

INSTITUTO MILITAR DE ENGENHARIA

ALEX ALVAREZ DA SILVA

**SIMULAÇÃO E ANÁLISE DA EFICÁCIA DAS TÉCNICAS DE
BLOQUEIO EM SISTEMAS DE COMUNICAÇÕES:
ÊNFASE NO SISTEMA GSM**

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia Elétrica do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Ciências em Engenharia Elétrica.

Orientador: José Carlos Araujo dos Santos, Ph.D.
Co-orientador: Maurício Henrique Costa Dias, Dr.

Rio de Janeiro
2009

Livros Grátis

<http://www.livrosgratis.com.br>

Milhares de livros grátis para download.

c2009

INSTITUTO MILITAR DE ENGENHARIA

Praça General Tibúrcio, 80-Praia Vermelha

Rio de Janeiro - RJ CEP 22290-270

Este exemplar é de propriedade do Instituto Militar de Engenharia, que poderá incluí-lo em base de dados, armazenar em computador, microfilmear ou adotar qualquer forma de arquivamento.

É permitida a menção, reprodução parcial ou integral e a transmissão entre bibliotecas deste trabalho, sem modificação de seu texto, em qualquer meio que esteja ou venha a ser fixado, para pesquisa acadêmica, comentários e citações, desde que sem finalidade comercial e que seja feita à referência bibliográfica completa.

Os conceitos expressos neste trabalho são de responsabilidade do(s) autor(es) e do(s) orientador(es).

537 Silva, Alex Alvarez da

S586s Simulação e Análise da Eficácia das Técnicas de Bloqueio em Sistemas de Comunicações: Ênfase no Sistema GSM / Alex Alvarez da Silva. - Rio de Janeiro: Instituto Militar de Engenharia, 2009.

142 p.: il.

Dissertação (mestrado) - Instituto Militar de Engenharia- Rio de Janeiro, 2009.

1. Eletromagnetismo. 2. Bloqueador de múltiplas frequências 3. Sistemas de Comunicações. II. Instituto Militar de Engenharia.

CDD 537

INSTITUTO MILITAR DE ENGENHARIA

ALEX ALVAREZ DA SILVA

**SIMULAÇÃO E ANÁLISE DA EFICÁCIA DAS TÉCNICAS DE
BLOQUEIO EM SISTEMAS DE COMUNICAÇÕES: ÊNFASE NO
SISTEMA GSM**

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia Elétrica do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Ciências em Engenharia Elétrica.

Orientador: José Carlos Araujo dos Santos, Ph.D.

Co-orientador: Maurício Henrique Costa Dias, Dr.

Aprovada em 24 de Julho de 2009 pela seguinte Banca Examinadora:

José Carlos Araujo dos Santos, Ph.D. do IME – Presidente

Maurício Henrique Costa Dias, Dr. do IME

Aristóteles de Souza Carvalho, Ph.D. da Embraer

Juraci Ferreira Galdino, Dr. do IME

Rio de Janeiro
2009

AGRADECIMENTOS

Inicialmente, gostaria de agradecer a Deus que me deu saúde e força durante todo o curso.

Agradecer aos meus pais, Marcos e Cristina, ao meu irmão, Alan, e à minha namorada, Anna Carolina, que souberam compreender a minha ausência nas horas dedicadas ao curso.

Aos meus professores, José Carlos Araújo dos Santos e Major Maurício Henrique Costa Dias, que passaram os conhecimentos necessários para a conclusão do curso com muita competência e dedicação.

Ao Instituto Militar de Engenharia e em especial à Seção de Engenharia Elétrica, que proporcionaram as condições necessárias para que eu pudesse desenvolver minhas atividades no curso de mestrado.

Aos meus companheiros da Omnisys Engenharia e do Instituto de Pesquisa da Marinha que me apoiaram e incentivaram durante o desenvolvimento do trabalho.

A todas as pessoas que, direta ou indiretamente, contribuíram para a execução desta Dissertação de Mestrado.

SUMÁRIO

LISTA DE ILUSTRAÇÕES	8	
LISTA DE TABELAS	13	
ABREVIATURAS	14	
1	INTRODUÇÃO	21
1.1	Objetivo	21
1.2	Contextualização	21
1.3	Justificativas	25
1.4	Composição do Trabalho	26
2	CONSIDERAÇÕES SOBRE OS SISTEMAS DE COMUNICAÇÕES CIVIS E MILITARES.....	27
2.1	Modulações	27
2.1.1	Modulações Analógicas	28
2.1.1.1	Modulação em Amplitude - AM	28
2.1.1.2	Modulação em Frequência – FM	31
2.1.1.3	Modulação em Fase – PM.....	31
2.1.2	Modulações Digitais.....	32
2.1.2.1	Modulação por Chaveamento de Amplitude – ASK.....	33
2.1.2.2	Modulação por Chaveamento de Frequência – FSK.....	34
2.1.2.3	Modulação por Chaveamento de Fase – PSK.....	36
2.1.2.4	Modulação de Amplitude em Quadratura – QAM.....	36
2.2	Sistemas com Espalhamento Espectral	37
2.2.1	Espalhamento Espectral por Sequência Direta - DSSS.....	38
2.2.2	Espalhamento Espectral por Salto em Frequência – FHSS.....	40
2.2.3	Espalhamento Espectral por Salto no Tempo – THSS.....	42
2.3	Sistemas Comerciais	44
2.3.1	CDMA.....	44
2.3.2	GSM.....	46
2.4	Sistemas Militares	49
2.4.1	A Norma MIL-STD-188-110B	50

3	SISTEMAS DE BLOQUEIO EM GUERRA ELETRÔNICA.....	51
3.1	Introdução.....	51
3.2	Tipos de Bloqueios Eletrônicos.....	53
3.2.1	Bloqueio por Ruído	53
3.2.2	Bloqueio com Varredura	55
3.2.3	Bloqueio por Tom	56
3.2.4	Bloqueio por Pulso	57
3.2.5	Bloqueio Seguidor.....	57
3.2.6	Bloqueio Inteligente	58
3.3	Bloqueio em Sistemas com Espalhamento Espectral.....	58
3.3.1	Bloqueio em Sistemas DSSS.....	58
3.3.2	Bloqueio em Sistemas com Salto em Frequência Rápido (FFH).....	60
3.3.3	Bloqueio em Sistemas com Salto em Frequência Lento (SFH)	63
3.4	Aplicação do Bloqueador em Sistemas de Comunicações.....	65
3.4.1	Cenário	65
3.4.2	Equação Básica dos Bloqueadores	66
3.4.3	Equação Básica para Avaliação de Sistemas Analógicos	67
3.4.4	Equação Básica para Avaliação de Sistemas Digitais.....	69
4	IMPLEMENTAÇÃO DOS SISTEMAS.....	70
4.1	Implementação da Modulação AM-DSB	70
4.2	Implementação dos Bloqueadores.....	73
4.3	Implementação dos Sistemas de Comunicações Comerciais	78
4.3.1	Implementação do Sistema CDMA.....	78
4.3.2	Implementação do Sistema GSM.....	80
4.4	Implementação dos Sistemas Militares	83
4.4.1	Implementação da Norma MIL-STD-188-110B.....	83
5	EFETIVIDADE DOS BLOQUEADORES SOBRE ALGUNS SISTEMAS DE COMUNICAÇÕES	85
5.1	Estrutura das Simulações	85
5.1.1	Avaliação da Metodologia Sobre a Modulação em Amplitude	85
5.2	Análise da Eficácia dos Bloqueadores	89

5.2.1	No Sistema CDMA	89
5.2.2	No Sistema GSM.....	93
5.2.3	Na Norma MIL-STD-188-110B.....	99
6	TESTES PRÁTICOS COM O SISTEMA GSM	103
6.1	Implementação e Teste de um Bloqueador para a Faixa de 1800 MHz.....	103
6.2	Ambiente de Realização	107
6.3	Efetividade do Bloqueador Sobre d Sistema de Telefonia Móvel GSM.....	109
6.4	Valores Simulados × Valores Práticos	114
7	CONCLUSÕES E SUGESTÕES.....	118
8	REFERÊNCIAS BIBLIOGRÁFICAS	122
9	APÊNCICES.....	126
9.1	Apêncice 1: Sistema Comercial GSM.....	127
9.2	Apêncice 2: Norma MIL-STD-188-110B	133
9.2.1	Bloco de Sequência de Dados	133
9.2.2	Bloco de Código Corretor de Erros (FEC).....	134
9.2.3	Bloco Entrelaçador	135
9.2.4	Bloco Decodificador Gray Modificado (MGD).....	136
9.2.5	Bloco de Formação de Símbolos.....	137
9.2.5.1	Unknown Data.....	137
9.2.5.2	Probe – Sequência de Treinamento	138
9.2.6	Bloco de Geração da Sequência de Sincronismo	139
9.2.7	Bloco de Embaralhamento	140
9.2.7.1	Gerador de Sequência Aleatória para Dados.....	141
9.2.7.2	Gerador de Sequências Aleatórias para o Sincronismo	141
9.2.8	Bloco Modulador.....	141
9.2.9	Bloco Receptor	142

LISTA DE ILUSTRAÇÕES

FIG. 2.1	Esquemas de modulações analógicas e digitais.	28
FIG. 2.2	Modulador AMDSB.	29
FIG. 2.3	Espectro de amplitude do sinal modulado em AMDSB.	30
FIG. 2.4	Espectro de potência do sinal modulado em AMDSB.	31
FIG. 2.5	Modulações Digitais.	33
FIG. 2.6	Representação de um sinal com modulação B-ASK.	34
FIG. 2.7	Modulação B-FSK.	35
FIG. 2.8	Exemplo de modulação B-PSK.	36
FIG. 2.9	Constelação de um sinal com modulação QAM. (a) 16-QAM e (b) 64-QAM.	37
FIG. 2.10	Exemplo básico de um Sinal DSSS.	39
FIG. 2.11	Transmissor e Receptor do sinal DSSS-BPSK.	39
FIG. 2.12	Sinal DSSS-BPSK no tempo.	40
FIG. 2.13	Transmissor de um sinal FHSS.	40
FIG. 2.14	FHSS rápido.	41
FIG. 2.15	FHSS lento.	42
FIG. 2.16	Rede GSM padrão.	47
FIG. 2.17	Técnicas de múltiplos acessos TDMA e FDMA.	48
FIG. 2.18	Canal de tráfego no GSM.	49
FIG. 3.1	CME e suas subdivisões.	51
FIG. 3.2	Topologia básica de um bloqueador BBN.	54
FIG. 3.3	Bloqueador PBN para canais contínuos e alternados.	54
FIG. 3.4	Topologia básica de um bloqueador banda estreita.	55
FIG. 3.5	Topologia básica de um bloqueador com varredura.	56

FIG. 3.6	Espectro do bloqueio por tom simples.	56
FIG. 3.7	Espectro do bloqueio por tom múltiplos.	57
FIG. 3.8	Bloqueador BBN em sistemas DSSS.	59
FIG. 3.9	Bloqueador PBN em sistemas DSSS com (a) sinal de bloqueio centrado na frequência central do sinal DSSS e com (b) sinal de bloqueio deslocado da frequência central.	59
FIG. 3.10	Bloqueador por tons em sistemas DSSS com (a) tons de bloqueio com mesma amplitude espaçados simetricamente da frequência central do sinal DSSS e com (b) tons de bloqueio de amplitudes diferentes e deslocados da frequência central.	60
FIG. 3.11	Bloqueador em sistemas FFH.	61
FIG. 3.12	Espectro de um sinal modulado em múltiplas frequências.	63
FIG. 3.13	Bloqueador PBN em sistemas SFH. (a) sinal e (b) bloqueio PBN	64
FIG. 3.14	Modelo de um sistema de comunicação na presença de um bloqueador.	66
FIG. 3.15	Diagrama de blocos de um sistema com modulação AMDSB.	68
FIG. 3.16	Diagrama de blocos de um sistema com modulação AM e bloqueador.	68
FIG. 4.1	Sub-Amostragem e translação de frequências entre as zonas de Nyquist.	71
FIG. 4.2	Diagrama do modulador e receptor AM-DSB.	72
FIG. 4.3	Espectro do sinal AM utilizando o teorema de sub-amostragem. (a) Amplitude do Sinal AM, (b) Potência do Sinal AM em Watts e (c) Potência do Sinal AM em dBm.	72
FIG. 4.4	Espectro do sinal AM utilizando o teorema de sub-amostragem. (a) Amplitude do Sinal AM, (b) Potência do Sinal AM em Watts e (c) Potência do Sinal AM em dBm.	73
FIG. 4.5	Diagrama do bloqueador BBN usado nas simulações.	74
FIG. 4.6	Sinal de saída do bloqueador BBN gerado pelo Simulink.	74
FIG. 4.7	Sinal de saída do bloqueador PBN gerado pelo Simulink.	75
FIG. 4.8	Sinal de saída do bloqueador NBN gerado pelo Simulink.	75

FIG. 4.9	Diagrama do bloqueador por tom simples simulado.....	76
FIG. 4.10	Sinal de saída do bloqueador por tom simples no Simulink.	76
FIG. 4.11	Diagrama do bloqueador por tons múltiplos simulado.	77
FIG. 4.12	Sinal de saída do bloqueador por tons múltiplos no Simulink.	77
FIG. 4.13	Diagrama do bloqueador por varredura simulado.....	78
FIG. 4.14	Bloqueador por varredura no Simulink mostrando (a) o início da varredura em 4GHz, (b) o sinal variando para 6GHz, (c) o sinal atingindo a varredura máxima e (d) o sinal retornando para varredura inicial.	78
FIG. 4.15	Canal direto de tráfego, modelo ponto-a-ponto, IS-95A, CDMA.....	79
FIG. 4.16	Sinal Transmitido pelo canal direto de tráfego, IS-95A, CDMA.....	79
FIG. 4.17	Processo de Codificação de Voz no GSM.	80
FIG. 4.18	Canal de tráfego do sistema GSM.....	81
FIG. 4.19	Bloco transmissor do GSM.	81
FIG. 4.20	Diagrama do processo de codificação do GSM utilizado nas simulações.	81
FIG. 4.21	Diagrama do processo de modulação do GSM utilizado nas simulações.	82
FIG. 4.22	Bloco receptor do GSM.....	82
FIG. 4.23	Espectro do sinal GSM transmitido com modulação GMSK.	82
FIG. 4.24	Canal de tráfego da norma MIL-STD-188-110B.....	83
FIG. 4.25	Constelação simulada do sinal transmitido utilizando a modulação 8-PSK.	84
FIG. 5.1	Diagrama do modulador por amplitude com bloqueador por varredura.	86
FIG. 5.2	Sinal AM na presença do bloqueador por varredura, teste 1.	87
FIG. 5.3	Sinal AM na presença do bloqueador por varredura, teste 5.	88
FIG. 5.4	Sinal AM na presença do bloqueador por varredura, teste 10.	88
FIG. 5.5	Canal de tráfego do sistema CDMA com bloqueador por varredura.	90

FIG. 5.6	Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema CDMA com um bloqueador por tom no canal de controle do sistema.	90
FIG. 5.7	Relação entre a BER e a razão J/S no receptor do sistema CDMA com um bloqueador PBN em toda banda do canal reverso do sistema.	91
FIG. 5.8	Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema CDMA com um bloqueador com varredura na banda de recepção do sistema móvel.	92
FIG. 5.9	Canal de tráfego do sistema GSM com bloqueador por varredura usado nas simulações.	95
FIG. 5.10	Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema GSM com um bloqueador PBN.	96
FIG. 5.11	Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema GSM com bloqueador por varredura.	97
FIG. 5.12	Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema GSM com bloqueador por varredura, considerando os ganhos das antenas.	98
FIG. 5.13	Canal de tráfego da norma MIL-STD-188-110B com bloqueador.	99
FIG. 5.14	Relação entre a BER e a razão J/S no receptor de um canal de tráfego da norma MIL-STD-118-110B com um bloqueador PBN.	100
FIG. 5.15	Relação entre a BER e a razão J/S no receptor de um canal de tráfego da norma MIL-STD-118-110B com um bloqueador pontual.	101
FIG. 5.16	Canal de tráfego da norma MIL-STD-118110B com bloqueador com varredura.	101
FIG. 6.1	Diagrama em blocos do dispositivo bloqueador implementado.	103
FIG. 6.2	Circuito implementado por Toscano (2006).	104
FIG. 6.3	Esquemáticos do VCO implementado, mostrando (a) circuito e (b) layout.	105
FIG. 6.4	Sinal de controle do VCO JTOS-2000.	105

FIG. 6.5	Circuito implementado com alimentação de +19VDC.	106
FIG. 6.6	Bloqueador GSM.....	106
FIG. 6.7	Sinal de saída do bloqueador implementado sem a antena, observado por um analisador de espectro.	107
FIG. 6.8	Arranjo de testes em laboratório.	108
FIG. 6.9	Mapeamento da potência do sinal recebido S (dBm).....	109
FIG. 6.10	Resultados dos testes.....	110
FIG. 6.11	Arranjo de teste para medir a potência de recepção S.....	111
FIG. 6.12	Potência de recepção S.....	112
FIG. 6.13	Resultados dos testes considerando os ganhos das antenas e perdas dos cabos. .	113
FIG. 6.14	Resultados simulados e práticos.....	115
FIG. 6.15	Resultados simulados e práticos, considerando os ganhos das antenas.	116
FIG. 9.1	Frame do GSM 900.....	127
FIG. 9.2	Rajada do sistema GSM.	128
FIG. 9.3	Timeslot, Quadro, Multiquadro e Superquadro do sistema GSM.....	129
FIG. 9.4	Canais lógicos do sistema GSM.....	130
FIG. 10.1	Diagrama do transmissor definido pela norma MIL-STD-188-110B.....	133
FIG. 10.2	Diagrama do codificador convolucional.	134
FIG. 10.3	Constelação da modulação 8-PSK.	138
FIG. 10.4	Registro de deslocamento para embaralhamento.	141

LISTA DE TABELAS

TAB. 2.1	Vantagens e desvantagens de sistemas com espalhamento espectral.....	43
TAB. 2.2	Bandas A e B do sistema CDMA.....	45
TAB. 2.3	Números dos canais do sistema CDMA.....	45
TAB. 2.4	Canais de tráfego do sistema CDMA.....	46
TAB. 5.1	Potência de saída do bloqueador por varredura.....	87
TAB. 5.2	Relação sinal ruído de um modulador AM na presença de um bloqueador por varredura.	89
TAB. 5.3	RxQual em função da BER.	95
TAB. 6.1	Valores J/S simulados para uma BER fixa.....	114
TAB. 9.1	Bandas de Operações para o GSM.....	127
TAB. 9.2	Níveis de potência no GSM.....	132
TAB. 10.1	Relação entre taxa de transmissão e taxas do código com código de repetição..	135
TAB. 10.2	Dimensões da matriz de entrelaçamento.....	135
TAB. 10.3	Numero de bits necessários para formação de um símbolo.....	136
TAB. 10.4	Decodificador Gray para 2400 bps e 4800 bps.....	136
TAB. 10.5	Decodificador Gray para 75 bps (frequência fixa) e 1200 bps.....	137
TAB. 10.6	Sequência de treinamento D1 e D2.....	139
TAB. 10.7	Mapeamento das sequência D1 e D2.....	139
TAB. 10.8	Mapeamento de dois a três bits na sequência de sincronismo.....	140
TAB. 10.9	Mapeamento das sequência C1, C2 e C3.....	140

ABREVIATURAS

1G	–	<i>First Generation</i> (Primeira Geração)
2G	–	<i>Second Generation</i> (Segunda Geração)
3G	–	<i>Third Generation</i> (Terceira Geração)
4G	–	<i>Fourth Generation</i> (Quarta Geração)
AGCH	–	<i>Access Grant Channel</i> (Canal de Concessão de Acesso)
AM	–	<i>Amplitude Modulation</i> (Modulação em Amplitude)
AMDSB	–	<i>Amplitude Modulation Double Side Band</i> (Modulação em Amplitude Banda Lateral Dupla)
AMDSB-SC	–	<i>Amplitude Modulation Double Side Band Supressed Carrier</i> (Modulação em Amplitude Banda Lateral Dupla e Portadora Suprimida)
AMPS	–	<i>Advanced Mobile Phone System</i> (Sistema de Telefone Móvel Avançado)
AMSSB-LSB	–	<i>Amplitude Modulation Single Side Band - Lower Side Band</i> (Modulação em Amplitude Banda Lateral Simples - Banda Lateral Inferior)
AMSSB-USB	–	<i>Amplitude Modulation Single Side Band - Upper Side Band</i> (Modulação em Amplitude Banda Lateral Simples - Banda Lateral Superior)
ARFCN	–	<i>Absolute Radio Frequency Channel Number</i> (Número Absoluto de Canal de Frequência de Rádio)
ARPANET	–	<i>Advanced Research Projects Agency</i> (EUA)
ASK	–	<i>Amplitude Shift Keying</i> (Modulação por Chaveamento de Amplitude)
AUC	–	<i>Authentication Center</i> (Central de Autenticação)
AWGN	–	<i>Additive White Gaussian Noise</i> (Ruído Branco Aditivo Gaussiano)
B-ASK	–	<i>Binary Amplitude Shift-Keying</i> (Chaveamento de Amplitude Binário)
BBN	–	<i>Broadband Noise</i> (Ruído Banda Larga)
BCCH	–	<i>Broadcast Control Channel</i> (Canal de Controle de Radiodifusão)

BER	– <i>Bit Error Rate</i> (Taxa de Erro de Bit)
B-FSK	– <i>Binary Frequency Shift-Keying</i> (Chaveamento de Frequência Binário)
B-PSK	– <i>Binary Phase Shift Keying</i> (Chaveamento de Fase Binário)
BSC	– <i>Base Station Controller</i> (Controlador da Estação Base)
BSS	– <i>Base Station System</i> (Estação Base de Sistemas)
BTS	– <i>Base Transceiver Station</i> (Estação Base Transceptora)
CCCH	– <i>Common Control Channel</i> (Canal de Controle Comum)
CDMA	– <i>Code Division Multiple Access</i> (Acesso Múltiplo por Divisão de Código)
CEPT	– <i>European Conference of Postal and Telecommunications Administrations</i> (Conferência Européia das administrações Postais e de Telecomunicações)
CME	– <i>Electronic Counter Measures</i> (Contra Medida Eletrônica)
CW	– <i>Continuous Wave</i> (Onda Contínua)
DCS	– <i>Digital Cellular System</i> (Sistema Celular Digital)
DSSS	– <i>Direct Sequence Spread Spectrum</i> (Espalhamento Espectral por Sequência Direta)
EA	– <i>Electronic Attack</i> (Ataque Eletrônico)
EIR	– <i>Equipment Identity Register</i> (Registro de Identidade de Equipamento)
EP	– <i>Electronic Protect</i> (Proteção Eletrônica)
ES	– <i>Electronic Support</i> (Suporte Eletrônico)
ETSI	– <i>European Telecommunications Standards Institute</i> (Instituto Europeu de Padrões em Telecomunicações)
EW	– <i>Electronic Warfare</i> (Guerra Eletrônica)
FCCH	– <i>Frequency Correction Channel</i> (Canal de Correção de Frequência)
FDMA	– <i>Frequency Division Multiple Access</i> (Acesso Múltiplo por Divisão de Frequência)

FFT	– <i>Fast Fourier Transform</i> (Transformada de Fourier Rápida)
FHSS	– <i>Frequency Hopping Spread Spectrum</i> (Espalhamento Espectral por Salto em Frequência)
FM	– <i>Frequency Modulation</i> (Modulação em Frequência)
FSK	– <i>Frequency Shift Keying</i> (Modulação por Chaveamento de Frequência)
GLO	– Garantia da Lei e da Ordem
GMSK	– <i>Gaussian Minimum Shift Keying</i> (Chaveamento por Deslocamento Mínimo Gaussiano).
GSM	– <i>Global System for Mobile</i> (Sistema Global para Comunicações Móveis)
HLR	– <i>Home Location Register</i> (Registro de Localização de Unidade Móvel Local)
IS-95	– <i>Interim Standard-95</i> (Padrão Interino-95)
J	– <i>Jamming Power</i> (Potência do Bloqueador)
M-ASK	– <i>Multiple Amplitude Shift-Keying</i> (Chaveamento de Amplitude Múltiplo)
MATLAB	– <i>MATrix LABoratory</i> (MATLAB)
M-FSK	– <i>Multiple Frequency Shift-Keying</i> (Chaveamento de Frequência Múltiplo)
MIL	– <i>Millitary</i> (Militar)
M-PSK	– <i>Multiple Phase Shift Keying</i> (Chaveamento de Fase Múltiplo)
M-QAM	– <i>Multiple Quadrature Amplitude Modulation</i> (Modulação de Amplitude em Quadratura Múltipla)
MS	– <i>Mobile Station</i> (Estação Móvel)
MSC	– <i>Mobile Service Center</i> (Centro de Serviço Móvel)
MSK	– <i>Minimum Shift-Keying</i> (Chaveamento Mínimo)
NBN	– <i>Narrow Band Noise</i> (Ruído Banda Estreita)
NCW	– <i>Network Centric Warfare</i>

NMS	– <i>Network Manger Center</i> (Centro de Gerenciamento de Rede)
NMT	– <i>Nordic Mobile Telecommunications</i> (Telecomunicações Móveis Nórdicas)
OMC	– <i>Opearational and Maintenance Center</i> (Centro de Operações e Manutenção)
PBN	– <i>Partial Band Noise</i> (Ruído em Parte da Larga)
PCH	– <i>Paging Channel</i> (Canal de Paginação)
PCS	– <i>Personal Communication System</i> (Sistema de Comunicação Pessoal)
PDC	– <i>Personal Digital Communications</i> (Comunicação Digital Pessoal)
PLMN	– <i>Public Land Mobile Network</i> (Redes Públicas Fixas de Telefonia Móvel)
PM	– <i>Phase Modulation</i> (Modulação em Fase)
PN	– <i>Pseudo-Noise</i> (Pseudo-Ruído)
PSK	– <i>Phase Shift Keying</i> (Modulação por Chaveamento de Fase)
QAM	– <i>Quadrature Amplitude Modulation</i> (Modulação de Amplitude em Quadratura)
Q-PSK	– <i>Quadrature Phase Shift Keying</i> (Chaveamento de Fase em Quadratura)
RACH	– <i>Random Access Channel</i> (Canal de Acesso Randômico)
RF	– <i>Radio Frequency</i> (Rádio Frequência)
S	– <i>Signal Power Transmitter</i> (Potência do Sinal Transmitido)
SCH	– <i>Synchronization Channel</i> (Canal de Sincronização)
SMG	– <i>Special Mobile Group</i> (Grupo Móvel Especial)
SMS	– <i>Short Message Service</i> (Serviço de Mensagens Curtas)
SNR	– <i>Signal to Noise Ratio</i> (Relação Sinal ruído)
STD	– <i>Standards</i> (Padrão)
TACS	– <i>Total Access Communication System</i> (Sistema de Comunicação de Acesso)

Total)

- TCH – *Traffic Channel* (Canal de Tráfego)
- TCP/IP – *Transmission Control Protocol/Internet Protocol* (Protocolo de Controle de Transmissão/Protocolo de Internet)
- TDMA – *Time Division Multiple Access* (Acesso Múltiplo por Divisão de Tempo)
- THSS – *Time Hopping Spread Spectrum* (Espalhamento Espectral por Salto no Tempo)
- UMTS – *Universal Mobile Telecommunication System* (Sistema de Telecomunicações Móveis Universal)
- VCO – *Voltage Controlled Oscillator* (Oscilador Controlado à Tensão)
- VLR – *Visitor Location Register* (Registro de Localização de Visitante)

RESUMO

Este trabalho aborda técnicas de interferências em sistemas de comunicações via rádio com a finalidade de identificar as melhores técnicas ou condições de bloqueio para cada sistema, comercial ou militar.

A revisão bibliográfica realizada para dar suporte a esta dissertação inclui aspectos diversos de sistemas de comunicações, em particular: tipos de modulações, técnicas de espalhamento espectral e técnicas de acesso múltiplo. Fundamentos sobre bloqueio de RF também foram identificados e destacados no trabalho.

É apresentado um estudo de caso para a condição de bloqueio sobre os sistemas de telefonia móvel comercial CDMA e GSM e para os sistemas militares baseados na norma MIL-STD-188-110B.

Complementarmente à teoria, foram realizadas simulações dos bloqueadores e dos sistemas de comunicações com o auxílio do programa de computador MATLAB®. A eficácia dos bloqueadores sobre os sistemas de telefonia móvel comercial CDMA e GSM e sobre os sistemas militares baseados na norma MIL-STD-188-110B foi avaliada para os bloqueadores e sistemas de comunicações implementados, permitindo a definição da melhor relação bloqueio/sinal para efetivo bloqueio dos sistemas considerados.

Paralelamente, um dispositivo bloqueador com varredura para a faixa de 1805 a 1880 MHz, projetado e implementado no escopo deste trabalho, permitiu a validação das observações teóricas através de avaliações práticas da eficácia do bloqueio, cujos resultados são reportados ao longo do trabalho.

ABSTRACT

This work addresses the subject of interference techniques for wireless communications systems, aiming at the identification of the most effective jamming technique for each system, either commercial or military.

The bibliographic review of this work includes a variety of subjects on communications systems, such as modulation, spreading spectrum and multiple accesses techniques. Further concepts about RF jamming are also identified and detailed in this work.

A case study is presented for RF jamming on CDMA (IS-95) and GSM commercial mobile systems, and on military systems based on MIL-STD-188-110B standard.

Complementarily to the theory, jammers and communications systems were implemented and simulated with the aid of MATLAB®. The effectiveness of jammers on the commercial mobile telephony systems CDMA and GSM, and on the military systems based on MIL-STD-188-110B standard was evaluated with the implemented systems, in order to identify the proper jammer to signal ratio at which jamming is actually effective.

Furthermore, a swept jamming device for the frequency band from 1805 to 1880 MHz was designed and implemented within the scope of this work, which allowed the validation of the theoretical investigations through practical evaluations of the jammer effectiveness.

1 INTRODUÇÃO

1.1 OBJETIVO

O presente trabalho tem como objetivo a análise da eficácia de bloqueadores de RF em sistemas de comunicações comerciais, particularmente o GSM (*Global System for Mobile Communications*) e o CDMA (*Code Division Multiple Access*), e em sistemas de comunicações militares na faixa de HF, como os rádios baseados na norma MIL-STD-188-110B de interesse do Exército Brasileiro. A formulação matemática do bloqueador com um determinado sistema de comunicação é abordada com a finalidade de identificar a melhor relação Sinal de Bloqueio/Sinal de Comunicações (*J/S*) para efetivo bloqueio de tal sistema. A comprovação prática de tais observações teóricas é realizada para o sistema GSM como parte complementar aos objetivos do trabalho.

1.2 CONTEXTUALIZAÇÃO

A comunicação é uma das grandes necessidades da sociedade humana desde os primórdios de sua existência. Há muitos anos, quando não existiam correios, telefones nem internet, as pessoas utilizavam pombos, sinais de fumaça e outros meios similares para enviar mensagens, com o objetivo de se comunicarem com comunidades distantes. Com o passar do tempo novas formas de comunicações surgiram, como telégrafos, rádios, telefones fixos, telefones móveis, entre outros.

Há aproximadamente 15 anos, o telefone móvel era um aparelho praticamente desconhecido, muito pesado, volumoso e caro. O sistema que mais se desenvolveu nos últimos anos foi o das redes de comunicações móveis. Nos dias atuais é possível observar nas ruas que quase toda população possui telefones móveis.

Hoje, a implementação de sistemas de comunicação à distância com oferta cada vez maior de serviços de transmissão de voz e dados dando ampla mobilidade aos seus usuários tornou-se tanto uma realidade quanto um grande desafio. Com o avanço tecnológico nas telecomunicações, são inúmeros os diferentes sistemas existentes. E a cada dia aparece uma novidade nesta área.

Os sistemas móveis celulares sofreram fortes mudanças estruturais ao longo do seu desenvolvimento. A primeira geração (1G – *1ST Generation*) surgiu no início da década de 1980 e foi baseada na tecnologia analógica (HARTE, 2006; STEELE, 1992). O serviço analógico implantado no Brasil foi denominado AMPS (*Advanced Mobile Phone System*). Nos países escandinavos, o serviço analógico implantado foi o NMT (*Nordic Mobile*

Telephone). No Reino Unido e em alguns países da Ásia este serviço foi denominado TACS (*Total Access Communication System*).

A segunda geração (2G – 2ND *Generation*) dos sistemas de comunicações móveis celulares emergiu a partir de 1990 e foi baseada na tecnologia digital (HARTE, 2006; STEELE, 1999). As principais tecnologias digitais são o TDMA (*Time Division Multiple Access*) e o CDMA, desenvolvidas na América do Norte, o GSM, inicialmente desenvolvido na Europa, e o PDC (*Personal Digital Communications*), desenvolvido no Japão. Nesta fase, além dos serviços de voz, houve a oferta de serviços de dados, como identificação de chamadas, fax e os serviços de mensagens curtas (SMS – *Short Message Service*).

O crescimento explosivo da internet também trouxe um grande impacto na demanda por novos serviços de comunicações sem fio. Entretanto, a taxa efetiva de dados dos sistemas 2G era relativamente baixa para o tráfego na internet. Como resultado, foram desenvolvidas novas tecnologias em uma fase posterior à 2G, conhecida como 2G+ ou 2,5G, para aumentar a velocidade de comunicações de dados.

A terceira geração (3G – 3RD *Generation*) dos sistemas de comunicações móveis celulares se consolidou em dois sistemas para transmissão de dados por pacote, o UMTS (*Universal Mobile Telecommunication System*) e o CDMA2000, já implantados em vários países do mundo (STEELE, 1999). O objetivo dos sistemas 3G é o provimento de taxas de dados mais altas em comparação com os sistemas 2G e 2,5G, e a possibilidade de oferecimento de serviços adicionais, como por exemplo, acesso rápido à internet, jogos on-line, vídeo, além dos serviços de voz e dados já oferecidos.

Pesquisas para o desenvolvimento dos sistemas de comunicações móveis celulares de quarta geração (4G – 4TH *Generation*) já foram iniciadas, com previsão de disponibilidade comercial para o ano de 2010 (HARTE, 2006).

Na área militar, Os sistemas de comunicações têm por finalidade promover as ligações necessárias entre os diversos escalões de uma Força Armada para conduzir as ordens aos elementos subordinados, assim como para receber as informações dos diversos ambientes que são utilizados durante as operações, para a tomada de decisões. O funcionamento correto das comunicações neste caso é essencial para o sucesso de uma operação militar.

Historicamente, as primeiras comunicações militares foram realizadas através do envio e recebimento de sinais, que podiam ser visuais ou sonoros, podendo ser codificados para evitar o reconhecimento pelo inimigo. Com o passar dos anos, as comunicações evoluíram em função da necessidade do envio e recebimento de ordens com rapidez, eficácia e eficiência.

A necessidade de evolução das comunicações militares ajudou a desenvolver diversos sistemas de comunicações difundidos atualmente para a população mundial. Um exemplo foi a criação, em 1969, da ARPANET (*Advanced Research Projects Agency Network*), que surgiu da necessidade do Departamento de Defesa dos Estados Unidos de conectar as bases militares e os departamentos de pesquisa do governo americano através de uma rede de comunicação que não os deixasse vulneráveis, caso houvesse algum tipo de ataque. Essa rede foi precursora da Internet.

As técnicas de espalhamento de espectro, desenvolvidas no âmbito militar para impedir a interceptação de mensagens pelo inimigo, foram precursoras das modernas técnicas de acesso em sistemas wireless atuais, como o próprio CDMA e o GSM.

A crescente importância das comunicações nos conflitos da era da informação modificou os conceitos das operações militares. Esta transformação, no âmbito das Forças Armadas, desloca-se atualmente da guerra clássica em plataformas para a guerra centrada em redes (NCW - *Network Centric Warfare*) (JR, 2004).

As comunicações militares utilizam diversos tipos de meios de transmissão de acordo com a característica da missão, o tipo de comunicação (que pode ser estratégica ou tática), o conteúdo a ser transmitido, a largura de banda desejada, o tipo de tráfego, o custo e o ambiente.

Apesar do grande avanço científico no desenvolvimento tecnológico de redes sem fio mais eficientes, tais como IEEE 802.11 (IEEE 802.11) e IEEE 802.16 (IEEE 802.16), que propiciam maior largura de banda e menor taxa de erros, existem cenários nos quais tais sistemas não podem ser empregados. Isso ocorre, por exemplo, em regiões como a amazônica (BARROSO, 2006), devido às suas características fisiográficas, como dimensão, vegetação e regime de chuvas, ou em regiões desérticas, pela falta de infra-estrutura de telecomunicações ou energia elétrica. Ainda podem surgir situações semelhantes na ocorrência de desastres ou calamidades, quando a estrutura de telecomunicações pode ficar parcialmente ou totalmente destruída, o que também pode ocorrer com o uso da força em conflitos militares.

