}}}{R_{\mathrm{b}}}. \tag{2.10}$$

A figura 2.9 ilustra um cenário de interferência intencional atuando sobre um sistema DSSS. Na entrada da antena receptora, a relação entre a potência de sinal e a potência de ruído mais interferência poderá ser muito baixa na prática, no entanto, ainda assim essa comunicação pode ser viável. Isso só é possível pela ação do ganho de processamento descrito anteriormente. No receptor DSSS, ocorrerá o desespalhamento do sinal de interesse, que voltará a ter uma banda estreia. Por outro lado, no mesmo momento, o sinal interferente de banda estreita será espalhado na frequência, reduzindo a sua DEP e, consequentemente, a potência interferente na banda do sinal de interesse (aumento de SINR). Perceba que quanto maior a taxa de chips, mais espalhada será a potência do interferente no receptor e maior será a SINR no instante de decisão, minimizando a BER.

Figura 2.9 – Interferência intencional atuando sobre uma comunicação DSSS.



Fonte: (30), modificado.

2.2.1.4 Margem de Interferência

Uma característica dos sinais com espalhamento espectral é a grande resistência a interferências. Contudo, existe um limite máximo para a relação entre a potência interferente (J) e a potência do sinal (P) que ainda mantenha uma dada probabilidade de erro de bit de interesse. Este parâmetro, denominado "margem de interferência", pode ser calculado pela expressão

$$M_{\mathrm{J}} = 10 \log \left(\frac{J}{P} \right) = G_{\mathrm{P}} \, [\mathrm{dB}] - \frac{E_{\mathrm{b}}}{J_0 + N_0} \, [\mathrm{dB}] \, , \tag{2.11}$$

em que $J_0 + N_0$ é a soma das densidades espectrais de potência do ruído e do sinal de interferência (33).

2.2.2 Atributos de sinais com espalhamento espectral

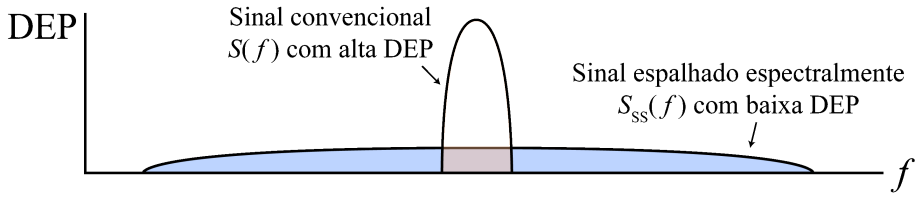
Sinais com espalhamento espectral, de forma geral, apresentam uma características em comum: uma baixa densidade espectral de potência. Desta propriedade derivam-se dois atributos: imunidade a interferências de faixa estreita e alta furtividade.

2.2.2.1 Baixa densidade espectral de potência e imunidade a interferências

A densidade espectral de potência (DEP) é, por definição, a medida do quão concentrada está a potência de um sinal em uma faixa de frequência. Uma alta DEP implica que o sinal tenha uma alta concentração de potência em uma faixa estreita. De forma semelhante, um sinal espalhado espectralmente tem sua potência dispersa por uma faixa relativamente grande do espectro. A figura 2.10 traz uma comparação entre dois sinais, um de baixa e outro de alta DEP, ambos de mesma potência.

Se um agente interceptador tenta dificultar uma comunicação SS por meio de um sinal de faixa estreita, a interferência atuaria somente sobre uma faixa estreita do sinal de informação, não sendo capaz de inviabilizar completamente a comunicação.

Figura 2.10 – Comparação entre a DEP de dois sinais de mesma potência total.



Fonte: O autor.

2.2.2.2 Furtividade e difícil interceptação

A baixa DEP dos sinais SS os tornam muito difíceis de se detectar. Caso a densidade espectral de potência seja pequena o suficiente, é possível até mesmo que o sinal fique abaixo do patamar de ruído. Na prática, um sinal nestas condições é quase indetectável a um receptor que não esteja deliberadamente tentando interceptar aquela comunicação.

A sequência de espalhamento forma outra camada de segurança. Para desespalhar o sinal, é necessário que a sequência seja conhecida pelo receptor. A chance de um interceptador sem prévio conhecimento da sequência replicá-la é extremamente baixa: a probabilidade de, ao acaso, acertar uma sequência de comprimento N é $1/2^N$ (33).

2.3 Interferências Intencionais em Sistemas de Telecomunicações

Interferência pode ser definida como um sinal intruso em uma determinada região do espectro onde ocorre uma comunicação.

Um parâmetro importante para a qualidade de uma comunicação é a razão entre a potência de sinal e a potência de interferência mais a do ruído (SINR) na recepção. Na presença de uma interferência, a SINR é reduzida, prejudicando a qualidade da comunicação.

Há vários tipos de interferência: elétrica — causada por ruídos de equipamentos elétricos e eletrônicos ou por descargas naturais —, intermodulação — decorrente de problemas dentro no próprio sistema, gerando sinais adicionais —, e por radiofrequência, que podem ser intencionais, ou não (33).

As interferências por radiofrequência operadas com intenção de prejudicar as comunicações de um adversário figuram entre uma das principais formas de guerra eletrônica. Existem diversas técnicas de contramedidas eletrônicas como o despistamento onde se tenta induzir o oponente ao erro, através da transmissão de sinais falsos e o uso de altas potências direcionadas ao receptor na intenção de danificá-lo. Este trabalho é focado em uma outra técnica: o bloqueio (também referido como *jamming*), que consiste no envio de um sinal interferente com o objetivo de impedir ou deteriorar uma comunicação (31).

O bloqueio de um sinal pode ser operado de várias formas. Richard A. Poisel, em (31), cita 7 tipos de técnicas de bloqueio: por ruído, por tom, por varredura, por pulso, bloqueio seguidor, bloqueio inteligente e bloqueio parcial de permanência aplicado em sistemas FHSS. Este projeto utiliza somente as quatro primeiras técnicas citadas.

2.3.1 Bloqueio por Ruído

Na técnica de *jamming* por ruído busca-se degradar a qualidade da comunicação introduzindo um sinal ruidoso no canal a ser interferido. Comumente este sinal é gaussiano, e sua largura de banda pode ser tão larga quanto o próprio espectro de comunicação, ou pode ter faixa mais estreita ou intermediária, a depender da finalidade (33).

Defina-se a capacidade de um canal de comunicação como a maior taxa de bits possível de ser transmitida neste meio sem perdas significativas. Supondo que o meio esteja sob efeito de um ruído gaussiano gerado intencionalmente para prejudicar a comunicação, a capacidade C é dada por

$$C = W \log_2 \left(1 + \frac{P}{N_{\mathrm{T}}}\right), \tag{2.12}$$

onde W é a largura média de banda do sinal, P é a potência média de sinal e $N_{\mathrm{T}} = W\,(N_0 + J_0)$ é a potência média de ruído mais interferência dentro da banda em análise.

Da equação 2.13 verifica-se que à medida que o ruído interferente aumenta em potência, a relação P/N_{T} diminui, o que irá aumentará a quantidade de erros na comunicação e, por consequência, provocará uma redução na capacidade de canal (31).

2.3.1.1 Bloqueio por ruído em banda larga (BBN)

Bloqueios por ruído em banda larga (BBN) buscam cobrir toda a faixa de frequências em que opera a comunicação alvo. A figura 2.11b mostra o espectro de um *jamming* BBN aplicada em uma faixa de vários canais, mostrado na figura 2.11a. Esta técnica é útil nos casos em que as informações sobre a caracterização espectral do sinal a ser interferido são limitadas.

Uma vez que esta modalidade de interferência está dispersa por uma grande faixa, o sinal de bloqueio tende a ter baixa DEP, podendo não ser capaz de afetar significativamente o alvo. Todavia, mesmo em situações em que a comunicação não é completamente inviabilizada, a redução da relação sinal–ruído ainda é capaz de limitar a distância da comunicação (33).

2.3.1.2 Bloqueio por ruído em parte da banda (PBN)

Bloqueios do tipo PBN inserem várias componentes de frequência ao longo da faixa de comunicação, continuamente ou não, mas que não cobrem todo o canal. A figura 2.11c mostra um bloqueio PBN contínuo e a figura 2.11d, um não-contínuo.

Nesta técnica, a DEP tende a ter um valor maior e mais capaz de atuar contra o interferido, em comparação com bloqueios BBN.

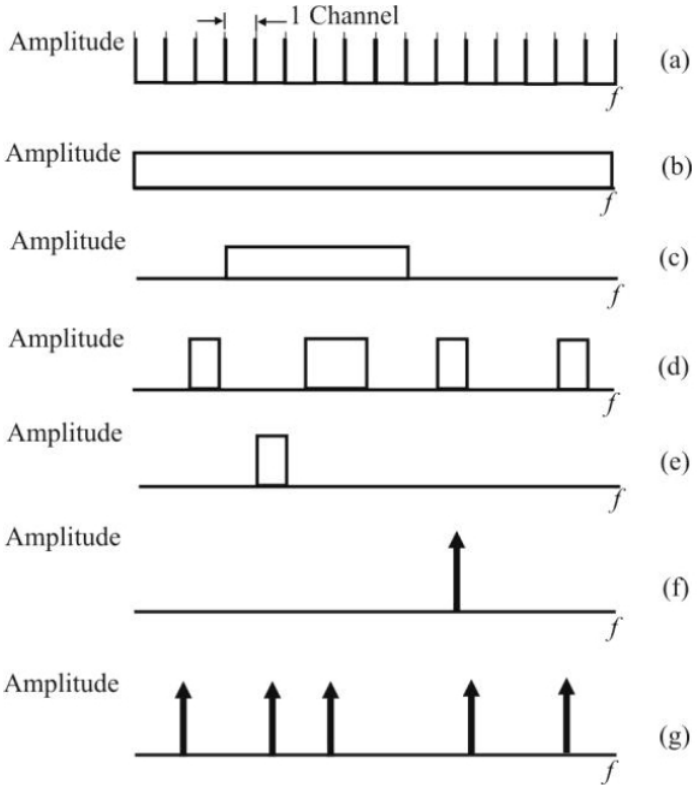
A fração do canal sob efeito do bloqueio é denominada ν. A figura 2.11 mostra a comparação de desempenho, em termos de BER, de um *jammer* PBN com vários valores de ν atuando sobre um sistema de comunicação do Tipo BFSK. Quanto maior o valor de P_{e}, melhor a eficácia do bloqueio. Conclui-se que para o cenário avaliado, quanto maior ν maior foi a eficácia do bloqueador PBN.

Bloqueios em parte da banda requerem um maior conhecimento sobre os parâmetros de frequência da comunicação, para uma escolha adequada da posição dos sinais interferentes no espectro (31).

2.3.1.3 Bloqueio por ruído em banda estreita (NBN)

A técnica de *jamming* NBN propõe obstruir apenas um canal de comunicação, sendo necessário saber exatamente em que posição do espectro ocorre a comunicação.

Figura 2.11 – Diferentes técnicas de bloqueio aplicadas em um espectro de múltiplos canais mostrado em (a), onde (b) é um bloqueio BBN, (c) um bloqueio PNB contínuo, (d) PBN não-contínuo, (e) bloqueio NBN, (f) bloqueio monotom e (g) um bloqueio multitom.



Fonte: (31).

O bloqueio NBN tem a vantagem de ter um melhor uso da potência, em comparação às técnicas de bloqueio por ruído apresentadas anteriormente.

2.3.2 Bloqueio por Tom

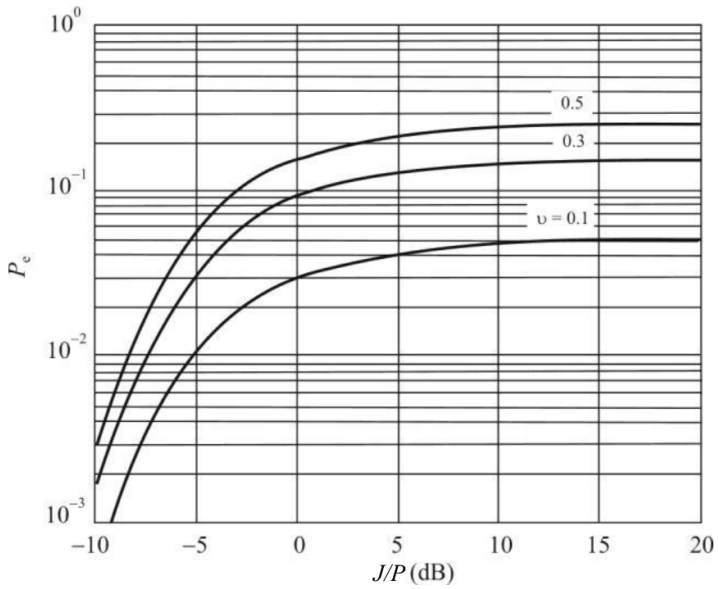
O bloqueio por tom (*tone jamming*) utiliza-se de um único ou de múltiplos sinais tonais interferentes.