Para esses cenários, as opções de meios de comunicação são restritas, ficando baseadas principalmente no uso de redes de satélites ou redes HF (*High Frequency*). Estes meios tornam-se eficazes porque podem cobrir grandes distâncias e ultrapassar obstáculos naturais. De forma geral, os equipamentos são portáteis, podendo funcionar com baterias ou geradores, além de permitirem integração com redes baseadas na arquitetura de protocolos TCP/IP

(*Transmission Control Protocol/Internet Protocol*) (JODALEN, 2004; JODALEN, 2005; DANTAS, 2006).

Apesar de uma rede de satélites permitir um tráfego maior de dados em relação aos enlaces de HF, o custo de sua operação é muito alto e são poucos os países que detêm o controle e o conhecimento necessários para e operar satélites de comunicações. Estrategicamente, o uso de enlaces controlados por empresas de outros países pode representar um risco para a segurança da informação. Dessa forma, o meio de comunicação militar mais viável em muitos casos torna-se a rede HF, que têm um custo baixo, pode ser rapidamente colocada em operação, não necessita de linha de visada e possui longo alcance. Um emprego real de redes HF ocorreu durante as operações de salvamento após o ataque de 11 de setembro de 2001 em Nova Iorque, onde a infra-estrutura de telecomunicações entrou em colapso (JODALEN, 2004). Para garantir o resgate das vítimas, a Guarda Nacional Americana utilizou redes HF para coordenar as operações.

O enlace de HF é o meio de comunicação empregado atualmente por diversos exércitos em operações táticas. Atualmente, existem pesquisas para a construção de rádios definidos por *software* (RDS) que permitem maior qualidade nas transmissões nesta faixa, para que os sistemas de comando e controle sejam operados de forma mais eficiente (DILLINGER, 2003).

O termo Rádio Definido por Software é usualmente utilizado para um rádio transceptor cujos parâmetros fundamentais podem ser definidos por software e os aspectos fundamentais da operação do rádio podem ser reconfiguráveis pela atualização do software do dispositivo.

A tecnologia RDS também tem origem nas pesquisas militares. O objetivo das pesquisas era criar um rádio em que se pudesse mudar parâmetros como o tipo de modulação, largura de banda do canal, taxa de dados e tipo de código de voz. Um rádio adaptável desse tipo poderia ser utilizado para anular as tentativas de espionagem do inimigo ou ser configurado para combinar exigências operacionais específicas. Tal sistema tem claramente enormes benefícios no teatro da guerra.

No mundo competitivo da comunicação móvel civil, o RDS pode ser utilizado para permitir que um operador ou um fornecedor de serviços ofereça benefícios ou serviços mais competitivos. Atualmente o estudo do RDS já foi ampliado para a área comercial, principalmente como um caminho para a convergência dos diversos sistemas de comunicação existentes.

Alguns modelos de rádios utilizados pelo Exército Brasileiro são o M3TR da *Rohde & Schwarz* e o HF-6000 da *Tadiran*. Os rádios citados utilizam alguns princípios de rádio definido por software e se baseiam na norma MIL-STD-188-110B para a fabricação de seus modems.

Nas situações em que os recursos de comunicações são mal utilizados, como, por exemplo, em presídios, em locais de realização de concursos, entre outros, torna-se necessário justamente inviabilizar o estabelecimento dos enlaces de comunicação. Para esta finalidade, pode-se utilizar um dispositivo denominado bloqueador de RF. Dispositivos nesta categoria também foram inicialmente desenvolvidos para aplicações militares em Guerra Eletrônica. Mais modernamente, são utilizados em situações onde é necessária a efetivação da Garantia da Lei e da Ordem (GLO) (BRASIL, 1999). Para os sistemas militares, os bloqueadores de RF são fabricados para controle das comunicações táticas, impossibilitando a interceptação das mensagens. Os bloqueadores devem possuir, de forma geral, característica multibanda e capacidade de reconfigurabilidade em frequência e potência, de forma a aumentar sua eficácia sobre os sistemas receptores modernos.

Devido às situações onde é necessário inviabilizar o estabelecimento do enlace de comunicação para o meio civil, surgiu uma nova área de pesquisa, relacionada ao desenvolvimento de bloqueadores para sistemas comerciais. Tais dispositivos genericamente têm como função inserir um sinal interferente no espectro eletromagnético para degradar a qualidade do sinal recebido pelo sistema, de forma a inviabilizar a transmissão da informação.

1.3 JUSTIFICATIVAS

O desenvolvimento das funcionalidades de dispositivos bloqueadores é de interesse do Exército Brasileiro, contido em seu Plano Básico de Ciência e Tecnologia – PBCT. Alguns estudos relacionados a dispositivos bloqueadores antecedentes ao presente trabalho foram desenvolvidos no Instituto Militar de Engenharia em nível de Graduação (FILHO ET AL., 2003; AGUIAR E BISPO, 2004) e em nível de Pós-Graduação (TOSCANO, 2006; RENATO, 2005).

Estes dispositivos também são de interesse da Marinha do Brasil, para sistemas de Contra Medidas Eletrônicas, sendo também utilizados na Garantia da Lei e da Ordem em território nacional.

1.4 COMPOSIÇÃO DO TRABALHO

O Capítulo 2 apresenta algumas considerações sobre sistemas civis e militares. É feita uma abordagem inicial de tipos de modulações analógicas e digitais, e técnicas de espalhamento espectral. Os sistemas de comunicações comerciais CDMA e GSM e o sistema de comunicação militar baseado na norma MIL-STD-188-110B são apresentados em maior detalhe.

O Capítulo 3 apresenta os tipos de ataques eletrônicos utilizados em sistemas de guerra eletrônica. São citados os tipos de bloqueio e algumas considerações sobre os sistemas que operam com a condição de espalhamento espectral (consequentemente, com ganho de processamento). É apresentado também um desenvolvimento teórico a respeito da relação entre as potências dos sinais de bloqueio e do sistema de comunicações em um receptor. Para efetivação do bloqueio, são apresentadas algumas condições importantes para a inserção do sinal interferente.

O Capítulo 4 apresenta o desenvolvimento de uma simulação computacional com uso do programa MatLab 7.0 (Simulink), envolvendo réplicas dos bloqueadores apresentados e dos canais de tráfego dos sistemas de comunicações comerciais, particularmente o CDMA e o GSM, e do sistema de comunicação militar baseado na norma MIL-STD-188-110B.

O Capítulo 5 apresenta a efetividade dos bloqueadores nos sistemas de comunicações comerciais (CDMA e GSM) e no sistema de comunicação militar referido, determinando a mínima relação J/S para efetivação do bloqueio em cada caso.

O Capítulo 6 apresenta o projeto e a implementação de um dispositivo bloqueador para a faixa de 1805 a 1880 MHz. Ainda neste capítulo, são descritos os testes de geração de interferência sobre o sistema de telefonia móvel GSM com o dispositivo bloqueador implementado e a análise dos resultados práticos.

Finalizando, o Capítulo 7 apresenta a conclusão do trabalho, destacando as principais contribuições e algumas sugestões para trabalhos futuros.

Detalhamentos do funcionamento do sistema GSM e dos sistemas baseados na norma MIL-STD-188-110B são apresentados no Apêndice 1 e no Apêndice 2, respectivamente.

2 CONSIDERAÇÕES SOBRE OS SISTEMAS DE COMUNICAÇÕES CIVIS E MILITARES

Um sistema de comunicação é composto basicamente por uma fonte de informação, um transmissor, um canal de comunicação, um receptor e o destino da informação. O principal desafio no projeto de sistemas de comunicação é fazer com que na recepção a mensagem originalmente enviada seja reproduzida com a maior fidelidade possível. O projeto de sistemas analógicos de telecomunicações visa normalmente à maximização da relação sinal-ruído (*SNR – Signal to Noise Ratio*), enquanto que em sistemas digitais busca-se a minimização da taxa de erro de bit (*BER – Bit Error Rate*).

Este capítulo apresenta os fundamentos envolvidos em sistemas de comunicação via rádio, tais como: técnicas de modulações analógicas e digitais, técnicas de espalhamento espectral, sistemas de comunicações comerciais, CDMA e GSM, e sistemas de comunicações militares baseado na norma MIL STD-188-110B.

2.1 MODULAÇÕES

O processo de modulação pode ser visualizado como a transformação de um sinal que contém informações úteis em seu formato original, banda-base, num sinal (passa-banda) adequado ao meio de transmissão que se pretende utilizar. Isto é feito por meio de uma portadora – um sinal senoidal cuja frequência é bem maior que a maior frequência contida no sinal original.

Através da modulação, o sinal de banda-base é transladado no espectro de frequências. Com isso, alguns benefícios podem ser obtidos, como o compartilhamento do espectro com outros sinais do mesmo tipo, em alguns casos, e a redução do tamanho dos dispositivos transmissores e receptores.

É possível identificar dois grupos básicos de modulação, de acordo com o tratamento da portadora pelo sinal modulante: analógico e digital. A FIG. 2.1 apresenta genericamente os esquemas de modulações analógicas e digitais.

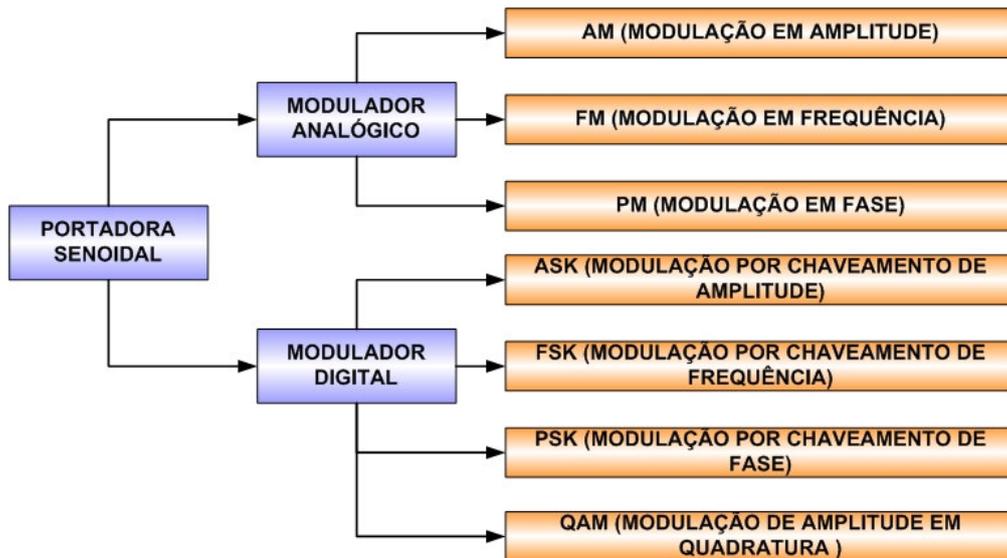


FIG. 2.1 - Esquemas de modulações analógicas e digitais.

Não há neste item a intenção de se exaurir todos os tipos de modulação existentes na atualidade. Contudo, as principais técnicas de modulação são apresentadas de forma a fornecer subsídios mínimos para melhor compreensão dos demais assuntos de interesse deste trabalho.

2.1.1 MODULAÇÕES ANALÓGICAS

Nas modulações analógicas a portadora é uma onda senoidal e o sinal modulante é um sinal analógico. As técnicas de modulação mais comuns para sinais analógicos são: Modulação em Amplitude (*AM – Amplitude Modulation*), Modulação em Frequência (*FM – Frequency Modulation*) e Modulação em Fase (*PM – Phase Modulation*).

2.1.1.1 MODULAÇÃO EM AMPLITUDE - AM

A modulação AM é usada como um laboratório inicial de estudo no presente trabalho, sendo descrita em maior detalhe a seguir. Nesta técnica, é possível definir toda a formulação matemática envolvida e, através dela, se familiarizar com todas as ferramentas de trabalho aplicadas na dissertação, em particular, com a ferramenta computacional MatLab 7.0 (*MATrix LABoratory*).

A modulação em amplitude está relacionada à alteração da amplitude de um sinal de alta frequência, a portadora, em função do comportamento de um sinal de baixa frequência, o sinal modulante. Dentre os sistemas de modulação em amplitude, destacam-se os seguintes:

- AMDSB - Modulação em amplitude com dupla banda lateral
 - Exemplo de aplicação: Rádio de áudio (rádio AM);
- AMDSB-SC - Modulação em amplitude com dupla banda lateral e portadora suprimida
 - Exemplo de aplicação: Misturador de frequência;
- AMSSB-USB - Modulação em amplitude banda lateral única superior
 - Exemplo de aplicação: Rádio amadorismo;
- AMSSB-LSB - Modulação em amplitude banda lateral única inferior
 - Exemplo de aplicação: Rádio amadorismo;

O digrama da FIG. 2.2 ilustra o modelo de modulação AMDSB, referenciado neste trabalho como AM por simplicidade¹. Tal modulador tem como entradas o sinal modulante $d(t)$ e a portadora $c(t)$, gerando o sinal AM $s(t)$.

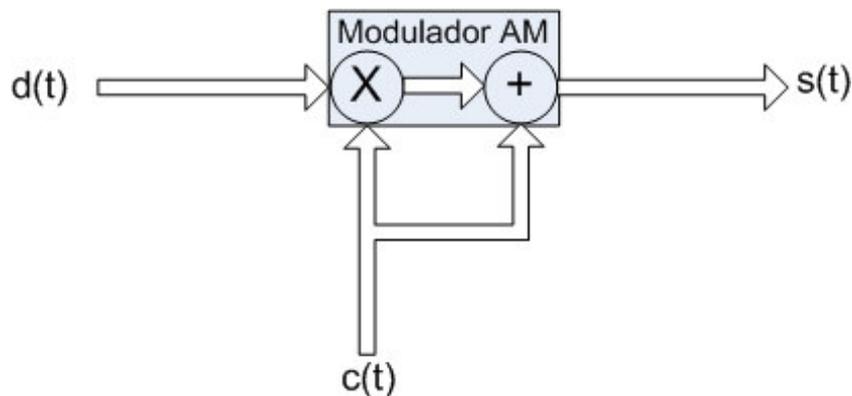


FIG. 2.2 - Modulador AMDSB.

A expressão particular do sinal modulado AMDSB pode ser escrita da seguinte forma (HAYKIN, 2001):

$$s(t) = E_p [1 + m \cos(2\pi f_m t)] \cos(2\pi f_p t) \quad (2.1)$$

onde E_p é a amplitude da portadora, f_p é a frequência da portadora, f_m é a frequência do sinal modulante e $m = E_m/E_p$ é o índice de modulação, sendo E_m a amplitude do sinal modulante.

Expandindo a EQ. 2.1, substituindo-se o produto de dois cossenos pela soma de duas ondas senoidais, uma em $f_p + f_m$ e outra em $f_p - f_m$, tem-se:

¹ Quando necessário, a referência explícita a este e a outro tipo de sinal AM será utilizada.

$$s(t) = E_p \cos(2\pi f_p t) + \frac{mE_p}{2} \cos(2\pi f_p t + 2\pi f_m t) + \frac{mE_p}{2} \cos(2\pi f_p t - 2\pi f_m t) \quad (2.2)$$

Assim, o espectro de amplitude de um sinal AMDSB, $\mathfrak{S}\{s(t)\} = S(f) [\text{V}]^2$, tem uma componente de portadora e duas bandas laterais, uma superior em $f_p + f_m$ e outra inferior em $f_p - f_m$, como mostra a FIG. 2.3.

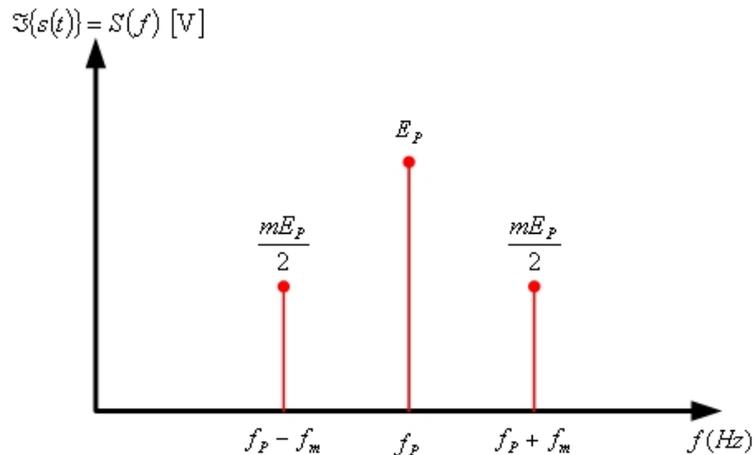


FIG. 2.3 - Espectro de amplitude do sinal modulado em AMDSB.

A potência média do sinal é representada pela seguinte equação (PROAKIS, 2002):

$$P_{AMDSB} = \frac{E_p^2}{2} + \frac{m^2 E_p^2}{8} + \frac{m^2 E_p^2}{8} \quad (2.3)$$

O espectro de potência do sinal AMDSB é representado na FIG. 2.4:

² $\mathfrak{S}\{x(t)\} = X(f)$ é a Transformada de Fourier da função $x(t)$.

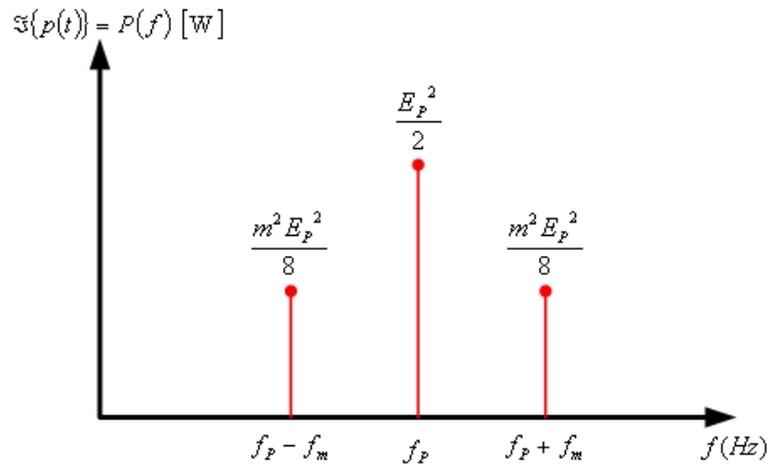


FIG. 2.4 - Espectro de potência do sinal modulado em AMDSB.

2.1.1.2 MODULAÇÃO EM FREQUÊNCIA – FM

Os principais fatores de degradação da qualidade de transmissão em sistemas de comunicações atuam sobre a amplitude do sinal, tais como o ruído térmico e a distorção não-linear. Como a modulação em amplitude está diretamente relacionada à amplitude do sinal, estes fatores atuam diretamente na qualidade do sinal demodulado.

Para contornar os problemas causados pela degradação da amplitude do sinal modulado, usa-se a modulação em frequência, que consiste na alteração (modulação) da frequência de uma portadora de alta frequência por um sinal de baixa frequência. A expressão básica de um sinal FM é dada por (HAYKIN, 2001):

$$s(t) = E_p \cos \left[2\pi f_p t + 2\pi K_f \int_0^t d(t) dt \right] \quad (2.4)$$

onde K_f é a constante de desvio em frequência.

2.1.1.3 MODULAÇÃO EM FASE – PM

A modulação em fase é um tipo de modulação analógica que se baseia na alteração da fase da portadora de acordo com o sinal modulante. A expressão básica de um sinal PM é dada por (HAYKIN, 2001):

$$s(t) = E_p \cos[2\pi f_p t + K_p d(t)] \quad (2.5)$$

onde K_p é a constante de desvio em fase.

2.1.2 MODULAÇÕES DIGITAIS

A modulação digital é utilizada em casos onde há interesse em transmitir uma forma de onda ou mensagem digital. Tais formas de onda se caracterizam por assumirem um conjunto finito de valores discretos. No caso da comunicação binária, as mensagens a serem transmitidas, ou seja, o sinal modulante possui apenas dois valores possíveis de amplitude, um representando o valor binário '1' e o outro o valor binário '0'. A diferença fundamental entre os sistemas de comunicações digitais e analógicos advém do fato que nos primeiros há um número finito de formas de onda conhecidas pelo receptor, o que facilita o processo de recuperação da informação transmitida, enquanto que nos sistemas analógicos há um número infinito ou infinitamente grande de formas de onda, o que dificulta sobremaneira a recuperação da mensagem transmitida.

Nas modulações digitais, bits sucessivos do sinal de informação são representados por símbolos. A modulação é responsável por mapear cada possível sequência de bits de um comprimento preestabelecido em um símbolo determinado. O conjunto de símbolos gerado por uma modulação é chamado de constelação, sendo que cada tipo de modulação gera uma constelação de símbolos diferente. Os símbolos nos quais as sequências de bits de um sinal de informação são transformadas são efetivamente transmitidos pela onda portadora.

Durante a transmissão, as formas de onda são distorcidas pela ação do canal de comunicação. Pelo menos uma distorção está sempre presente nos sistemas de comunicações: ruído térmico aditivo. Assim sendo, após a retirada da portadora na demodulação, os símbolos ficam corrompidos pela ação do ruído. A partir dessa versão corrompida, cabe ao detector decidir qual dos possíveis símbolos foi transmitido. Uma vez tomada a decisão, sendo esta correta, a forma de onda original é recuperada, e a sequência binária que a gerou é restabelecida.

Do mesmo modo que há diversas técnicas de modulação para sinais analógicos, as informações digitais também podem ser colocadas sobre uma portadora em diferentes modos. As técnicas de modulação digitais mais utilizadas são: modulação por chaveamento de amplitude (*ASK - Amplitude Shift-Keying*), modulação por chaveamento de frequência (*FSK -*

Frequency Shift-Keying), modulação por chaveamento de fase (*PSK - Phase Shift-Keying*) e modulação de amplitude em quadratura (*QAM - Quadrature Amplitude Modulation*). A FIG. 2.5 ilustra as principais técnicas de modulações digitais e as suas principais variantes (HAYKIN, 2001).

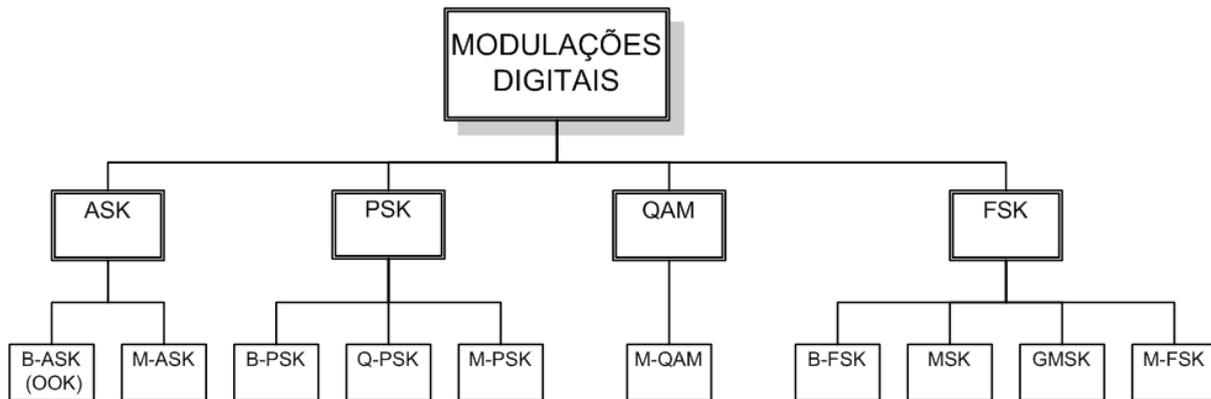


FIG. 2.5 - Modulações Digitais.

2.1.2.1 MODULAÇÃO POR CHAVEAMENTO DE AMPLITUDE – ASK

ASK é a técnica de modulação mais simples dentre as utilizadas para modular sinais digitais. Consiste na alteração da amplitude da onda portadora em função do sinal digital a ser transmitido.

A modulação por chaveamento de amplitude é indicada nas situações em que existe pouco ruído para interferir na recepção do sinal ou quando o baixo custo é essencial. A modulação ASK é utilizada em aplicações como transmissão via fibra óptica, transmissão de dados por infravermelho, controle remoto por meio de raios infravermelhos, entre outras.

As principais variantes do sinal ASK são: B-ASK (B-ASK – *Binary Amplitude Shift-Keying*) se o sinal for binário (0 ou 1), e M-ASK (M-ASK – *Multiple Amplitude Shift-Keying*), se o sinal tiver m níveis de amplitudes.

O sinal B-ASK é a forma mais simples de modulação digital, também conhecida como modulação *on-off* (OOK – *ON-OFF Keying*), e consiste em representar os símbolos zeros e uns de um sinal digital pela ausência ou pela presença do sinal de portadora.

A FIG. 2.6 apresenta a técnica de modulação B-ASK, onde $y(t)$ é o sinal modulado e $m(t)$ é o sinal modulante. Nesse tipo de modulação, a fase e a frequência da portadora não se alteram.

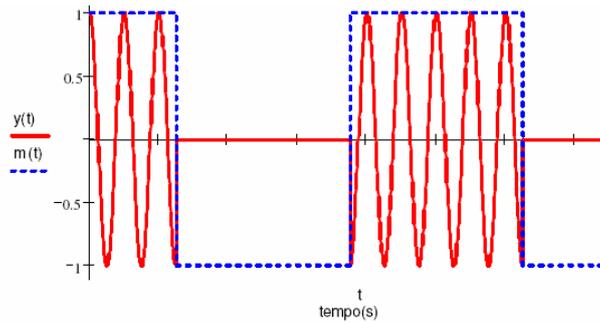


FIG. 2.6 - Representação de um sinal com modulação B-ASK.

O sinal M-ASK possui m amplitudes possíveis, o qual pode ser obtido em uma seleção de vários divisores de tensão, possibilitando que a saída tenha diversos níveis de amplitudes.

2.1.2.2 MODULAÇÃO POR CHAVEAMENTO DE FREQUÊNCIA – FSK

O processo de modulação FSK consiste em variar a frequência da onda portadora em função do sinal a ser transmitido. Este tipo de modulação pode ser considerado equivalente a modulação FM para sinais analógicos.

As principais variantes da modulação FSK são (HAYKIN, 2001): B-FSK (B-FSK – *Binary Frequency Shift-Keying*), MSK (MSK - *Minimum Shift-Keying*), GMSK (GMSK – *Gaussian Minimum Shift-Keying*) e M-FSK (M-FSK – *Multiple Frequency Shift-Keying*).

Em sua forma mais simples, B-FSK, os símbolos zeros e uns são associados a diferentes valores de frequência, ou seja, para transmitir o símbolo '1', a portadora assume a frequência f_1 , e, para transmitir o símbolo '0', a portadora assume a frequência f_2 . Um exemplo do FSK binário é ilustrado na FIG. 2.7, onde $f_1 > f_2$. Nesse tipo de modulação, a amplitude e a fase não se alteram.

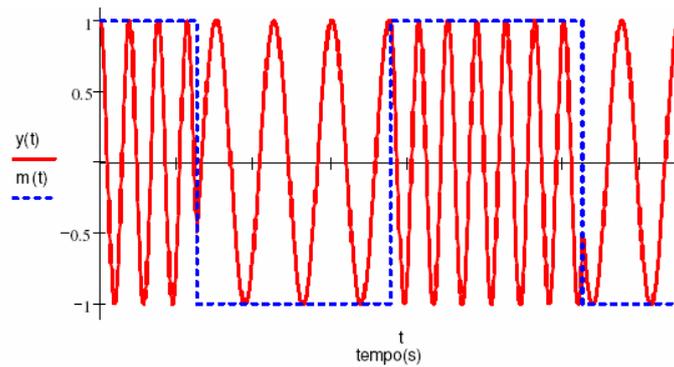


FIG. 2.7 - Modulação B-FSK.

O MSK é uma modulação FSK com a separação mínima entre as portadoras utilizadas de modo a garantir a ortogonalidade entre elas, com o objetivo de se obter uma detecção confiável do sinal recebido, pois sinais ortogonais são independentes, ou seja, facilmente diferenciáveis. Das técnicas de modulação digitais para comunicações móveis, o MSK apresenta a menor complexidade de implementação.

A modulação GMSK é uma modificação do MSK, na qual a sequência de bits de entrada do modulador é filtrada por um filtro passa-baixa com resposta a um pulso retangular gaussiano. A saída desse filtro é então responsável por modular em MSK as portadoras utilizadas.

O GMSK é um tipo especial de modulação de faixa estreita que transmite os dados na fase da portadora, resultando num sinal de envoltória constante. Isto permite o uso de amplificadores menos complexos, sem produzir distúrbios harmônicos, e reduz a complexidade dos sistemas, tornando seu custo mais baixo em relação às demais modulações existentes.

O GSM utiliza o formato de modulação digital 0,3GMSK. O “0,3G” descreve a banda do filtro gaussiano de pré-modulação utilizado para reduzir o espectro do sinal modulado e o “MSK” é a transição dos bits ‘1’ e ‘0’, que são representados por deslocamento de frequência da portadora de RF.

O M-FSK é composto de várias frequências diferentes utilizadas para codificar um determinado estado. A distribuição espectral uniforme das frequências que geram o sinal M-FSK propicia um melhor aproveitamento do espectro.

2.1.2.3 MODULAÇÃO POR CHAVEAMENTO DE FASE – PSK

PSK é uma forma de modulação em que a informação do sinal digital é embutida na fase da portadora. As principais variantes da modulação PSK são: B-PSK (B-PSK - *Binary Phase Shift Keying*), Q-PSK (Q-PSK – *Quadrature Phase Shift Keying*) e M-PSK (M-PSK – *Multiple Phase Shift Keying*).

Em sua forma mais simples, o B-PSK (*Binary Phase Shift Keying*), a fase da portadora assume apenas dois valores de acordo com os bits gerados pela fonte. Quando há uma transição de um bit '0' para um bit '1' ou de um bit '1' para um bit '0', a onda portadora sofre uma alteração de fase de 180°. Quando não há nenhuma destas transições, ou seja, quando bits subsequentes são iguais, a portadora continua a ser transmitida com a mesma fase.

A técnica BPSK é ilustrada na FIG. 2.8, onde se nota a inversão de 180° da fase da portadora a cada mudança de símbolo.

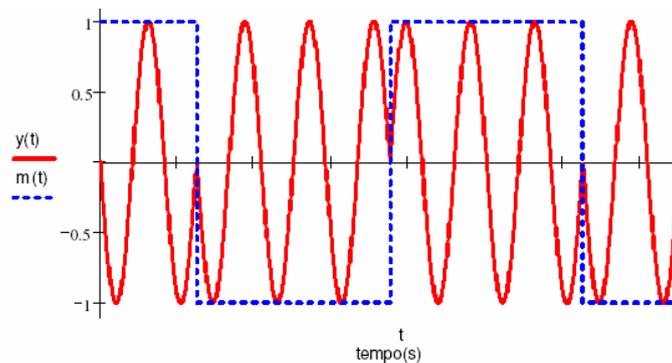


FIG. 2.8 - Exemplo de modulação B-PSK.

Um sistema de quatro fases, conhecido como QPSK, codifica dois bits para cada fase. O modulador QPSK pode ser implementado com o uso simultâneo de dois moduladores BPSK defasados de 180°. Isto duplica a quantidade de informação transmitida.

O sinal M-PSK possui uma codificação onde cada nível do sinal digital de entrada representa uma fase diferente da portadora.

2.1.2.4 MODULAÇÃO DE AMPLITUDE EM QUADRATURA – QAM

No sinal QAM, os símbolos são mapeados em um diagrama de fase e quadratura, sendo que cada símbolo apresenta uma distância específica da origem do diagrama que representa a sua amplitude, diferentemente da modulação PSK, na qual todos os símbolos estão a igual

distância da origem. Isto significa que as informações são inseridas nos parâmetros de amplitude e quadratura da onda portadora.

No caso do 16QAM, a constelação³ apresenta 16 símbolos, o que significa que cada símbolo representa 4 bits. Pode-se ter também, por exemplo, o modo 64QAM, cuja constelação apresenta 64 símbolos, cada um deles representando 6 bits. A FIG. 2.9a ilustra a constelação gerada pela modulação 16QAM e a FIG. 2.9b ilustra a constelação gerada pela modulação 64QAM.

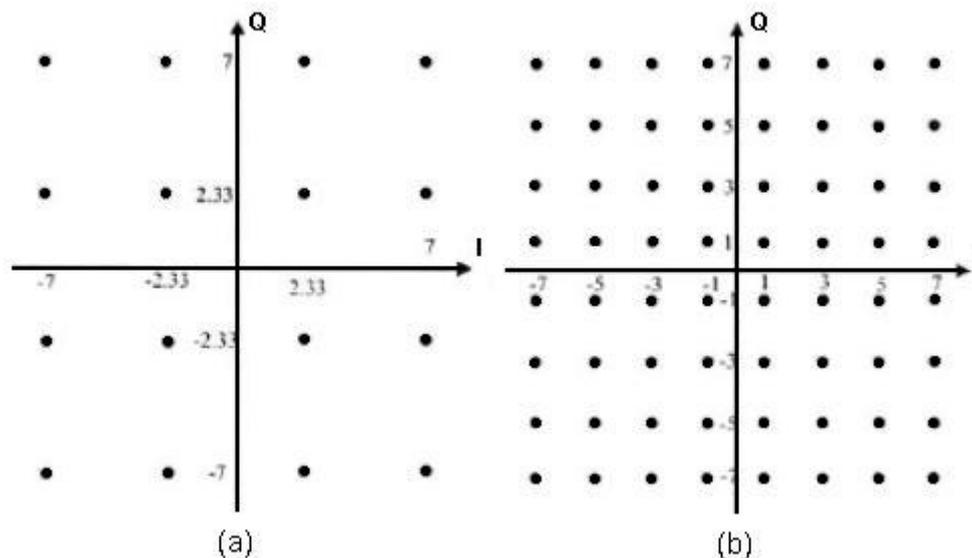


FIG. 2.9 - Constelação de um sinal com modulação QAM: (a) 16-QAM e (b) 64-QAM.

2.2 SISTEMAS COM ESPALHAMENTO ESPECTRAL

A tecnologia de Espalhamento Espectral é hoje um dos processos mais utilizados para interligação de sistemas sem fio com confiabilidade e sigilo. A principal razão disso é a sua capacidade de codificação, que faz com que seja muito difícil a interpretação ou interceptação dos sinais emitidos por unidades não autorizadas.

As técnicas de espalhamento espectral foram originalmente desenvolvidas pelos militares a partir da Segunda Guerra Mundial com o objetivo de transformar as informações a serem transmitidas num sinal parecido com um ruído, evitando assim monitoração pelas forças inimigas. São essencialmente técnicas anti-bloqueio (POISEL, 2004).

³ A constelação de símbolos é um diagrama com representação vetorial de cada símbolo transmitido pelo sistema. Nesse caso, cada símbolo associado ao seu deslocamento de fase e amplitude é representado no diagrama como sendo um ponto. A distância desse ponto ao centro dos eixos corresponde à amplitude do símbolo e sua posição angular em relação ao eixo das abscissas corresponde ao deslocamento de fase do símbolo.

No espalhamento espectral, o sinal de informação é codificado e modificado, “espalhando” a informação no espectro de frequências. A largura de banda de transmissão é muito maior que a banda mínima necessária para transmitir a informação.

Algumas vantagens podem ser destacadas com o uso das técnicas de espalhamento espectral (LEE, 1995):

- Dispõem de Ganho de Processamento que em geral é definido como a razão entre a largura de banda originada pelo processo de espalhamento e a largura de banda mínima requerida para o sinal a transmitir.
- Permitem a utilização simultânea da mesma banda de frequências por um número grande de usuários (acesso múltiplo).
- Protegem contra o desvanecimento provocado por multipercursos, que é um grande obstáculo nas comunicações urbanas.
- Dispõem de elevada tolerância a sinais interferentes, especialmente aos sinais de banda estreita, propriedade esta conhecida como anti-bloqueio. Tal propriedade é consequência do processo do espalhador e do correlator efetuados pelo transmissor e receptor, respectivamente.
- Possui baixa probabilidade de interceptação, que é consequência direta da baixa densidade espectral de potência resultante do processo de espalhamento, o que faz com que o sinal se confunda com o ruído.

Entre as desvantagens pode ser citada a complexidade envolvida no projeto de um equipamento com espalhamento espectral, que é superior a dos sistemas convencionais. Além disso, em sistemas não-celulares, a eficiência espectral é significativamente mais baixa.

As principais técnicas de espalhamento espectral são (LEE, 1995; POISEL, 2004): multiplicação por sequência direta (*DSSS - Direct Sequence Spread Spectrum*), salto em frequência (*FHSS - Frequency Hopping Spread Spectrum*) e salto no tempo (*THSS - Time Hopping Spread Spectrum*).

2.2.1 ESPALHAMENTO ESPECTRAL POR SEQUÊNCIA DIRETA - DSSS

Na técnica de espalhamento DSSS a informação do sinal é multiplicada diretamente por uma sequência pseudo-aleatória PN na transmissão. Para se obter o espalhamento do sinal desejado, a taxa do sinal PN deve ser bem maior que a taxa do sinal de informação. Um

exemplo básico de um sinal transmitido com espalhamento DSSS é ilustrado na FIG. 2.10, onde T é o tempo de duração de um bit e T_C é o tempo de duração de um *chip* (padrão de bits).