2.3.2.1 Bloqueio por Tom Único

Uma interferência por tom único ou monotônica (*single tone jamming*) consiste em um sinal de onda contínua e frequência única — como mostra o seu espectro na figura 2.11(f) –, portanto sua implementação é bastante simples.

Este tipo de bloqueio pode ser bem-sucedido contra comunicações DSSS. Tendo uma potência suficientemente alta no *jammer*, o sinal interferente pode ser capaz de

Figura 2.12 – Desempenho de um bloqueio PBN sobre uma comunicação BFSK.



Fonte: (31), modificado.

superar o ganho de processamento e comprometer o sinal na etapa do desespalhamento (31).

2.3.2.2 Bloqueio por Múltiplos Tons

É também referido como *multi-tone jamming* ou multitom. Nesta modalidade, uma variedade de tons é posicionada ao longo do espectro, seja em frequências selecionadas ou aleatoriamente. Em situações em que não se tem amplo conhecimento sobre a comunicação a ser interferida, o uso deste tipo de técnica amplia a probabilidade de sucesso, sob o custo de dividir a potência do interferidor e aumentar a complexidade de implementação. A figura 2.11(g) mostra uma faixa do espectro coberta por vários tons interferentes (33).

2.3.3 Bloqueio por Varredura

Em bloqueadores por varredura (*swept jammers*), um sinal de banda estreita (podendo ser um sinal de bloqueio por ruído em banda estreita, ou mesmo um sinal tonal) tem sua posição espectral variável com o tempo. Em um instante específico, a interferência está centrada em apenas uma região do espectro, mas como se desloca em frequência, o sinal de bloqueio consegue agir sobre uma extensa faixa. Bloqueios por varredura são especialmente úteis contra sistemas FHSS, que alteram dinamicamente sua posição espectral durante a comunicação.

Um aspecto importante a ser levado em conta no uso de *jammers* por varredura é a adequação do período entre saltos de frequência. Se a varredura for rápida demais,

uma porção do tempo de permanência do alvo pode ficar descoberta. Se for muito lenta, por outro lado, poderá haver saltos da comunicação alvo não atingidos por interferência alguma (31).

2.3.4 Bloqueio por Pulso

O *jamming* por pulso consiste em um sinal interferente que pulsa em intervalos periódicos (33). Diferente dos bloqueios PBN, em que o coeficiente ν corresponde à porção do espectro coberta pela interferência em um certo instante, no bloqueio por pulso ν se refere à fração de tempo em que o *jammer* fica ativo. Considerando uma potência interferente fixa, quanto menor o tempo de atividade maior será a potência instantânea interferente dentro desse intervalo, aumentando as chances afetar com sucesso o alvo. Em comparação às demais técnicas, este bloqueio requer um menor nível médio de potência para uma eficácia similar (31).

Capítulo 3

Materiais e Métodos

O objetivo do trabalho é avaliar, por meio de simulação, o desempenho de diferentes tipos de interferência intencional atuando tanto sobre sistemas de comunicação digital convencionais, quanto sobre sistemas com espalhamento espectral. Para isso, o projeto é estruturado em uma metodologia baseada em estudos teóricos, seguido de implementação em simulação. Os resultados obtidos possibilitam avaliar qual técnica de interferência é mais efetiva em cada cenário testado.

3.1 Métodos

Para realizar, por meio de simulação, as análises das diversas técnicas de interferência intencional propostas, inicialmente, foi realizado um estudo teórico em artigos, livros, dissertações, normas e teses que embasem e viabilizem a implementação.

O estudo partiu de conceitos gerais sobre sistemas de comunicação com modulações digitais convencionais, com aprofundamento na modulação BPSK. Na sequência, foi explorada a técnica de espalhamento espectral por sequência direta (DSSS). Posteriormente, foram abordados conceitos básicos de interferências intencionais bem como diversas técnicas de bloqueio.

Completado o estudo teórico, foi desenvolvida uma simulação no *software* MATLAB® de dois sistemas de transmissão e recepção: um com modulação digital BPSK convencional e outro com BPSK DSSS. Com o sistema implementado, diferentes técnicas de interferência intencional foram incorporadas à simulação.

A avaliação dos sistemas de comunicação ocorre da seguinte forma:

1. A observação inicial é feita sobre uma operação em canal AWGN e sem interferência;

2. Então, os sistemas em canal AWGN são submetidos a cada um dos bloqueios e comparados com a situação inicial.

Em cada um dos cenários e para cada um dos sistemas considerados no trabalho foram coletados os dados de BER que serviram de parâmetro para avaliar a eficiência de cada técnica de bloqueio em inviabilizar a comunicação dos sistemas sob teste.

3.2 Recursos Necessários

A fim de executar as etapas descritas na seção 1.4.2 foram necessários os seguintes recursos:

a) Computador com *software* matemático capaz de simular sistemas de comunicação: para este projeto, o MATLAB® foi escolhido;

b) Acesso à biblioteca digital IEEE Xplore® para pesquisa e estudo de materiais referentes ao tema.

Capítulo 4

Simulação

O objetivo do projeto é avaliar a eficácia de cada técnica de interferência em comprometer comunicações convencionais e com espalhamento espectral. Para tal, foi implementada uma simulação no *software* MATLAB®, que abrange dois sistemas de transmissão e recepção: um BPSK e outro BPSK DSSS. Além deles, foram implementados interferidores dos tipos:

a) Tom único (*single tone*);

b) Múltiplos tons (*multi-tone*);

c) Por ruído de banda estreita (*NBN*);

d) Por pulso tonal (*tone pulse*);

e) Por pulso ruidoso de banda estreita (*NBN pulse*);

f) Por varredura (*swept*).

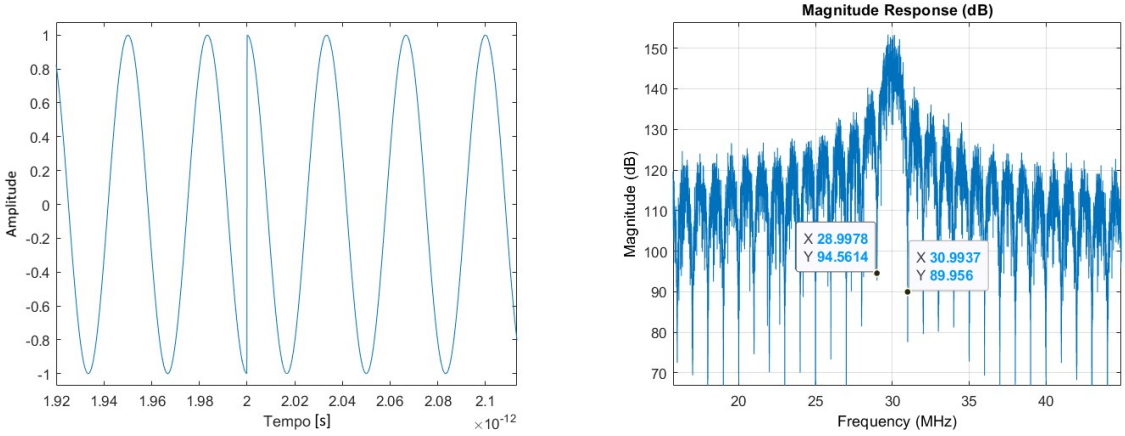
Cada um dos módulos desenvolvidos para este trabalho se encontram no apêndice A deste documento. A seguir, é feita uma descrição de cada um dos módulos que compõem a simulação.

4.1 Sistema de transmissão e recepção BPSK

O sistema BPSK é composto pelos módulos de transmissão (apêndice A.5) e de recepção (apêndice A.6). Entre eles há um bloco que simula os efeitos do canal sobre o sinal. O sistema opera a partir de parâmetros de entrada como taxa de transmissão, energia média de símbolos, frequência de portadora e quantidade de amostras por símbolo.

Figura 4.1 – Gráficos temporal e em frequência do sinal BPSK simulado.

(a) Sinal no tempo. **(b)** DEP do sinal.



Fonte: O autor.

4.1.1 Transmissão BPSK

A função recebe os parâmetros da simulação, bem como os bits de informação, que são convertidos para a forma bipolar. Estes coeficientes são então sobreamostrados (de acordo com número de amostras definidos inicialmente) e tem-se o vetor sinal no tempo discreto. Este sinal é multiplicado termo-a-termo pela função-base conforme equação (2.3). A saída é o sinal BPSK modulado.

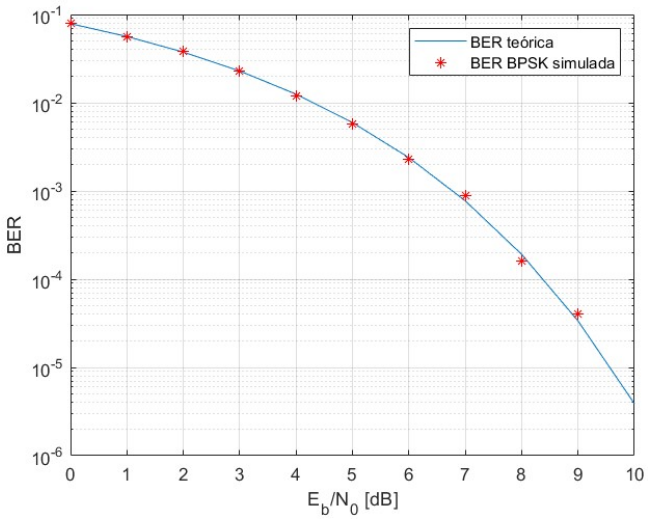
A figura 4.1a mostra o sinal BPSK no tempo detalhando a mudança de fase entre um bit 0 e um bit 1. A figura 4.1b, por sua vez, mostra a DEP com ênfase na largura de banda do lóbulo principal de $2R_\mathrm{b} = 2$ MHz, uma vez que foi utilizado uma taxa de 1 Mbps e uma frequência de portadora de 30 MHz.

4.1.2 Recepção BPSK

O sinal BPSK gerado passa por um módulo que simula um canal AWGN (apêndice A.2) e a saída deste módulo é o vetor de entrada do receptor. O sinal corrompido com ruído e/ou interferência é correlacionado com a função-base local do receptor multiplicando-se os vetores termo-a-termo, rearranjando o resultado e integrando os termos correspondentes a cada símbolo. A estimação dos bits enviados é feita comparando-se o resultado do correlator com o limiar igual a zero.

Lançando mão de várias rodadas de simulação, considerando a transmissão e recepção de 10^6 bits em cada uma delas, para diferentes valores de SNR gera-se uma curva de BER simulada, coerente com o valor teoricamente calculado através da equação (2.5), conforme mostra a figura 5.7.

Figura 4.2 – BER teórica e simulada para o sistema BPSK.



Fonte: O autor.

4.2 Sistema de transmissão e recepção BPSK DSSS

Os sistemas operando em DSSS são uma adaptação dos módulos BPSK convencionais adicionados de funções para operar o espalhamento e desespalhamento espectral.

4.2.1 Transmissão BPSK DSSS

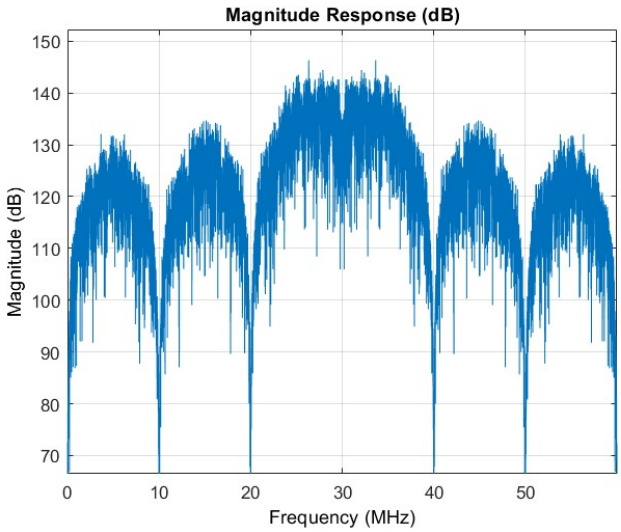
O módulo de transmissão DSSS (A.7) opera de forma idêntica ao BPSK comum até a sobreamostragem dos coeficientes. Para que ocorra o espalhamento do símbolos, a função recebe, além dos parâmetros convencionais, a taxa de chips e a sequência de espalhamento. A sequência de chips também passa por uma sobreamostragem e o seu resultado é multiplicado ao vetor de coeficientes sobreamostrados, operando o espalhamento no espectro, conforme o processo mostrado na figura 2.7. O resultado é modulado em BPSK e transmitido de forma igual ao caso convencional.

A figura 4.3 mostra um sinal DSSS BPSK gerado pela simulação considerando uma taxa de bits de 1 Mbps e uma taxa de chips de $10R_\mathrm{b} = 10$ Mchips/s. Para essa configuração, a banda do sinal DSSS, considerando apenas o lóbulo principal, fica dada por $2R_\mathrm{c} = 20$ MHz, muito maior que os 2 MHz utilizados pela modulação BPSK convencional para transmissão da mesma taxa de bits.