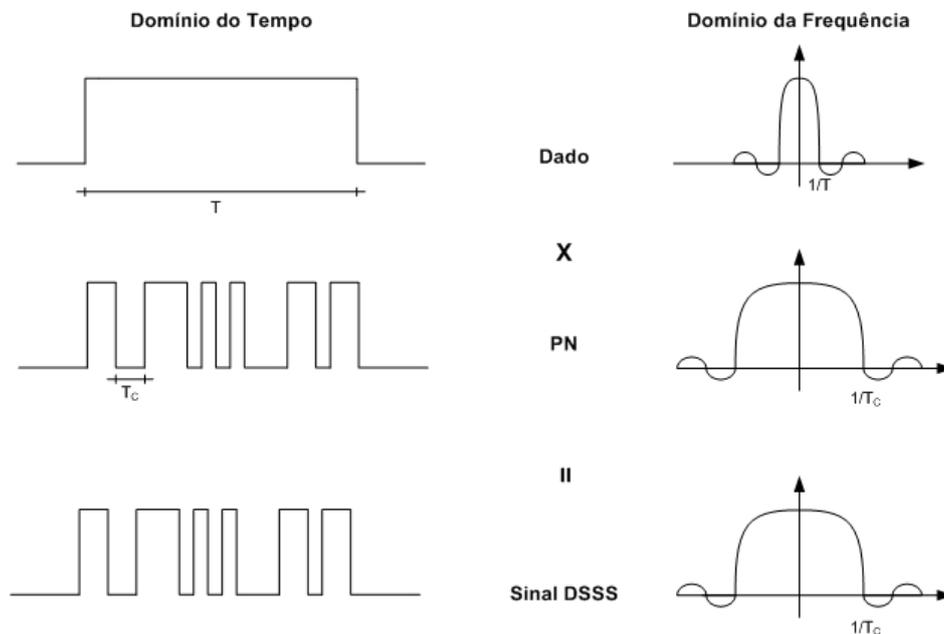


FIG. 2.10 – Exemplo básico de um Sinal DSSS.

Na recepção, o sinal é sincronizado e multiplicado pela sequência PN e posteriormente demodulado, recuperando a sequência binária de entrada. O padrão IS-95 é baseado na modulação DS-SS-SSB.

O diagrama em bloco da FIG. 2.11 ilustra a forma básica de transmissor e receptor que utilizam a técnica de espalhamento DS com modulação digital BPSK.

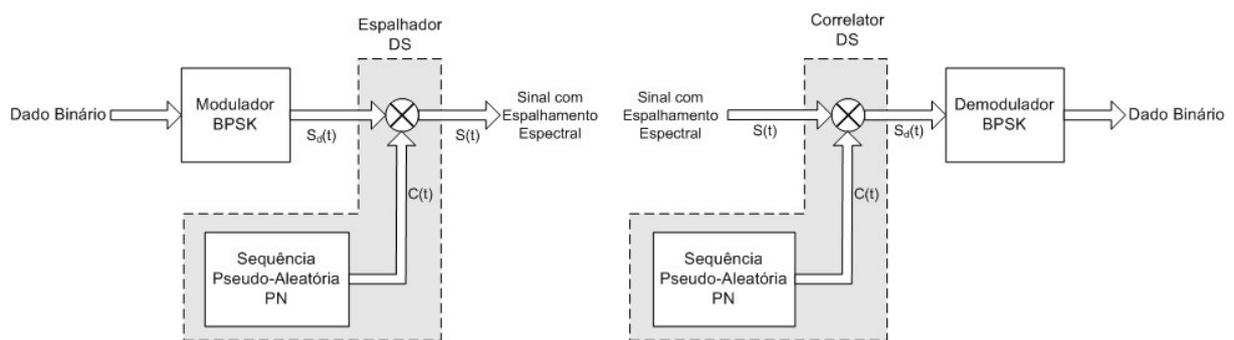


FIG. 2.11 - Transmissor e Receptor do sinal DSSS-BPSK.

A FIG. 2.12 ilustra o sinal com espalhamento espectral no tempo. A FIG. 2.12a mostra o sinal de dados, a FIG. 2.12b o sinal de dados com modulação BPSK, a FIG. 2.12c o código de espalhamento e a FIG. 2.12d o sinal de dados com espalhamento DSSS.

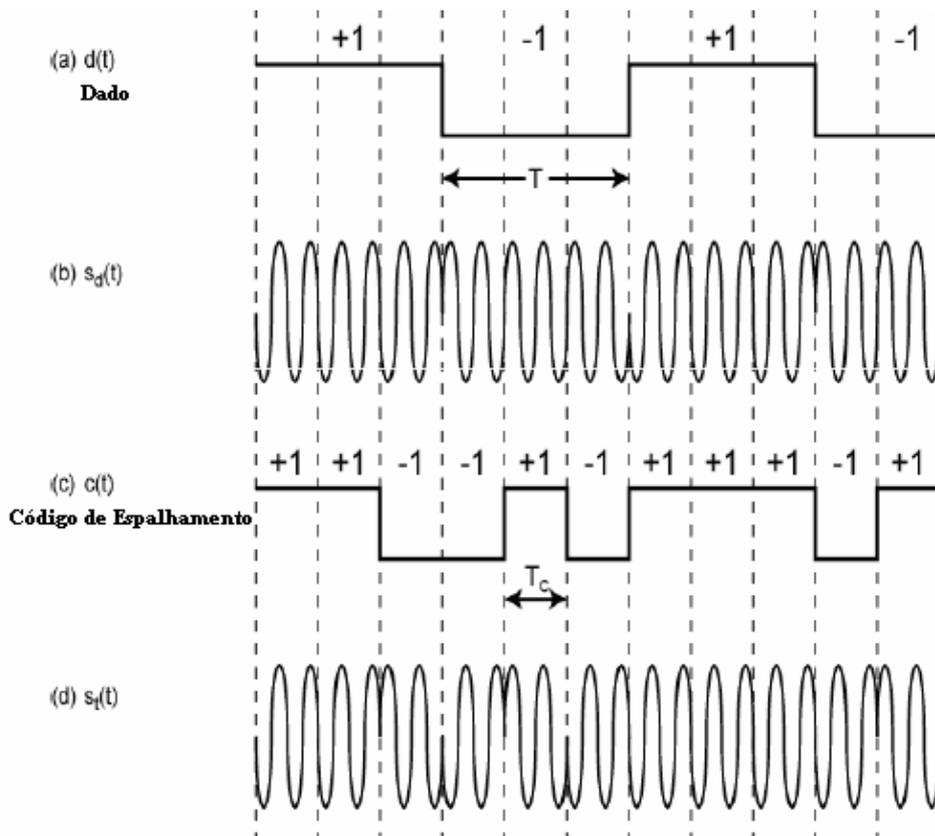


FIG. 2.12 - Sinal DSSS-BPSK no tempo.

2.2.2 ESPALHAMENTO ESPECTRAL POR SALTO EM FREQUÊNCIA – FHSS

A técnica de espalhamento por saltos em frequência FHSS é similar à técnica DSSS, só que neste caso o sinal de dados é modulado em frequência antes de ser misturado com o sintetizador de frequências. A frequência desse sintetizador é controlada pela saída de um gerador de seqüências pseudo-aleatórias, como ilustrado na FIG. 2.13.

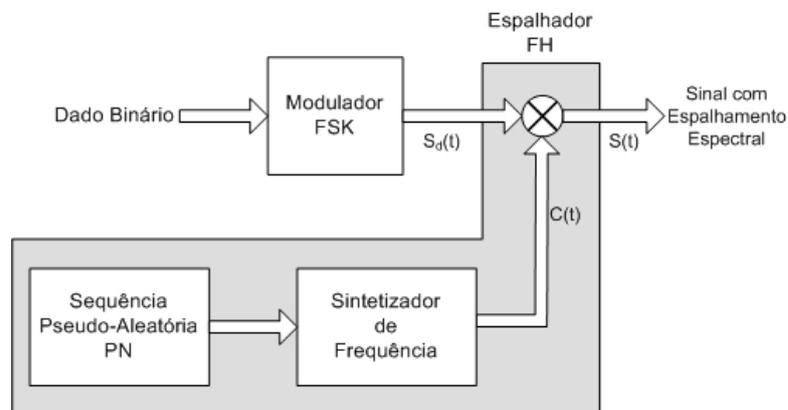


FIG. 2.13 – Transmissor de um sinal FHSS.

Existem duas variantes para a técnica de FHSS:

- Salto em Frequência Rápido (FFH) – quando um bit é dividido por vários saltos, ou seja, a taxa de ocorrência de saltos é maior que a taxa de símbolos. A FIG. 2.14 ilustra esta situação, que caracteriza o FHSS rápido.

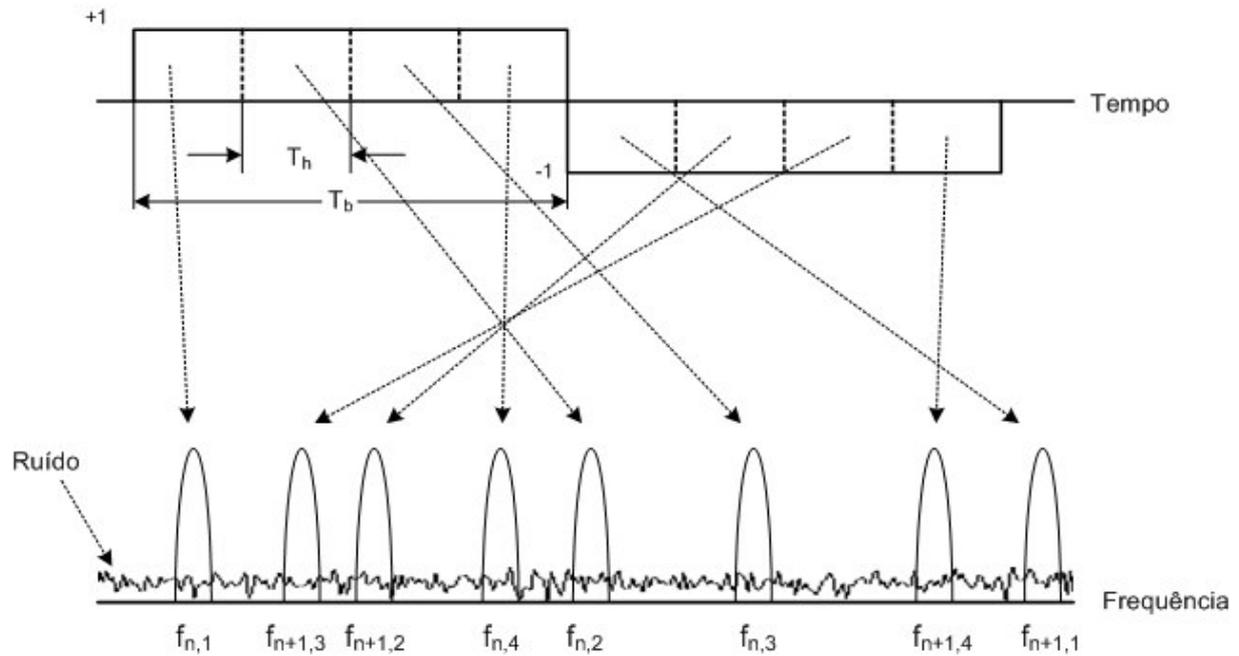


FIG. 2.14 - FHSS rápido.

- Salto em Frequência Lento (SFH) – quando um ou mais bits são transmitidos por um único salto em frequência, ou seja, a taxa de ocorrência de saltos é menor que a taxa de símbolos (FIG. 2.15). Neste caso é forçosa a utilização de código corretor de erros, pois se houver bloqueio em uma das frequências de salto, haverá perda de um ou mais bits.

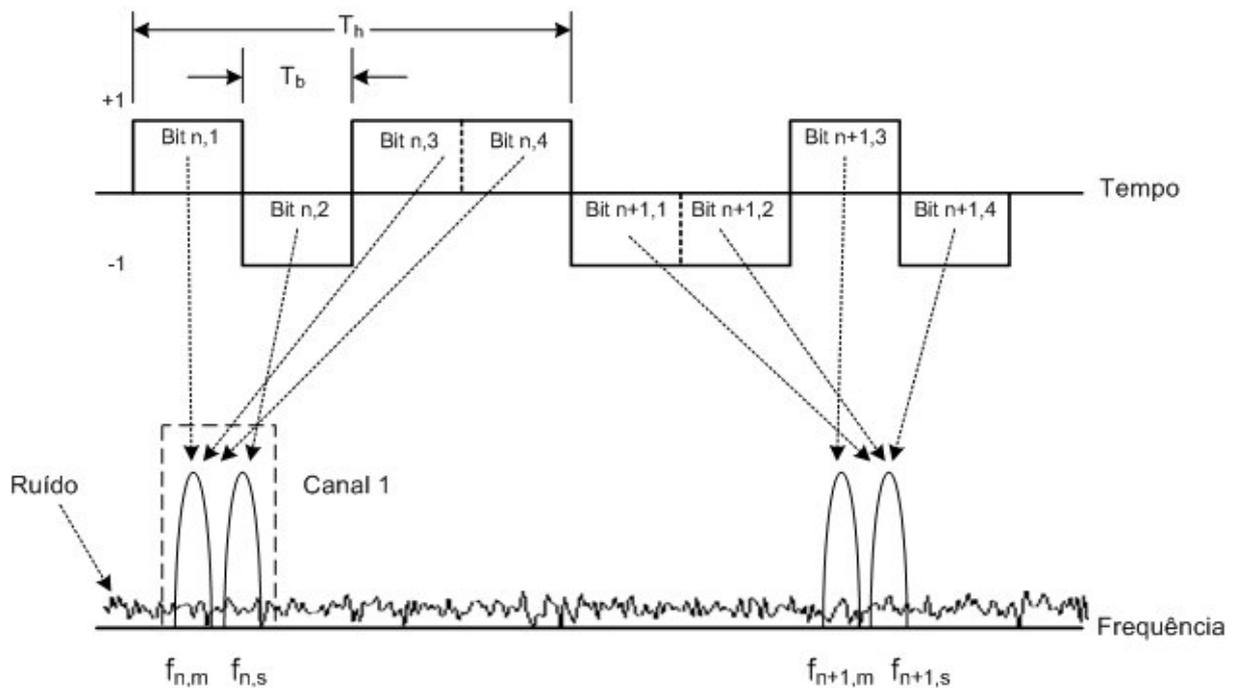


FIG. 2.15 - FHSS lento.

Dentre as principais vantagens na implementação do FHSS pode-se destacar o custo dos equipamentos, que nesse tipo de técnica de espalhamento é mais barato que a da técnica DSSS, e a possibilidade de uso de faixas de frequência não-contíguas, reduzindo possíveis interferências não-intencionais de faixa estreita. Entretanto, tem-se dificuldades na implementação de sintetizadores de frequência na etapa de modulação, e a demodulação coerente é afetada pelos problemas de manter relações de fase durante os saltos em frequência.

2.2.3 ESPALHAMENTO ESPECTRAL POR SALTO NO TEMPO – THSS

No esquema THSS o sinal correspondente à informação é transmitido em rápidos surtos de intervalos de tempo determinados pelas sequências atribuídas a cada usuário. O eixo do tempo é dividido em quadros, e cada quadro é dividido em M intervalos de tempo (*timeslots*). Durante cada quadro, o usuário transmite em um dos M *timeslots*, sendo a escolha do *timeslot* feita de acordo com a sequência associada ao usuário. Durante a transmissão, toda a largura de banda alocada ao sistema é ocupada por um determinado usuário, sendo então necessária a minimização da probabilidade de ocorrência de conflitos em transmissões simultâneas.

A implementação da técnica THSS é mais simples que a FHSS e permite a transmissão em altos níveis de potência nos curtos intervalos de tempo.

A TAB. 2.1 sintetiza as vantagens e desvantagens de cada técnica de espalhamento espectral.

TAB. 2.1 - Vantagens e desvantagens de sistemas com espalhamento espectral.

Técnica	Vantagens	Desvantagens
DSSS	<ul style="list-style-type: none"> – Melhor desempenho na presença de interferências intencionais – Mais difíceis de detectar – Os multipercursos são menos prejudiciais – O circuito gerador de frequência (sintetizador) é mais simples, pois não tem necessidade de trocar de frequência constantemente – O processo de espalhamento é simples, pois é realizado através da multiplicação do sinal de informação por um código – Maior capacidade de transmissão 	<ul style="list-style-type: none"> – Tempo de aquisição de sincronismo demorado – Necessitam de um gerador PN rápido – Sofrem do problema perto-longe⁴ – Mais vulneráveis a bloqueadores com ruído pulsado – Equipamentos de maior custo
FHSS	<ul style="list-style-type: none"> – Maior imunidade as interferências – Podem ser programados para evitar certas porções do espectro – São menos afetados pelo problema perto-longe – Os canais que o sistema utiliza para operação não precisam ser sequenciais – A probabilidade de diferentes usuários utilizarem a mesma seqüência de canais é muito pequena – Equipamentos de menor custo 	<ul style="list-style-type: none"> – Sintetizador de frequência complexo – Mais vulneráveis a ataques de bloqueadores de banda parcial – O sincronismo entre a transmissão e a recepção é mais crítico. – Baixa capacidade de transmissão
THSS	<ul style="list-style-type: none"> – Implementação mais simples que FH – Problema perto-longe é evitável num sistema coordenado 	<ul style="list-style-type: none"> – Tempo de aquisição demorado

⁴ O fenômeno perto-longe pode ser explicado através de uma situação em que duas unidades móveis estão tentando se comunicar com o mesmo ponto de acesso, e que a unidade A está mais perto que a B, e ambas estão dentro da mesma área de cobertura. Como a unidade A está mais perto, seu sinal de rádio é mais forte. Se as duas unidades tentarem transmitir ao mesmo tempo, pode acontecer de a unidade B nunca conseguir um acesso porque o sinal mais forte (A) prejudica a recepção de sinais mais fracos (B).

2.3 SISTEMAS COMERCIAIS

Nos últimos anos os sistemas de comunicações vêm apresentando uma grande evolução tecnológica e vários são os serviços de telecomunicação oferecidos. Os sistemas de comunicações móveis têm se destacado muito nesse contexto. A elevada demanda para os serviços de telecomunicações é a razão para tanto esforço no sentido de prover avanços que os tornem cada dia mais atrativos economicamente e tecnologicamente mais versáteis.

Com a evolução dos sistemas de comunicações e o conseqüente aumento dos usuários, as operadoras desenvolvedoras de sistemas de telefonia móvel concentram sua ação no melhor aproveitamento do espectro e no desenvolvimento de sistemas resistentes à interferência e à interceptação. As técnicas de múltiplo acesso foram desenvolvidas com estes objetivos. O esquema mais antigo implementado em sistemas de rádio móvel foi o acesso múltiplo por divisão em frequência (FDMA - *Frequency Division Multiple Access*), tipicamente aplicado em sistemas analógicos. Com o advento dos sistemas digitais, surgiram as técnicas de acesso múltiplo por divisão no tempo (TDMA) e acesso múltiplo por divisão em código (CDMA).

Sistemas FDMA fazem uso de pequenas porções da banda total disponível para a transmissão durante todo tempo, enquanto que sistemas que empregam a técnica TDMA permitem que um transmissor faça uso de toda banda disponível para a transmissão por uns pequenos intervalos de tempo. Por outro lado, a técnica CDMA permite que todos os transmissores tenham acesso ao canal simultaneamente usando toda a banda disponível ao mesmo tempo, através do uso de técnicas de espalhamento espectral.

O padrão GSM utiliza uma combinação entre multiplexação FDMA e TDMA como método de acesso ao meio. Usando a técnica FDMA, atribui-se uma frequência a cada usuário e a técnica TDMA permite que vários usuários compartilhem o mesmo canal.

No presente trabalho, os sistemas de comunicações comerciais CDMA e GSM são abordados. Em função disso, as suas principais características e funcionalidades são resumidas a seguir.

2.3.1 CDMA

No Brasil, o sistema CDMA é baseado no padrão IS-95, que é utilizado em duas bandas, conforme a TAB. 2.2. O padrão IS-95 é especificado na norma TIA/EIA/IS-95A (2000) e ABU-RGHEFF (2007). O estado do Rio de Janeiro utiliza à banda A, sub-banda 0, em sua operação.

TAB. 2.2 - Bandas A e B do sistema CDMA.

Designador do Sistema	Sub-Bandas	Banda de Frequência de Transmissão (MHz)	
		Estação Móvel	Estação Base
A	0	824,025 – 835,005 844,995 – 846,495	869,025 – 880,005 889,995 – 891,495
	1	824,025 – 835,005 844,995 – 848,495	869,025 – 880,005 889,995 – 893,495
B	0	835,005 – 844,995 846,495 – 848,985	880,005 – 889,995 891,495 – 893,985
	1	835,005 – 844,995	880,005 – 889,995

Um conceito importante dentro da tecnologia CDMA, definido na norma IS-95, é a designação de duas portadoras chamadas de "primária" e "secundária", mostradas na TAB. 2.3 (LEE, 1998). Essas portadoras são utilizadas pelo terminal móvel para acesso inicial ao sistema. Depois do acesso inicial, caso exista alguma outra portadora disponível na célula, o terminal móvel pode receber a sinalização para trocar de portadora.

TAB. 2.3 - Números dos canais do sistema CDMA.

Sub-Bandas	Designador do Sistema	Números dos Canais
0	A	283 (Primária) e 691 (Secundária)
	B	384 (Primária) e 777 (Secundária)
1	A	779 (Primária) e 738 (Secundária)
	B	486 (Primária) e 568 (Secundária)

Conforme a norma TIA/EIA/IS-95A (2000), o *link* direto IS-95 suporta a família de taxas de dados de 9.600 bps em 4 tipos de canais de dados, como apresentado na TAB. 2.4.

TAB. 2.4 - Canais de tráfego do sistema CDMA.

CANAL	SYNC	PAGING		TRÁFEGO			
Taxa de dados [bps]	1200	4800	9600	1200	2400	4800	9600
Repetição de Código	2	2	1	8	4	2	1
Taxa de modulação de símbolo [bps]	4800	19200	19200	19200	19200	19200	19200
PN chips/ modulação de símbolo	256	64	64	64	64	64	64
PN chips/bit	1024	256	128	1024	512	256	128

Em sistemas digitais, como o CDMA, a qualidade do sinal é medida através da relação entre a energia de bit e a densidade espectral de potência dos sinais de ruído inerentes ao meio de transmissão (E_b/N_0), (ABU-RYHEFF, 2007). Para os receptores dos terminais móveis tipicamente utilizados em sistemas CDMA comerciais, a faixa média de E_b/N_0 suficiente para garantir a qualidade do sistema varia de 3 a 9 dB. Estes valores são indicados para manutenção da taxa de erro de bits (BER) em 0,001 (TIA/EIA/IS-95A, 2000).

Do ponto de vista de bloqueio do sistema CDMA, a grande estratégia a ser seguida pelo bloqueador é tentar fazer com que o móvel não consiga efetuar a aquisição do sistema, mantendo o mesmo fora de operação na rede, como abordado em TOSCANO (2007). A proposta é gerar interferência no canal direto recebido pelo terminal móvel, mais precisamente sobre a portadora primária, que no Rio de Janeiro é o canal 283. Segundo a norma, este canal está definido por $0,03 \cdot 283 + 870 \text{ MHz} = 878,49 \text{ MHz}$. A portadora primária é definida como padrão, sendo a secundária utilizada somente em casos excepcionais. Assim, fica evidente onde deverá ocorrer a geração da interferência, ou seja, sobre o canal 283. A largura de banda do sinal de bloqueio deverá ser a mesma de um canal do CDMA (1,23 MHz).

2.3.2 GSM

O GSM surgiu em 1982, a partir dos trabalhos de um comitê da Conferência Européia das Administrações Postais e de Telecomunicações (CEPT - *European Conference of Postal and*

Telecommunications Administrations), dando origem a uma organização de padronização européia, criada com o objetivo de definir um novo padrão para comunicações móveis na faixa de 900 MHz. O comitê, nomeado *Groupe Spéciale Mobile*, que remetia até então à sigla GSM, decidiu que o novo padrão usaria tecnologia digital. Anos mais tarde, o CEPT foi incorporado pelo Instituto Europeu de Padrões em Telecomunicações (ETSI - *European Telecommunication Standard Institute*). O grande mérito do comitê foi abandonar diferentes padrões que já estavam em funcionamento em alguns países membros e criar um novo padrão de comunicações, que seria adotado internacionalmente posteriormente.

Em 1991, o primeiro sistema GSM foi colocado em operação. No mesmo ano, houve a mudança de nome do comitê para Grupo Móvel Especial (SMG - *Special Mobile Group*), e o GSM passou a definir o nome do novo padrão. Também em 1991, o padrão GSM foi estendido para a faixa de 1800 MHz, que foi chamada de Sistema Digital Celular 1800 (DCS 1800 - *Digital Cellular System 1800*), sistema implementado no Brasil. Nos Estados Unidos da América, o DCS 1800 foi adaptado para 1900 MHz, sendo chamado de Sistema de Comunicação Pessoal 1900 (PCS 1900 - *Personal Communications System 1900*). No Brasil, os primeiros sistemas GSM começaram a ser implantados somente depois de 2002, estando em plena expansão.

A rede GSM padrão está representada pela FIG. 2.16.

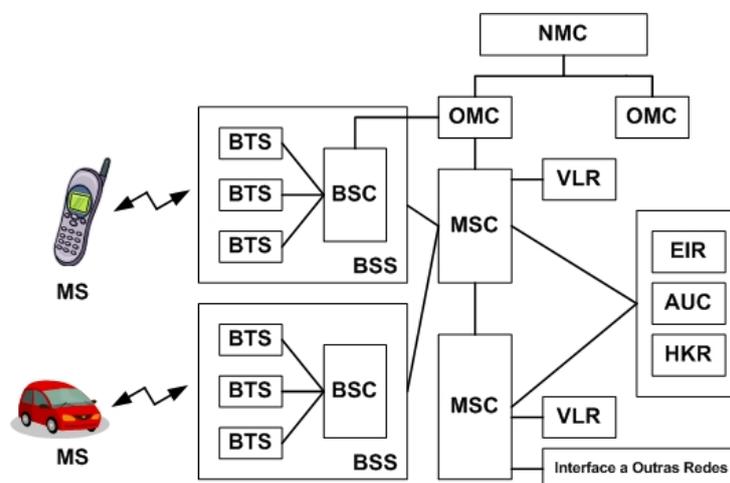


FIG. 2.16 - Rede GSM padrão.

As estações móveis (MS - *Mobile Station*) se comunicam com o Sistema da Estação Base (BSS - *Base Station System*) pela interface aérea de RF. O BSS é formado por uma Estação Base Transceptora (BTS - *Base Transceiver Station*) e um Controlador de Estação Base (BSC - *Base Station Controller*). As BSC são frequentemente ligadas à BTS por *links* de microondas. Por sua vez, diversas BSS são subordinadas a uma Central de Comutação e

Controle (MSC – *Mobile Service Center*), que controla o tráfego entre diversas células diferentes. Basicamente a BSS possui algumas funcionalidades, como: controlar a mobilidade, controlar a sinalização entre a estação móvel e a BSC (comunicação feita pelo ar) e a estação transceptora e a interface com a MSC.

Cada MSC tem um Registro de Localização de Visitante (VLR – *Visitor Location Register*), no qual as unidades móveis que estiverem fora das células de sua área local são listadas, de forma que a rede saiba onde encontrá-las. A MSC é também conectada ao Registro de Localização de Unidade Móvel Local (HLR – *Home Location Register*), à Central de Autenticação (AUC – *Authentication Center*) e ao Registro de Identidade do Equipamento (EIR – *Equipment Identity Register*), de forma que o sistema possa verificar se os usuários e equipamentos são assinantes em situação legal (o que ajuda a evitar o uso de unidades móveis roubadas ou fraudadas). Há também instalações dentro do sistema para as organizações de Operações e Manutenção (OMC – *Operational and Maintenance Center*) e de Gerenciamento da Rede (NMC – *Network Manager Center*). A MSC também possui uma interface para outras redes, como as Redes Públicas Fixas de Telefonia Móvel (PLMN – *Public Land Mobile Network*).

A interface aérea no GSM assume dois esquemas de técnicas de múltiplos acessos (FIG. 2.17): TDMA e FDMA.

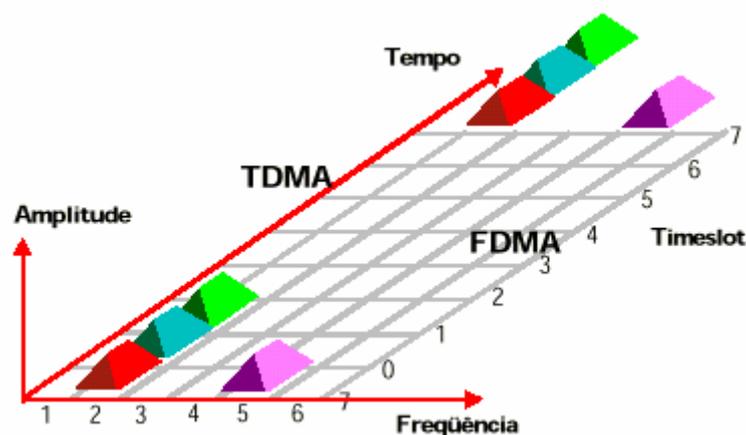
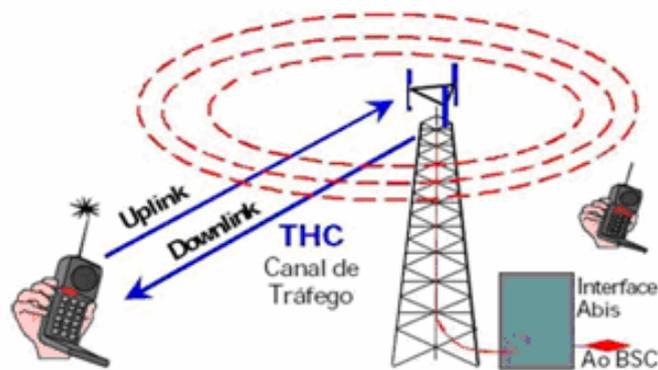


FIG. 2.17 - Técnicas de múltiplos acessos TDMA e FDMA.

As unidades móveis em chamada usam um canal de tráfego TCH (*Traffic Channel*). O TCH é um canal bidirecional usado para a troca de informações de conversação entre a unidade móvel e a estação base (GSM 05.02, 2001). As informações são divididas em *uplink* e *downlink*, dependendo da direção do fluxo (FIG. 2.18).



	Downlink	Uplink
GSM900	935-960 MHz	890-915 MHz
DCS1800	1805-1880 MHz	1710-1785 MHz

FIG. 2.18 - Canal de tráfego no GSM.

Além do canal de tráfego, o GSM possui canais de controle e sinalização: canais de correção de frequência FCCH (*Frequency Correction Channel*), o canal de sincronização SCH (*Sincronization Channel*), o canal de controle broadcast BCCH (*Broadcast Control Channel*) e o canal de controle comum CCCH (*Common Control Channel*). O canal CCCH é dividido em: PCH (*Paging Channel*), canal de concessão de acesso AGCH (*Access Grant Channel*), e canal de acesso randômico RACH (*Random Access Channel*) (GSM 05.02, 2001).

Para o entendimento do GSM foram utilizadas cinco normas do Instituto Europeu de Padrões em Telecomunicações (GSM 05.01, 2000; GSM 05.02, 2001; GSM 05.03, 2005; GSM 05.04, 2001; GSM 05.05, 2005; GSM 05.08, 2000). O propósito desta revisão foi apoiar a fabricação de um dispositivo bloqueador para o sistema GSM, para testes de campo, como apresentado no Cap. 6. A descrição detalhada do GSM é apresentada no Apêndice 1.

2.4 SISTEMAS MILITARES

O Exército Brasileiro utiliza os rádios M3TR da Rohde&Schwarz e HF-6000 da Tadiran, os quais adotam o Padrão Militar 188-110B em seus modems⁵.

⁵ Modems servem de interface entre a fonte de informação e o equipamento rádio, tanto no lado de transmissão quanto no de recepção.

O modem realiza basicamente as técnicas de modulação, filtragem de transmissão e recepção, sincronização, equalização, controle automático de ganho e codificação de canal.

Alguns estudos relacionados à norma MIL-STD-188-110B foram desenvolvidos no Instituto Militar de Engenharia em nível de Graduação. BITTENCOURT (2008), por exemplo, trata do desenvolvimento e avaliação de desempenho de algoritmos utilizáveis na transmissão digital na faixa de áudio de rádios HF.

2.4.1 A NORMA MIL-STD-188-110B

O Padrão Militar 188-110B (MIL STD-188-110B) estabelece formas de ondas e requisitos de desempenho para garantir a interoperabilidade entre os modems que operam na faixa de frequência de voz para transmissão de longo alcance e em sistemas de comunicações táticas na faixa de HF.

As definições do funcionamento e dos requisitos de desempenho do Padrão Militar 188-110B no modo tom simples (MIL STD-188-110B) são apresentadas no Apêndice 2.

3 SISTEMAS DE BLOQUEIO EM GUERRA ELETRÔNICA

3.1 INTRODUÇÃO

Guerra Eletrônica (EW - *Electronic warfare*) é conjunto de ações militares com objetivo de controlar o espectro eletromagnético (ADAMY, 2003). Modernamente, Guerra Eletrônica é constituída por três áreas: Ataque Eletrônico (EA - *Electronic Attack*), Suporte Eletrônico (ES - *Electronic Support*), e Proteção Eletrônica (EP - *Electronic Protect*).

EA de comunicações corresponde à utilização de sinais ativos para evitar que um sistema de comunicações troque informações, sendo constituído por três principais atividades: bloqueio eletrônico, despistamento e energia dirigida. ES tem como função dar suporte à área de EA. EP tem como função proteger as atividades de EA e ES contra supostos ataques.

O presente trabalho concentra-se na subdivisão do EA de bloqueio eletrônico, anteriormente denominada de Contramedidas Eletrônicas (CME). O propósito de todas as contramedidas eletrônicas é interferir no uso efetivo do espectro eletromagnético pelo inimigo. O uso do espectro envolve a transmissão de informação de um ponto a outro, e tal informação pode tomar a forma de voz, vídeo, dados, sinais de comando/controle, sinais radar, entre outros.

A técnica básica de contramedida utilizada é a inserção de um sinal interferente no receptor inimigo, concorrente com o sinal desejado. A interferência torna-se efetiva quando o sinal interferente é forte o bastante para evitar que o inimigo recupere a informação desejada. Isto ocorre quando o conteúdo da informação do sinal desejado está saturado pelo sinal de interferência, ou quando o sinal desejado mais o sinal de interferência possui características que impossibilitam o processador inimigo de extrair a informação do sinal adequadamente.

As contramedidas eletrônicas podem ser divididas em três categorias (ADAMY, 2004; SILVA, 2007), como mostrado na FIG. 3.1: radar, infravermelho & lasers, e comunicações.

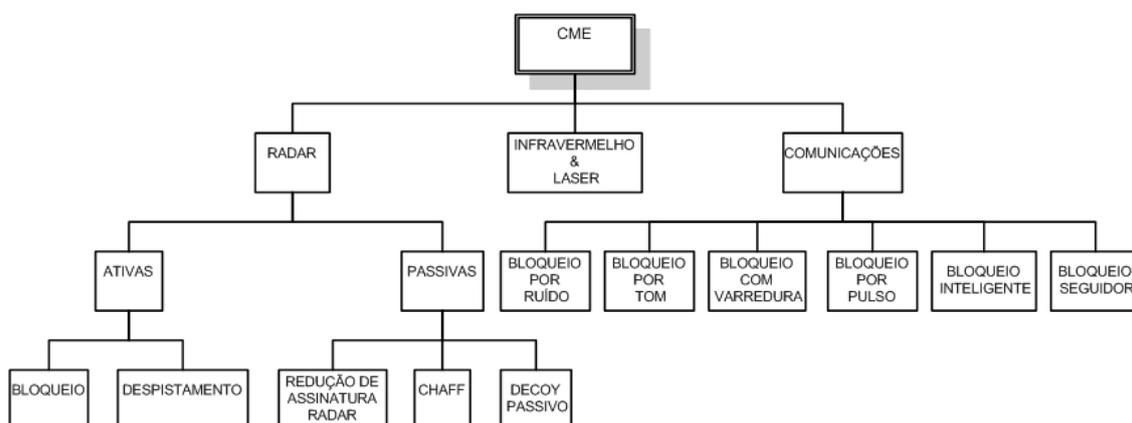


FIG. 3.1 - CME e suas subdivisões.

As contramedidas eletrônicas do tipo radar ativas podem ser classificadas em bloqueio e despistamento. Bloqueio é a irradiação ou reflexão deliberada de energia eletromagnética com o objetivo de anular a efetividade de dispositivos, equipamentos, ou sistemas eletrônicos usados pela força inimiga. Despistamento é a irradiação, re-irradiação, alteração, absorção ou reflexão deliberada de energia eletromagnética com o intuito de confundir intencionalmente a força inimiga no que diz respeito à interpretação ou uso da informação recebida pelos seus sistemas eletrônicos.