4.2.2 Recepção BPSK DSSS

O sinal DSSS BPSK, depois de passar pelo canal, é correlacionado com a função-base da mesma forma que no caso convencional. O resultado é multiplicado pelo vetor

Figura 4.3 – DEP do sinal espalhado no espectro.

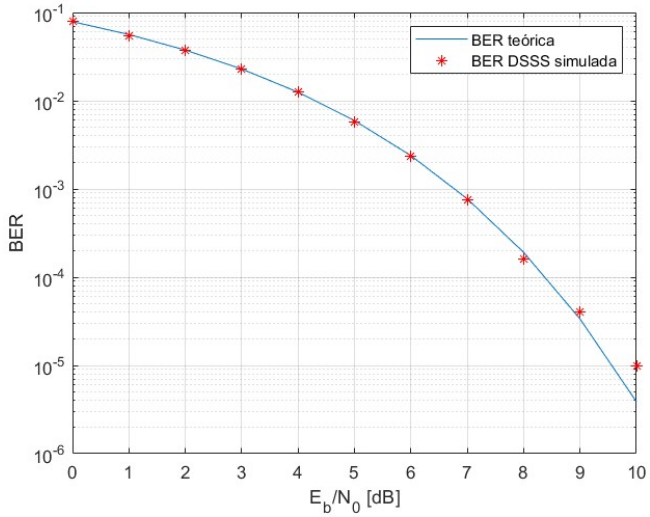


Fonte: O autor.

da sequência PN, o sinal é desespalhado e é feita a correlação símbolo-a-símbolo para detecção dos bits no receptor.

Os bits estimados são comparados com os enviados e simulando o processo para vários valores de SNR é possível gerar uma curva de BER, como mostrado na figura 5.8. Comparando com a figura 5.7 verifica-se que a probabilidade de erro é a mesma do caso convencional.

Figura 4.4 – BER teórica e simulada para o sistema DSSS BPSK.



Fonte: O autor.

4.3 Interferidores

Foram implementados seis técnicas de bloqueio, como citado no preâmbulo deste capítulo. Uma vez habilitado, o bloqueio atua entre a transmissão e a recepção degradando o sinal.

O módulo de interferência (apêndice A.3) recebe o sinal a ser interferido, gera o sinal de bloqueio conforme os parâmetros de entrada e o tipo de técnica escolhida, normaliza a potência para que a relação J/P correta seja inserida e soma os sinais.

A seguir, há uma descrição da implementação de cada uma das técnicas de *jamming*.

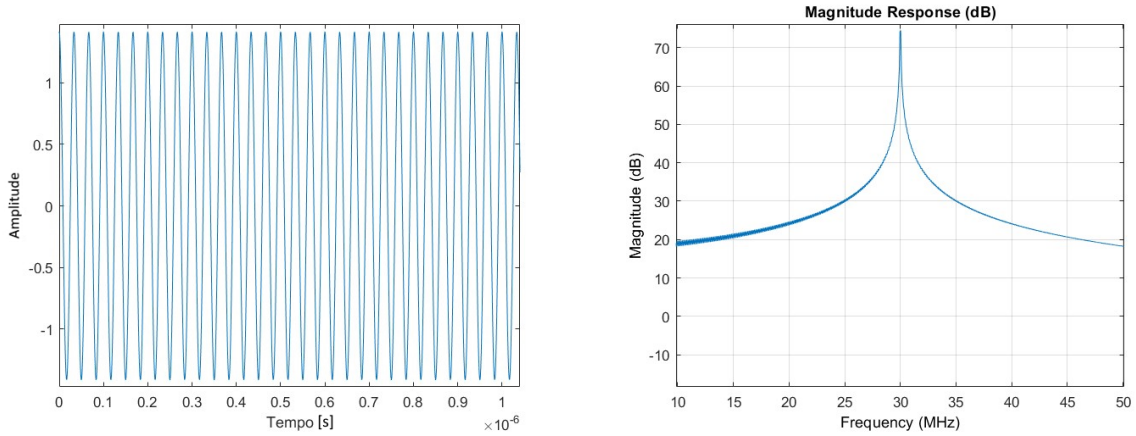
4.3.1 Bloqueio por tom único

O sinal de bloqueio consiste em uma única cossenoide $\cos(2\pi f_c t)$, onde f_c é a posição espectral do tom interferente e é um parâmetro configurável. A figura 4.5 mostra as respostas no tempo e em frequência do *jammer* ativo, considerando $f_c = 30$ MHz.

Figura 4.5 – Gráficos temporal e em frequência do sinal interferente de tom único.

(a) Bloqueio no tempo, com escala ampliada para melhor visualização.

(b) DEP da interferência *single tone*.



Fonte: O autor.

4.3.2 Bloqueio por múltiplos tons

Nesta técnica, o sinal interferente implementado consiste na soma de três cossenoides de diferentes frequências. Assim como no *jamming* por tom único, um dos parâmetros de entrada é a frequência do tom central. Os dois tons laterais são igualmente espaçados da frequência central por um parâmetro de espaçamento definido em proporção à taxa de bits.

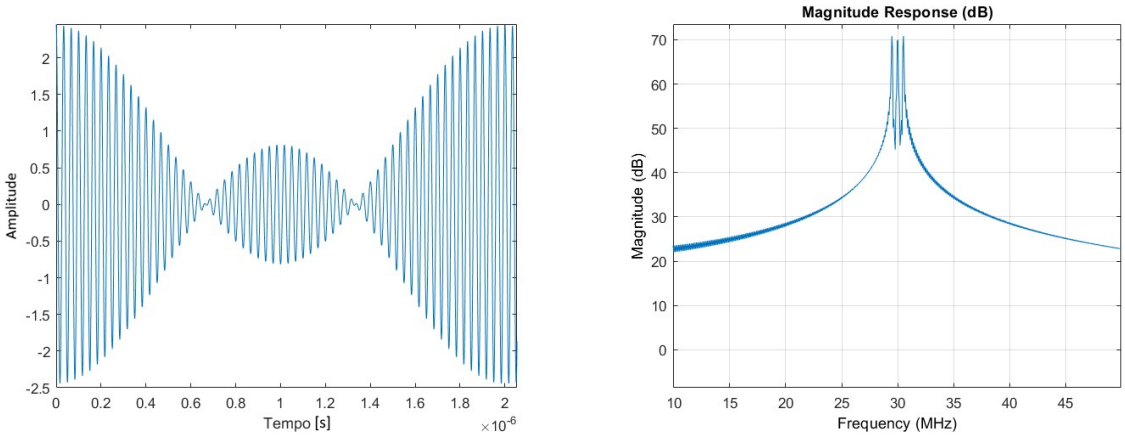
A figura 4.6a mostra o sinal interferente no tempo, considerando $f_c = 30$ MHz e o espaçamento em relação ao tom central de 1 MHz para os demais tons. A DEP do sinal

resultante é mostrada na figura 4.6b, onde é possível observar a presença de 3 tons (29 MHz, 30 MHz e 31 MHz).

Figura 4.6 – Gráficos temporal e em frequência do sinal interferente de múltiplos tons.

(a) Bloqueio no tempo, com escala ampliada para melhor visualização.

(b) DEP da interferência multitom.



Fonte: O autor.

4.3.3 Bloqueio por ruído de banda estreita (NBN)

O primeiro passo para produzir o sinal de bloqueio NBN é a geração de um vetor contendo amostras de ruído AWGN, que possui uma DEP constante em toda faixa de frequência avaliada. Na sequencia, o sinal ruidoso passa por um filtro passa-baixas gerando o sinal interferente em banda-base, que é então transladado para a frequência desejada. É o filtro passa-baixas que controla a largura de banda do sinal interferente. A figura 4.8 mostra o sinal NBN no tempo e na frequência, considerando $f_c = 30$ MHz e uma banda do sinal NBN de 1 MHz..

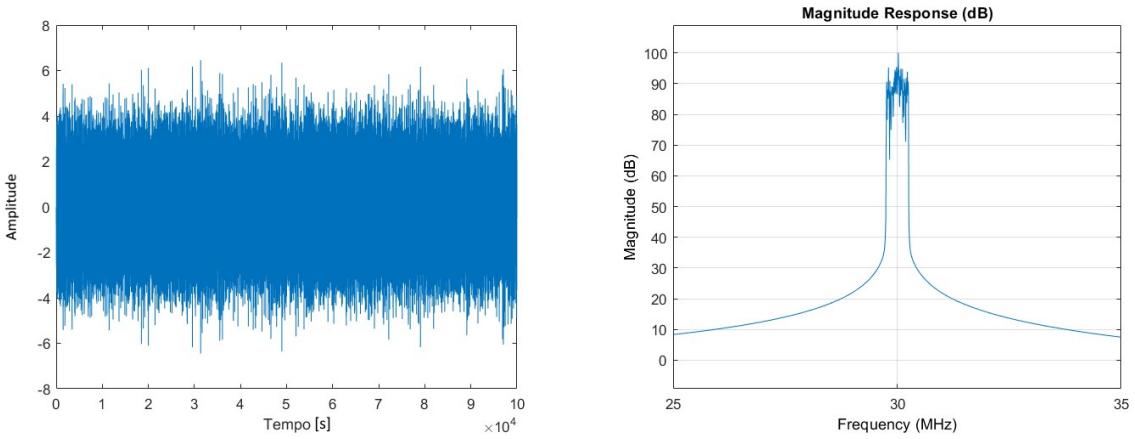
4.3.4 Bloqueio por pulso tonal

Este módulo recebe dois parâmetros de entrada: a frequência central de operação e o tempo em que o interferidor fica ativo. Inicialmente é gerada uma cossenoide que é definida em todo o tempo de simulação. Depois, é feita uma composição do vetor-sinal interferente, selecionando somente as posições dentro do tempo ativo. O tempo ativo é contado a partir do começo da transmissão, e é medido em porcentagem do tempo total de simulação.

A caracterização no tempo do sinal (figura 4.8a) mostra que a cossenoide existe até certo instante, e depois cessa a sua atividade. A figura 4.8b mostra a DEP do sinal concentrada na frequência central de 30 MHz durante o período de atividade. Observe

Figura 4.7 – Gráficos temporal e em frequência do sinal NBN.

(a) Bloqueio no tempo. **(b)** DEP da interferência.

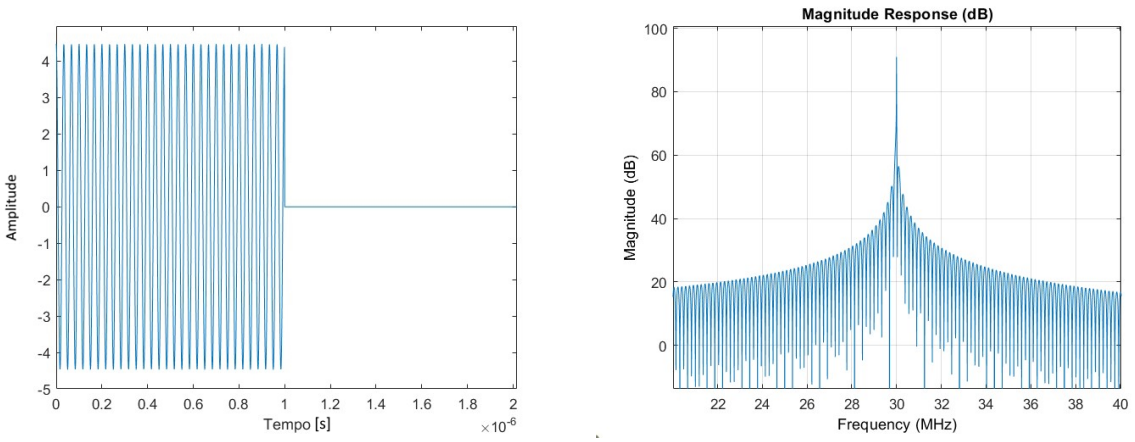


Fonte: O autor.

que, neste caso, para uma mesma potência média de transmissão, há uma maior densidade espectral interferente durante o período de atividade.

Figura 4.8 – Gráficos temporal e em frequência do sinal de interferência por pulso.

(a) Bloqueio no tempo. **(b)** DEP da interferência.



Fonte: O autor.

4.3.5 Bloqueio por pulso NBN

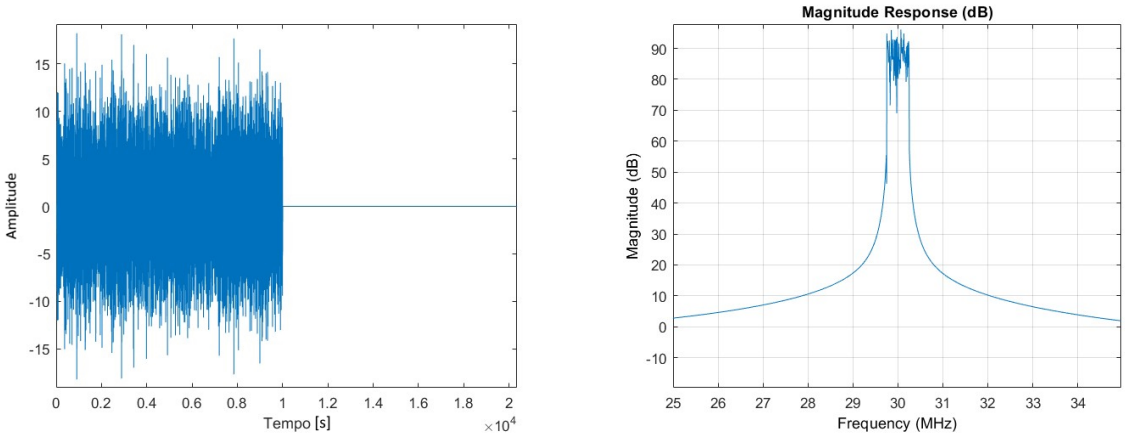
Um *jamming* por pulso NBN é uma combinação das duas técnicas descritas nas seções 4.3.3 e 4.3.4. Para gerar o vetor-sinal interferente, o módulo deste *jammer* gera um sinal NBN convencional e depois o limita na faixa de tempo definida, de forma igual à descrita em 4.3.4.

Na figura 4.9a fica perceptível que o sinal interferente é um pulso — uma vez que fica ativo durante o tempo estipulado, depois cessa — e tem característica de ruído. A

figura 4.9b revela um espectro muito semelhante ao do bloqueio NBN convencional (figura 4.7b).

Figura 4.9 – Gráficos temporal e em frequência do sinal de interferência por pulso NBN.

(a) Bloqueio no tempo. **(b)** DEP da interferência.



Fonte: O autor.

4.3.6 Bloqueio por varredura

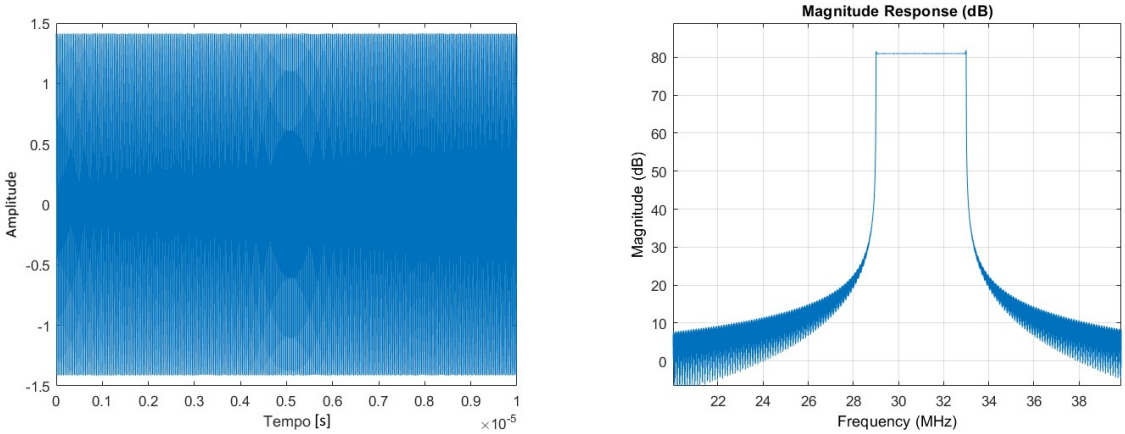
O módulo de bloqueio por varredura recebe duas entradas: uma frequência central e um parâmetro que representa metade da faixa do espectro a ser coberta pela interferência. Com estes parâmetros se define a faixa de frequências coberta pela varredura. Cria-se então um vetor de frequências igualmente espaçadas que vai do mínimo ao máximo valor definido anteriormente. O sinal de *jamming* é um vetor de uma cossenoide com frequência variável.

A figura 4.10b mostra uma representação do espectro do sinal *swept*, considerando uma varredura de 29 MHz até 33 MHz. Contudo um ponto importante deve ser destacado: o que é mostrado é uma sobreposição da interferência de toda a faixa de frequências afetada ao longo do tempo pois, na realidade, um único tom está ativo a cada instante de tempo.

Na figura 4.10a é mostrado o sinal de bloqueio por varredura no domínio do tempo, representado por uma cossenoide que aumenta a sua frequência à medida em que o tempo passa. Como o aumento de frequência é gradual, não fica tão explicito pela análise visual da figura 4.10a essa mudança do sinal interferente.

Figura 4.10 – Gráficos temporal e em frequência do sinal de interferência por varredura.

(a) Bloqueio no tempo. **(b)** DEP da interferência.



Fonte: O autor.

Capítulo 5

Resultados e Análise

A fim de comparar e analisar o desempenho dos sistemas BPSK e DSSS BPSK sob efeito de cada uma das técnicas de interferência, foram traçadas em um mesmo gráfico as curvas de BER resultantes da simulação.

Para a geração das curvas de desempenho desta seção, a relação J/P — também chamada de *jammer to signal ratio* (JSR) — foi variada unitariamente em simulação de 0 dB a 30 dB e os respectivos valores de BER foram estimados. Além disso, considerou-se, em todos os casos, um canal simulado do tipo AWGN com relação E_b/N_0 de 20 dB (100 vezes em escala linear). Esse valor foi escolhido pois trata-se de um valor tipicamente encontrado na prática e que viabilizaria uma boa comunicação em sistemas digitais na ausência de interferência externa.

Os demais parâmetros dos sistemas de comunicação foram definidos como segue:

- energia média de símbolo: $E_\mathrm{b} = 1$ Joule;
- taxa de bits: $R_\mathrm{b} = 1$ Mbps;
- frequência da portadora: $f_\mathrm{c} = 30$ MHz;
- número de bits transmitidos: 100 000 bits.

Adicionalmente, para o sistema DSSS BPSK, além dos parâmetros anteriores, foram também considerados os seguintes:

- taxa de chips: $R_\mathrm{c} = 10$ Mchips/s;
- sequência PN com comprimento de 15 chips.

Em todos os casos apresentados a simulação operou com uma frequência de amostragem de 100 MHz, equivalente a 100 amostras por símbolo.

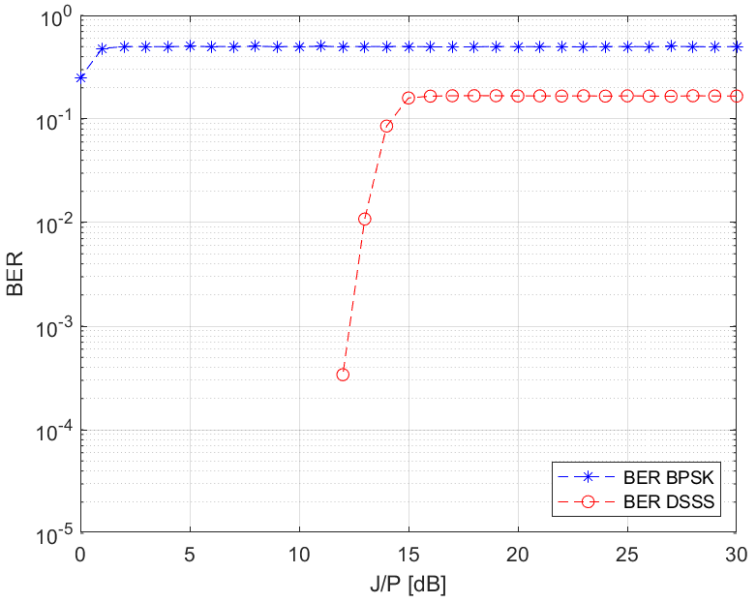
5.1 Curvas do Bloqueio por Tom Único

O *jammer single-tone* foi configurado para operar com uma frequência central interferente de 30 MHz (mesma frequência da portadora dos sinais a serem interferidos).

As curvas de BER resultantes são mostradas na figura 5.1. Pela a figura percebe-se que o sistema BPSK é completamente inviabilizado, mesmo para baixos valores de JSR. A partir de $J/P = 1$ dB tem-se BER = 0,5, demonstrando a baixa robustez do sistema BPSK contra esse tipo de interferência.

Por outro lado, o sistema DSSS obteve valores de BER simulada nula para $J/P < 12$ dB, indicando que nenhum bit foi detectado com erro nos 100 000 transmitidos. Depois deste valor a BER cresce vertiginosamente e a partir de $J/P = 15$ dB se estabiliza em 0,15. Os resultados demonstram a grande robustez do sistema DSSS frente ao bloqueio do tipo tom único, que se deve principalmente ao ganho de processamento desta técnica.

Figura 5.1 – Curva de BER dos sistemas BPSK e DSSS BPSK sob bloqueio por tom único.



Fonte: O autor.

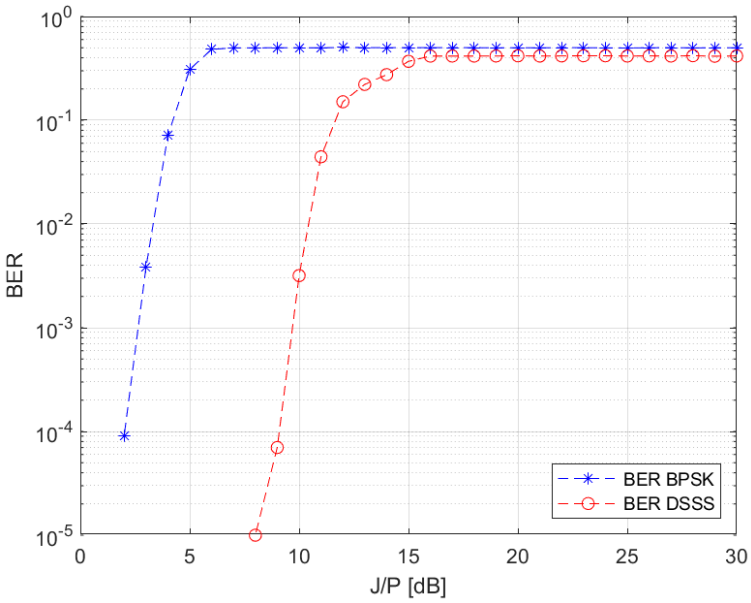
5.2 Curvas do Bloqueio por Múltiplos Tons

O bloqueador *multitone* foi configurado com uma frequência central de 30 MHz. Os dois tons laterais ficam espaçados da frequência central por 0,5 MHz. Portanto, os três tons interferentes foram posicionados nas frequências de: 29,5 MHz, 30 MHz e 30,5 MHz.

Como mostra a figura 5.2, foi obtida BER = 0 para o BPSK quando $J/P < 2$ dB e para o DSSS quando $J/P < 8$ dB. A partir de $J/P = 6$ dB (BPSK) e $J/P = 16$ dB (DSSS) os valores de BER se estabilizam ambos em torno de 0,5, significando uma inviabilização total da comunicação.

A eficácia deste *jammer* contra o sistema DSSS tende a se aproximar daquela do sistema BPSK, uma vez que consegue cobrir uma maior parte do espectro que sua contraparte de tom único. O espalhamento espectral contudo exige do bloqueio uma maior relação J/P para a eficácia.

Figura 5.2 – Curva de BER dos sistemas BPSK e DSSS BPSK sob bloqueio por múltiplos tons.



Fonte: O autor.

Conclui-se que na tentativa de inviabilizar a comunicação de um sistema DSSS é mais adequado utilizar um sistema de bloqueio com múltiplos (ao invés do bloqueio de tom único). Por outro lado, para inviabilizar a operação do sistema BPSK convencional, o bloqueio de tom único é mais efetivo.

5.3 Curvas do Bloqueio NBN

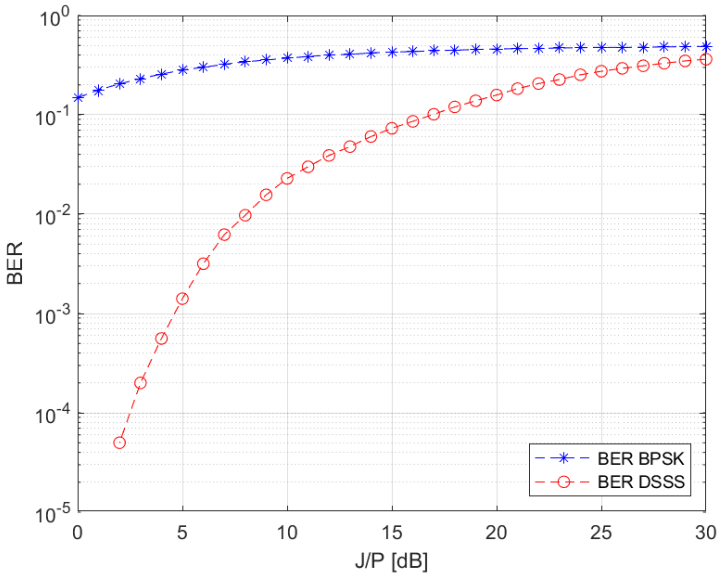
O primeiro dos parâmetros de bloqueio NBN a ser definido é a largura de banda do sinal definida em 0,5% da frequência de amostragem, ou seja, $B = 0,5$ MHz. O filtro passa baixas é configurado como do tipo IIR (*Infinite impulse response*) com ordem 35.