As contramedidas eletrônicas passivas do tipo radar são classificadas em: redução de assinatura radar, *chaff* e *decoy* passivo. A tecnologia de redução de assinatura radar passou a ser essencial e pode ser decisiva em combate. Ela torna a detecção mais difícil para os sistemas de sensores e postergam decisões táticas de comando. Um exemplo dessa tecnologia é a aplicação de material absorvedor de radiação eletromagnética como revestimento externo. O *chaff* consiste em um conjunto de diminutos dipolos metálicos lançado na atmosfera com o objetivo de criar uma região (nuvem de *chaff*) de alta refletividade, que mascara a presença de alvos a serem protegidos. *Decoys* passivos são utilizados para aumentar a probabilidade de sobrevivência de aeronaves e de navios, criando informações de alvos falsos nos sistemas de armas inimigos.

As contramedidas eletrônicas do tipo infravermelho funcionam como despistadoras e são empregadas contra mísseis com guiamento final por infravermelho (ADAMY, 2004). Um despistador é constituído de *flares* que emitem radiação infravermelha na faixa de emissão do alvo e com maior intensidade. Essas cargas são lançadas em direções específicas, em relação ao alvo, de forma a atrair o míssil. As contramedidas eletrônicas do tipo laser são utilizadas contra mísseis com guiamento final por raios laser. A CME laser é constituída de um produto capaz de refletir o raio laser com o objetivo de “cegar” o míssil. Um exemplo da técnica de CME Infravermelho & Laser é a Contramedida Infra-Vermelha Direcional (DIRCM). O sistema DIRCM utiliza um método ativo de bloqueio de míssil infravermelhos que procuram a ameaça através da abertura do sensor. Ao localizar a ameaça, o sistema DIRCM emite *flashes* de pulsação de energia infravermelhos que confundem o sistema de orientação de míssil.

As contramedidas eletrônicas para sistemas de comunicação são constituídas genericamente por uma interferência gerada sobre o enlace de comunicações.

A CME de comunicação é o foco principal deste trabalho, sendo tratada em mais detalhes no item a seguir. No item 3.3 é descrito como um sistema com espalhamento espectral se

comporta na presença de determinadas contramedidas eletrônicas do tipo comunicação. No item 3.4 são apresentadas as equações para um modelo genérico de bloqueio da recepção de um sinal em sistemas de comunicações e as considerações para contabilizar o efeito da condição de espalhamento espectral (ganho de processamento).

3.2 TIPOS DE BLOQUEIOS ELETRÔNICOS

De forma genérica, o bloqueio eletrônico caracteriza-se pela irradiação ou re-irradiação intencional de energia eletromagnética com o objetivo de degradar a qualidade do sinal a ser recebido pelo receptor de um sistema de comunicação.

Há diferentes técnicas para impedir que os sistemas de comunicações funcionem. Segundo POISEL (2002; 2004), as estratégias mais comuns de CME de bloqueio sobre um sistema são:

- Bloqueio por ruído (*Noise Jamming*);
- Bloqueio por tom (*Tone Jamming*);
- Bloqueio com varredura (*Swept Jamming*);
- Bloqueio por pulso (*Pulse Jamming*);
- Bloqueio seguidor (*Follower Jamming*);
- Bloqueio inteligente (*Smart Jamming*)

3.2.1 BLOQUEIO POR RUÍDO

No bloqueio por ruído, a portadora do sinal de bloqueio é modulada por um sinal de ruído aleatório. A intenção é degradar a comunicação através da inserção desse ruído aleatório no receptor do sistema a ser interferido. Normalmente o ruído inserido no espectro para causar tal interferência é um ruído branco⁶.

O bloqueio por ruído pode ser realizado de três formas, no que diz respeito à ocupação do espectro:

⁶ O ruído branco caracteriza-se por ter uma intensidade média constante ao longo de seu espectro. Em outras palavras, os sinais se distribuem aleatoriamente no espectro com intensidade constante.

- Bloqueio com ruído em banda larga (BBN - *Broadband Noise Jamming*)

No bloqueio BBN o sinal de bloqueio é irradiado em todo o espectro de comunicação de interesse, cobrindo assim, várias frequências simultaneamente, podendo inclusive atingir canais de comunicação intermediários de outros sistemas que não se deseje interferir na ocasião. Um bloqueador BBN pode ser composto de gerador de ruído banda larga, portadora banda larga, amplificador banda larga, filtro passa-banda sintonizável e antena. Um exemplo dessa topologia básica é apresentado na FIG. 3.2.

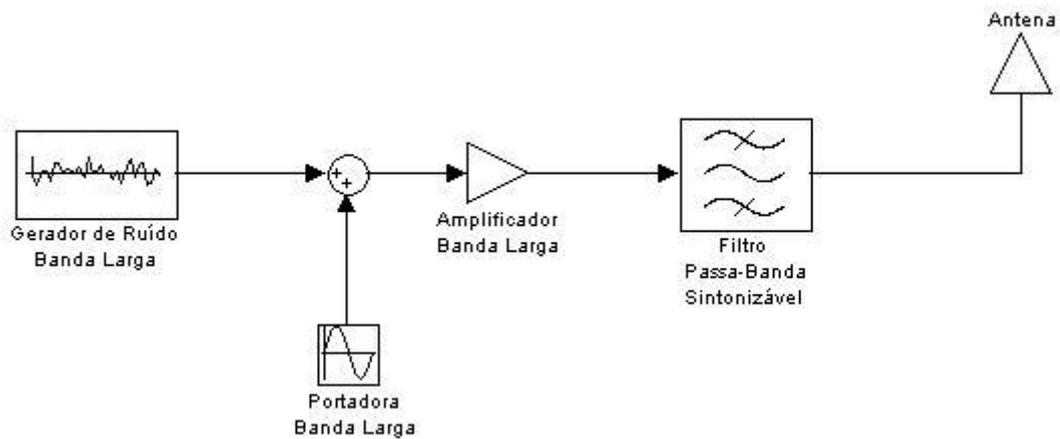


FIG. 3.2 - Topologia básica de um bloqueador BBN.

- Bloqueio com ruído em parte da banda (PBN - *Partial-Band Noise Jamming*)

No bloqueio PBN, o sinal de bloqueio é inserido em múltiplos (mas, não todos) canais do espectro utilizados pelo sistema a ser interferido. Esses canais podem ou não ser contínuos, FIG. 3.3.

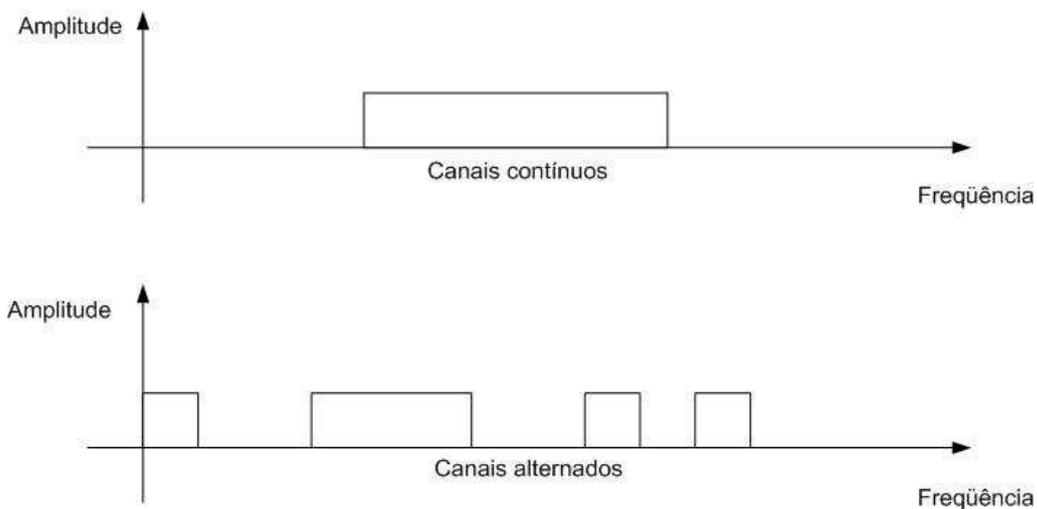


FIG. 3.3 - Bloqueador PBN para canais contínuos e alternados.

A topologia sugerida na FIG. 3.2 pode ser utilizada para o bloqueio PBN (canais contínuos), desde que o filtro passa-faixa sintonizável seja ajustado somente para uma parte da banda de frequências utilizada pelo sistema a ser interferido.

- Bloqueio com ruído em banda estreita (NBN - *Narrowband Noise Jamming*)

No bloqueio NBN, o sinal de bloqueio é inserido em uma faixa estreita do sistema. Uma característica deste tipo de bloqueio é o maior valor de densidade espectral de potência conseguido na prática, em virtude da largura de banda do sinal de bloqueio ser estreita, quando comparada, por exemplo, à do bloqueio BBN. Essa técnica pode ser importante quando o objetivo é atuar somente sobre um canal específico de determinado sistema.

Um bloqueador banda estreita pode ser composto por um gerador de ruído, por um modulador de RF para a geração de uma portadora RF modulada com o ruído, um amplificador, filtro passa-faixa, e por uma Antena (FIG. 3.4).

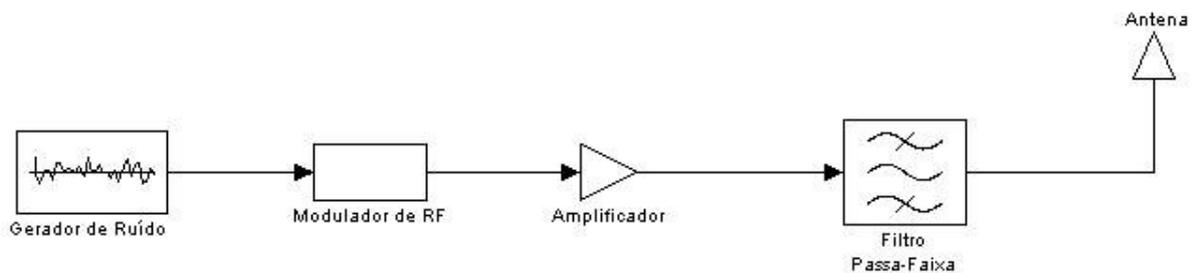


FIG. 3.4 - Topologia básica de um bloqueador banda estreita.

3.2.2 BLOQUEIO COM VARREDURA

No bloqueio com varredura o sinal de bloqueio varre a banda de frequências de interesse ao longo do tempo. A cada instante, somente uma frequência específica e uma região estreita em torno desta frequência é degradada pelo sinal de bloqueio. A faixa de varredura é controlada através de um sinal de varredura. Esse método permite operar com uma alta densidade espectral de potência do sinal de bloqueio na forma de banda estreita aplicada por um curto intervalo de tempo nas frequências da faixa de varredura de interesse.

Uma possível topologia do bloqueador com varredura é ilustrada na FIG. 3.5. O dispositivo é composto de gerador de ruído, um sinal variante no tempo do tipo onda triangular ou dente de serra, somador, oscilador controlado por tensão, amplificador e antena. O ruído é adicionado ao sinal do tipo onda triangular, que, em conjunto, controlam a

varredura do VCO, gerando um sinal de RF modulado com ruído. Um controle manual/automático pode ser incluído para ajustar a frequência de varredura da onda triangular e a largura de banda do ruído.

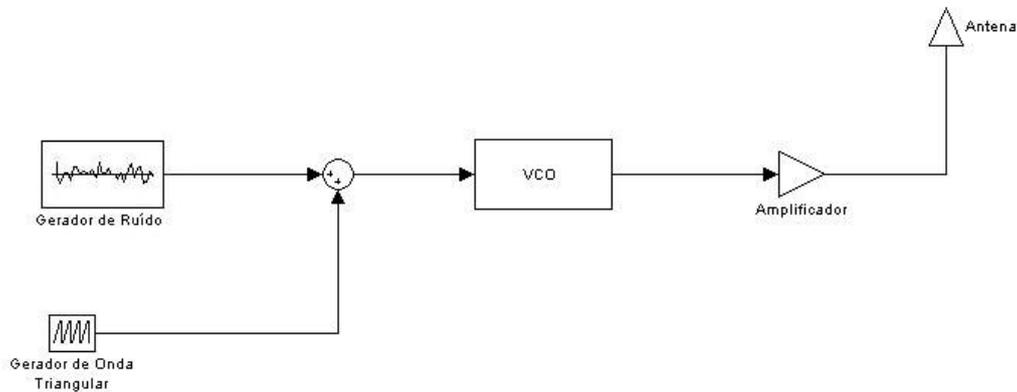


FIG. 3.5 - Topologia básica de um bloqueador com varredura.

3.2.3 BLOQUEIO POR TOM

O bloqueador por tom também é conhecido como bloqueador por portadora singela ou bloqueador pontual.

Um ou mais sinais de tom são estrategicamente inseridos no espectro para provocar a condição de bloqueio. O bloqueio por tom pode ser realizado de duas formas:

- Bloqueio por tom simples

Neste tipo de bloqueio, um sinal de tom é inserido de forma contínua em uma única frequência do espectro utilizado pelo sistema a ser interferido, sendo classificado também como de tom simples, bloqueio pontual, ou de "onda contínua" (CW), FIG. 3.6.

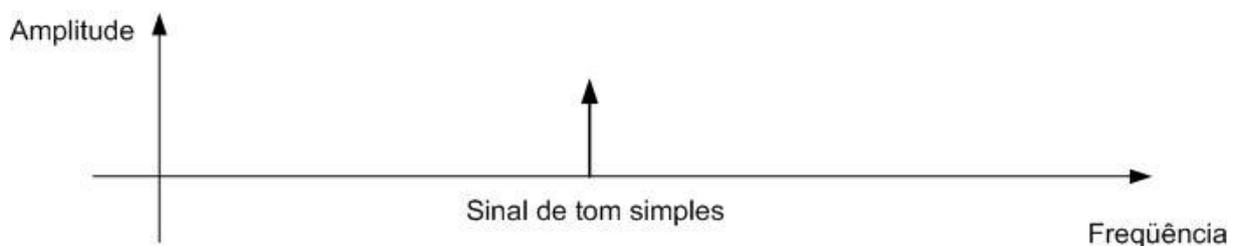


FIG. 3.6 - Espectro do bloqueio por tom simples.

- Bloqueio por tons múltiplos

Neste tipo de bloqueio, múltiplos sinais são inseridos no espectro de interesse de forma aleatória ou em frequências específicas, FIG. 3.7.

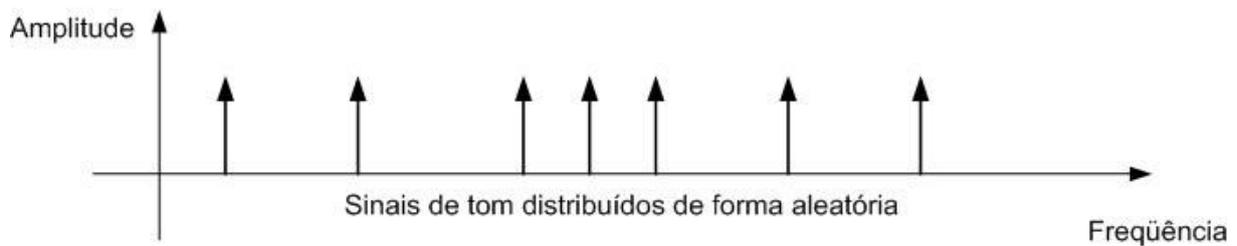


FIG. 3.7 - Espectro do bloqueio por tom múltiplos.

A composição e a topologia sugeridas na FIG. 3.5 podem também ser utilizadas para o bloqueio por tom simples, desde que seja retirado o somador, o gerador de onda triangular e o gerador de ruído, usando-se em seus lugares um nível de tensão DC constante para controlar o VCO. A faixa do espectro do sistema a ser interferida é controlada pelo VCO.

3.2.4 BLOQUEIO POR PULSO

O bloqueio por pulso é similar ao conceito utilizado no bloqueio por ruído, onde o bloqueio atua em uma fração do espectro. Nesse caso a fração corresponde ao tempo pelo qual o bloqueio permanece ligado e desligado. O trabalho estatístico é elaborado para ser o mesmo, os pulsos curtos têm o conteúdo espectral largo e são conseqüentemente similares ao ruído de faixa larga quando estão ligados (POISEL, 2004).

O bloqueio por pulso pode ter baixa potência média comparada com as técnicas de bloqueio mencionada nesse trabalho e o bloqueio pode ser tão ou mais eficiente. O *duty cycle* do pulso determina a relação entre a potência média e a potência de pico.

3.2.5 BLOQUEIO SEGUIDOR

No bloqueio seguidor, o dispositivo bloqueador implementado possui a funcionalidade de tentar atuar sobre a banda de frequências que está sendo utilizada pelo sistema a ser interferido, considerando, por exemplo, um sistema que utiliza várias bandas de frequências de operação de forma alternada. O bloqueador tenta localizar a frequência de saltos do sistema a ser interferido, identificando o sinal como de interesse e emite o sinal de bloqueio em torno da frequência desejada.

O sinal de bloqueio pode ser na forma de um ruído, tom simples ou pode ser modulado por múltiplos tons, usando modulação FM. Este tipo de bloqueio também pode ser referido como "bloqueio responsivo" (*responsive jamming*) e "bloqueio repetidor" (*repeater jamming*) (POISEL, 2004).

3.2.6 BLOQUEIO INTELIGENTE

No bloqueio inteligente, o sinal de bloqueio é inserido em partes específicas do espectro utilizado pelo sistema a ser interferido, em frequências fundamentais para o funcionamento do sistema.

Para implementação de um bloqueador inteligente é necessário um conhecimento das características de operação do sistema a ser bloqueador. Como exemplo, pode-se citar os sistemas que necessitam de sincronismo para operar corretamente. Neste caso, pode-se buscar a invalidação dos mesmos através da inserção do sinal de bloqueio somente sobre os canais de sincronismo.

3.3 BLOQUEIO EM SISTEMAS COM ESPALHAMENTO ESPECTRAL

3.3.1 BLOQUEIO EM SISTEMAS DSSS

Frequentemente sinais com espalhamento espectral DSSS estão abaixo do nível de ruído, dito ruído de fundo, na recepção. Apesar de poderem ser detectados abaixo do nível de ruído, a existência do problema perto-longe discutido no item 2.2, em sistemas de múltiplos acessos DSSS apóia a idéia de que esses sistemas podem ser bloqueados. O problema perto-longe é criado por um sinal significativamente mais forte que o sinal DSSS dentro da mesma largura de banda, desta forma o sinal mais forte prejudica a recepção dos sinais mais fracos (PRASAD, 1993). Isso é similar a técnica empregada por bloqueadores (POISEL, 2004).

O desempenho dos bloqueadores em sistemas DSSS depende do comprimento da sequência de espalhamento. Em uma sequência de espalhamento curta se repete cada um ou poucos bits de dados, enquanto em uma sequência de espalhamento longa se repete sobre muitos bits de dados. Por isso, sistemas com sequências de espalhamento curtas são mais vulneráveis que com sequências de espalhamentos longas. Portanto, sequências de espalhamento curtas são mais vulneráveis a ES, e por conseguinte a EA, do que as sequências de espalhamento longas.

As técnicas de bloqueios mais empregadas em sistemas DSSS são (POISEL, 2004): bloqueador BBN, bloqueador PBN, bloqueador por pulso e bloqueador por tom.

O bloqueio BBN em sistemas DSSS acontece quando o sinal de bloqueio possui aproximadamente a mesma largura de banda que o sinal DSSS, mas com potência significativamente mais forte. O bloqueio BBN é ilustrado na FIG. 3.8.

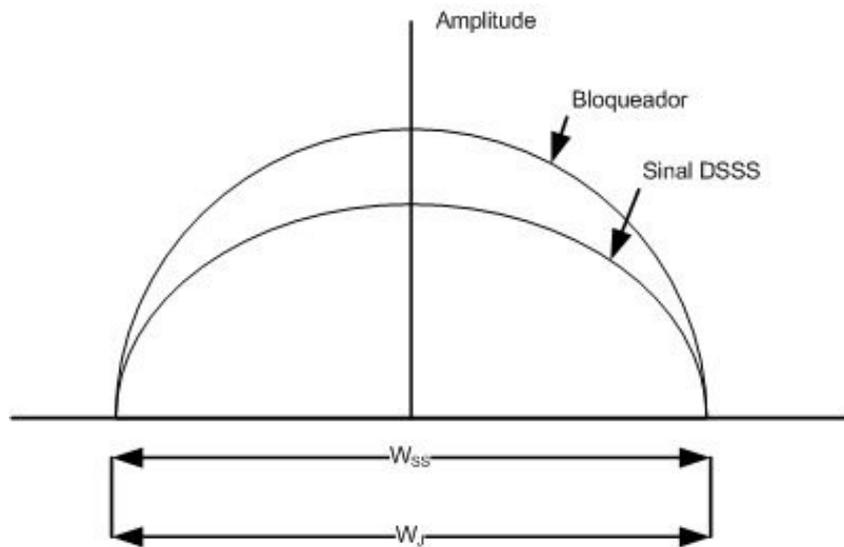


FIG. 3.8 - Bloqueador BBN em sistemas DSSS.

Em bloqueio PBN, a potência do sinal de bloqueio é espalhada sobre uma largura de banda (W_B) mais restrita que a largura de banda do sinal DSSS (W_{DSSS}). A FIG. 3.9 ilustra o sinal de bloqueio PBN em sistemas DSSS. A condição mais favorável para o bloqueio é obtida com o centro da banda do sinal de bloqueio no centro da banda do sinal DSSS.

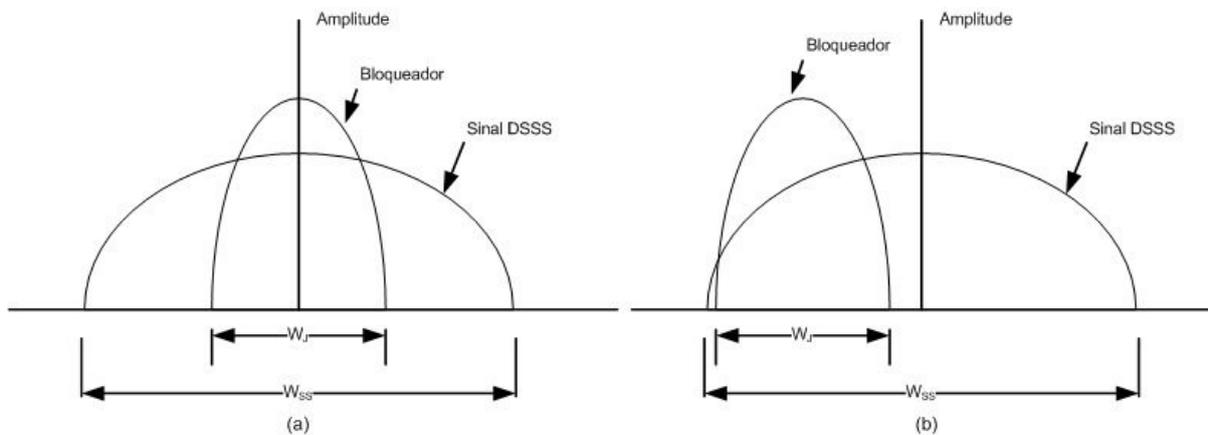


FIG. 3.9 - Bloqueador PBN em sistemas DSSS com (a) sinal de bloqueio centrado na frequência central do sinal DSSS e com (b) sinal de bloqueio deslocado da frequência central.

O bloqueador por pulso transmite potência por uma fração de tempo e fica inoperante por um determinado tempo. Segundo POISEL (2004), para produzir efeito, a largura de banda do bloqueador por pulso deve ser a mesma do sinal DSSS.

Para tons simples, dois casos são considerados em relação à posição do espectro onde o sinal de bloqueio atua (POISEL, 2004):

- O primeiro caso é quando a frequência do sinal de bloqueio é a mesma da portadora do sinal DSSS, cuja situação não é a mais favorável, porque o sinal de bloqueio sofre diversas atenuações devido ao processo de correlação do receptor DSSS.
- O segundo caso ocorre quando a frequência do sinal de bloqueio está deslocada da frequência da portadora do sinal DSSS, no qual a faixa de frequência onde o bloqueador por tom simples atua depende do alvo e do objetivo a ser alcançado.

No bloqueio por tons múltiplos, os tons do espectro do bloqueador podem ser distribuídos arbitrariamente na banda do sistema DSSS. Os tons de bloqueios podem ser inseridos no espectro com as mesmas amplitudes e espaçados simetricamente em torno da frequência central do sistema DSSS ou deslocados da frequência central do sistema DSSS e amplitudes diferentes, FIG. 3.10. Estudos relacionados aos efeitos de bloqueadores por múltiplos tons em sistemas DSSS foram realizados por MILSTEIN (1982).

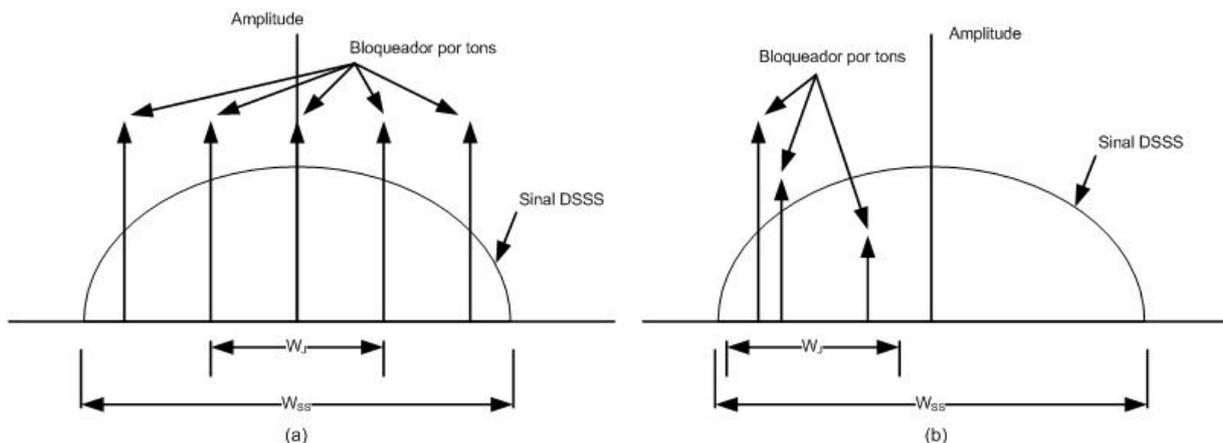


FIG. 3.10 - Bloqueador por tons em sistemas DSSS com (a) tons de bloqueio com mesma amplitude espaçados simetricamente da frequência central do sinal DSSS e com (b) tons de bloqueio de amplitudes diferentes e deslocados da frequência central.

3.3.2 BLOQUEIO EM SISTEMAS COM SALTO EM FREQUÊNCIA RÁPIDO (FFH)

Nos sistemas FFH existe um ou mais saltos de frequência por bit. Tais sistemas foram concebidos como uma forma de anti-bloqueio.

Se o salto em frequência é muito rápido o bloqueio poderá não ser eficiente. Isso ocorre porque o sinal de bloqueio não é rápido o suficiente para cobrir a mesma faixa do espectro de frequência do sinal a ser bloqueado. Por exemplo: um sistema está emitindo numa frequência f_1 , segundos depois o bloqueador emite o sinal de bloqueio na mesma frequência f_1 . Devido

ao tempo de resposta do bloqueador, o sistema já saltou para outra frequência f_2 , tornando assim o bloqueio ineficiente. Esse tempo de resposta pode ser consequência do posicionamento do bloqueador em relação ao sistema a ser bloqueado.

Segundo POISEL (2004), o bloqueador com melhor desempenho para sistemas com salto em frequência lento (SFH) não é necessariamente o melhor para sistemas FFH. Por exemplo, um bloqueador seguidor que seja ineficiente para sistemas com saltos rápidos pode ser eficiente para sistemas com saltos mais lentos.

Para se realizar uma análise do problema, assume-se que o bloqueador conhece todos os parâmetros do alvo, exceto o código de espalhamento. A banda de saltos, largura de banda do canal, frequência central, entre outros, deverão ser conhecidos para a implementação correta do bloqueador (POISEL, 2004).

A estrutura do canal FFH na presença do bloqueador está ilustrada na FIG. 3.11, onde se observa um bloqueio contínuo em parte da banda. Dependendo da estratégia de bloqueio, a parte da banda onde o bloqueio estiver agindo pode ser alterada.

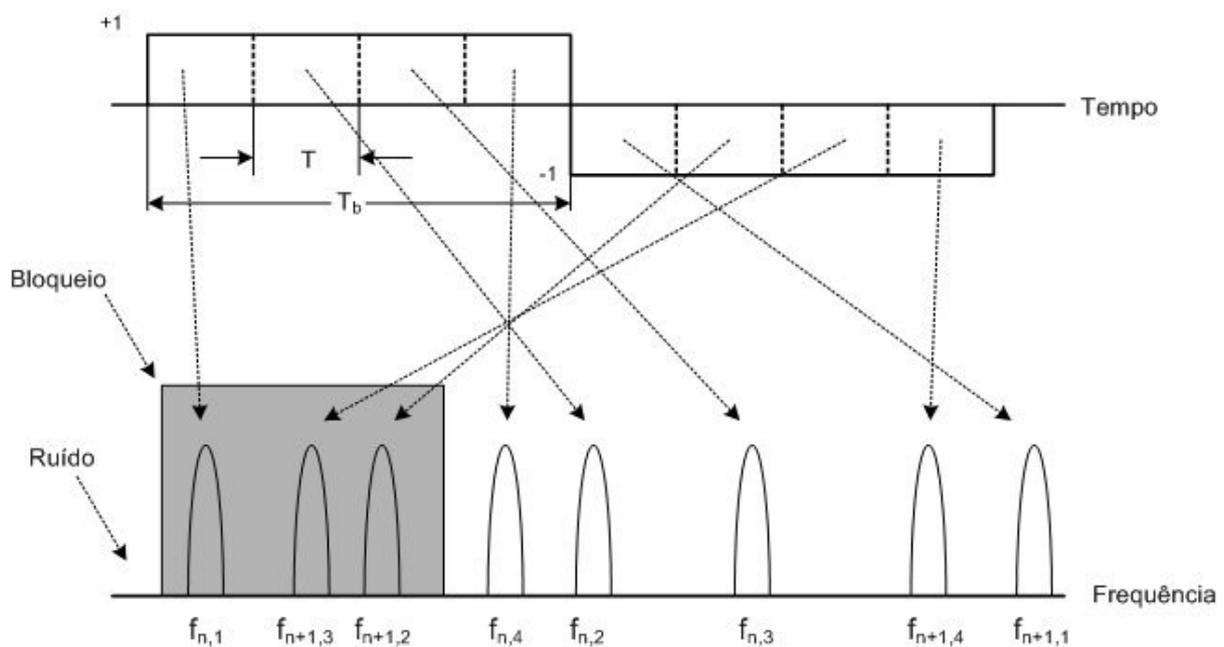


FIG. 3.11 - Bloqueador em sistemas FFH.

Existem dois efeitos particulares que devem ser considerados em sistemas com espalhamento FFH. O primeiro é o efeito de múltiplas fatias de tempo por dados de bit. A simples falha de uma fatia de tempo recebida com erro no receptor não garante que esse bit de dado seja detectado com erro, desde que existam múltiplas fatias de tempo para o mesmo bit de dado. O segundo é o efeito do bloqueio em partes das fatias de tempo correspondente a um

bit de dado. Esta condição pode ser dividida em três partes: no bloqueio seguidor, quando o sinal deve ser detectado primeiro a fim de ser bloqueado; no bloqueio PBN, quando somente uma parte do espectro é coberta pelo bloqueio; e no bloqueio parcial por tons, quando múltiplos tons são irradiados no espectro, mas nem todos dados de frequência estão cobertos pelo sinal de bloqueio.

As técnicas de bloqueio mais empregadas em sistemas FFH são (POISEL, 2004): bloqueador BBN, bloqueador PBN, bloqueador seguidor e bloqueador por tom,.

O bloqueio BBN em sistemas FFH é similar ao bloqueio BBN em sistemas DSSS. O ruído de fundo em todos os canais é aumentado pela densidade de potência do ruído do bloqueador e por essa razão a efetividade do bloqueador pode ser determinada pela mesma maneira que um ruído somente. Para isso, basta somar a potência do bloqueador com a potência do ruído.

O bloqueio seguidor pode bloquear o próprio canal de comunicação, bloquear o canal adjacente ou pode bloquear ambos os canais. A interferência em um canal adjacente ocorre quando dois ou mais pontos de acesso estão usando canais que se sobrepõem e estão próximos o suficiente uns dos outros. Esse tipo de interferência pode ter o mesmo tipo de efeito que a interferência no próprio canal. Para o bloqueio seguidor em sistemas FFH a velocidade necessária para executar a classificação e a emissão do bloqueio na mesma frequência do sinal de comunicação agrava o problema. Para alguns cenários, é possível determinar a taxa de saltos para qual o bloqueio pode ser ou não ser efetivo.

O bloqueio seguidor NBN em canais adjacentes produz um aumento da BER na maioria dos casos. Comparando o bloqueio seguidor NBN com o bloqueio seguidor por tom verificase que quando o bloqueio atua em um ou dois canais adjacentes, a performance são as mesmas. Para outras aproximações do bloqueio seguidor, usar tons é relativamente mais eficiente.

O bloqueio PBN também é útil em sistemas FFH. O sinal é bloqueado quando salta para a parte do espectro que contém o sinal de bloqueio, embora isto não necessariamente cause erro na detecção do bit. Do mesmo modo, quando o bit se encontra na parte do espectro que não está bloqueada, o ruído térmico pode causar erro na detecção mesmo que não haja sinal de bloqueio presente.

Na banda de VHF baixa (30 a 90 MHz, com canais de 25 kHz) existem aproximadamente 2400 canais. Bloqueando 10% deles resulta em 240 canais, enquanto 30% deles resultam em bloqueio de 720 canais. Para UHF (225 a 400 MHz, com canais de 50 kHz), a banda de

frequência possui 3500 canais. Nesse caso, 10 e 30% da quantidade de canais são, respectivamente, 350 e 1050 canais. Então, o bloqueio com ruído facilmente causa uma degradação na comunicação. Bloqueio para largas porções do espectro deve ser somente aplicado sobre circunstâncias especiais, devido à alta potência de transmissão necessária para a sua efetivação.

O bloqueio NBN só é efetivo quando a largura de banda do sinal de bloqueio ocupa o canal de comunicação do sistema.

O bloqueio por tons simples não é uma técnica viável e não é usada para sistemas FFH. Por outro lado, o bloqueio por múltiplos tons pode ser efetivo em sistemas FFH. Os tons de bloqueio são colocados em N_J frequências. Por simplicidade é considerado que as possíveis localizações dos saltos de frequências no espectro são conhecidas, embora a sequência de saltos não seja conhecida. Os tons de bloqueio devem ser colocados nas frequências dos tons de dados para o bloqueio ser eficiente. A desvantagem em utilizar bloqueador com múltiplos tons em sistemas FFH ocorre quando o tom é colocado no canal adjacente associado com o salto. Como no caso de bloqueador PBN, os múltiplos tons não precisam ser contínuos.

Segundo POISEL (2004), o bloqueador por pulso não é efetivo para sistemas com espalhamento espectral FHSS, diferentemente do caso de sistemas DSSS.

3.3.3 BLOQUEIO EM SISTEMAS COM SALTO EM FREQUÊNCIA LENTO (SFH)

O salto lento em frequência acontece quando o sistema de comunicação muda a frequência e existe mais de um bit sendo transmitido por cada frequência nova. Um valor típico para a taxa de salto é por volta de 100 saltos por segundo, de forma que o transmissor permaneça em cada frequência por um tempo de aproximadamente 10 ms.

Em estudo realizado por POISEL (2004), considera-se que os tons de frequências do alvo são dados por f_1, f_2, \dots, f_N , como mostrado na FIG. 3.12. É assumido que esses tons de frequência são inseridos no espectro simetricamente em cada lado da frequência da portadora f_0 . A largura de banda do ruído é dada por W_J e a largura de banda do sistema SFH é dada por W_{SS} .

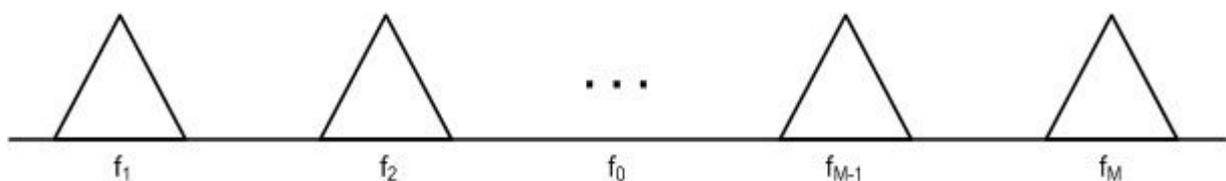


FIG. 3.12 - Espectro de um sinal modulado em múltiplas frequências.