Avaliando a curva de BER apresentada na figura 5.3 é possível perceber que mesmo para $J/P = 0$ dB o sistema BPSK apresenta BER superior a 0,01. A comunicação DSSS,

contudo, apresenta baixos valores de BER, para baixa JSR, e cresce gradativamente até convergir para uma inviabilização total em valores próximos de $J/P = 30$ dB.

Comparando os sistemas com espalhamento espectral e convencional fica evidente o melhor desempenho do primeiro, uma vez que proporcionalmente uma fração menor do espectro fica comprometida. Nota-se também que a curva apresenta uma forma mais parecida com um gráfico de BER convencional (em função de SNR) uma vez que a interferência é gerada com AWGN.

Figura 5.3 – Curva de BER dos sistemas BPSK e DSSS BPSK sob bloqueio NBN.



Fonte: O autor.

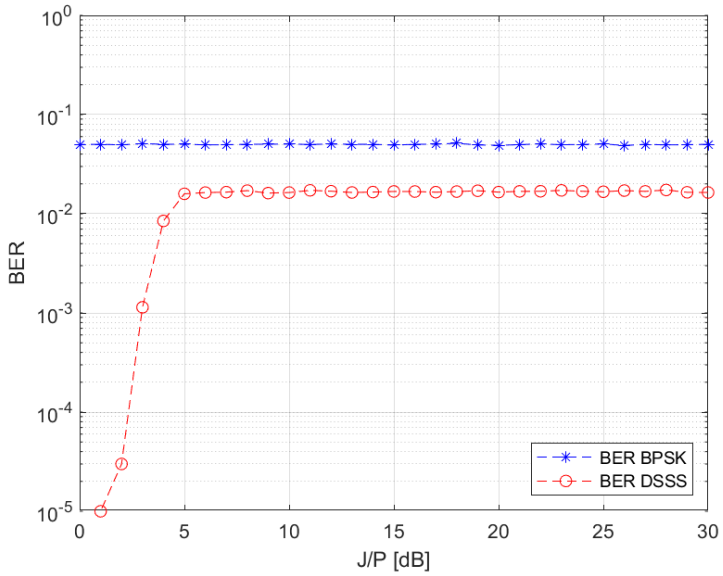
Interessantemente, esse tipo de bloqueio já degrada a comunicação do sistema DSSS para baixos valores de relação J/P, diferente do que ocorria nas técnicas anteriores com tons. Entretanto, para a inviabilização total da comunicação, a relação J/P para o bloqueio NBN deve ser muito maior que aquela dos bloqueios anteriores.

5.4 Curvas do Bloqueio por Pulso tonal

Para a operação do *jammer* por pulso tonal, o tempo ativo foi definido como 10% do tempo total de transmissão, com tom centrado em 30 MHz. A figura 5.4 mostra as curvas de BER.

Analisando os resultados da figura 5.4 é possível constatar que para o sistema BPSK, BER = 0,05 para qualquer valor de JSR, implicando que 5% dos bits foram efetivamente corrompidos. Já para o sistema DSSS, a BER se mantém constante em 0,017 para $J/P \geq 5$ dB, resultando em somente 1,7% dos bits foram comprometidos de forma eficaz.

Figura 5.4 – Curva de BER dos sistemas BPSK e DSSS BPSK sob bloqueio por pulso tonal.



Fonte: O autor.

O comportamento dos sistemas sob bloqueio por pulso é derivado do fato de que como a interferência só atua sobre uma fração dos bits (aqueles transmitidos no período ativo do *jammer*), a partir do ponto em que os bits possíveis de serem afetados já sucumbiram à interferência, o aumento da JSR não produz aumento de BER.

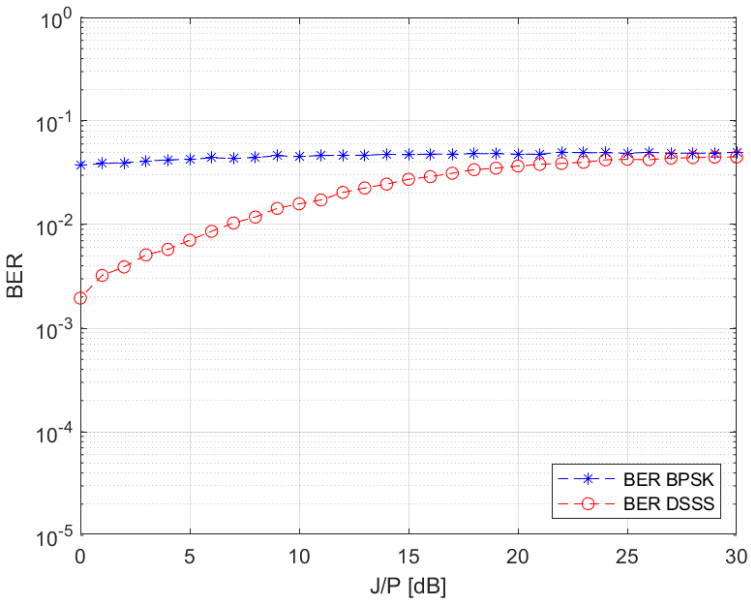
Se comparada com a técnica de tom único, sua versão pulsada consegue afetar drasticamente a comunicação dos sistemas sob interferência com uma potência interferente menor, ou seja, com uma relação J/P menor (deslocamento para a esquerda das curvas de desempenho). No entanto, a máxima BER obtida com esse tipo de técnica (para altos valores de J/P) fica abaixo daquela obtida com a técnica de tom único (deslocamento das curvas para baixo).

5.5 Curvas do Bloqueio por pulso NBN

Sendo esta técnica de bloqueio, uma junção de técnica pulsada com NBN, para uma comparação justa, os parâmetros de operação do jammer foram: tempo ativo igual a 10% (mesmo da técnica de pulso tonal), largura de banda de 0,5% da frequência de amostragem e filtro de ordem 35 (mesmo da técnica NBN).

A resposta dos sistemas (mostrada na figura 5.5) também pode ser descrita como uma combinação das técnicas NBN e por pulso: o comportamento geral das curvas é semelhante à do NBN convencional, mas neste caso convergindo para uma BER = 0,05, como na interferência por pulso tonal.

Figura 5.5 – Curva de BER dos sistemas BPSK e DSSS BPSK sob bloqueio por pulso NBN.



Fonte: O autor.

Como nos casos anteriores, o sistema DSSS apresenta melhor desempenho que o caso convencional demandando mais potência interferente para que seu comportamento se aproxime deste último. Verifica-se também que o bloqueio NBN pulsado consegue degradar mais a comunicação do sistema DSSS para baixos valores de relação J/P que a versão NBN convencional. Portanto, quando houver limitação de recursos de potência do bloqueador, o bloqueio NBN pulsado poderá ser mais efetivo que o sistema convencional.

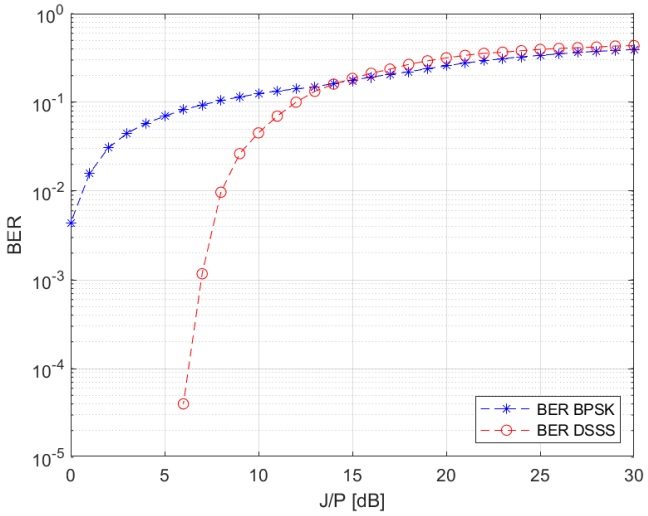
5.6 Curvas do Bloqueio por Varredura

Para a atuação do *swept jammer*, foi definida uma faixa de varredura de $\pm R_b$ em torno da frequência de 30 MHz. Desta forma a varredura acontece de 29 a 31 MHz ao longo do período de transmissão.

As curvas de BER (figura 5.6) apresentam um comportamento de convergência entre as respostas BPSK e DSSS. O sistema convencional apresenta BER significativa a partir de $J/P = 0$ dB, já o sistema com espalhamento espectral precisa de uma relação $J/P \approx 8$ dB para obter uma BER ≈ 0.01.

Visto que esta técnica cobre uma fração maior do espectro, ela consegue aproximar a BER do sistema DSSS à do BPSK com uma menor JSR.

Figura 5.6 – Curva de BER dos sistemas BPSK e DSSS BPSK sob bloqueio por varredura.



Fonte: O autor.

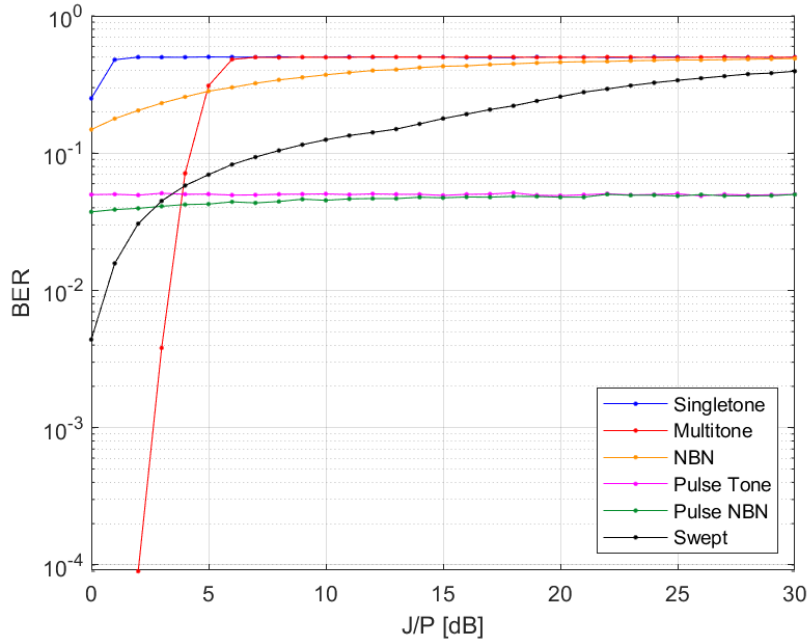
5.7 Comparação dos bloqueios sobre BPSK

Das curvas de BER (figura 5.7) de cada um dos bloqueios operando sobre BPSK se observa que em valores de $J/P < 5$ dB o método *single tone* já consegue inviabilizar completamente a comunicação sendo o mais eficaz neste caso.

Para valores de $J/P > 5$ dB o método *multitone* passa a apresentar o mesmo resultado que sua contraparte de tom único. O bloqueio NBN, apesar de convergir para uma BER $= 0,5$, apresenta desempenho ligeiramente inferior que ambas as técnicas já mencionadas. O bloqueio por varredura apresenta desempenho inferior aos demais supracitados. Os bloqueios por pulso tonal e pulso NBN apresentam BER aproximadamente constante de 0,05 para qualquer valores de JSR.

Em uma comunicação de banda estreita, a maior parte da informação está concentrada na frequência central (ver figura 2.5). A interferência por tom único, ao concentrar sua potência nesta posição espectral, tem maior sucesso em atrapalhar a comunicação que as demais técnicas. De forma similar, o método NBN também concentra potência interferente em f_c, ainda que menos efetivamente. No *jamming multitone*, o sinal está distribuído em três tons e menos concentrado em f_c, fazendo com que seu desempenho seja menor em baixas JSRs, e igual ao do *jamming singletone* para $J/P \geq 6$ dB, este último é de construção mais simples e portanto mais adequado.

Figura 5.7 – Curva de BER do sistema BPSK sob cada uma das interferências.



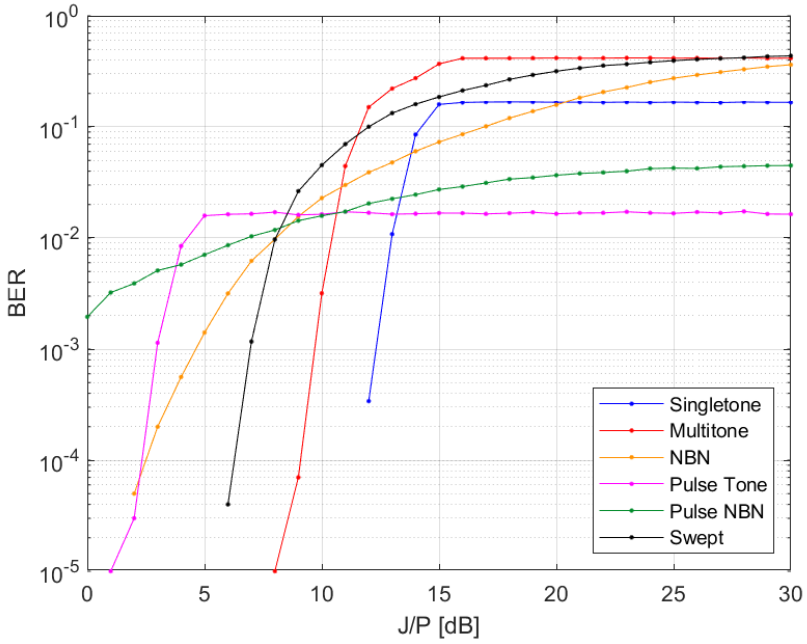
Fonte: O autor.