O bloqueador BBN para sistema SFH produz efeito similar ao do bloqueador BBN em sistema FFH, onde o ruído de fundo em todos os canais é aumentado pela densidade de potência do ruído do bloqueador. Portanto, o desempenho da comunicação pode ser determinado pela mesma maneira que um ruído de fundo.

Para o bloqueador PBN é importante ressaltar que o sinal de bloqueio não precisa ser adjacente ao sinal que deverá ser bloqueado. O bloqueador poderia deslocar a sua energia ao longo de vários canais separados, como na FIG. 3.13.

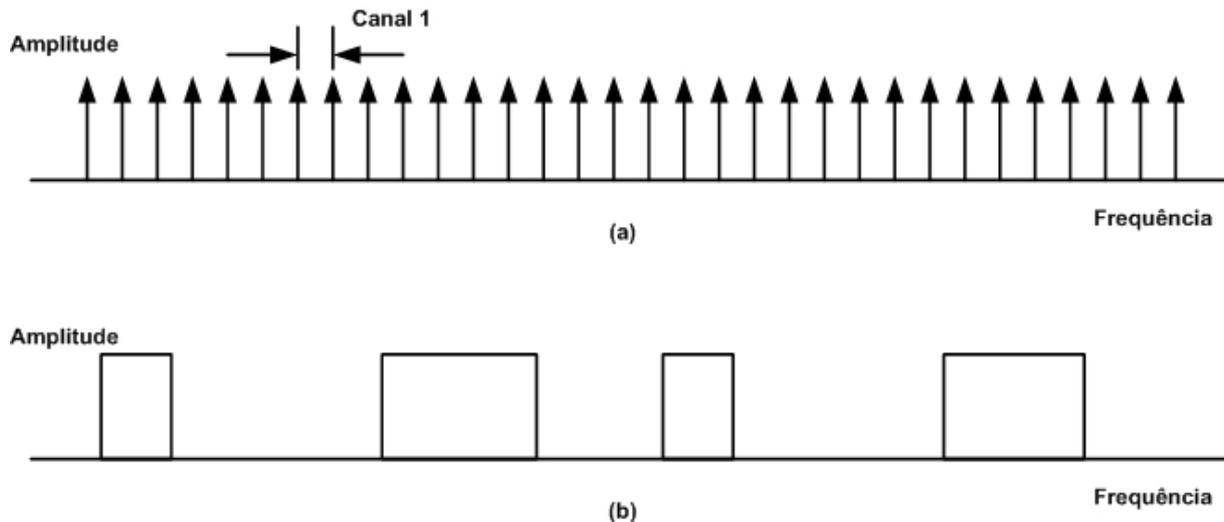


FIG. 3.13 - Bloqueador PBN em sistemas SFH. (a) sinal e (b) bloqueio PBN

No bloqueador PBN, quando o sinal salta para uma nova frequência, o canal pode ser transmitido na banda que está sendo bloqueada ou não. Se for transmitido na banda bloqueada, então a potência total de ruído presente será a soma do ruído do bloqueador com o ruído térmico. Se o canal não estiver sendo bloqueado, o sinal será degradado apenas pela presença do ruído térmico.

O bloqueador por múltiplos tons pode ser utilizado em sistemas SFH. Não é necessário conhecer o tom de frequência exato que será bloqueado. Para isso basta emitir o sinal de bloqueio dentro da banda passante dos filtros dos receptores e o bloqueio será eficiente (POISEL, 2004).

Dois efeitos particulares devem ser considerados em bloqueios por múltiplos tons em sistemas SFH: o primeiro quando um tom de bloqueio está localizado na mesma porção do espectro do sinal a ser bloqueado e um ou mais tons estão ocupando outras porções do espectro; e o segundo quando não há tons localizados na mesma porção do espectro do sinal a ser bloqueado. Para o primeiro caso, se o tom do bloqueador e o sinal estão no mesmo canal e com a mesma potência, então o receptor terá que decidir qual sinal será processado. No

segundo caso, o sucesso do bloqueio vai depender do nível de potência relativa entre o sinal e os tons de bloqueios. Quando a potência do bloqueador é maior que a potência do sinal no canal de comunicação, somente um tom de bloqueio no canal é necessário para realizar o bloqueio. Então um tom simples por canal pode ser a melhor escolha para bloquear o sistema.

Como no sistema FFH, o bloqueador seguidor tenta seguir o sinal SFH para tentar identificar como o sistema muda de frequência. Medições na interceptação da energia são feitas e suas características são extraídas para tentar correlacionar um salto com seu predecessor.

O desempenho do bloqueador seguidor depende do esquema a ser adotado. O que faz o bloqueio seguidor ser diferente para sistemas SFH e FFH pode ser explicado em função de dois fatores: o canal adjacente pode ser determinado por medições, portanto ele não é desconhecido; e diversos bits de dados são enviados por uma fatia de tempo. O sucesso do bloqueio do canal resulta em bloquear os bits de dados. Para o sistema FFH, os bits de dados são transmitidos por uma ou mais fatias de tempo.

No bloqueio seguidor com ruído o sinal pode cobrir um ou mais canais. No último caso, o desempenho do bloqueio é o mesmo para bloqueador PBN. No bloqueio seguidor por tom, quando tons não modulados são usados como forma de onda de bloqueio, assume-se que os tons são colocados dentro da banda passante dos filtros do receptor. Os tons não precisam estar exatamente na mesma frequência que os tons de dados para elevar eficazmente o nível de energia no canal.

O tempo e a habilidade para identificar precisamente o novo salto são fatores críticos pertencentes ao objetivo de interesse de bloqueador seguidor em sistemas SFH.

3.4 APLICAÇÃO DO BLOQUEADOR EM SISTEMAS DE COMUNICAÇÕES

3.4.1 CENÁRIO

Um exemplo genérico de um modelo de sistema de comunicações com sinais de bloqueio, usado como referência no presente trabalho, é ilustrado na FIG. 3.14 (ADAMY, 2003; ADAMY, 2004). O modelo representa um sistema de comunicação com seu respectivo transmissor e receptor. São consideradas as seguintes variáveis: potência (P_T) de transmissão do sinal de comunicação, ganho (G_R) da antena receptora, ganho (G_T) da antena transmissora, ganho (G_J) da antena do bloqueador, potência (P_R) recebida, potência (P_J) do sinal de

bloqueio, ganho (G_{RJ}) da antena receptora na direção do bloqueador, distância (R_{JR}) entre o bloqueador e o receptor, e distância (R_{TR}) entre o transmissor e o receptor.

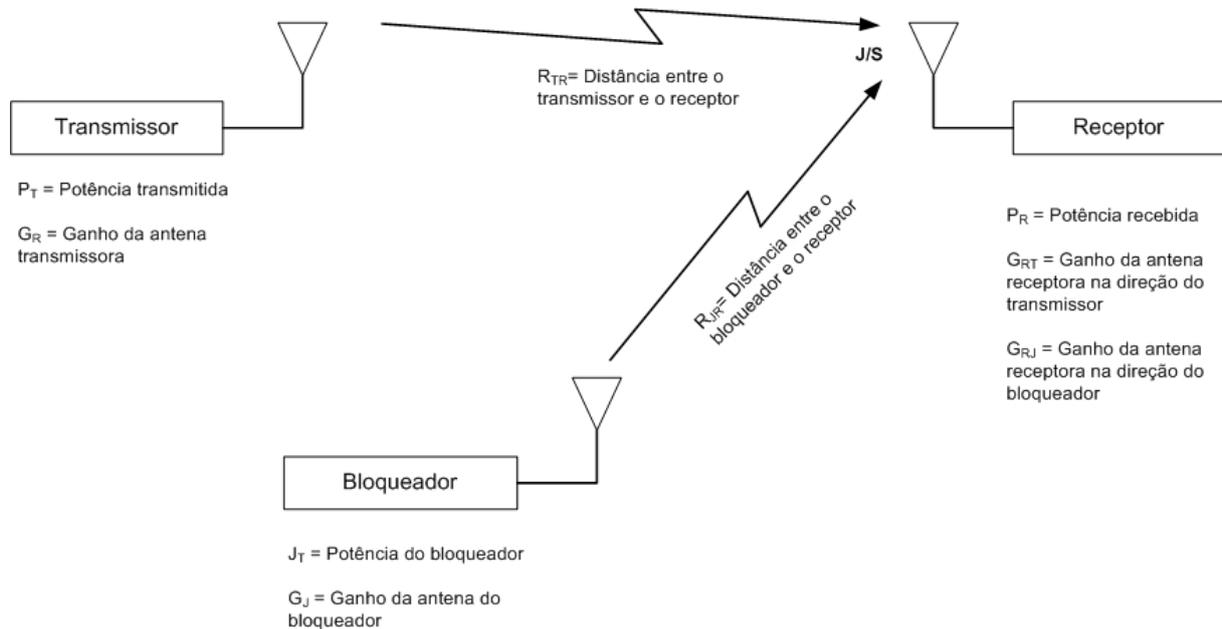


FIG. 3.14 - Modelo de um sistema de comunicação na presença de um bloqueador.

3.4.2 EQUAÇÃO BÁSICA DOS BLOQUEADORES

Mesmo sem a presença de uma fonte de bloqueio atuante sobre um determinado sistema de comunicação, todo sinal transmitido sofre diversos tipos de perturbações, caracterizando assim, uma relação sinal-ruído SNR_i na entrada do receptor do sistema:

$$SNR_i = \frac{S_i}{N_i} \quad (3.1)$$

onde S_i é a potência de entrada do sinal e N_i é o ruído de entrada na banda de operação do sistema.

Na presença de um sinal de bloqueio (ruído banda larga), a EQ. 3.1 passa a ser expressa por (GIT, 2001):

$$SNR_i = \frac{S_i}{N_i + J} \quad (3.2)$$

onde J é a potência de sinal interferente na entrada do receptor do sistema.

O valor de N_i aparece somado ao valor de J . Considerando apenas os sinais gerados intencionalmente, o valor de N_i é retirado da EQ. 3.2, que passa a ser expressa por S_i/J ou alternativamente por J/S_i , visto que o interesse é verificar a relação da potência do sinal interferente J sobre a potência do sinal do sistema S_i na entrada do receptor. No presente trabalho, a relação J/S_i será expressa simplesmente por J/S .

Considerando que os sinais que compõem a relação J/S são inseridos no espectro por fontes distintas, cada um possui os seus respectivos parâmetros de irradiação de energia eletromagnética. Geralmente, as variáveis de um sistema utilizadas para o cálculo da potência recebida por um receptor em função da distância são a potência de transmissão, o ganho da antena transmissora, o ganho da antena receptora, a frequência de transmissão, a distância do enlace e o fator relacionado a perdas de implementação do próprio sistema.

O cálculo da relação J/S segue o mesmo princípio do cálculo de um enlace de rádio. Pelo modelo proposto na FIG. 3.14 e assumindo propagação no espaço livre, tal relação pode ser escrita como (ADAMY, 2003; ADAMY, 2004):

$$\frac{J}{S} = \frac{P_J G_J G_{RJ} R_{TR}^2}{P_T G_T G_R R_{JR}^2}, \text{ onde} \quad (3.3)$$

onde $J = P_J - 32 - 20\log(f) - 20\log(R_{TR}) + G_J + G_{RJ}$, $S = P_T - 32 - 20\log(f) - 20\log(R_{JR}) + G_T$, P_J é a potência do sinal de bloqueio, P_T a potência de transmissão, G_{RJ} o ganho da antena do receptor na direção do bloqueador, G_R o ganho da antena receptora, G_T o ganho da antena transmissora, G_J o ganho da antena do bloqueador, R_{JR} a distância entre o bloqueador e o receptor, R_{TR} a distância entre o bloqueador e o receptor e f é a frequência de operação do sistema.

3.4.3 EQUAÇÃO BÁSICA PARA AVALIAÇÃO DE SISTEMAS ANALÓGICOS

Um parâmetro importante relacionado à medida da fidelidade de um sistema de comunicação analógico é a relação sinal-ruído (*SNR – Signal to Noise Ratio*). Para encontrar a relação sinal-ruído na entrada de um receptor que utiliza a técnica de modulação AMDSB com demodulador coerente⁷ foi montado o diagrama em blocos da FIG. 3.15, que ilustra o caminho percorrido por um sinal no sistema AMDSB.

⁷ Um demodulador coerente é aquele que utiliza um processo de detecção coerente. Este processo consiste em multiplicar o sinal modulado por um sinal de mesma frequência e fase do sinal modulado. Para tal, o oscilador local do sinal de demodulação deve estar sincronizado com o sinal modulado.

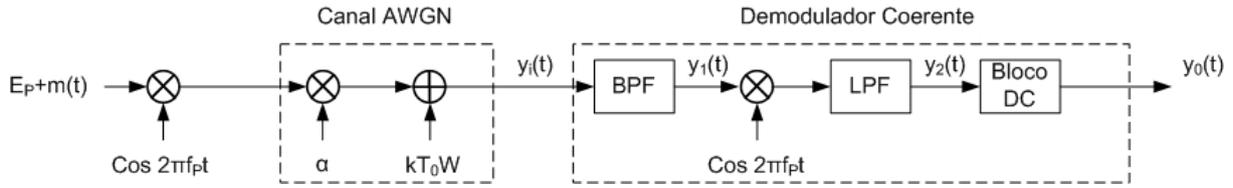


FIG. 3.15 - Diagrama de blocos de um sistema com modulação AMDSB.

Os valores para a potência transmitida (P_T) e a potência na entrada do receptor (P_{Ri}) são definidos, respectivamente, por:

$$P_T = \frac{E_p^2 + P_m}{2} = P_{AMDSB} \quad (3.4)$$

onde $P_m = \frac{m^2 E_p^2}{2}$.

$$P_{R,i} = \alpha_i^2 P_T = \frac{\alpha_i^2 E_p^2 P_m}{2} \quad (3.5)$$

Então a relação sinal-ruído na entrada do receptor passa a ser definida por:

$$SNR_i = \frac{P_{R,i}}{kT_0W} \quad (3.6)$$

Retirando-se o canal AWGN e inserindo um somador com um sinal de bloqueio em uma das entradas, tem-se a configuração da FIG. 3.16.

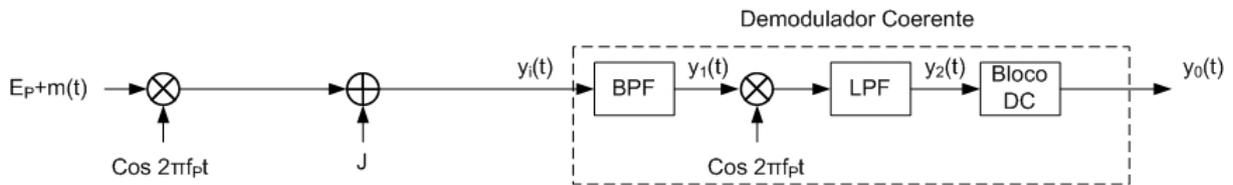


FIG. 3.16 - Diagrama de blocos de um sistema com modulação AM e bloqueador.

A relação sinal-ruído para um sistema com modulação AMDSB na entrada do receptor passa a ser definida por:

$$SNR = \frac{P_{R,i}}{J} \quad (3.7)$$

onde P_T é o valor da potência transmitida e J é o valor da potência transmitida pelo bloqueador.

3.4.4 EQUAÇÃO BÁSICA PARA AVALIAÇÃO DE SISTEMAS DIGITAIS

Para os sistemas que utilizam o espalhamento espectral, a relação J/S necessária para efetuar o bloqueio não pode ser definida diretamente pela SNR_i mínima de operação do sistema, devido à robustez inerente do sistema a interferências. Esta robustez pode ser traduzida por um parâmetro do sistema conhecido como ganho de processamento (G_P). Para sistemas DSSS, o G_P é dado por (GOODMAN, 1997):

$$G_P = \frac{T_b}{T_c} = \frac{R_c}{R_b} \quad (3.8)$$

onde T_B é a duração de bit, T_C é a duração do chip, R_c é a taxa de espalhamento em chips por segundo (ch/s) e R_b é a taxa de informação da fonte em bits por segundo (bps).

Para sistemas que operam com o salto em frequência, o ganho de processamento é uma função direta do número de canais de salto nos quais a informação é transmitida. Neste tipo de espalhamento espectral, o ganho de processamento é dado por (LEE, 1995):

$$G_P = \frac{WN}{R_b} \quad (3.9)$$

onde W é a largura de banda utilizada para o envio dos bits de informação através de um único canal, e N é o número de canais de frequências disponíveis para o salto. Cada canal tem a mesma largura W . Assumindo que W é aproximadamente igual à R_b , G_P fica dado por N .

Quando existe ganho de processamento, a relação bloqueio-sinal mínima (J/S_{min}) na entrada do receptor é definida pelo parâmetro Margem de Bloqueio (M_J), dado por (STAHLBERG, 2000):

$$M_J = G_P (dB) - (E_b / N_0)_{(REQ)} (dB) - L (dB) \quad (3.10)$$

onde $(E_b/N_0)_{(REQ)}$ é a relação entre a energia de bit e a densidade espectral de potência de ruído requerida pelo demodulador do sistema para um determinado valor de taxa de erro de bits (BER) típico, e L é a perda de implementação do próprio sistema (quando existente).

4 IMPLEMENTAÇÃO DOS SISTEMAS

O presente Capítulo tem o propósito de verificar a funcionalidade da modulação AM, como laboratório inicial de estudo, sinais de bloqueio e sistemas de comunicações comerciais e militares. Todas as simulações são realizadas através da ferramenta computacional *Simulink* do MatLab 7.0.

O *Simulink* opera com diagramas em blocos que simulam circuitos e possui uma vasta biblioteca de sistemas de engenharia. Em geral, é possível alterar as características desses blocos conforme a necessidade da simulação em questão.

Os modelos implementados nesse capítulo (modulação AM, dispositivos bloqueadores, sistemas CDMA e GSM e a norma MIL-STD-188-110B) são utilizados no Capítulo 5 para determinar até que nível de interferência um sistema é capaz de manter as suas características na presença de um dispositivo bloqueador.

4.1 IMPLEMENTAÇÃO DA MODULAÇÃO AM-DSB

Um sistema de radiodifusão comercial de áudio, que utiliza a técnica de modulação AMDSB, trabalha na faixa de 530 kHz a 1600 kHz. Segundo o teorema de Nyquist, a amostragem de um sinal limitado em frequência requer uma taxa de amostragem maior ou igual a duas vezes a frequência mais alta do sistema, garantindo a sua total reconstrução sem distorção (LI, 2007). Se a frequência de amostragem for menor que o dobro da maior frequência analógica do sinal, um fenômeno conhecido como *aliasing* ocorre e o sinal original não pode ser recuperado. Assumindo um sinal AM com portadora $c(t)$ em 800 kHz e sinal modulante de 5 kHz, o sistema necessitaria de uma frequência de amostragem maior que 1600 kHz, isto considerando todos os sinais de interesse dentro da primeira zona de Nyquist. A FIG. 4.1a ilustra este caso, onde a banda hachurada representa a primeira zona de Nyquist. Na recomposição do sinal, imagens da banda original de frequências aparecem em cada uma das outras zonas de Nyquist.

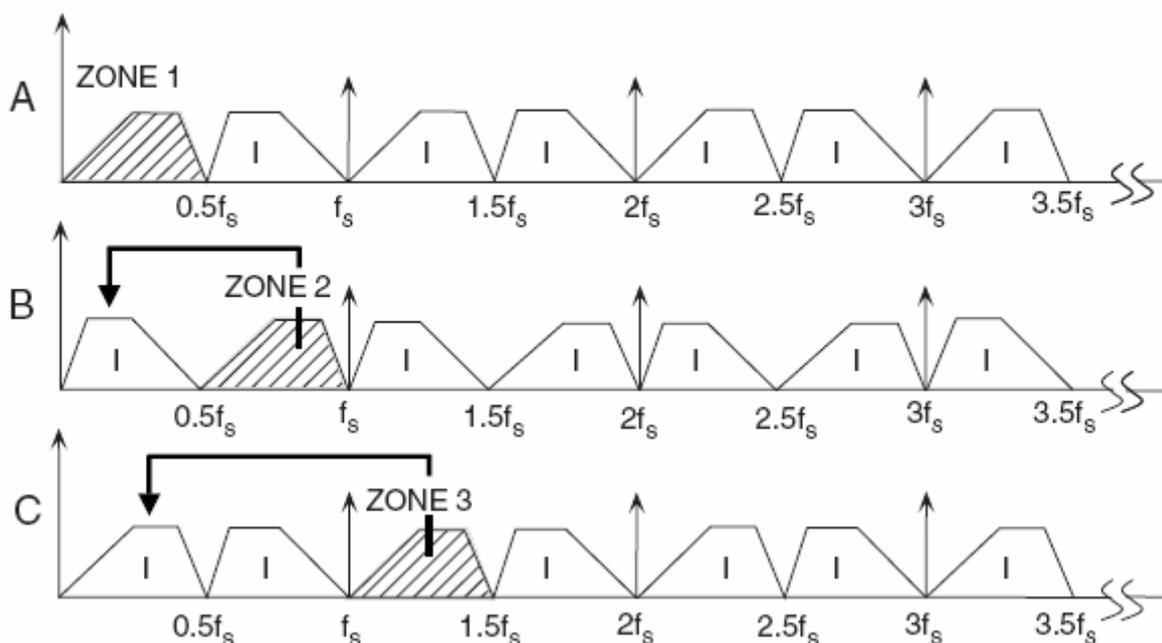


FIG. 4.1 - Sub-Amostragem e translação de frequências entre as zonas de Nyquist

O processo de amostrar um sinal fora da primeira zona de Nyquist é frequentemente referido como sub-amostragem, ou amostragem harmônica. Considere o caso da FIG. 4.1b, onde a banda amostrada do sinal encontra-se inteiramente dentro da segunda zona de Nyquist. O sinal é amostrado com a mesma taxa utilizada no caso da FIG. 4.1a. Na recomposição do sinal, as imagens que aparecem na primeira zona de Nyquist contêm toda a informação do sinal original, com exceção da ordem dos componentes de frequências do espectro, a qual é invertida (o que pode ser facilmente corrigido reordenando-se a saída da transformada de *Fourier*).

A FIG. 4.1c apresenta um sinal amostrado restrito à terceira zona de Nyquist. Note que a imagem na primeira zona de Nyquist não possui frequências reversas. De fato, as frequências do sinal a ser amostrado podem estar unicamente em qualquer zona de Nyquist, sendo que a imagem surgida na primeira zona de Nyquist ainda será uma representação precisa do sinal (com exceção de frequências que podem ocorrer na ordem reversa quando o sinal está localizado em zonas pares de Nyquist). Neste ponto, pode-se claramente restabelecer o critério de Nyquist da seguinte forma: um sinal deve ser amostrado em uma taxa igual ou superior a duas vezes a sua largura de banda para que se preserve toda a informação (LOPES, 2006).

Para o exemplo citado, o sinal AM-DSB com sinal modulante $M(t)$ de 5 kHz, largura de banda de 10 kHz, e portadora $C(t)$ em 800 kHz necessita de uma frequência de amostragem de 20 kHz, utilizando o teorema da sub-amostragem.

A FIG. 4.2 apresenta o modelo do sistema com modulação em amplitude, seguindo o que foi descrito no item 2.1.1.1, para análise do processo de sub-amostragem. A FIG. 4.3a mostra o espectro de amplitude do sinal gerado.

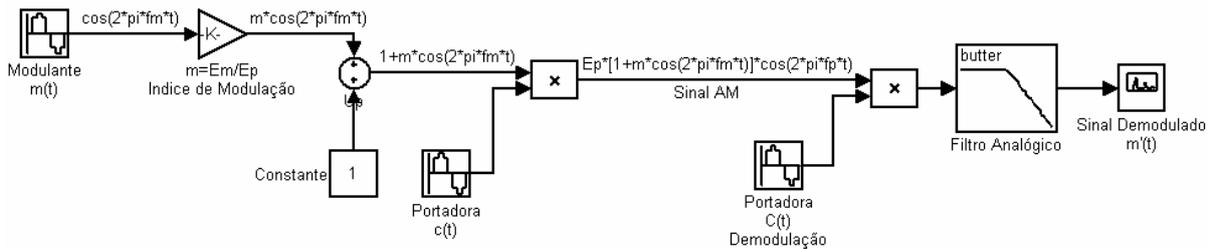


FIG. 4.2 - Diagrama do modificador e receptor AM-DSB.

Simulando o modelo proposto da FIG. 4.2 para $E_m = E_p = 1$, encontra-se pela EQ. 2.3 o valor da potência do sinal modulado AM-DSB, que é igual a 0,75 W. A FIG. 4.3b ilustra este caso, somando os picos de potência.

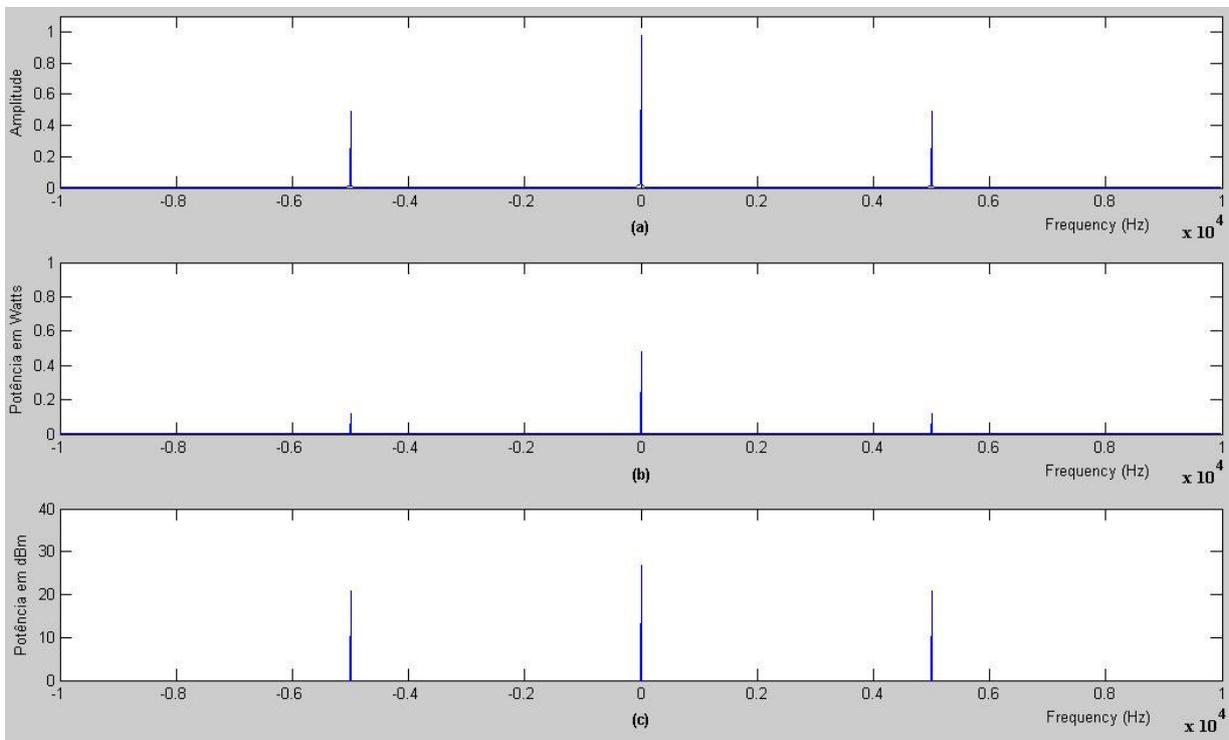


FIG. 4.3 - Espectro do sinal AM utilizando o teorema de sub-amostragem. (a) Amplitude do Sinal AM, (b) Potência do Sinal AM em Watts e (c) Potência do Sinal AM em dBm

Simulando o mesmo modelo proposto para $E_m = 1$, $E_p = 2$ e $m = 0.5$, tem-se o resultado da FIG. 4.4.

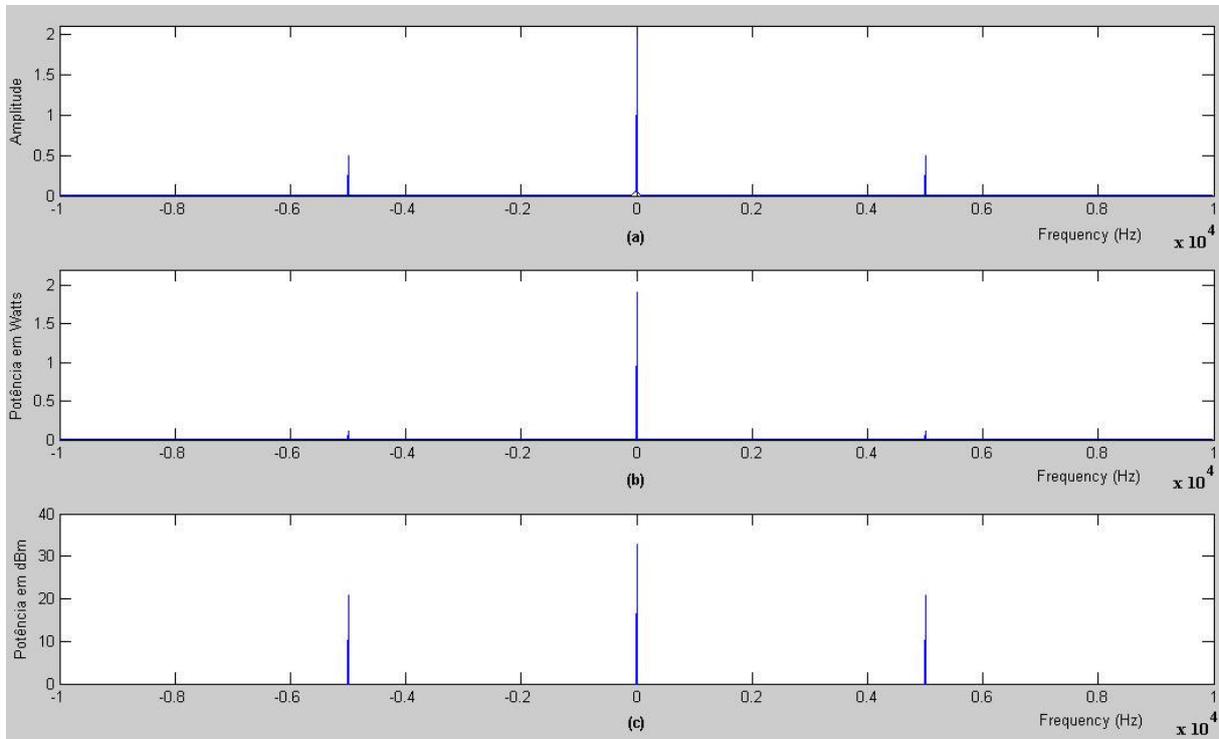


FIG. 4.4 - Espectro do sinal AM utilizando o teorema de sub-amostragem. (a) Amplitude do Sinal AM, (b) Potência do Sinal AM em Watts e (c) Potência do Sinal AM em dBm

Pela EQ. 2.3, a potência total do sinal AM é igual a 2,25 W. Comparando com o valor encontrado na FIG. 4.4b, verifica-se que o resultado do valor da potência total, P_{AMDSB} , é o mesmo, comprovando que os resultados da simulação estão de acordo com a teoria.

A abordagem anterior foi necessária para certificação de que os resultados da simulação estariam em correspondência com os teóricos, uma vez que algumas rotinas do MatLab produzem saídas normalizadas, dificultando a interpretação de seu significado físico.

4.2 IMPLEMENTAÇÃO DOS BLOQUEADORES

As estratégias mais comuns para aplicação do bloqueio sobre um sistema de comunicações são implementadas a seguir, como: bloqueio por ruído, bloqueio por tom e bloqueio com varredura.

No bloqueio por ruído, um sinal aleatório é emitido no espectro. A intenção é perturbar a comunicação através da inserção desse sinal no receptor do sistema a ser interferido, na sua

banda de operação. O bloqueio com ruído pode ser realizado de três formas, como mencionado no Capítulo 3: BBN, PBN e NBN.

O primeiro tipo de bloqueio com ruído é definido por bloqueio em banda larga (BBN), onde o sinal de bloqueio é irradiado em todo o espectro de comunicação de interesse, cobrindo assim, várias frequências simultaneamente. A FIG. 4.5 apresenta a composição do dispositivo bloqueador BBN simulado.

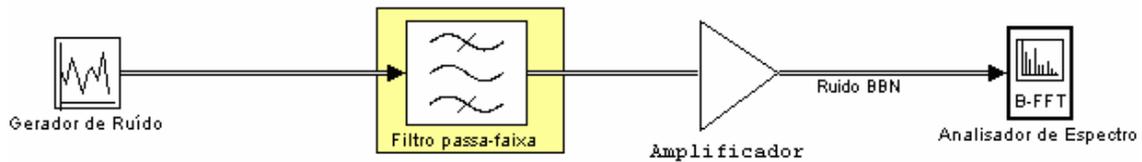


FIG. 4.5 - Diagrama do bloqueador BBN usado nas simulações.

O bloqueador BBN é composto de gerador de ruído banda larga, filtro passa-banda, que pode ser usado para ajustar a largura de banda de saída do ruído e amplificador, como detalhado no item 3.2.1. Foi utilizado um filtro de *Chebyshev* de quarta ordem. O analisador de espectro da FIG. 4.5 é usado para verificar o resultado da simulação. A FIG. 4.6 apresenta o resultado da simulação de um ruído banda larga com banda de 58 MHz, visto através do analisador de espectro em um determinado instante de tempo.

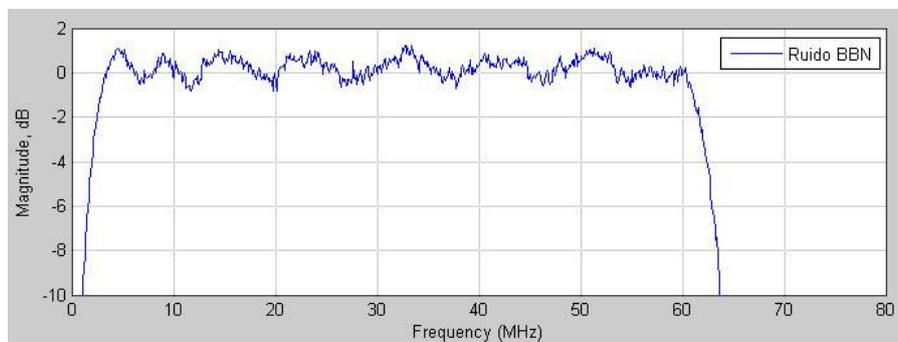


FIG. 4.6 - Sinal de saída do bloqueador BBN gerado pelo Simulink.

O segundo tipo de bloqueio com ruído é definido bloqueio com ruído em parte da banda (PBN), onde o sinal de bloqueio é inserido em múltiplos canais do espectro utilizados pelo sistema a ser interferido. A topologia FIG. 4.5 pode ser utilizada para implementar o dispositivo bloqueador PBN, bastando mudar a faixa de operação do filtro *Chebyshev*. O bloqueador PBN foi detalhado no item 3.2.1.

A FIG. 4.7 apresenta o sinal de ruído gerado pelo bloqueador PBN, visto através do analisador de espectro em um determinado instante de tempo. O filtro passa-banda foi sintonizado de 72 MHz a 78 MHz.

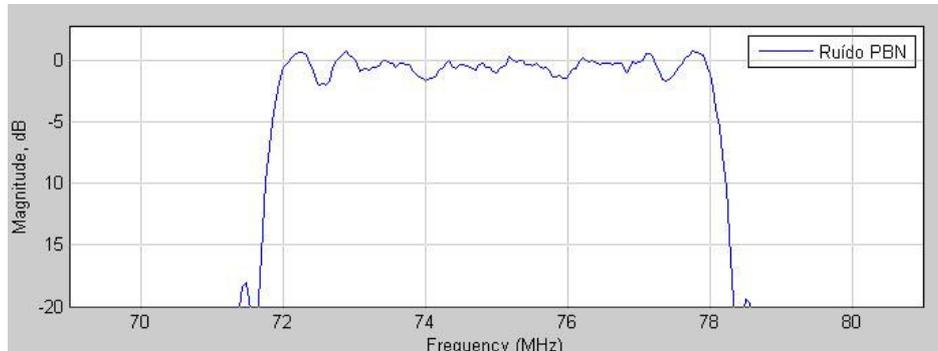


FIG. 4.7 - Sinal de saída do bloqueador PBN gerado pelo Simulink.

O terceiro tipo de bloqueio com ruído é o bloqueio com ruído em banda estreita (NBN), onde o sinal de bloqueio é inserido em um único canal do sistema. A topologia da FIG. 4.5 pode ser utilizada para implementar o dispositivo bloqueador PBN, para isto basta mudar a faixa de operação do filtro *Chebyshev*. O bloqueador NBN é similar ao bloqueador PBN. A diferença está no tipo de filtro utilizado. Para o bloqueador NBN simulado o filtro é um passa-faixa, configurado com largura de banda de 1 MHz. A FIG. 4.8 apresenta o ruído banda estreita gerado pelo bloqueador, visto através do analisador de espectro em um determinado instante de tempo.

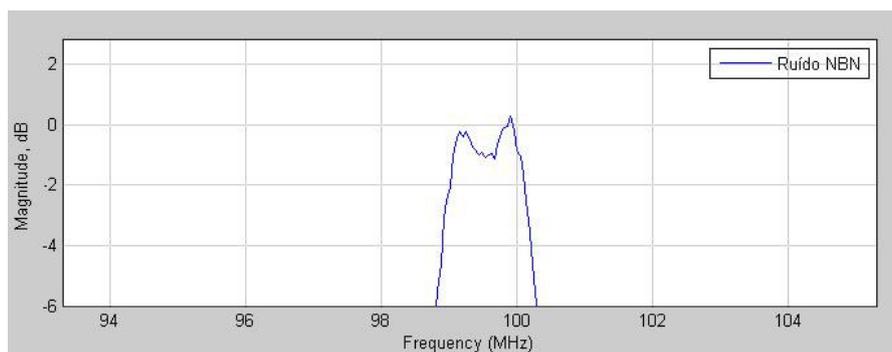


FIG. 4.8 - Sinal de saída do bloqueador NBN gerado pelo Simulink.

No bloqueio por tom, um ou mais sinais de tom são estrategicamente inseridos no espectro para provocar a condição de bloqueio. O bloqueio por tom pode ser realizado de duas formas, como mencionado no Capítulo 3, item 3.2.3. O primeiro tipo de bloqueio por tom é definido por bloqueio por tom simples, onde o sinal de bloqueio é inserido de forma contínua

em uma única frequência do espectro utilizado pelo sistema a ser interferido. A FIG. 4.9 apresenta a composição do dispositivo bloqueador por tom simples usado nas simulações. Apesar do VCO não ser necessário para este bloqueador, o dispositivo foi mantido para facilitar a implementação dos demais tipos de bloqueadores com uma única topologia de circuito no Simulink. Tal configuração permite ainda a fácil inserção de um ruído de banda estreita superposto ao sinal DC no bloqueador, se e quando necessário.

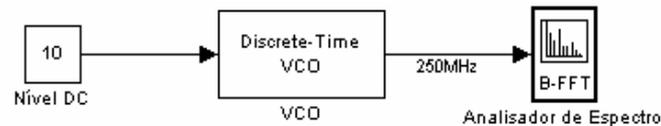


FIG. 4.9 - Diagrama do bloqueador por tom simples simulado.

Na forma mais elementar, como simulado, o bloqueador por tom simples é composto de um nível DC constante, que tem por finalidade manter fixa a frequência de saída do bloqueador. Na configuração da FIG. 4.9 o VCO também tem a finalidade de ajustar em que tom de frequência o bloqueador vai atuar. A FIG. 4.10 apresenta o sinal gerado pelo bloqueador, visto através do analisador de espectro do Simulink. O VCO foi sintonizado neste exemplo em 250 MHz.

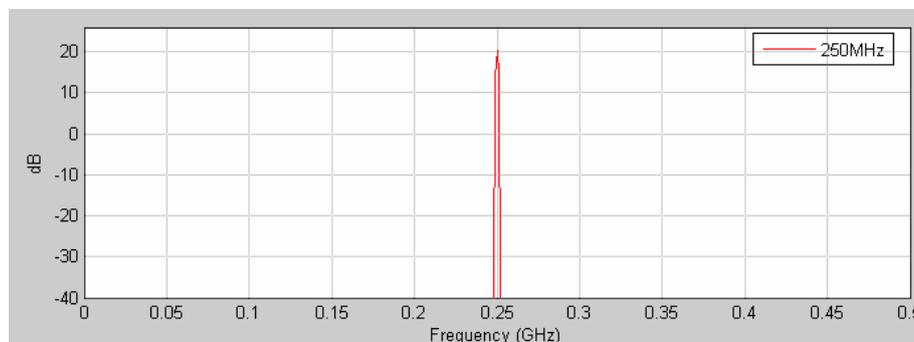


FIG. 4.10 - Sinal de saída do bloqueador por tom simples no Simulink.

O segundo tipo de bloqueio por tom é definido por bloqueio por tons múltiplos, onde múltiplos tons são inseridos no espectro de forma aleatória ou em frequências específicas. A FIG. 4.11 apresenta a composição do dispositivo bloqueador por tons múltiplos simulado neste trabalho, que é similar ao bloqueador por tom simples. Os valores dos tons são fixos e foram escolhidos apenas para a demonstração de um exemplo de funcionamento do dispositivo bloqueador. A diferença reside no uso de vários VCOs, sintonizados em frequências diferentes. Esse tipo de bloqueador pode se tornar economicamente inviável, visto que o custo de um VCO é alto. Na simulação foi utilizado o VCO por simplicidade de implementação e programação.

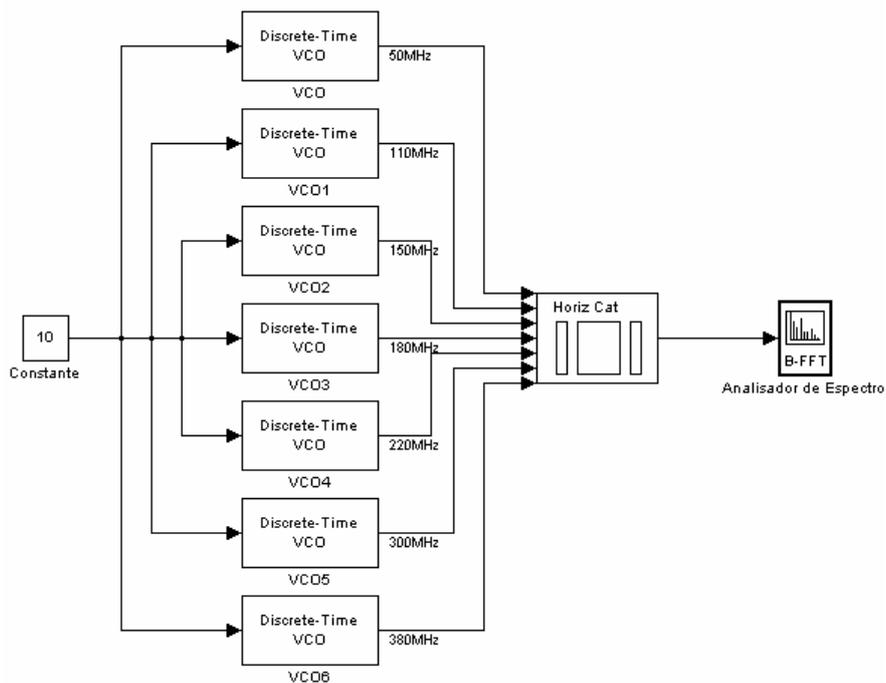


FIG. 4.11 - Diagrama do bloqueador por tons múltiplos simulado.

A FIG. 4.12 apresenta o sinal de saída gerado pelo bloqueador, visto através do analisador de espectro do Simulink. Os valores sintonizados nos VCOs são fixos e foram escolhidos apenas para ilustrar o funcionamento do dispositivo bloqueador simulado.

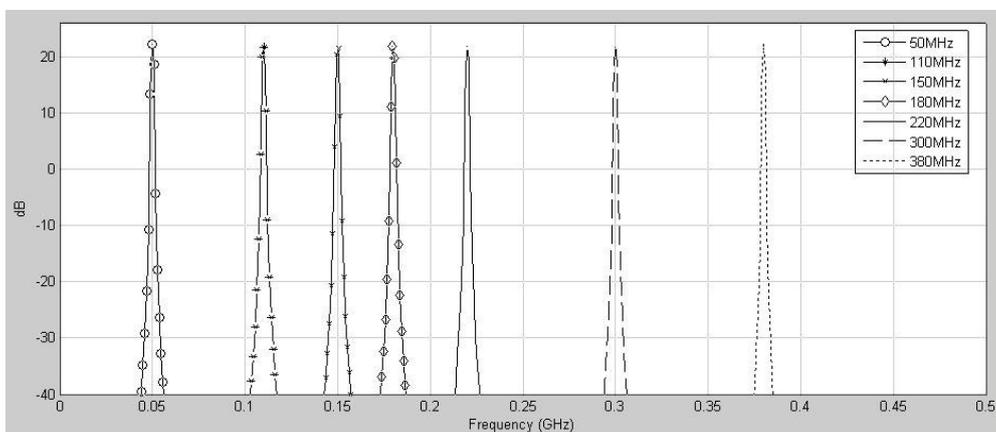


FIG. 4.12 - Sinal de saída do bloqueador por tons múltiplos no Simulink.

No bloqueio com varredura, o sinal de bloqueio é varrido no tempo ao longo da banda de frequências de interesse, como mencionado no 3.2.2. A cada instante de tempo, somente uma frequência específica e uma região estreita em torno dessa frequência estão ocupadas com o sinal de bloqueio. A FIG. 4.13 apresenta a composição do dispositivo bloqueador por varredura simulado, seguindo o que foi descrito no Capítulo 3.

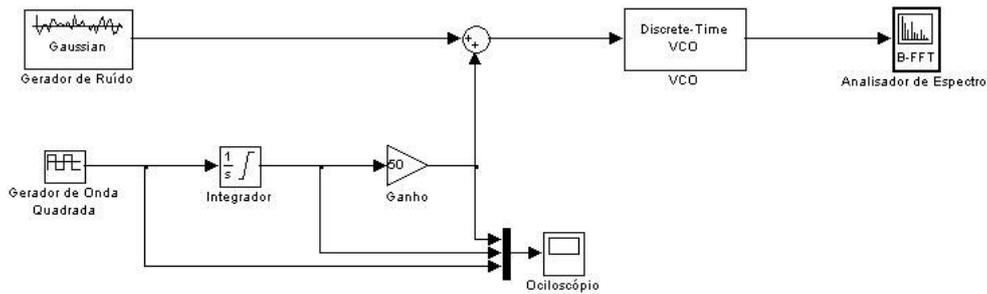


FIG. 4.13 - Diagrama do bloqueador por varredura simulado.

O bloqueador com varredura é composto de gerador de ruído Gaussiano, gerador de onda quadrada, integrador, que em conjunto com o gerador de onda quadrada gera um sinal variante no tempo do tipo onda triangular modulado com ruído, amplificador, somador e VCO, controlado pela onda triangular modulada com ruído.

A FIG. 4.14 apresenta o sinal gerado pelo bloqueador, visto através do analisador de espectro. O VCO foi sintonizado em 4 GHz, sendo este o ponto inicial de varredura do bloqueador. A FIG. 4.14a ilustra o início da varredura em 4 GHz, a FIG. 4.14b o sinal variando em frequência, a FIG. 4.14c o sinal alcançando a varredura máxima, de 8,5 GHz, e a FIG. 4.14d o sinal retornando ao seu ponto inicial de varredura.

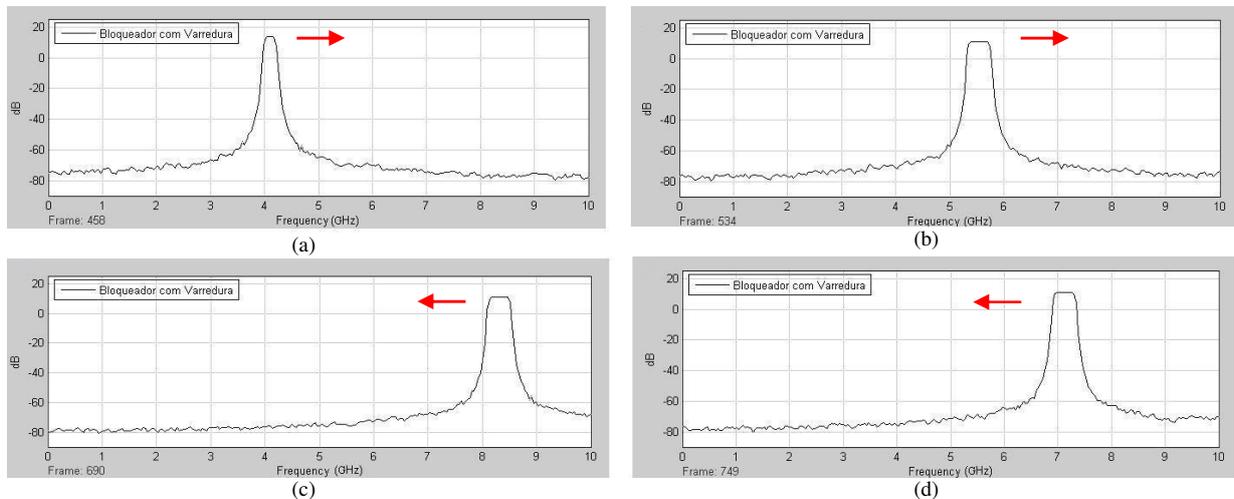


FIG. 4.14 - Bloqueador por varredura no Simulink mostrando (a) o início da varredura em 4GHz, (b) o sinal variando para 6GHz, (c) o sinal atingindo a varredura máxima e (d) o sinal retornando para varredura inicial.

4.3 IMPLEMENTAÇÃO DOS SISTEMAS DE COMUNICAÇÕES COMERCIAIS

4.3.1 IMPLEMENTAÇÃO DO SISTEMA CDMA

O Simulink do Matlab 7.0 possui uma biblioteca para o sistema CDMA onde pode-se encontrar um diagrama em blocos do canal direto de tráfego do CDMA, modelo ponto-a-

ponto, de acordo com a norma IS-95A, o qual é mostrado na FIG. 4.15. O sinal transmitido pelo sistema CDMA está ilustrado na FIG. 4.16, em um determinado instante de tempo.

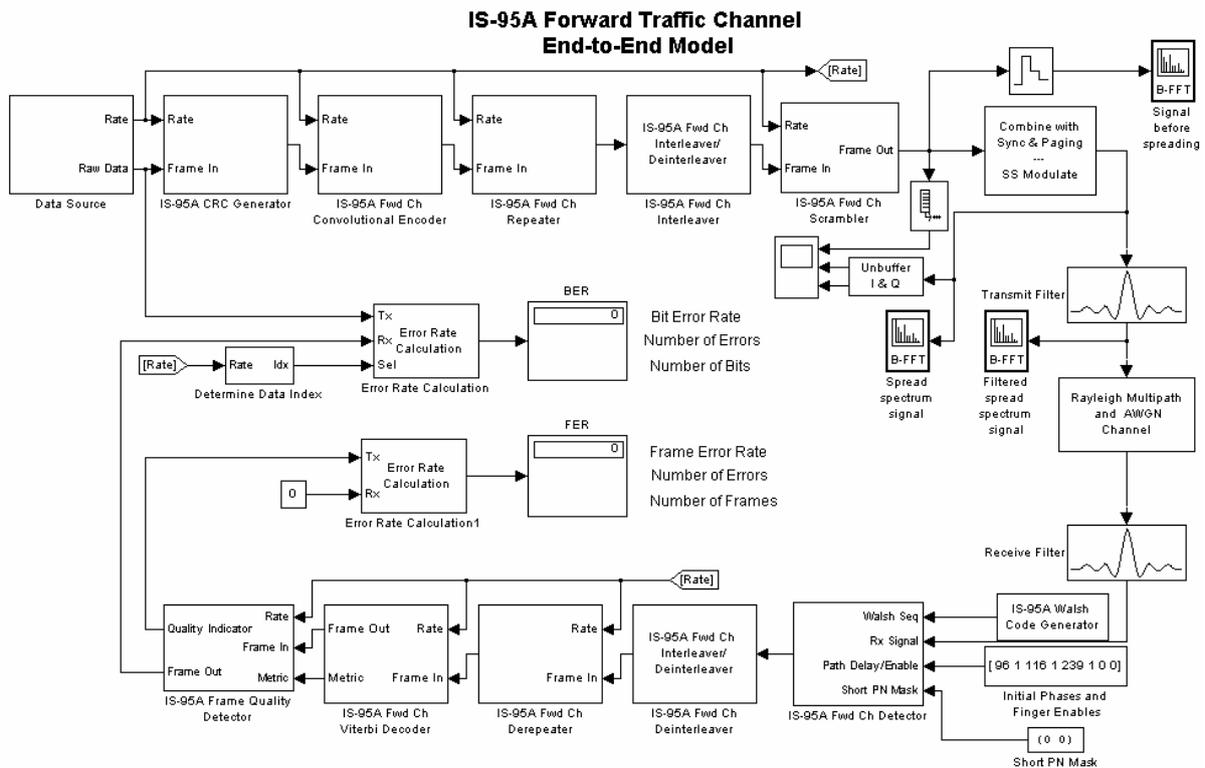


FIG. 4.15 - Canal direto de tráfego, modelo ponto-a-ponto, IS-95A, CDMA.

Simulando o digrama do sistema CDMA da figura, verificou-se que a BER se alterava pouco em todo tempo de simulação, permanecendo sempre abaixo do limite especificado para o sistema (10^{-3}), para as condições brandas do canal simulado.

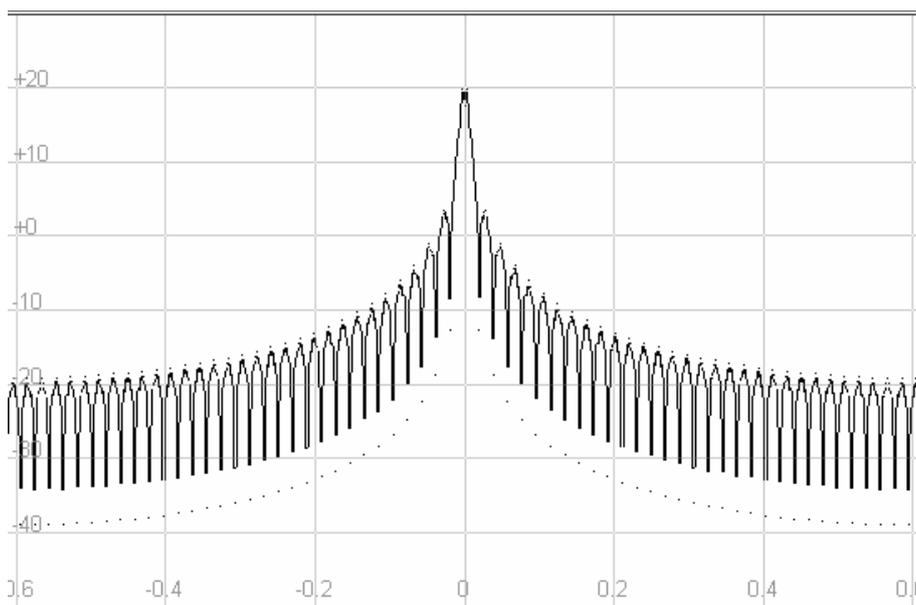


FIG. 4.16 - Sinal Transmitido pelo canal direto de tráfego, IS-95A, CDMA.

4.3.2 IMPLEMENTAÇÃO DO SISTEMA GSM

O modelo proposto de simulação para o GSM implementa a rajada (*burst*) de um canal de voz TCH.

O processo de codificação recebe o frame de voz não codificado de 260 bits e são separados em 50 bits da classe Ia, 132 bits da classe Ib e 78 bits não protegidos da classe II. Os bits são codificados e o Frame de voz é gerado com 456 bits de dados de conversação, como apresentado no Apêndice 1 e na FIG. 4.17.

Os bits codificados do Frame de voz passam pelo processo de *interleaving* e são divididos em 8 blocos de 57 bits codificadores.

Cada rajada do TCH transporta dois blocos de 57 bits codificadores de dados provenientes de dois segmentos diferentes dos 456 bits codificados.

Definições do canal de voz TCH e da rajada do GSM são apresentadas com maiores detalhes no Apêndice 1.

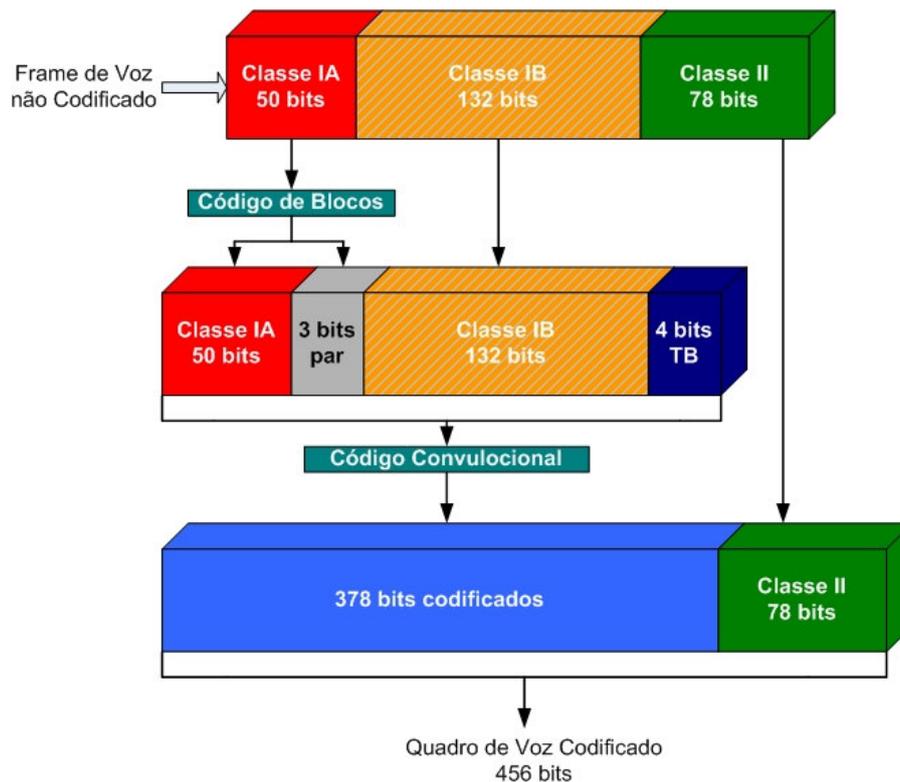


FIG. 4.17 - Processo de Codificação de Voz no GSM.

O modelo em blocos do sistema GSM implementado no simulink está exemplificado na FIG. 4.18. O sistema é composto de um bloco transmissor, um canal AWGN e um bloco receptor.

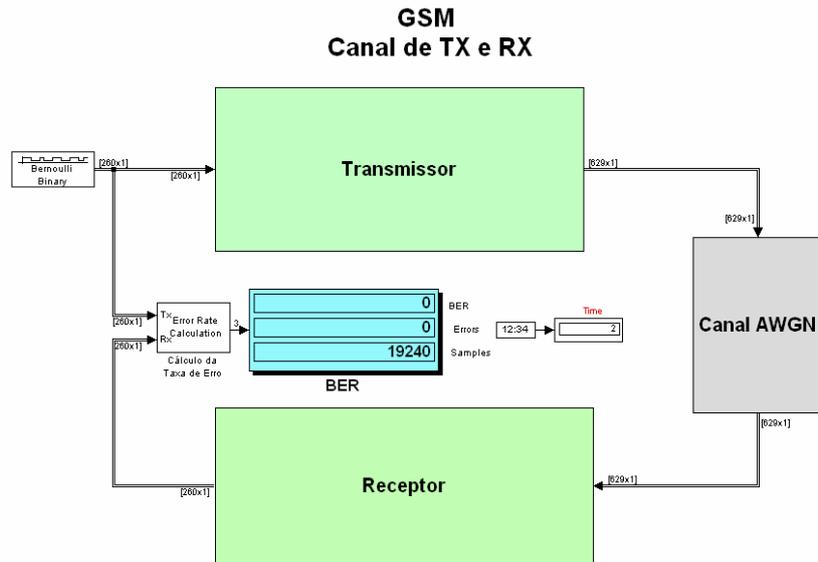


FIG. 4.18 - Canal de tráfego do sistema GSM.

O bloco transmissor é composto pelo bloco de codificação, que monta a rajada do GSM, e o bloco modulação, que modula o sinal utilizando a técnica GMSK, ambos mostrados na FIG. 4.19.

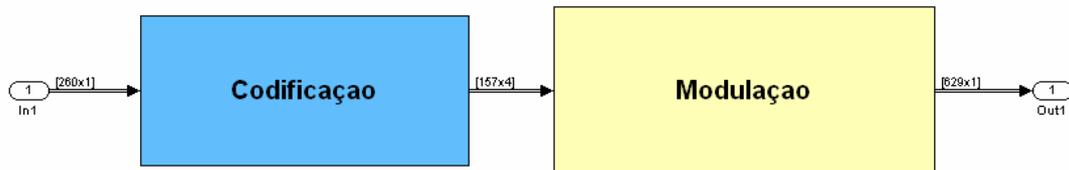


FIG. 4.19 - Bloco transmissor do GSM.

O bloco codificação tem como finalidade gerar a rajada do GSM a partir dos bits da classe Ia, classe Ib e classe II, como especificado anteriormente. FIG. 4.19 mostra o diagrama do processo de codificação utilizado nas simulações.

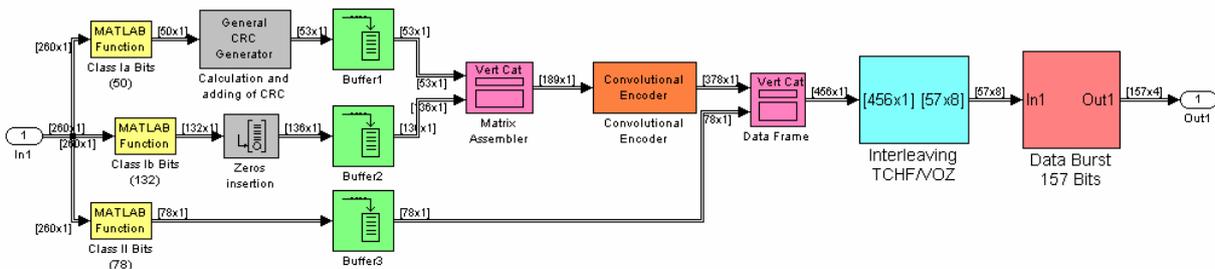


FIG. 4.20 - Diagrama do processo de codificação do GSM utilizado nas simulações.

O bloco modulação recebe a rajada do bloco de codificação e transmite o sinal utilizando a técnica GMSK. A FIG. 4.21 mostra este processo.

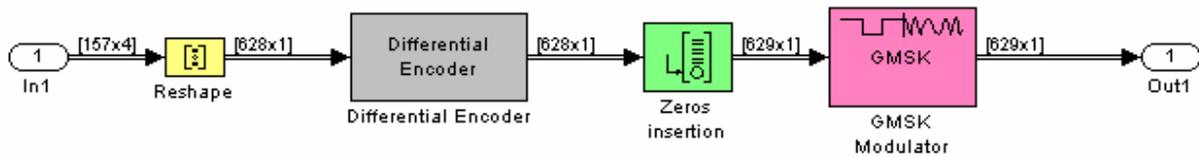


FIG. 4.21 - Diagrama do processo de modulação do GSM utilizado nas simulações.

O bloco receptor, mostrado na FIG. 4.22, processa o caminho inverso do sinal, o qual passa por um bloco de demodulação e um bloco de decodificação.

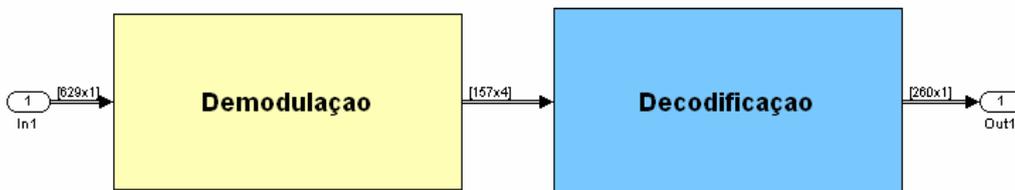


FIG. 4.22 - Bloco receptor do GSM.

Para verificar a eficácia do sistema proposto, foi inserido o bloco BER, que calcula a taxa de erro do sistema. Configurando o tempo de duração de 2 s e o número de amostras de 19.240, a BER permaneceu sempre abaixo do limite especificado para o sistema para as condições brandas do canal simulado. A FIG. 4.23 ilustra o espectro do sinal GSM transmitido em banda base, com modulação GMSK, em um determinado instante de tempo.

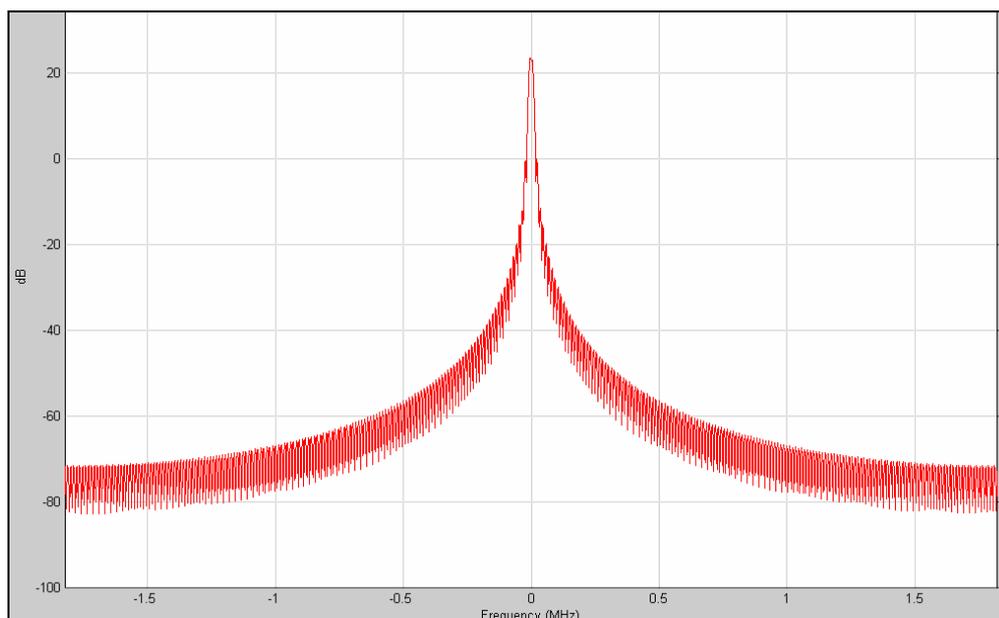


FIG. 4.23 - Espectro do sinal GSM transmitido com modulação GMSK.

4.4 IMPLEMENTAÇÃO DOS SISTEMAS MILITARES

4.4.1 IMPLEMENTAÇÃO DA NORMA MIL-STD-188-110B

Após a realização de algumas pesquisas e estudos foi encontrada na internet uma simulação da norma em questão. A simulação é um dos exemplos de bibliotecas do MatLab. O diagrama em blocos da norma MIL-STD-188-110B da biblioteca do MatLab está mostrado na FIG. 4.24. O Apêndice 2 detalha o funcionamento da norma Militar 188-110B.

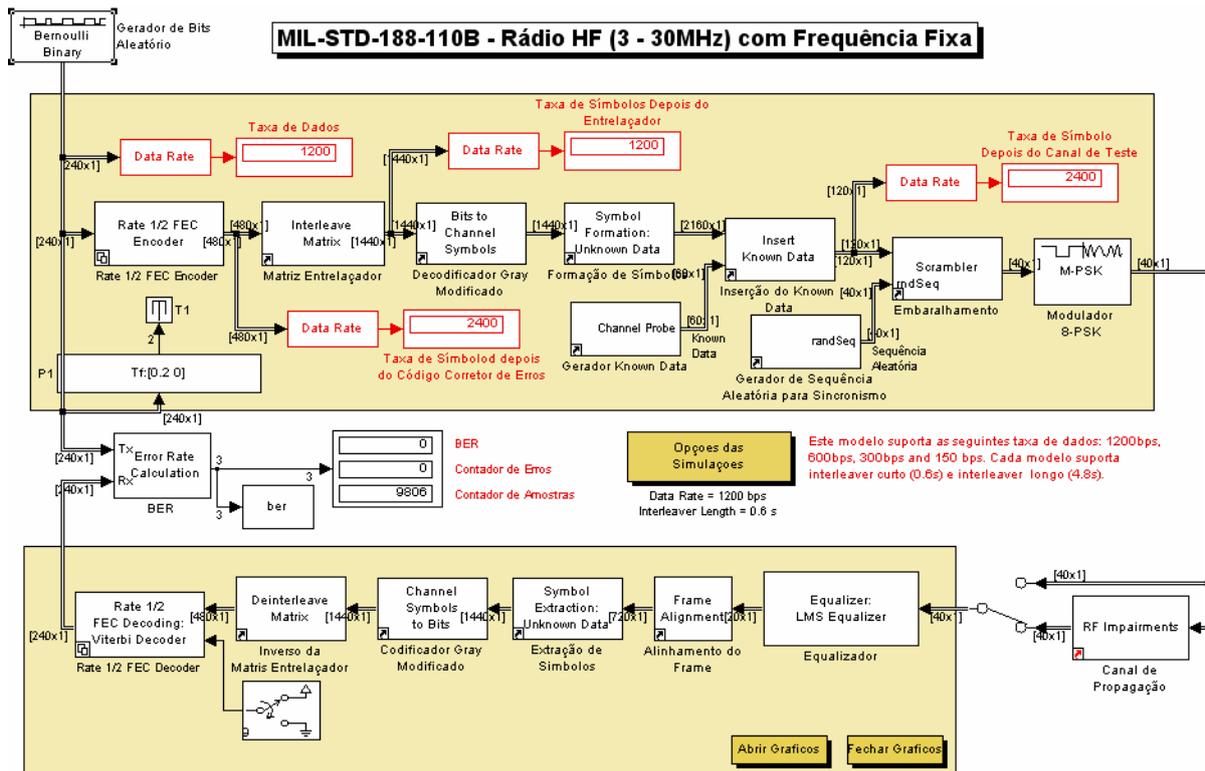


FIG. 4.24 - Canal de tráfego da norma MIL-STD-188-110B.

O modelo apresentado na FIG. 4.24 implementa a forma de onda serial, tom simples, Apêndice 2, e suporta as taxas de dados de 1200 bps, 600 bps, 300 bps e 150 bps. Cada taxa pode ser configurada para um entrelaçador curto de 0,6s ou um entrelaçador longo de 4,8s.

Conforme a norma, foi utilizada a modulação 8-PSK. A FIG. 4.25 ilustra o digrama da constelação do sinal transmitido, em um determinado instante de tempo.

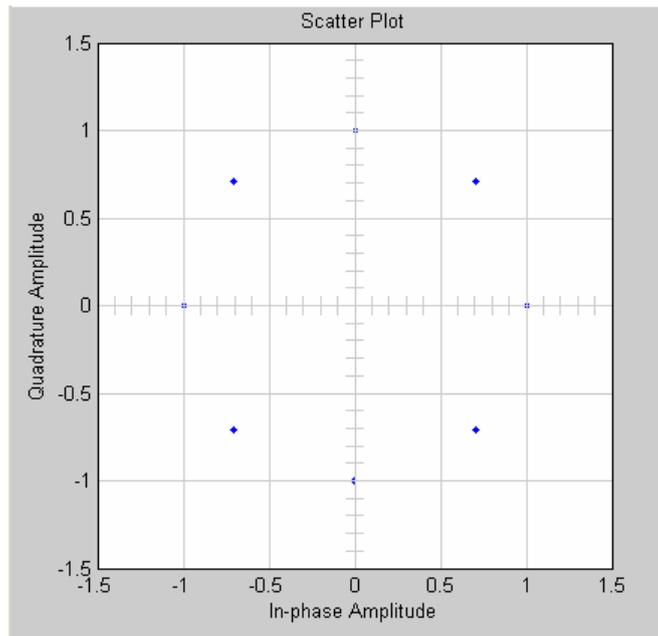


FIG. 4.25 - Constelação simulada do sinal transmitido utilizando a modulação 8-PSK.

A constelação dos símbolos do sinal transmitido, FIG. 4.25, está de acordo com o sinal especificado na norma, FIG. 9.7 do Apêndice 2, para a transmissão dos sinais com modulação 8-PSK.

5 EFETIVIDADE DOS BLOQUEADORES SOBRE ALGUNS SISTEMAS DE COMUNICAÇÕES

Este capítulo apresenta os resultados das simulações da modulação AM (item 4.1), dos sistemas CDMA (item 4.3.1) e GSM (item 4.3.2), e do sistema militar baseado na norma MIL-STD-188-110B (item 4.4.1) em conjunto com os dispositivos bloqueadores (item 4.2). O propósito das simulações é verificar a condição de geração de interferência sobre tais sistemas, ou seja, determinar até que nível de interferência o sistema é capaz de manter as suas características de funcionamento, sem perder qualidade.

Para o sistema com modulação AM, um valor para a relação sinal ruído correspondente à EQ. 2.10 é encontrado. Para os sistemas CDMA, GSM e os baseados na norma MIL-STD-188-110B, é determinada a correspondente relação J/S do sistema incluindo o conceito de margem de bloqueio.

Para os sistemas de comunicações GSM e o Padrão Militar STD-188 não foi implementada a técnica de espalhamento FHSS, ou seja, os sistemas operam sem saltos em frequência.