5.8 Comparação dos bloqueios sobre DSSS BPSK

A partir das curvas de desempenho dos interferidores atuando sobre o sistema DSSS BPSK mostradas na figura 5.8 percebe-se que para uma $J/P < 4$ dB o bloqueio por pulso NBN é o único a introduzir efetivamente alguma BER (na ordem de 10^{-3}). A partir daí até uma $J/P \leq 8$ dB o bloqueio por pulso tonal passa a ter um desempenho ligeiramente melhor que o mencionado anteriormente, mas se mantém constante neste valor (0,016) para todas JSRs subsequentes. Nesta faixa, a interferência NBN têm desempenho não-nulo, mas inferior aos demais já mencionados. Para $9 \leq J/P \leq 11$ dB, há uma sobressalência do bloqueio por varredura; nesta faixa a maioria das curvas de BER se cruzam. A partir de $J/P \approx 20$ dB cada uma das curvas tende para o seu patamar de estabilização (máxima BER de cada técnica); neste caso, o bloqueio por tons múltiplos é o mais eficaz.

Sintetizando, três das técnicas tendem a uma BER próxima a 50% em altos valores de JSR: *multitone*, *swept* e NBN, nesta ordem de eficácia. Nesta faixa, o bloqueio *singletone* apresenta desempenho inferior aos anteriores, uma vez que estando concentrado em um ponto do espectro tem menos poder contra o sinal com espalhamento espectral, além disso, o ganho de processamento tem mais efeito sob interferências de faixa estreita. Os *jammers* menos eficazes em alta JSR foram respectivamente o por pulso tonal e por pulso NBN, visto que tendem a concentrar a sua potência interferente apenas em uma fração do tempo total de atuação do bloqueador.

Figura 5.8 – Curva de BER do sistema DSSS BPSK sob cada uma das interferências.



Fonte: O autor.

Capítulo 6

Conclusões

Levando em conta os resultados colhidos a partir da simulação foi possível comparar o desempenho sob interferência de dois sistemas de comunicação digital: um sistema operando com modulação BPSK convencional e outro com espalhamento espectral por sequência direta (DSSS). Foram também comparadas diferentes técnicas de interferência intencional (por tom único, por tom múltiplo, NBN, por pulso tonal, por pulso NBN e por varredura) e suas efetividades em comprometer cada um dos sistemas de comunicação.

Conclui-se que o espalhamento espectral traz um considerável ganho de desempenho em uma operação sob canal AWGN e sob interferência.O ganho de desempenho é especialmente grande para valores mais baixos de JSR, comprovando a grande robustez deste tipo de sistema em cenários de interferência intencional.

Conclui-se também que para o caso analisado de um sistema BPSK operando sob canal AWGN — dentre as técnicas de bloqueio analisadas e operando com os parâmetros especificados — o bloqueio por tom único (*singletone*) é o melhor para comprometer um sistema de comunicação digital convencional.

Para a inviabilização de um sistema DSSS, contudo, a avaliação da técnica de interferência mais efetiva é dependente da JSR. Para $J/P < 4$ dB a mais eficaz é um pulso NBN; para $4 < J/P \leq 8$ dB a melhor é um pulso tonal; para $9 \leq J/P \leq 11$ dB, bloqueio por varredura; e para uma relação $J/P > 11$ dB a melhor técnica é um bloqueio por múltiplos tons.

Em suma, este trabalho contribuiu para o avanço do conhecimento sobre uma ampla gama de interferências intencionais que afetam sistemas de comunicação convencionais e com espalhamento espectral. As conclusões apresentadas não apenas aprimoram a compreensão teórica sobre as técnicas e sobre os sistemas avaliados, mas também auxiliam na determinação da técnica mais efetiva em cenários específicos de aplicação prática,

sob diferentes condições de operação, o que poderá ser determinante para o sucesso da inviabilização da comunicação do sistema alvo.

Como trabalhos futuros propõem-se:

i) Implementação prática em rádio definido por software de algumas das técnicas de interferências apresentadas neste trabalho, com o objetivo de inviabilizar a comunicação de sistemas que utilizam DSSS e também de sistemas convencionais;

ii) Avaliação em simulação de interferências intencionais sobre sistemas de múltiplas portadoras OFDM (*Orthogonal Frequency Division Multiplexing*);

iii) Desenvolvimento de novas técnicas de interferência combinadas, por exemplo, pulso tonal com NBN, ou bloqueio por varredura com pulso tonal, dentre outras possíveis combinações.

Referências

1 HILLYER, M. **How has technology changed - and changed us - in the past 20 years?** 2020. Acesso em: 22 mar. 2023. Disponível em: https://www.weforum.org/agenda/2020/11/heres-how-technology-has-changed-and-changed-us-over-the-past-20-years/.

2 NUMBER of people using the internet. 2020. Acesso em: 22 mar. 2023. Disponível em: https://www.weforum.org/agenda/2020/11/heres-how-technology-has-changed-and-changed-us-over-the-past-20-years/.

3 OLHAR DIGITAL. **Metade da população mundial possui um smartphone, revela relatório**. 2021. Acesso em: 22 mar. 2023. Disponível em: https://olhardigital.com.br/2021/06/28/reviews/metade-da-populacao-possui-smartphone-revela-relatorio/.

4 COOK, S. **60+ IoT statistics and facts**. 2022. Acesso em: 1 abr. 2023. Disponível em: https://www.comparitech.com/internet-providers/iot-statistics/.

5 FISHER, T. **5G Availability Around the World**. 2023. Acesso em: 1 abr. 2023. Disponível em: https://www.lifewire.com/5g-availability-world-4156244.

6 KARALE, A. The challenges of iot addressing security, ethics, privacy, and laws. **Internet of Things**, Elsevier, v. 15, p. 100420, 2021.

7 SUESS, J. **Jamming and Cyber Attacks: How Space is Being Targeted in Ukraine**. 2022. Acesso em: 22 mar. 2023. Disponível em: https://www.rusi.org/explore-our-research/publications/commentary/jamming-and-cyber-attacks-how-space-being-targeted-ukraine.

8 AXE, D. **Russia's Electronic-Warfare Troops Knocked Out 90 Percent Of Ukraine's Drones**. 2022. Acesso em: 22 mar. 2023. Disponível em: https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/.

9 INSIDER INTELLIGENCE. **Drone market outlook in 2023: industry growth trends, market stats and forecast**. 2023. Acesso em: 1 abr. 2023. Disponível em: https://www.insiderintelligence.com/insights/drone-industry-analysis-market-trends-growth-forecasts/.

10 ASSOCIATION OF THE UNITED STATES ARMY (AUSA). **The Role of Drones in Future Terrorist Attacks**. 2021. Acesso em: 22 mar. 2023. Disponível em: https://www.ausa.org/publications/role-drones-future-terrorist-attacks.

11 THE WASHINGTON POST. **Use of weaponized drones by ISIS spurs terrorism fears**. 2017. Acesso em: 22 mar. 2023. Disponível em: https:

//www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.

12 BBC NEWS BRASIL. **12 Drone com carga de droga cai na fronteira México-EUA**. 2015. Acesso em: 22 mar. 2023. Disponível em: https://www.bbc.com/portuguese/noticias/2015/01/150122_drone_drogas_mexico_fn.

13 WRIGHT, T. **How Many Drones Are Smuggling Drugs Across the U.S. Southern Border?** 2020. Acesso em: 31 mar. 2023. Disponível em: https://www.smithsonianmag.com/air-space-magazine/narcodrones-180974934/.

14 SANCHEZ, A. **Worst Case Scenario: The Criminal Use of Drones**. 2015. Acesso em: 31 mar. 2023. Disponível em: https://www.coha.org/worst-case-scenario-the-criminal-use-of-drones/.

15 ALECRIM, E. **DroneGun Tactical, bloqueador que "derruba" drones, é aprovado pela Anatel**. 2021. Acesso em: 2 abr. 2023. Disponível em: https://tecnoblog.net/noticias/2021/07/23/dronegun-tactical-bloqueador-drones-homologacao-anatel-brasil/.

16 G1. **Agentes penitenciários de Itapetininga passam por treinamento com primeira arma antidrone da região**. 2022. Acesso em: 2 abr. 2023. Disponível em: https://g1.globo.com/sp/itapetininga-regiao/noticia/2022/07/20/agentes-penitenciarios-de-itapetininga-passam-por-treinamento-com-primeira-arma-antidrone-da-regiao.ghtml.

17 BISCHOFF, W. **Entenda como funciona a 'arma' que derrubou drone suspeito durante a posse de Lula**. 2023. Acesso em: 2 abr. 2023. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2023/01/01/entenda-com16o-funciona-a-arma-que-derrubou-drone-suspeito-durante-a-posse-de-lula.ghtml.

18 ŠIMON, O.; GÖTTHANS, T.; POPELA, M. Commercial uav jamming possibilities. In: IEEE. **2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA)**. 2022. p. 1–6. Acesso em: 2 abr. 2023. Disponível em: https://ieeexplore.ieee.org/document/9764904.

19 JIN, W.-C.; KIM, K.; CHOI, J.-W. Robust jamming algorithm for location-based uav jamming system. In: IEEE. **2019 IEEE Asia-Pacific Microwave Conference (APMC)**. 2019. p. 1581–1583. Acesso em: 2 abr. 2023. Disponível em: https://ieeexplore.ieee.org/document/9038440.

20 TAN, X.; SU, S.; SUN, X. Research on narrowband interference suppression technology of uav network based on spread spectrum communication. In: IEEE. **2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS)**. 2020. p. 335–338. Acesso em: 28 mar. 2023. Disponível em: https://ieeexplore.ieee.org/document/9194891.

21 SCHOLTZ, R. Notes on spread-spectrum history. **IEEE Transactions on Communications**, IEEE, v. 31, n. 1, p. 82–84, 1983. Acesso em: 19 mar. 2023. Disponível em: https://ieeexplore.ieee.org/document/1095718.

22 MUNIR, M. A.; MAUD, A. R. M. Direct-sequence spread spectrum with variable spreading sequence for jamming immunity. In: IEEE. **2019 16th International Bhurban**

Conference on Applied Sciences and Technology (IBCAST). 2019. p. 933–937. Acesso em: 30 mar. 2023. Disponível em: https://ieeexplore.ieee.org/document/8667119.

23 MA, L. et al. Comparison of jamming methods for underwater acoustic dsss communication systems. In: **2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC)**. [s.n.], 2018. p. 1340–1344. Acesso em: 19 mar. 2023. Disponível em: https://ieeexplore.ieee.org/document/8469430.

24 WU, Y.; HUO, Y. A survey of cooperative jamming-based secure transmission for energy-limited systems. **Wireless Communications and Mobile Computing**, Hindawi Limited, v. 2021, p. 1–11, 2021. Acesso em: 19 mar. 2023. Disponível em: https://www.hindawi.com/journals/wcmc/2021/6638405/.

25 ZHONG, C.; YAO, J.; XU, J. Secure uav communication with cooperative jamming and trajectory control. **IEEE Communications Letters**, v. 23, n. 2, p. 286–289, 2019. Acesso em: 29 mar. 2023. Disponível em: https://ieeexplore.ieee.org/document/8589002.

26 HUO, Y. et al. A cross-layer cooperative jamming scheme for social internet of things. **Tsinghua Science and Technology**, v. 26, n. 4, p. 523–535, 2021. Acesso em: 29 mar. 2023. Disponível em: https://ieeexplore.ieee.org/document/9312780.

27 ZHONG, Y. et al. Cooperative jamming-aided secure wireless powered communication networks: A game theoretical formulation. **IEEE Communications Letters**, v. 24, n. 5, p. 1081–1085, 2020. Acesso em: 29 mar. 2023. Disponível em: https://ieeexplore.ieee.org/document/8990072.

28 ANJOS, A. A. **GEE531 — Comunicações Digitais I**. 2022. Notas de aula.

29 GUIMARÃES, D. **Digital Transmission: A Simulation-Aided Introduction with VisSim/Comm (Signals and Communication Technology)**. [S.l.]: Springer, 2010. ISBN: 978-3642013584.

30 GUIMARÃES D.; SOUZA, R. **Transmissão Digital: Princípios e aplicações**. 2. ed. [S.l.]: Érica, 2012. ISBN: 978-8536504391.