5.1 ESTRUTURA DAS SIMULAÇÕES

5.1.1 AVALIAÇÃO DA METODOLOGIA SOBRE A MODULAÇÃO EM AMPLITUDE

Inicialmente, a partir da montagem do diagrama em blocos do dispositivo bloqueador pontual com varredura, FIG. 4.13, e do sistema com modulação em amplitude, FIG. 3.15, usou-se um somador para inserção dos dois sinais na entrada do receptor do sistema. Para verificar o nível de bloqueio máximo, usou-se um sinal modulante de onda quadrada, monitorando-se o sistema pelo sinal demodulado, que idealmente deve reproduzir a onda quadrada do sinal modulante. Quando o sinal demodulado perde suas características, ou seja, a onda quadrada se aproxima de um nível constante (nível de ruído), o sistema pode ser considerado inoperante. A técnica é semelhante à análise da sensibilidade tangencial deste receptor. A FIG. 5.1 apresenta a composição do dispositivo bloqueador simulado em conjunto com o sistema de modulação em amplitude.

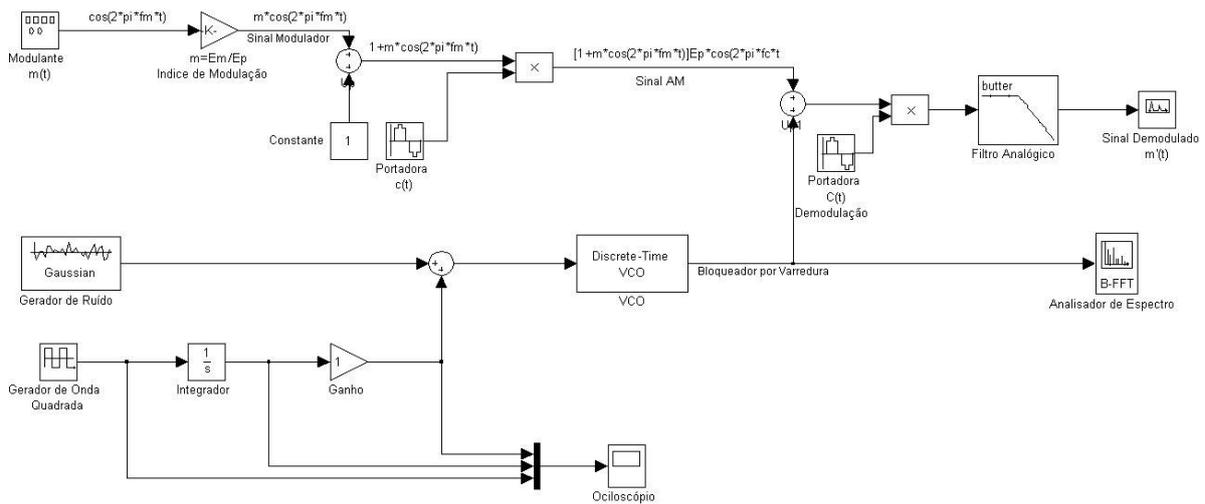


FIG. 5.1 - Diagrama do modulador por amplitude com bloqueador por varredura.

O sinal com modulação em amplitude tem largura de banda de 10 kHz, sinal modulante $m(t)$ de 5 kHz com amplitude igual a 1, portadora $c(t)$ em 800 kHz com amplitude igual a 1 e frequência de amostragem de 20 kHz. O sistema está transmitindo uma potência de 28,75 dBm.

O VCO foi sintonizado em 5 kHz, mesma frequência do sinal modulante, com amplitude inicial de 0,1 V. A potência de saída do bloqueador por varredura, calculada pelo valor médio quadrático, dado pela EQ. 5.1, vale 28,99 dBm, considerando uma resistência de carga R_L de 50Ω. Nestas condições, o bloqueador não afeta o sistema, como pode ser visto na FIG. 5.2.

$$J = \frac{AVCO^2}{2R_L} \quad [W] \quad (5.1)$$

onde $AVCO$ é a amplitude do sinal do VCO e R_L é a resistência de carga.

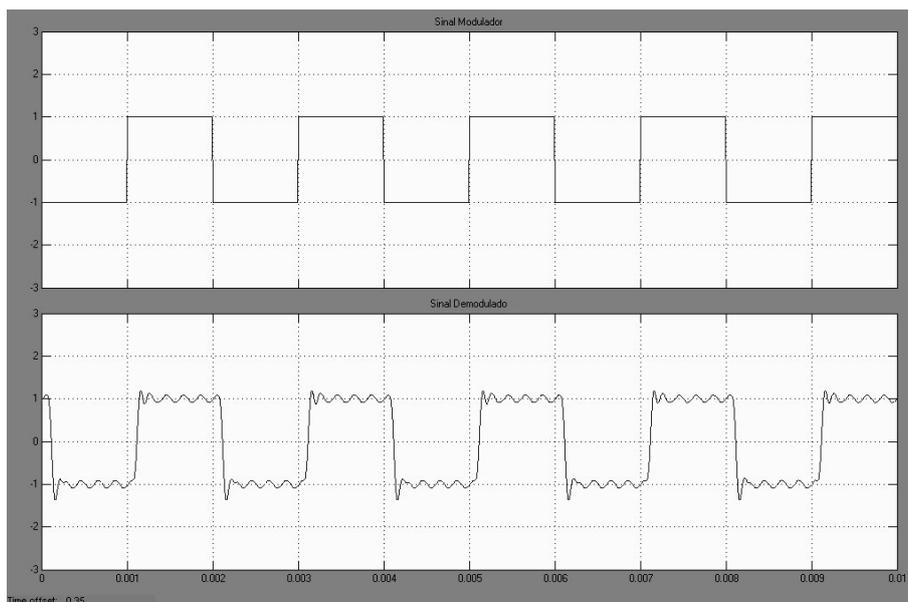


FIG. 5.2 - Sinal AM na presença do bloqueador por varredura, teste 1.

O nível de bloqueio foi aumentado, conforme a TAB. 5.1, e o nível de potência do sinal AM foi mantido sempre constante.

TAB. 5.1 - Potência de saída do bloqueador por varredura.

Teste	Amplitude VCO	J (dBm)
1	0,10	-10,00
2	0,30	-0,46
3	0,50	3,98
4	0,70	6,90
5	0,80	8,06
6	0,90	9,08
7	1,00	10,00
8	1,20	11,58
9	1,40	12,92
10	1,50	13,52

Com o nível de bloqueio configurado no teste 5 (TAB. 5.1), o sinal começou a perder as suas características, mas ainda guardando semelhança a uma onda quadrada, como mostrado na FIG. 5.3.



FIG. 5.3 - Sinal AM na presença do bloqueador por varredura, teste 5.

Para o nível de potência configurado no teste 10 (TAB. 5.1) e o nível de potência do sinal AM constante, o sinal perde as suas características, concluindo que com essa potência de bloqueio o sistema não funcionará adequadamente.

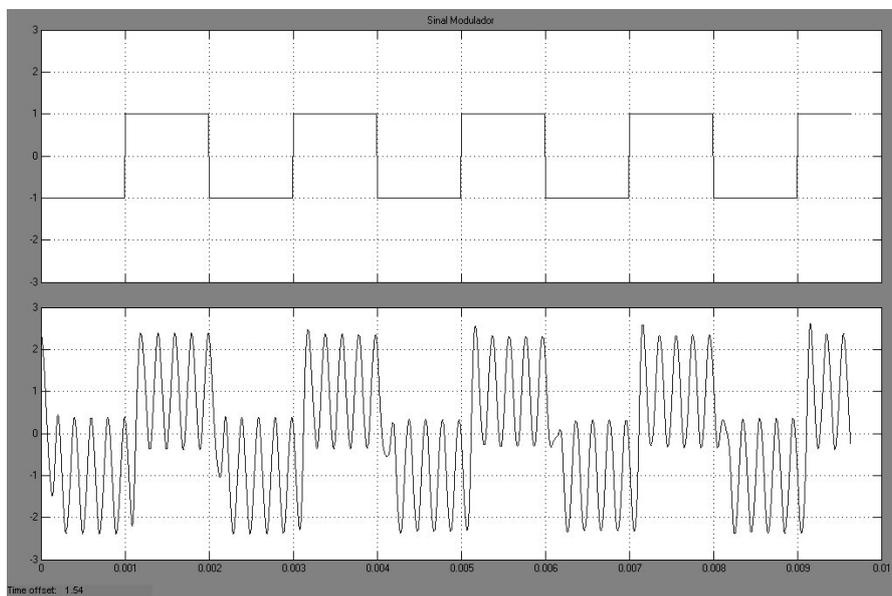


FIG. 5.4 - Sinal AM na presença do bloqueador por varredura, teste 10.

Com o valor da potência transmitida de um modulador AM e a potência de bloqueio, pela EQ. 3.8 determina-se o valor da relação sinal ruído, SNR, na entrada do receptor, TAB. 5.2. O valor limite para o sistema foi para $SNR = 15,23 \text{ dB}$.

TAB. 5.2 - Relação sinal ruído de um modulador AM na presença de um bloqueador por varredura.

Teste	Amplitude VCO	J (dBm)	SNR (dB)
1	0,10	-10,00	38,75
2	0,30	-0,46	29,21
3	0,50	3,98	24,77
4	0,70	6,90	21,85
5	0,80	8,06	20,69
6	0,90	9,08	19,67
7	1,00	10,00	18,75
8	1,20	11,58	17,17
9	1,40	12,92	15,83
10	1,50	13,52	15,23

5.2 ANÁLISE DA EFICÁCIA DOS BLOQUEADORES

5.2.1 NO SISTEMA CDMA

O sistema CDMA utiliza espalhamento espectral DSSS e, sendo assim, existe a condição de ganho de processamento. Considerando $R_c = 1228800$ ch/s e $R_b = 9600$ b/s, onde R_c é a taxa de chaveamento da portadora digital em chips por segundo (ch/s) e R_b é a taxa de informação da fonte em bits por segundo (bps) do sistema CDMA, chega-se ao valor do ganho de processamento G_p de 21 dB, através da EQ. 3.9.

Com G_p de 21 dB espera-se um valor de 18 dB para margem de bloqueio, considerando o sistema sem perdas de implementação ($L = 0$ dB), EQ. 3.11. Assim, o valor teórico mínimo da relação J/S é de 18 dB para que o sistema mantenha as suas características de funcionamento. Nesse caso, valores de J/S superiores a 18 dB devem ser suficientes para efetuar o bloqueio no CDMA.

No sistema CDMA implementado da FIG. 4.15, o bloco que representa o canal de comunicação foi substituído por um somador para a inserção do sinal de bloqueio no sistema. O canal de propagação foi retirado porque é considerado pior caso o sistema que tiver o canal de propagação ideal. Qualquer interferência gerada no canal de propagação só vai melhorar a condição de bloqueio no sistema. A FIG. 5.5 apresenta a composição do dispositivo bloqueador em conjunto com o modelo do canal de tráfego do sistema CDMA.

Para possibilitar uma maior linearidade nos resultados apresentados, o tempo de duração de cada evento de simulação ($T = 0,56$ s) e o total de bits transmitidos (13.268 bits) foram os mesmos em todos os eventos realizados no Sistema CDMA.

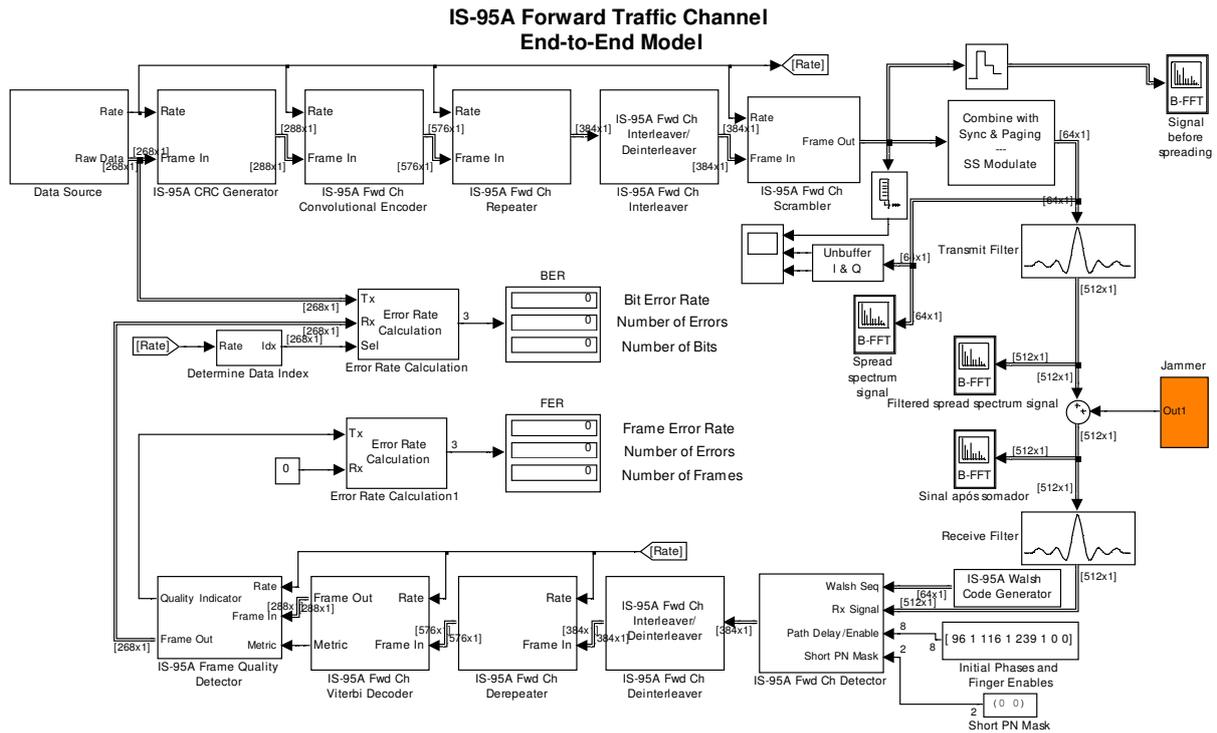


FIG. 5.5 - Canal de tráfego do sistema CDMA com bloqueador.

Alterando-se os valores de J e S na simulação, pode-se observar o comportamento da BER do sistema para definir diversos valores da relação J/S . O propósito desta simulação é verificar a partir de que ponto da relação J/S provoca a ocorrência de erro de bits que inviabilize o enlace entre transmissor e receptor.

Para o sistema CDMA com um bloqueador pontual (FIG. 4.9) no canal de comunicação (canal 283), o sistema apresentou o resultado ilustrado na FIG. 5.6.

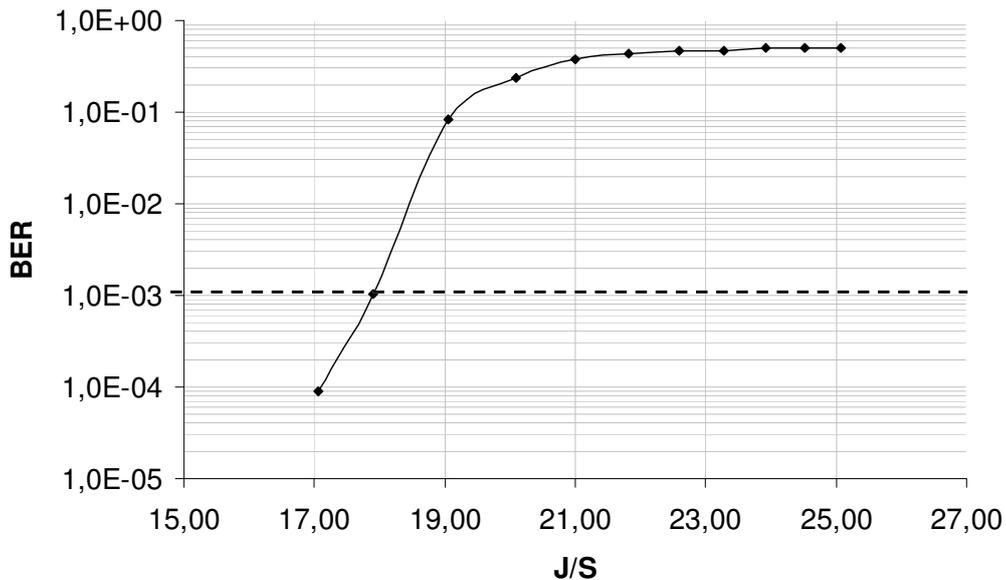


FIG. 5.6 - Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema CDMA com um bloqueador por tom no canal de controle do sistema.

Para valores de J/S menores que 17,7 dB o sistema indicou pouca ocorrência de erro de bits e quadros com erro e a BER ficou dentro do limite esperado, sendo a referência o valor de BER de 10^{-3} . Entretanto, a partir deste valor, a BER aumentou, caracterizando assim, uma degradação na qualidade do sinal imposta pela presença do bloqueador. O aumento da quantidade de bits errados acompanhou diretamente o aumento da relação J/S . Para valores maiores de J/S , acima de 24 dB, por exemplo, o valor da BER se aproximou de 0,5, em virtude de os bits 0 e 1 terem probabilidade iguais para ocorrência de erros de leitura no demodulador do sistema (probabilidade de 0,5).

Utilizando o mesmo modelo da FIG. 5.5, mas agora com um bloqueador parte da banda (FIG. 4.5), cobrindo uma faixa de 23 MHz, configurado na banda do canal reverso do sistema CDMA, o sistema apresentou o resultado ilustrado na FIG. 5.7.

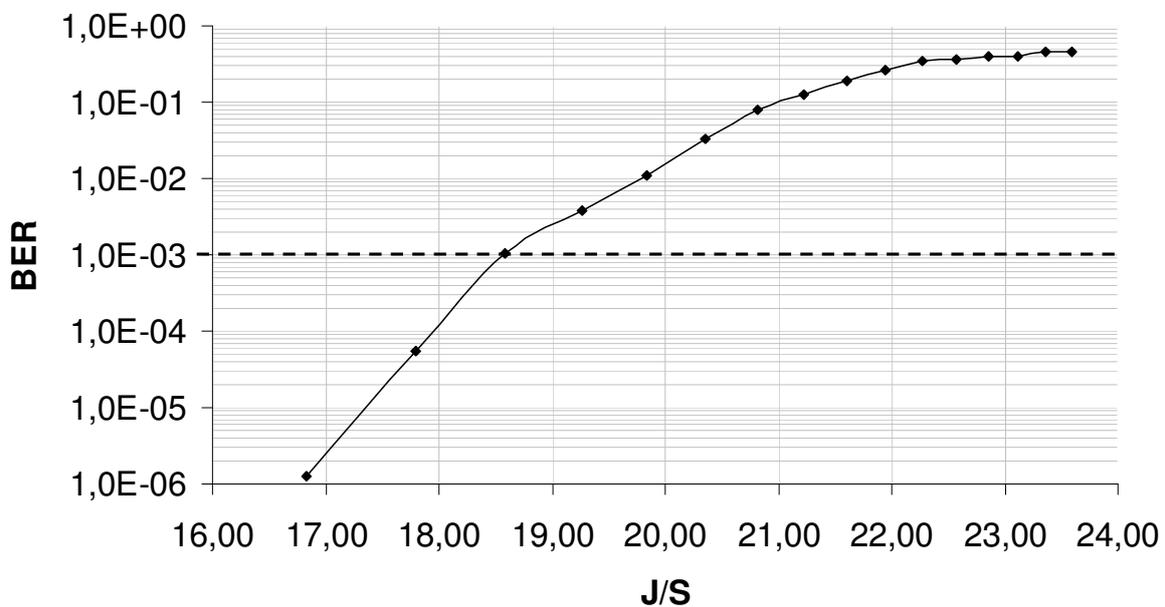


FIG. 5.7 - Relação entre a BER e a razão J/S no receptor do sistema CDMA com um bloqueador PBN em toda a banda do canal reverso do sistema.

Para valores de J/S menores que 18,4 dB, o sistema não indicou a ocorrência de bits e quadros com erro e a BER ficou dentro do limite esperado para o sistema CDMA. Entretanto, a partir de 18,4 dB, a BER aumentou, caracterizando assim, uma degradação na qualidade do sinal imposta pela presença do bloqueador. O sistema com bloqueador PBN apresentou o comportamento similar ao sistema com bloqueador pontual. Isso era esperado porque o bloqueador PBN atua em toda a banda do canal reverso, e conseqüentemente o canal de comunicação utilizado pelo sistema é bloqueado.

O terceiro passo foi implementar o mesmo modelo proposto da FIG. 5.5, mas com um bloqueador com varredura (FIG. 4.13). O objetivo dessa simulação é variar a frequência de varredura do bloqueador e verificar como o sistema se comporta para varredura lenta e varredura rápida.

Inicialmente o bloqueador foi configurado com uma varredura lenta, 20 Hz. Desta forma, o sinal de bloqueio interfere poucas vezes no canal de comunicação, porém causa uma degradação maior em cada vez que afeta o canal de comunicação. A velocidade de varredura do bloqueador foi incrementada para 400 Hz, 2 kHz e 20 kHz, conseqüentemente o sinal de bloqueio passa a interferir mais vezes no canal de comunicação. A FIG. 5.8 mostra a relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema CDMA com um bloqueador com varredura. O bloqueador foi configurado para varrer uma banda de 23 MHz, equivalente a banda de recepção do terminal móvel (824 a 847 MHz).

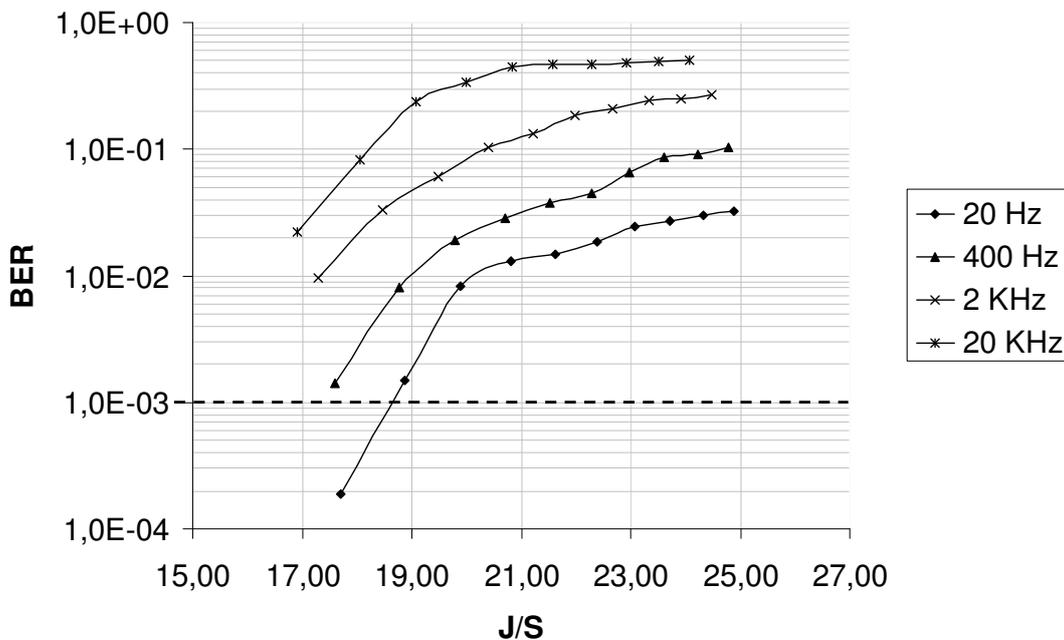


FIG. 5.8 - Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema CDMA com um bloqueador com varredura na banda de recepção do sistema móvel.

Para a varredura do bloqueador configurada em 20 Hz, com valores de J/S menores que 18,8 dB o sistema indicou pouca ocorrência de bits e quadros com erro e a BER ficou dentro do limite esperado para o sistema CDMA. Entretanto, a partir de 18,8 dB, a BER aumentou consideravelmente, caracterizando assim uma degradação da qualidade do sinal imposta pela presença do bloqueador. Para de J/S menor que 17,6 dB o sistema não indicou erro nas simulações e a BER permaneceu sempre nula.

Aumentado a varredura para 400 Hz, o sistema indicou ocorrência de bits e quadros com erro em quase todas as simulações. Para valores de J/S menores que 17,6 dB a BER não apresentou erro, permanecendo sempre em zero. A partir do valor de 17,6 dB, a BER aumentou e ficou na região de bloqueio em todas as simulações. Com o aumento do sinal de varredura o sistema apresenta uma degradação maior, comparado com os parâmetros do sinal de varredura gerado com 20 Hz, porque o sinal de bloqueio passa um número maior de vezes no canal e o código corretor de erros do sistema não consegue corrigir os erros gerados pelo ruído.

Verificou-se que com o aumento da varredura o sistema apresentou indicação de erro, BER, para valores menores da relação J/S . Com o aumento do sinal de varredura o sinal de bloqueio interfere mais vezes no canal de comunicação, aumentando a degradação imposta pela presença do sinal de bloqueio. Conclui-se que quanto mais rápida a varredura do sinal de bloqueio, menor será a potência de bloqueio necessária para degradar a qualidade do sinal de um sistema de comunicação CDMA.

5.2.2 NO SISTEMA GSM

No sistema GSM, o bloqueador pode monitorar o canal físico BCCH e com isso identificar os saltos em frequência com antecedência. A velocidade de saltos em frequências no GSM é um pouco acima de 200 saltos por segundo

Uma outra maneira é bloquear a faixa de *downlink* ou *uplink*, utilizando um bloqueador parte da banda. Como a estação base da antena fica normalmente longe da estação móvel ou em lugares altos, o mais adequado é bloquear o *downlink*, por requerer um nível de potência menor. O problema de bloquear a faixa inteira ou as frequências de *uplink* reside no fato de o bloqueador ter que romper a comunicação na BTS. Para isto necessita de um transmissor de potência muito alta para criar um sinal forte o bastante para alcançar o BTS. Além disso, esta ação gera uma SNR grande na BTS, causando a perda de todos os sinais de entrada na estação, fato não desejado de forma geral, para não prejudicar outros serviços essenciais do sistema. Em contraste, se for criada uma perturbação sobre as frequências de *downlink*, necessita-se de um transmissor com potência suficiente o bastante para criar um sinal que rompa a comunicação na área desejada, de forma localizada e seletiva. Isto causa o bloqueio nas estações móveis desta área, deixando outras fora do bloqueio.

Em um cenário mais específico e contundente, o bloqueio deve visar o canal de controle RACH. Isso impede que a MS se comunique com qualquer célula, uma vez que toda solicitação de serviço é feita por esse canal. Entretanto, essa técnica de bloqueio não será capaz de cortar uma ligação ativa e, portanto, poderá não ser efetiva em alguns casos.

Examinando a arquitetura do canal GSM, para os objetivos deste trabalho, conclui-se que é mais eficaz a atuação do bloqueador sobre o canal de controle da banda de *downlink*, possibilitando que o bloqueio interfira na sincronização da informação e previna que a MS detecte uma rede GSM válida.

O sistema GSM utiliza espalhamento espectral FHSS e, sendo assim, existe a condição de ganho de processamento, que é uma função direta do número de canais de salto nos qual a informação é transmitida. Um sistema GSM 1800 possui no mínimo 317 canais de salto, totalizando um ganho de processamento acima de 25 dB, usando-se a EQ. 3.9. A velocidade de saltos no GSM é de 217 saltos por segundo (LEE, 1995). Dependendo do tipo de bloqueador utilizado na ação, o salto em frequência no sistema GSM não oferece real proteção contra o bloqueio. Quando o bloqueador é do tipo pontual, a condição de proteção ocorre devido ao salto em frequência do sistema.

Segundo STAHLBERG (2000), o bloqueador requer uma taxa de J/S de -5 dB para bloquear o canal GSM com sucesso, sem considerar o ganho de processamento. Assumindo-se o ganho de processamento de 25 dB, a relação J/S passa a ser de 20 dB.

No sistema GSM implementado, o bloco que representa o canal de comunicação foi retirado, sendo substituído por um somador na entrada do receptor para a inserção do sinal de bloqueio no sistema. O canal de propagação foi retirado porque é considerado como pior caso o sistema que tiver o canal de propagação ideal. Qualquer interferência gerada no canal de propagação só vai melhorar a condição de bloqueio no sistema. A FIG. 5.9 apresenta a composição do dispositivo bloqueador em conjunto com o modelo do canal de tráfego do sistema GSM. A qualidade do sinal recebido em um sistema GSM é definida por $RxQUAL$, a média da taxa de erro (BER) medida na recepção. A TAB. 5.3 apresenta a definição da qualidade do sinal recebido ($RxQUAL$) em relação à BER, segundo a norma GSM 05.08 (2000) e STEELE (2001).

TAB. 5.3 - RxQual em função da BER.

RxQual	BER
0	BER < 0,2%
1	0,2% < BER < 0,4%
2	0,4% < BER < 0,8%
3	0,8% < BER < 1,6%
4	1,6% < BER < 3,2%
5	3,2% < BER < 6,4%
6	6,4% < BER < 12,8%
7	12,8% < BER

Para TSENG (2001) e WIGARD (1999), o sistema GSM mantém a qualidade do sinal para RxQual de 0 a 4. Para RxQual maior que 4 o sistema é considerado inoperante.

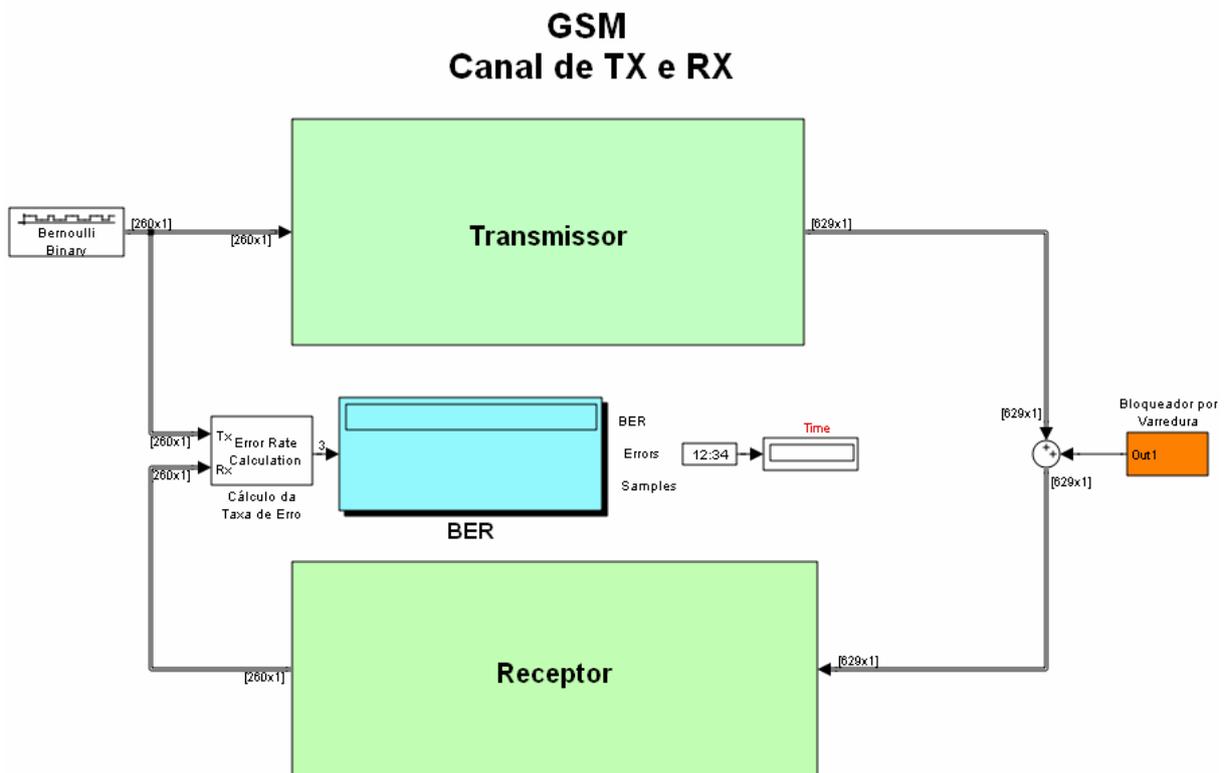


FIG. 5.9 - Canal de tráfego do sistema GSM com bloqueador por varredura usado nas simulações.

A primeira abordagem sugere o preenchimento de toda a banda de frequência do canal de *downlink* com o sinal proveniente de um dispositivo bloqueador PBN. Outra sugestão seria a utilização de um dispositivo bloqueador pontual com varredura. Se a frequência de varredura

do dispositivo for alta, os quadros deverão sofrer o efeito do sinal interferente várias vezes por segundo, o que pode vir a causar degradação da qualidade do enlace no sistema. O bloqueador pontual não é eficaz devido ao salto em frequência do sistema GSM.

Para possibilitar uma maior linearidade nos resultados apresentados, o tempo de duração de cada evento de simulação ($T = 0,61$ s) e o total de bits transmitidos (1.220.180 bits) foram os mesmos em todos os eventos realizados no Sistema GSM.

Para o bloqueador PBN (FIG. 4.5) no canal de comunicação, o sistema apresentou o resultado ilustrado na FIG. 5.10. Foi considerado que o limite de BER aceitável em todas as simulações é de 3,2%, conforme a TAB. 5.3, correspondendo à linha pontilhada nos próximos gráficos.

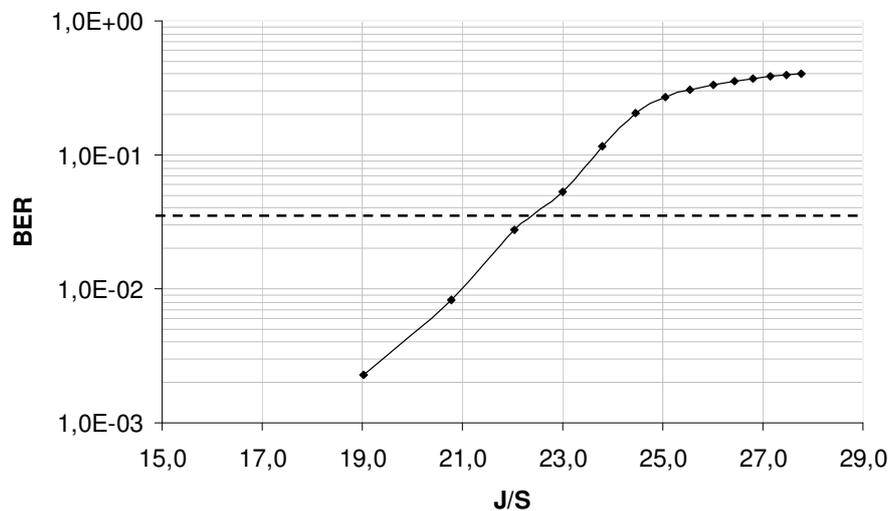


FIG. 5.10 - Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema GSM com um bloqueador PBN.

Para valores de J/S menores que 22,5 dB, o sistema indicou ocorrência de bits e quadros com erro, indicando uma BER dentro do limite esperado para o sistema GSM. Entretanto, a partir do valor de 22,5 dB, a BER aumentou e o sistema ficou na condição de bloqueio

Utilizando o mesmo modelo proposto da FIG. 5.9, mas com um bloqueador com varredura (FIG. 4.13) passando por toda a banda de comunicação (*downlink*) e com frequência de varredura variável, o sistema apresentou o resultado ilustrado na FIG. 5.11.

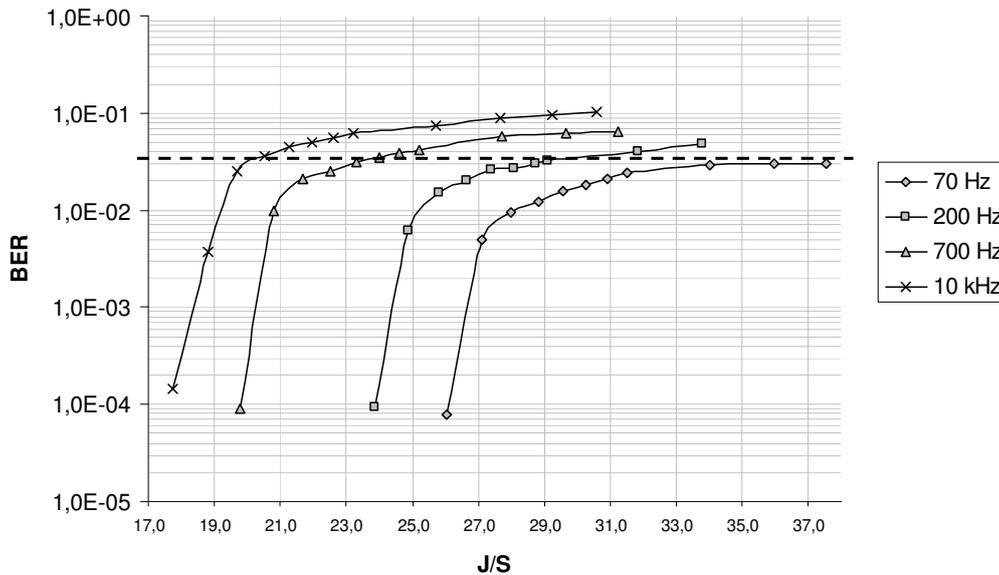


FIG. 5.11 - Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema GSM com bloqueador por varredura.