31 POISEL, R. **Modern Communications Jamming Principles and Techniques**. 2. ed. [S.l.]: Norwood: Artech House, 2011. ISBN: 13 978-1-60807-165-4.

32 ABBAS, M. J.; AWAIS, M.; HAQ, A. U. Comparative analysis of wideband communication techniques: Chirp spread spectrum and direct sequence spread spectrum. In: IEEE. **2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)**. [S.l.], 2018. p. 1–6.

33 ANJOS, A. A. **Interferência em sistemas de comunicação digital — Apostila EX007**. 2016. Notas de aula.

APÊNDICE A

Código em MATLAB®

A.1 Modulo Principal

```
%% Simulacao PFC 2%% Transmissor e Receptor sob Interferencia %%
% Autores: Murilo Pereira dos Reis e Prof. Dr. Andre Antonio dos Anjos
% Data 30/06/2023

%%
clear all;
close all;
clc;

%% Definicao de configuracoes da simulacao
% Simulation Type: 0-AWGN; 1-Jammer; 2 - Jammer + AWGN
Param.Sim.Type = 0;
%Tipo de transmissor 0-BPSK; 1-DSSS
Param.Tx.Type = 0;
%Jammer tipo: 0-single tone, 1-multitone, 2-noise jamming NBN, 3-Pulse
%Tone, 4-Pulse NBN, 5 Swept
Param.Sim.Jammer.Type = 0;
%Quantidade de amostras por simbolo
Param.Sim.OverSampling = 100;
```

```
20 %Relacao Sinal ruido ou interferencia considerada na
       simulacao
21 Param.Sim.EbNodB = 0:1:10;
22 %Taxa de simbolo de simulacao (Freq. de amostragem e
       relacionada)
23 Param.Tx.BitRate = 1*10^6;
24 %Energia media de simbolo
25 Param.Tx.SymbolEnergy = 1;
26 %Frequencia de portadora (deve ser multiplo inteiro da taxa
       de bits)
27 Param.Tx.CarrierFrequency = 30*Param.Tx.BitRate;
28 %Numero de simbolos transmitidos para levantar cada ponto das
        curvas de BER
29 Param.Tx.NumberBitsTx = 10%1*10.^5;
30 %Para DSSS define a taxa de chip em funcao da taxa de bit Ex:
        10 Rb
31 Param.Tx.DSSS.ChipRate = 10*Param.Tx.BitRate;
32 % %Sequencia PN (m) de comprimento 2^3 - 1 = 7 chips,
       polinomio (3,1),
33 % %carregamento inicial 110
34 % Param.Tx.DSSS.PNbase = [-1 1 1 -1 1 1 -1];
35 %Sequencia PN (m) de comprimento 2^4 - 1 = 15 chips,
       polinomio (4,1),
36 Param.Tx.DSSS.PNbase = [1 -1 1 -1 1 1 -1 -1 1 -1 -1 -1 1 1
       1];
37
38 %% Parametros Derivados das configuracoes iniciais
39 %Frequencia de amostragem (relacionada com a taxa de simbolo)
40 Param.sim.SampleRate= Param.Sim.OverSampling*Param.Tx.BitRate
       ;
41 %Vetor de Eb/No em escala linear
42 Param.sim.Eb_No_lin = 10.^(Param.Sim.EbNodB/10);
43 %Numero de chips total na simulacao em caso de DSSS
44 Param.Tx.DSSS.ChipNumbers = Param.Tx.NumberBitsTx*Param.Tx.
       DSSS.ChipRate/Param.Tx.BitRate;
45 %Vetor de tempo para geracao de todos os simbolos a cada run
       da simulacao
46 Param.sim.TxRxTime =[0:1:Param.Tx.NumberBitsTx*Param.Sim.
       OverSampling-1]*1/Param.sim.SampleRate;
```

```
47
48 %% Parametros relacionados com o Jammer
49 %Frequencia central do sinal interferente
50 Param.Sim.Jammer.CenterToneFrequency = 30*Param.Tx.BitRate;
51 %Em caso de MultitoneJamming 3 tons: tons em fc e em fc +-
      FreqSpace
52 Param.Sim.Jammer.MultiTone.FreqSpace = 0.5*Param.Tx.BitRate;
53 %Em caso de Noise Jamming BW normalizada (fracao da
      frequencia de amostragem)
54 Param.Sim.Jammer.Noise.BW =0.5/100*Param.sim.SampleRate;
55 %Em caso de Pulse Jamming NBN ou ton 0% ate 100%
56 Param.Sim.Jammer.AtiveTime = 10/100;
57 %Em caso de Sweept Jamming faixa de variacao de frequencia no
       entorno de fc
58 %FreqRange = Fc+-SweeptJammingFreqRange Ex: fc +-Rb (Hz)
59 Param.Sim.Jammer.SweeptJammingFreqRange = Param.Tx.BitRate;
60 %Relacao Sinal Interferencia na entrada do Rx P/J
61 Param.Sim.Jammer.Relacao_P_J_dB = -30:1:0;
62 %Converte relacao anterior para linear
63 Param.Sim.Jammer.Relacao_P_J_lin = 10.^(Param.Sim.Jammer.
      Relacao_P_J_dB/10);
64
65 %% BER BPSK/DSSS-BPSK teorica AWGN
66 if Param.Sim.Type == 0;
67     figure(1)
68     BER = 1/2*erfc(sqrt(Param.sim.Eb_No_lin));
69     semilogy(Param.Sim.EbNodB,BER)
70     xlabel('E_b/N_0 [dB]')
71     ylabel('BER')
72     grid on;
73     %axis([min(Param.Sim.EbNodB) max(Param.Sim.EbNodB) 10.^-6
           1]);
74     pause(0.0001)
75 end
76 tic
77
78 %% Verifica qual vetor sera variado Eb/No ou P/J
79 if Param.Sim.Type == 0
80     Loop_vec = Param.sim.Eb_No_lin;
```

```
81 elseif Param.Sim.Type == 1
82     Loop_vec = Param.Sim.Jammer.Relacao_P_J_lin ;
83 else
84     Loop_vec = Param.Sim.Jammer.Relacao_P_J_lin ;
85 end
86 BER_sim = zeros(1,length(Loop_vec));
87 for i=1 : length(Loop_vec)
88
89     %% Geracao de bits
90     %Bits aleatorios
91     BitsTx = randi([0 1],1,Param.Tx.NumberBitsTx);
92
93     %% Transmissor 0-BPSK; 1-DSSS
94     if Param.Tx.Type == 0
95         [SimbTxTime,Eb] = func_BPSK_TX(BitsTx,Param);
96     else
97         [SimbTxTime,Eb] = func_DSSS_TX(BitsTx,Param);
98     end
99
100    %% Canal 0-AWGN; 1-Jammer ou 2-ambos
101    if Param.Sim.Type == 0
102        [Rx] = func_AWGN_Channel(SimbTxTime,Eb,Param,Param.
               sim.Eb_No_lin(i));
103    elseif Param.Sim.Type == 1
104        [Rx] = func_Jammer(SimbTxTime,Eb,Param,Param.Sim.
               Jammer.Relacao_P_J_lin(i));
105    else
106        [Rx] = func_Jammer(SimbTxTime,Eb,Param,Param.Sim.
               Jammer.Relacao_P_J_lin(i));
107        % Em cenario de ruido om interferencia considerar Eb/
               No fixo de 20dB = 100 vezes
108        [Rx] = func_AWGN_Channel(Rx,Eb,Param,100);
109    end
110
111    %% Receptor 0-BPSK; 1-DSSS
112    if Param.Tx.Type == 0
113        [BitsRx] = func_BPSK_RX(Rx,Param);
114    else
115        [BitsRx] = func_DSSS_RX(Rx,Param);
```

```
116     end
117
118     %% Monitoramento de BER
119     [BER_sim(i)] = func_BER_Monitoring(BitsTx,BitsRx);
120
121     %% Plot da Curva BER (teorica e simulada)
122
123     if Param.Sim.Type == 0
124         figure(1)
125         hold on;
126         plot(Param.Sim.EbNodB(i),BER_sim(i),'*r')
127         if Param.Tx.Type == 0
128             legend('BER teorica','BER BPSK simulada')
129         else
130             legend('BER teorica','BER DSSS simulada')
131         end
132         pause(0.00001)
133     else
134         figure(1)
135         semilogy(-Param.Sim.Jammer.Relacao_P_J_dB(i),BER_sim(
              i),'*b')
136         hold on;
137         xlabel('J/P [dB]')
138         ylabel('BER')
139         grid on;
140         if Param.Tx.Type == 0
141             legend('BER BPSK simulada sob interferencia')
142         else
143             legend('BER DSSS simulada sob interferencia')
144         end
145         pause(0.00001)
146     end
147 end
148 toc
```

A.2 Modulo 'func_AWGN_Channel'

```
1 %% AWGN Channel
```

```
% Funcao responsavel por contaminar o sinal com ruido AWGN com a densidade espectral configurada
% Entradas: SimbTxTime(Simbolos no tempo), Param(Parametros do sistema), Eb_No_lin (SNR em escala linear), Eb (Energia media de bit simulada)
% Saida: Rx (Sinal transmitido condaminado com o ruido AWGN)

function [Rx] = func_AWGN_Channel(SimbTxTime,Eb,Param,Eb_No_lin)

%Determinando a densidade espectral em W/Hz
No = Eb/Eb_No_lin;

%Determinadno a potencia de ruido em simulacao para que tenha a
%densidade espectral desejada No = PoweNoise/(sampleRate/2)
Power_Noise = No*Param.sim.SampleRate/2;

%Gera a mesma quantidade de amostras transmitidas com a Potencia
%adequada de ruido. Pode ser ruido real ou circularmente simetrico
NoiseTime = sqrt(Power_Noise)*randn(1,length(Param.sim.TxRxTime));
%NoiseTime = sqrt(Power_Noise)*(1*randn(1,length(Param.sim.TxRxTime))+1i*1*randn(1,length(Param.sim.TxRxTime)));

%Adiciona ruido ao sinal no tempo
Rx = SimbTxTime + NoiseTime;

%Espectro do sinal recebido
%fvtool(Rx,1,'Fs',Param.sim.SampleRate)
```

A.3 Modulo ‘func_Jammer’

```
%% Jammer
%Funcao responsavel por contaminar o sinal com interferencia
```

```
3  %Entradas: SimbTxTime(Simbolos no tempo), Eb (energia media
       de bit), Param(Parametros do sistema), i(numero da
       iteracao), Eb (Energia media de bit simulada) J/P (relacao
        sinal interferencia em escala linear)
4  %Saida: Rx (Sinal transmitido condaminado com o ruido AWGN)
5
6  function [Rx] = func_Jammer(SimbTxTime,Eb,Param,
       Relacao_P_J_lin)
7
8  %Determinando a potencia do sinal desejado
9  PowerSignal = sum(abs(SimbTxTime).^2)/length(SimbTxTime);
10
11 %Encontrando a potencia do interferente
12 Power_Jammer = PowerSignal/Relacao_P_J_lin;
13
14 % Power_Jamming = PowerSignal/Eb_Jo_lin;
15 % %Determinando a densidade espectral em W/Hz
16 % Jo = Eb/Eb_Jo_lin;
17 % %Determinadno a potencia de ruido em simulacao para que
       tenha a
18 % %densidade espectral desejada No = PoweNoise/(sampleRate/2)
19 % Power_Jammer = Jo*Param.sim.SampleRate/2;
20
21 if Param.Sim.Jammer.Type == 0
22     %Single Tone
23     Jammer_Signal = cos(2*pi*Param.Sim.Jammer.
           CenterToneFrequency*Param.sim.TxRxTime);
24 elseif Param.Sim.Jammer.Type == 1
25     %MultiTone
26     Jammer_Signal = cos(2*pi*Param.Sim.Jammer.
           CenterToneFrequency*Param.sim.TxRxTime) ...
27     + cos(2*pi*(Param.Sim.Jammer.CenterToneFrequency+Param.
           Sim.Jammer.MultiTone.FreqSpace)*Param.sim.TxRxTime) ...
28     + cos(2*pi*(Param.Sim.Jammer.CenterToneFrequency-Param.
           Sim.Jammer.MultiTone.FreqSpace)*Param.sim.TxRxTime);
29 elseif Param.Sim.Jammer.Type == 2
30     %NBN
31     %Gera amostras de ruido
```

```
32      AWGNnoise = randn(1,length(Param.sim.TxRxTime)); % Gera
          ruido branco
33      %Filtra ruido na banda desejada
34      fc = Param.Sim.Jammer.Noise.BW/2;
35      order = 35; % Ordem do filtro (ajuste conforme necessario
          )
36      cutoff = fc/(Param.sim.SampleRate/2); % Frequencia de
          corte normalizada
37      %Cria o filtro Passa baixa
38      FilterTaps = designfilt('lowpassiir', 'FilterOrder',
          order, 'PassbandFrequency', cutoff);
39      %Gera ruido filtrado em banda base
40      JammerBB = filter(FilterTaps,AWGNnoise);
41      %Converte para a frequencia desejada
42      Jammer_Signal = JammerBB.*cos(2*pi*Param.Sim.Jammer.
          CenterToneFrequency*Param.sim.TxRxTime);
43  elseif Param.Sim.Jammer.Type == 3
44      %Pulse tone
45      Jammer_Signal_aux = cos(2*pi*Param.Sim.Jammer.
          CenterToneFrequency*Param.sim.TxRxTime);
46      %Pulso ficara ativo apenas parte da simulacao
47      Jammer_Signal = zeros(1,length(Jammer_Signal_aux));
48      %Pega apenas X % do tempo total de simulacao
49      Jammer_Signal(1:Param.Sim.Jammer.AtiveTime*length(
          Jammer_Signal))=Jammer_Signal_aux(1:Param.Sim.Jammer.
          AtiveTime*length(Jammer_Signal));
50  elseif Param.Sim.Jammer.Type == 4
51      %Gera amostras de ruido
52      AWGNnoise = randn(1,length(Param.sim.TxRxTime)); % Gera
          ruido branco
53      %Filtra ruido na banda desejada
54      fc = Param.Sim.Jammer.Noise.BW/2;
55      order = 35; % Ordem do filtro (ajuste conforme necessario
          )
56      cutoff = fc/(Param.sim.SampleRate/2); % Frequencia de
          corte normalizada
57      %Cria o filtro Passa baixa
58      FilterTaps = designfilt('lowpassiir', 'FilterOrder',
          order, 'PassbandFrequency', cutoff);
```

```
59      %Gera ruido filtrado em banda base
60      JammerBB = filter(FilterTaps,AWGNnoise);
61      %Converte para a frequencia desejada
62      Jammer_Signal_aux = JammerBB.*cos(2*pi*Param.Sim.Jammer.
            CenterToneFrequency*Param.sim.TxRxTime);
63      %Apenas em fracao da simulacao ocorre um pulso de
            interferente do tipo
64      %Pulso ficara ativo apenas parte da simulacao
65      Jammer_Signal = zeros(1,length(Jammer_Signal_aux));
66      %Pulse NBN
67      Jammer_Signal(1:Param.Sim.Jammer.AtiveTime*length(
            Jammer_Signal))=Jammer_Signal_aux(1:Param.Sim.Jammer.
            AtiveTime*length(Jammer_Signal));
68  else
69      %Sweept Jammer
70      MinFreq = Param.Sim.Jammer.CenterToneFrequency - Param.
            Sim.Jammer.SweeptJammingFreqRange;
71      MaxFreq = Param.Sim.Jammer.CenterToneFrequency + Param.
            Sim.Jammer.SweeptJammingFreqRange;
72      %Cria um vetor crecente da frequencia minima ate maxima
73      FreqVector = linspace(MinFreq,MaxFreq,length(Param.sim.
            TxRxTime));
74      %Gera Jammer com frequencia que varia do valor minimo ao
            maximo durante
75      %um periodo completo de transmissao e recepcao de bits.
76      Jammer_Signal = cos(2*pi*FreqVector.*Param.sim.TxRxTime);
77
78  end
79  %Normalizando a potencia do interferente para inserir
        potencia adequada
80  PowerJ = sum(abs(Jammer_Signal).^2)/length(Jammer_Signal);
81  Jammer_Signal = Jammer_Signal/sqrt(PowerJ)*sqrt(Power_Jammer)
        ;
82  PowerJ = sum(abs(Jammer_Signal).^2)/length(Jammer_Signal);
83
84  J_div_P_dB = 10*log10(PowerJ/PowerSignal)
85
86  %NoiseTime = sqrt(Power_Noise)*(1*randn(1,length(Param.sim.
        TxRxTime))+1i*1*randn(1,length(Param.sim.TxRxTime)));
```

```
87 %Adiciona ruido ao sinal no tempo
88 Rx = SimbTxTime + Jammer_Signal;
89 %Espectro do sinal recebido
90 %fvtool(Jammer_Signal,1,'Fs',Param.sim.SampleRate)
```

A.4 Modulo 'func_BER_Monitoring'

```
1  %% Monitoramento de BER
2  %Funcao responsavel por estimar a BER via simulacao
3  %Entradas: BitsTx (Bits transmitidos); BitsRx (Bits estimados
       no RX)
4  %Saida: BER_sim (BER estimada via simulacao)
5
6  function [BER_sim] = func_BER_Monitoring(BitsTx,BitsRx)
7
8  %Contabiliza o numero de bits errados
9  NumErrors = sum(BitsTx~=BitsRx);
10
11 %Estima BER via simulacao
12 BER_sim = NumErrors/length(BitsTx);
```

A.5 Modulo 'func_BPSK_TX'

```
1  %% Transmissor BPSK
2  %Funcao responsavel por modular os bits em simbolos BPSK,
       alem de calcular Eb simulado
3  %Entradas: BitsTx(Bits de entrada); Param(Parametros do
       sistema).
4  %Saida: SimbTxTime (Sinal de transmissao BPSK no tempo); Eb (
       Energia media de bit simulada)
5
6  function [SimbTxTime,Eb] = func_BPSK_TX(BitsTx,Param)
7
8  %Conversao de bits em coeficientes +- sqrt(Eb)
9  SimbTxCoe = (BitsTx*2-1)*sqrt(Param.Tx.SymbolEnergy);
10
11 %Calculando a Energia media dos simbolos transmitidos
12 Eb = sum(abs(SimbTxCoe).^2)/length(SimbTxCoe);
```

```
13
14 %Sobreamostragem dos simbolos para geracao do sinal no tempo
15 SimbTxCoeOverSampled = repelem(SimbTxCoe, Param.Sim.
      OverSampling);
16
17 %Geeracao da forma de onda do simbolo no tempo s(t) =+-sqrt(
      Eb)*phi_1
18 %Funcao base
19 phi_t =sqrt(2*Param.Tx.BitRate)*cos(2*pi*Param.Tx.
      CarrierFrequency*Param.sim.TxRxTime);
20 SimbTxTime = SimbTxCoeOverSampled.*phi_t;
21
22 %Para ver espectro, descomentar linha abaixo
23 %fvtool(SimbTxTime,1,'Fs',Param.sim.SampleRate)
```

A.6 Modulo 'func_BPSK_RX'

```
1 %% Receptor BPSK
2 %Funcao responsavel por demodular os bits modulados em BPSK.
3 %Entradas: Rx(Sinal corrompido com ruido e/ou Interferencia);
      Param(Parametros do sistema).
4 %Saida: BitsRx
5
6 function [BitsRx] = func_BPSK_RX(Rx,Param)
7
8 %Funcao base do receptor
9 phi_r =sqrt(2*Param.Tx.BitRate)*cos(2*pi*Param.Tx.
      CarrierFrequency*Param.sim.TxRxTime);
10
11 %Correlacao y = integral(rx*phi)dt -- para cada simbolo
12 Rx_times_phi_r= Rx.*phi_r;
13
14 %Rearranja o vetor anteriro em Oversamples linhas e Ntx bits
      colulas e implementando a correlacao simbolo a simbolo.
15 RxSymbols= sum(reshape(Rx_times_phi_r, Param.Sim.OverSampling
      , length(Rx_times_phi_r)/Param.Sim.OverSampling))*1/Param.
      sim.SampleRate;
16
```

```
%figure;
%plot(real(RxSymbols),imag(RxSymbols),'*');
%legend('Simbolos Recebidos');

%Decisao na saida do correlator
%Comparador com o limiar 0 e decisao no receptor
BitsRx = (real(RxSymbols) >0);
```

A.7 Modulo 'func_DSSS_TX'

```
%% Transmissor DSSS
%Funcao responsavel por modular os bits em simbolos DSSS-BPSK
   , alem de calcular Eb simulado
%Entradas: BitsTx(Bits de entrada); Param(Parametros do
   sistema).
%Saida: SimbTxTime (Sinal de transmissao BPSK no tempo); Eb (
   Energia media de bit simulada)

function [SimbTxTime,Eb] = func_DSSS_TX(BitsTx,Param)

%Conversao de bits em coeficientes +- sqrt(Eb)
SimbTxCoe = (BitsTx*2-1)*sqrt(Param.Tx.SymbolEnergy);

%Calculando a Energia media dos simbolos transmitidos
Eb = sum(abs(SimbTxCoe).^2)/length(SimbTxCoe);

%Sobreamostragem dos simbolos para geracao do sinal no tempo
SimbTxCoeOverSampled = repelem(SimbTxCoe, Param.Sim.
   OverSampling);

%% Espalhamento do simbolos em Banda base
%Verficando quantas vezes a sequencia PN completa se repetira
NumbSeqPN = fix(Param.Tx.DSSS.ChipNumbers/length(Param.Tx.
   DSSS.PNbase));

%Chips que faltam para completar o total
NumbChipPN = mod(Param.Tx.DSSS.ChipNumbers,length(Param.Tx.
   DSSS.PNbase));
```

```
23
24 %Gera sequencia de chips
25 PN = [repmat(Param.Tx.DSSS.PNbase,1,NumbSeqPN) Param.Tx.DSSS.
      PNbase(1:NumbChipPN)];
26
27 %Sobreamostra a sequencia de chipas para a frequencia de
      amostragem Sample
28 %Rate/ChipRte
29 PN_Oversampled = repelem(PN, Param.sim.SampleRate/Param.Tx.
      DSSS.ChipRate );
30
31 %Espalhamento Espectral por sequencia direta
32 SpreadSimbTxCoeOverSampled = SimbTxCoeOverSampled.*
      PN_Oversampled;
33 % fvtool(SimbTxCoeOverSampled,1,SpreadSimbTxCoeOverSampled
      ,1,'Fs',Param.Sim.OverSampling*Param.Tx.BitRate)
34
35
36 %%
37 %Geeracao da forma de onda do simbolo no tempo s(t) =+-sqrt(
      Eb)*phi_1
38 %Funcao base
39 phi_t =sqrt(2*Param.Tx.BitRate)*cos(2*pi*Param.Tx.
      CarrierFrequency*Param.sim.TxRxTime);
40 SimbTxTime = SpreadSimbTxCoeOverSampled.*phi_t;
41
42 %Para ver espectro, descomentar linha abaixo
43 % fvtool(SimbTxTime,1,'Fs',Param.sim.SampleRate)
```

A.8 Modulo 'func_DSSS_RX'

```
1 %% Receptor DSSS
2 %Funcao responsavel por demodular os bits modulados em DSSS-
      BPSK.
3 %Entradas: Rx(Sinal corrompido com ruido e/ou Interferencia);
       Param(Parametros do sistema).
4 %Saida: BitsRx
5
```

```
6  function [BitsRx] = func_DSSS_RX(Rx,Param)
7
8  %Funcao base do receptor
9  phi_r =sqrt(2*Param.Tx.BitRate)*cos(2*pi*Param.Tx.
       CarrierFrequency*Param.sim.TxRxTime);
10
11 %Correlacao y = integral(rx*phi)dt -- para cada simbolo
12 Rx_times_phi_r= Rx.*phi_r;
13
14 %% Desespalhamento do sinal
15 %Verficando quantas vezes a sequencia PN completa se repetira
16 NumbSeqPN = fix(Param.Tx.DSSS.ChipNumbers/length(Param.Tx.
       DSSS.PNbase));
17
18 %Chips que faltam para completar o total
19 NumbChipPN = mod(Param.Tx.DSSS.ChipNumbers,length(Param.Tx.
       DSSS.PNbase));
20
21 %Gera sequencia de chips
22 PN = [repmat(Param.Tx.DSSS.PNbase,1,NumbSeqPN) Param.Tx.DSSS.
       PNbase(1:NumbChipPN)];
23
24 %Sobreamostra a sequencia de chipas para a frequencia de
       amostragem Sample
25 %Rate/ChipRte
26 PN_Oversampled = repelem(PN, Param.sim.SampleRate/Param.Tx.
       DSSS.ChipRate );
27
28 %Desespalha o sinal no receptor
29 Rx_BB_DeSpread = Rx_times_phi_r.*PN_Oversampled;
30 %Para ver espectro, descomentar linha abaixo
31 %fvtool(Rx_BB_DeSpread,1,'Fs',Param.sim.SampleRate)
32
33 %%
34 %Rearranja o vetor anteriro em Oversamples linhas e Ntx bits
       colulas e
35 %implementando a correlacao simbolo a simbolo.
36 RxSymbols= sum(reshape(Rx_BB_DeSpread, Param.Sim.OverSampling
       , length(Rx_BB_DeSpread)/Param.Sim.OverSampling))*1/Param.
```

```
   sim.SampleRate;
% figure;
% plot(real(RxSymbols),imag(RxSymbols),'*');
% legend('Simbolos Recebidos');

%Decisao na saida do correlator
%Comparador com o limiar 0 e decisao no receptor
BitsRx = (real(RxSymbols) >0);
```