Para a varredura do bloqueador configurada com 70 Hz o sistema indicou pouca ocorrência de bits e quadros com erro e a BER ficou dentro do limite esperado para o sistema GSM. Com essa frequência de varredura o bloqueador não é eficaz.

Aumentado a varredura para 200 Hz, o sistema indicou mais ocorrência de bits e quadros com erro. Para valores de J/S menores que 29,12 dB a BER ficou dentro do limite esperado. A partir do valor de 29,12 dB, a BER aumentou e o sistema ficou na condição de bloqueio em todas as simulações, caracterizando a degradação na qualidade do sinal imposta pela presença do bloqueador. Com o aumento do sinal de varredura, o sistema apresentou uma degradação maior, quando comparado aos parâmetros do sinal de varredura gerado com 70 Hz.

Aumentado a varredura para 700 Hz, para valores de J/S menores que 24,62 dB a BER ficou dentro do limite esperado para o sistema GSM. A partir do valor de 24,62 dB, a BER aumentou e ficou na região de bloqueio em todas as simulações.

Com o bloqueador configurado com varredura de 10 kHz, a razão J/S de bloqueio passou a ser de 20,53 dB.

Considerando os ganhos das antenas e a perda dos cabos o sistema apresentou os seguintes resultados (FIG. 5.12):

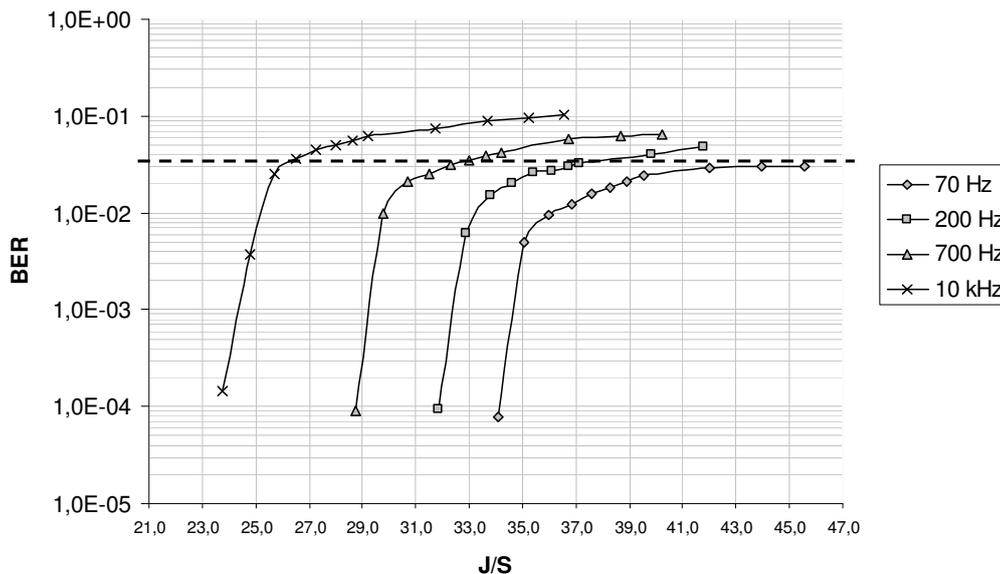


FIG. 5.12 - Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema GSM com bloqueador por varredura, considerando os ganhos das antenas.

Para a varredura do bloqueador configurada com 70 Hz o sistema indicou pouca ocorrência de bits e quadros com erro e a BER ficou dentro do limite esperado para o sistema GSM. Com essa frequência de varredura o bloqueador não é eficaz.

Aumentado a varredura para 200 Hz, o sistema indicou mais ocorrência de bits e quadros com erro. Para valores de J/S menores que 37,5 dB a BER ficou dentro do limite esperado. A partir do valor de 37,5 dB, a BER aumentou e o sistema ficou na condição de bloqueio em todas as simulações, caracterizando a degradação na qualidade do sinal imposta pela presença do bloqueador. Com o aumento do sinal de varredura, o sistema apresentou uma degradação maior, quando comparado aos parâmetros do sinal de varredura gerado com 70 Hz.

Aumentado a varredura para 700 Hz, para valores de J/S menores que 33 dB a BER ficou dentro do limite esperado para o sistema GSM. A partir do valor de 33 dB, a BER aumentou e ficou na região de bloqueio em todas as simulações.

Com o bloqueador configurado com varredura de 10 kHz, a razão J/S de bloqueio passou a ser de 25,53 dB.

Similarmente ao sistema CDMA, com o aumento da varredura o sistema GSM apresentou indicação de erro para valores J/S mais baixos. Com o aumento do sinal de varredura o sinal de bloqueio interfere mais vezes no canal de comunicação, aumentando a degradação imposta pela presença do sinal de bloqueio. Como esperado, para frequências de varredura mais altas o bloqueador requer menor potência para bloquear o sistema GSM.

Para todas as frequência de varreduras simuladas o código corretor de erros do sistema GSM não conseguiu corrigir erros gerados pela presença do sinal do dispositivo bloqueador.

5.2.3 NA NORMA MIL-STD-188-110B

O desempenho de medida da norma MIL STD-188-110B no modo tom simples, utilizando frequência fixa, está relacionado com a BER do sistema, que deve se menor ou igual a 10^{-3} . Para valores maiores que 10^{-3} o sistema começa a degradar e é considerado inoperante.

Com o sistema da norma devidamente implementado, o bloco que representa o canal de comunicação foi substituído por um somador para a inserção do sinal de bloqueio. O canal de propagação foi retirado por ser considerado como pior caso o sistema que tem o canal de propagação ideal. Qualquer interferência gerada no canal de propagação só tende a melhorar a condição de bloqueio no sistema. A FIG. 5.13 apresenta a composição do dispositivo bloqueador em conjunto com o modelo do canal de tráfego da norma MIL STD-188-110B.

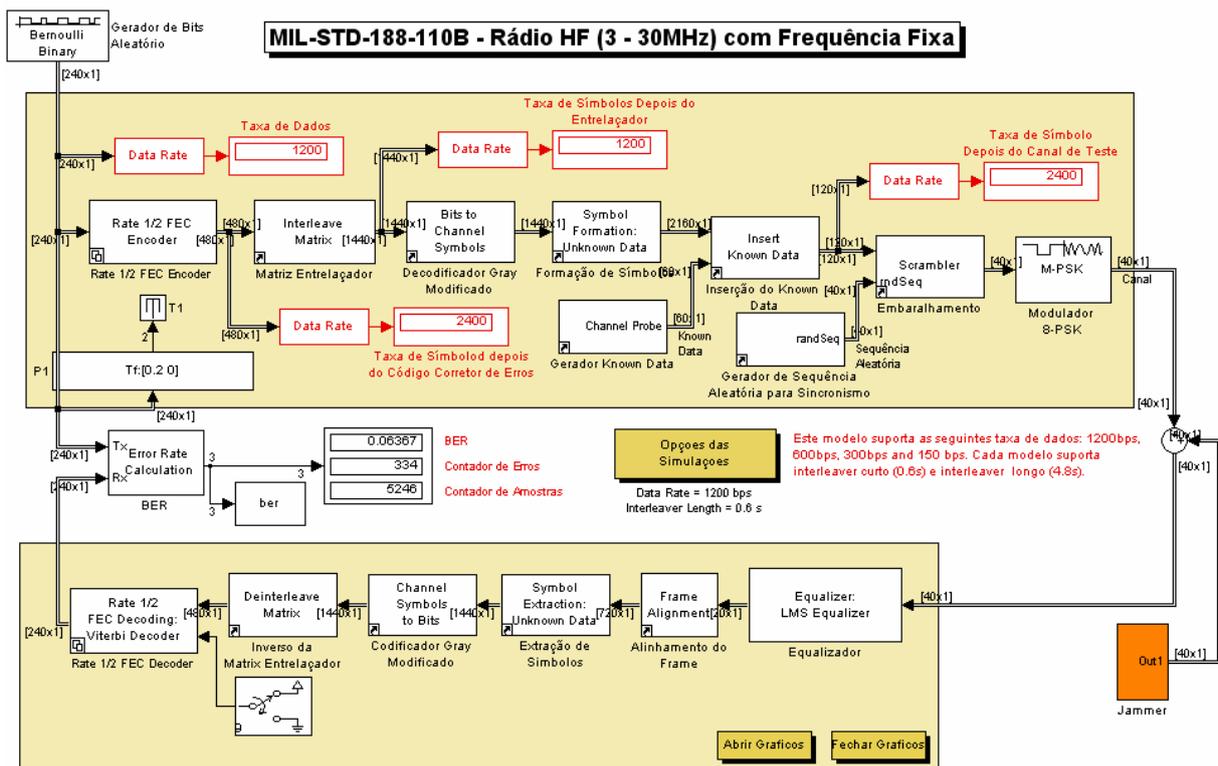


FIG. 5.13 - Canal de tráfego da norma MIL-STD-188-110B com bloqueador.

A primeira abordagem implementada gera um sinal de bloqueio cobrindo toda a banda de frequência do canal de comunicação com o sinal proveniente de um dispositivo bloqueador BBN. A segunda abordagem é a utilização de um bloqueio por tom em cima do canal de comunicação, já que foi implementado um canal de trafego da norma no modo tom simples,

ou seja, sem salto em frequência. A terceira opção é a utilização de um dispositivo bloqueador pontual com varredura, da mesma forma que para os sistemas CDMA e GSM.

Para possibilitar uma maior linearidade nos resultados apresentados, o tempo de duração de cada evento de simulação ($T = 96$ s) e o total de bits transmitidos (113.246 bits) foram os mesmos em todos os eventos realizados na norma MIL-STD-188-110B.

Para o sistema baseado na norma em conjunto com um bloqueador BBN (FIG. 4.5) no canal de comunicação, o sistema apresentou o resultado ilustrado na FIG. 5.14.

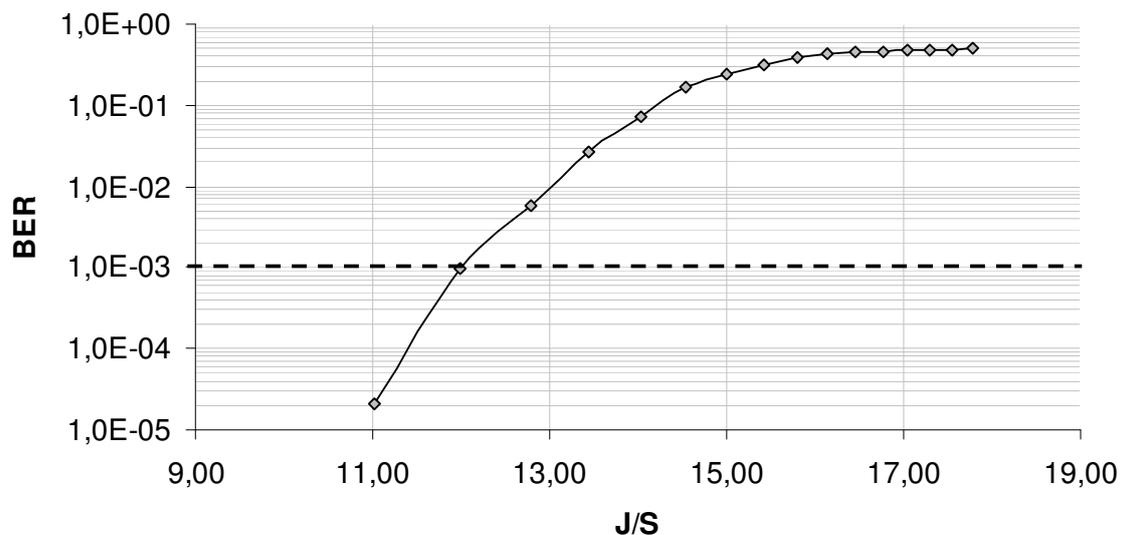


FIG. 5.14 - Relação entre a BER e a razão J/S no receptor de um canal de tráfego da norma MIL-STD-118-110B com um bloqueador PBN.

Para valores de J/S menores que 11 dB, o sistema não indicou a ocorrência de bits e quadros com erro. Entretanto, de 11 a 12 dB, a BER aumentou, caracterizando assim, uma degradação na qualidade do sinal imposta pela presença do bloqueador, mas permaneceu com valores abaixo da região de bloqueio. Para valores de J/S acima de 12 dB, o valor da BER passou a região de bloqueio e o sistema foi considerado como inoperante nessa região.

Utilizando o mesmo modelo proposto da FIG. 5.13, mas com um bloqueador pontual (FIG. 4.9) no canal de comunicação do sistema, o sistema apresentou o resultado ilustrado na FIG. 5.15. O limiar de J/S para a condição de bloqueio neste caso foi de 9,6 dB. Para valores de J/S próximos a 17 dB, o valor da BER se aproximou de 0,5.

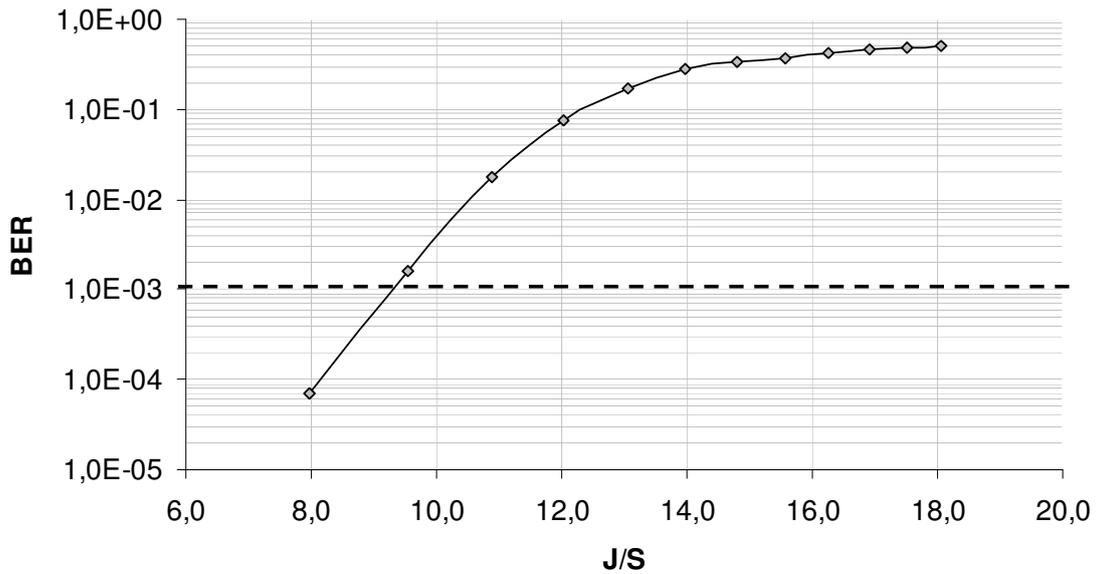


FIG. 5.15 - Relação entre a BER e a razão J/S no receptor de um canal de tráfego da norma MIL-STD-118-110B com um bloqueador pontual.

A terceira implementação utiliza o mesmo modelo proposto da FIG. 5.13, mas com um bloqueador por varredura (FIG. 4.13) cobrindo toda banda de comunicação do sistema. Neste caso, os resultados da relação de BER com J/S são mostrados na FIG. 5.16.

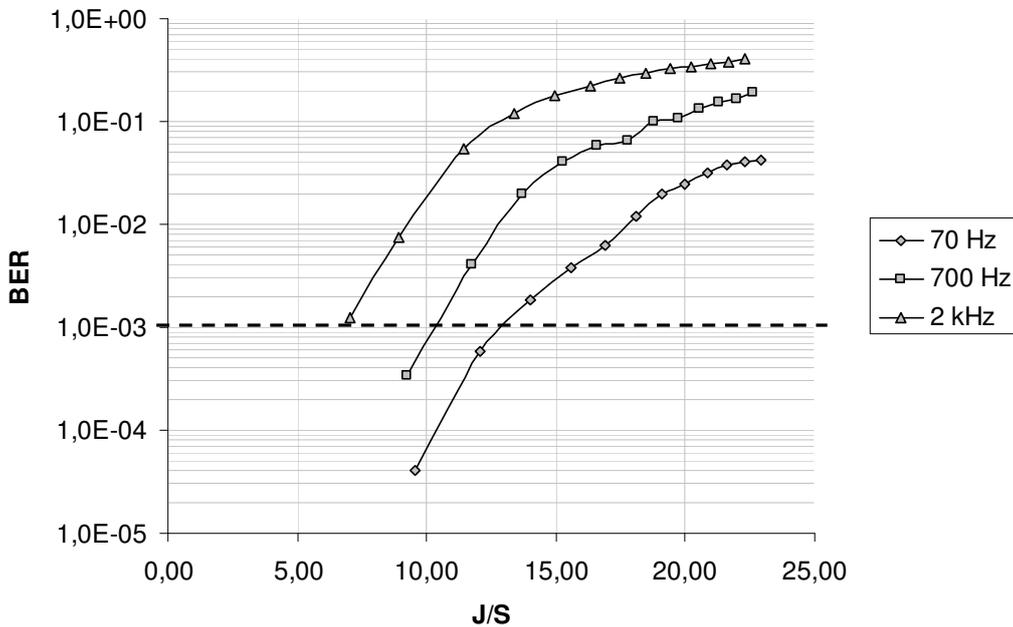


FIG. 5.16 - Canal de tráfego da norma MIL-STD-118-110B com bloqueador com varredura.

Similarmente aos sistemas CDMA e GSM, o bloqueador por varredura foi configurado para diferentes frequências: 70 Hz, 700 Hz e 2 kHz. Para a varredura de 70 Hz, valores de J/S menores que 12 dB resultam num sistema com ocorrência de bits e quadros com erro.

Entretanto, a partir do valor de 12 dB, a BER aumenta, caracterizando uma degradação na qualidade do sinal imposta pela presença do bloqueador e a condição de bloqueio. Para valores de J/S menores que 9,5 dB o sistema não indicou erro (BER nula).

Aumentando a varredura para 700 Hz, com valores de J/S menores que 10,3 dB o sistema indicou pouca ocorrência de bits e quadros com erro. A partir de 10,3 dB, a BER aumentou e o sistema permaneceu na região de bloqueio. Para valores de J/S menores que 9,2 dB a BER permaneceu nula. Para a varredura de 2 kHz, o limiar de bloqueio foi de aproximadamente 7 dB.

Assim como nos sistemas CDMA e GSM, com o aumento do sinal de varredura o sistema apresenta uma degradação maior. Com o aumento do sinal de varredura o sinal de bloqueio interfere mais vezes no canal de comunicação, aumentando a degradação imposta pela presença do sinal de bloqueio. Para frequências de varredura mais altas o bloqueador requer menor potência para bloquear o sistema.

Para todos os sistemas apresentados (CDMA, GSM e a norma MIL-STD-188-110B), aumentando-se a frequência de varredura, é possível que se chegue a um ponto em que o sinal de bloqueio passe no canal de comunicação por um instante de tempo muito curto, e o código corretor de erros consiga minimizar o número de erros gerados pelo sinal do bloqueador. Isto, contudo, não foi observado nas simulações para as frequências de varredura analisadas.

6 TESTES PRÁTICOS COM O SISTEMA GSM

Uma das propostas do trabalho é a implementação de um dispositivo bloqueador para operar seguindo o conceito de CME do tipo bloqueio pontual com varredura. Os estudos e pesquisas apresentadas nos Capítulos 2 e 3 possibilitaram a simulação do sistema de comunicação GSM (item 4.3.2) e do bloqueador do tipo pontual com varredura (item 4.2). Com a implementação do sistema GSM na presença do bloqueador (item 5.2.2), o trabalho possibilitou a avaliação dos resultados da geração de interferência na faixa de operação do sistema GSM, 1800 MHz.

6.1 IMPLEMENTAÇÃO E TESTE DE UM BLOQUEADOR PARA A FAIXA DE 1800 MHZ

Posteriormente à análise dos resultados das simulações, passou-se à implementação de um dispositivo bloqueador do tipo pontual com varredura para a faixa de 1800 MHz, especificamente sobre o sistema de telefonia móvel GSM. Tal procedimento foi semelhante ao adotado por TOSCANO (2006), sendo o bloqueador implementado uma versão modificada do bloqueador utilizado naquele trabalho.

A FIG. 6.1 apresenta o dígrama em blocos do dispositivo bloqueador implementado, para inserção de ruído em uma única banda de frequências.

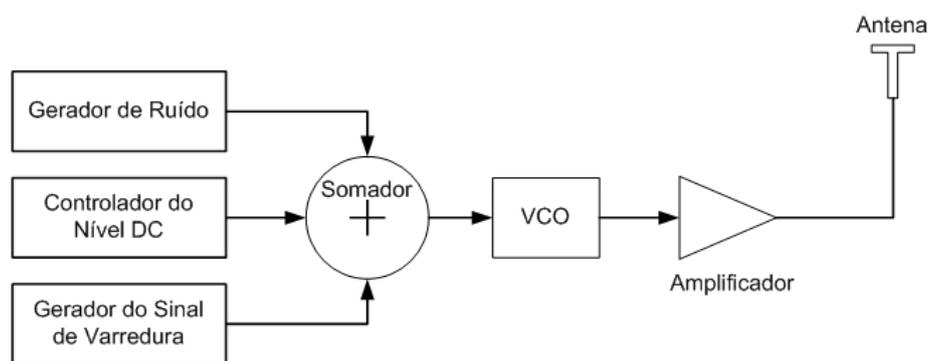


FIG. 6.1 - Diagrama em blocos do dispositivo bloqueador implementado.

Os blocos do sistema da FIG. 6.1 têm as seguintes funções:

- O Gerador de Ruído gera um sinal pseudo-aleatório que é inserido no espectro para causar a interferência requerida;

- O Controlador do nível DC tem como finalidade gerar um nível DC para que seja possível o estabelecimento de um nível quiescente sobre o qual será adicionado o ruído e outros sinais;
- O Gerador de Sinal de Varredura gera um sinal com a forma de onda triangular, para que seja produzido o efeito da varredura em frequência;
- O Somador soma os sinais de ruído, varredura e nível DC;
- O VCO é responsável por gerar um sinal de RF a partir de um nível DC em sua entrada;
- O Amplificador tem como função amplificar o sinal do bloqueador para um nível de potência que seja suficiente para efetuar o bloqueio;
- A Antena tem como finalidade irradiar para o espaço livre a energia eletromagnética gerada pelo dispositivo bloqueador.

Para a implementação do bloqueador na faixa de 1800 MHz foi utilizado como base o dispositivo de TOSCANO (2006). No referido trabalho foi feito um estudo de bloqueador em sistemas IS-95 (CDMA) na faixa de 900 MHz. Foram aproveitados o Circuito Gerador de Ruído, o Circuito Gerador do Sinal de Varredura, o Controlador do Nível DC e o Somador (FIG. 6.2).



FIG. 6.2 - Circuito implementado por Toscano (2006).

Para o circuito operar em 1800 MHz foi implementado o circuito VCO, utilizando JTOS-2000, que opera nessa faixa. O circuito do VCO e o layout gerado estão ilustrados na FIG. 6.3.

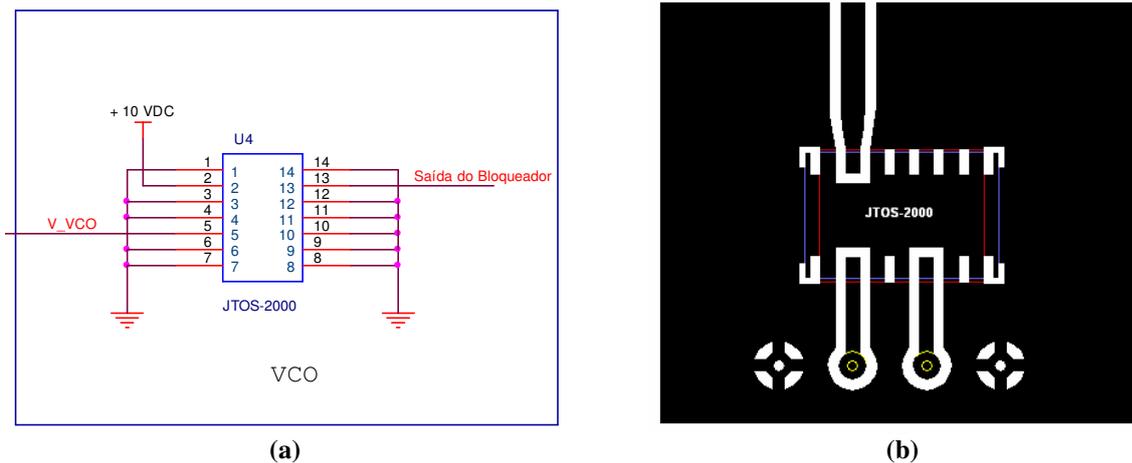


FIG. 6.3 - Esquemáticos do VCO implementado, mostrando (a) circuito e (b) layout.

No sistema implementado por TOSCANO (2006), o valor da amplitude do sinal de varredura é de aproximadamente $9 V_P$. Para o bloqueador operar na faixa de *downlink* do GSM (1805 a 1880 MHz) com o JTOS-2000, o sinal de varredura deve ter valor de amplitude de $13 V_P$ a $15 V_P$, conforme especificações do fabricante mostradas na FIG. 6.4.

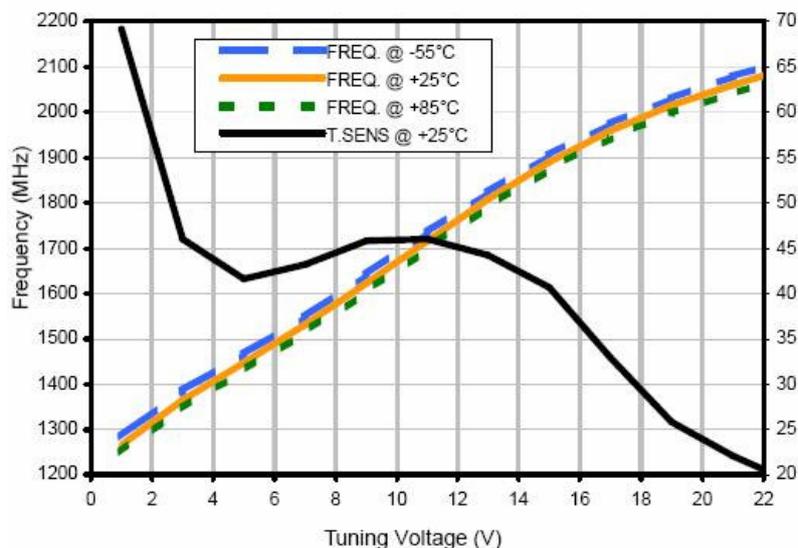


FIG. 6.4 - Sinal de controle do VCO JTOS-2000.

Para chegar ao nível de tensão de 13 V, foram implementados um novo circuito somador não inversor e um novo circuito controlador do nível DC. Parte do sistema foi alimentada com uma fonte de +19 VDC, conforme mostrado na FIG. 6.5. O novo sinal de varredura do VCO (V_VCO) é a soma de um nível DC ($V2$) com o sinal de varredura gerado pelo circuito implementado por TOSCANO (2006) ($V1$).

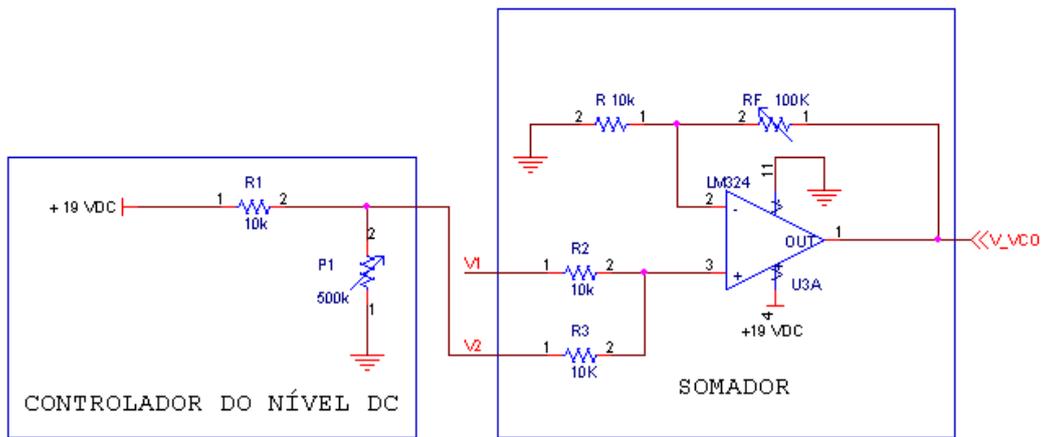


FIG. 6.5 - Circuito implementado com alimentação de +19VDC.

Após a montagem de todos os blocos necessários, o bloqueador foi implementado em uma única placa para facilitar a interligação de todos os seus componentes, cujo circuito final é mostrado na FIG. 6.6.

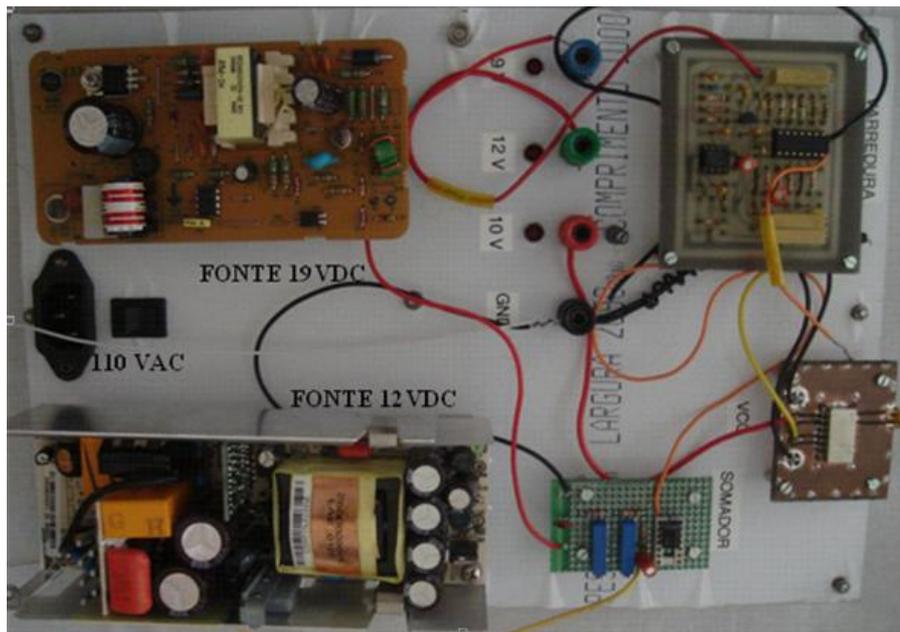


FIG. 6.6 - Bloqueador GSM.

Com o auxílio de um analisador de espectro foi possível verificar o espectro de saída do VCO e configurar o bloqueador na faixa de frequência desejada, de 1805 a 1880 GHz. O bloqueador montado foi ligado diretamente ao analisador de espectro. O resultado é apresentado na FIG. 6.7.

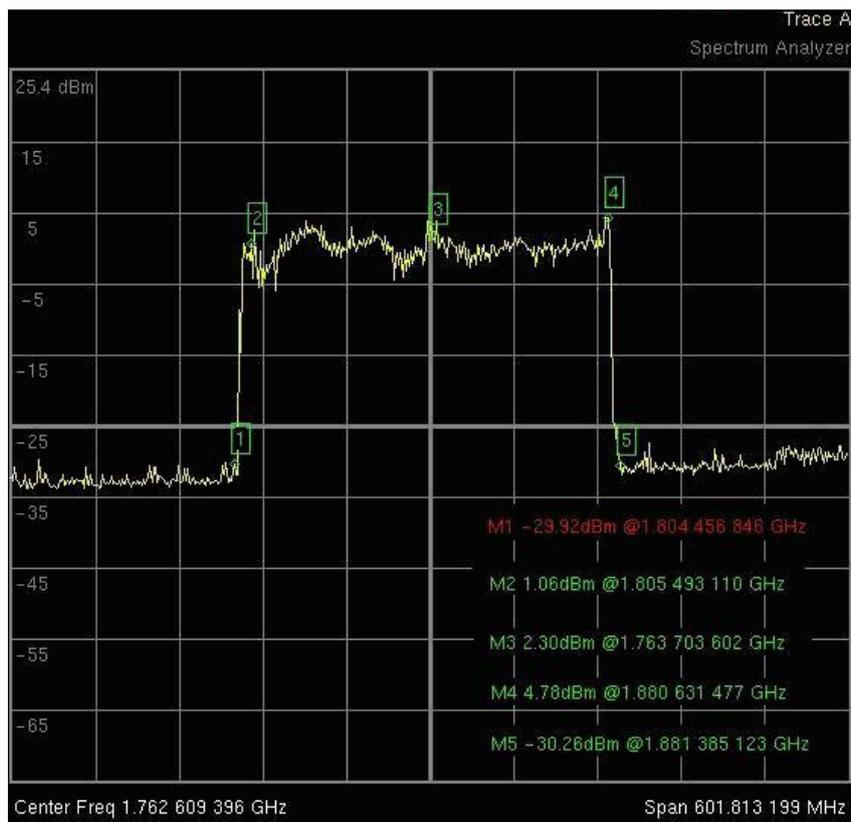


FIG. 6.7 - Sinal de saída do bloqueador implementado sem a antena, observado por um analisador de espectro.

6.2 AMBIENTE DE REALIZAÇÃO

Os testes foram realizados no laboratório do Instituto de Pesquisas da Marinha (IPqM). Os equipamentos e dispositivos utilizados foram os seguintes:

- Dispositivo bloqueador implementado;
- Analisador de Espectro (Agilent E4408B);
- Gerador de Funções (HP 8116A);
- Atenuador Variável (HP 8494B - 11 dB);
- Atenuador Variável (HP 8496B - 110 dB);
- Amplificador (HP 8349B);
- Antena Corneta Padrão de 1 – 18 GHz;
- Cabos e conectores;
- Terminal móvel Motorola V555 – Operadora Claro;
- Aparelho Nokia 2100 - Operadora Claro.

O arranjo do dispositivo bloqueador para a realização dos testes de interferência no sistema GSM é ilustrado na FIG. 6.8.

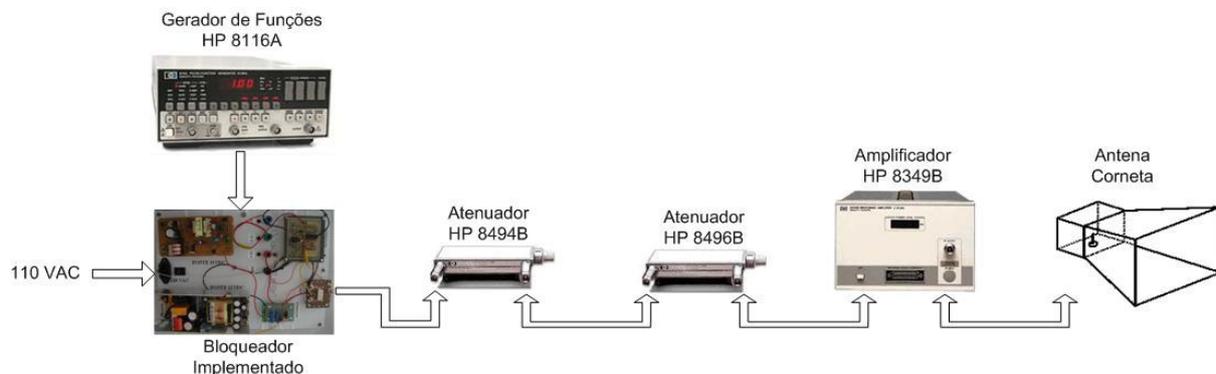


FIG. 6.8 - Arranjo de testes em laboratório.

O gerador de funções HP 8116A foi utilizado para gerar o sinal de varredura do tipo onda triangular nas mesmas frequências utilizadas nas simulações da seção 5.2.2: 70 Hz, 200 Hz, 700 Hz e 10 kHz. Foi necessária a utilização do gerador porque a placa geradora do sinal de varredura não gera sinais com frequências superiores a 1 kHz.

Foram utilizados dois atenuadores variáveis de 11 dB (passo de 1 dB) e 110 dB (passo de 10 dB), ligados em série, tanto para restringir o limite máximo de potência de 0 dBm na entrada do amplificador quanto para variar a potência de saída do bloqueador com o objetivo de encontrar a potência mínima de bloqueio. O amplificador apresenta ganho de 20 dB na faixa próxima a 1800 MHz.

O celular Motorola V555 foi habilitado no modo campo de teste. Essa funcionalidade permite verificar em seu visor os níveis de potência de recepção do sinal S no ambiente de realização dos testes. O aparelho Nokia 2100 foi utilizado para verificar a condição de bloqueio na presença do dispositivo bloqueador. A FIG. 6.9 apresenta o ambiente onde o mapeamento do valor potência recebida pelo terminal móvel foi realizado. Os testes foram realizados no Laboratório 1 do Grupo de Guerra Eletrônica, no Instituto de Pesquisas da Marinha. Os valores do sinal recebido também estão mostrados na figura.

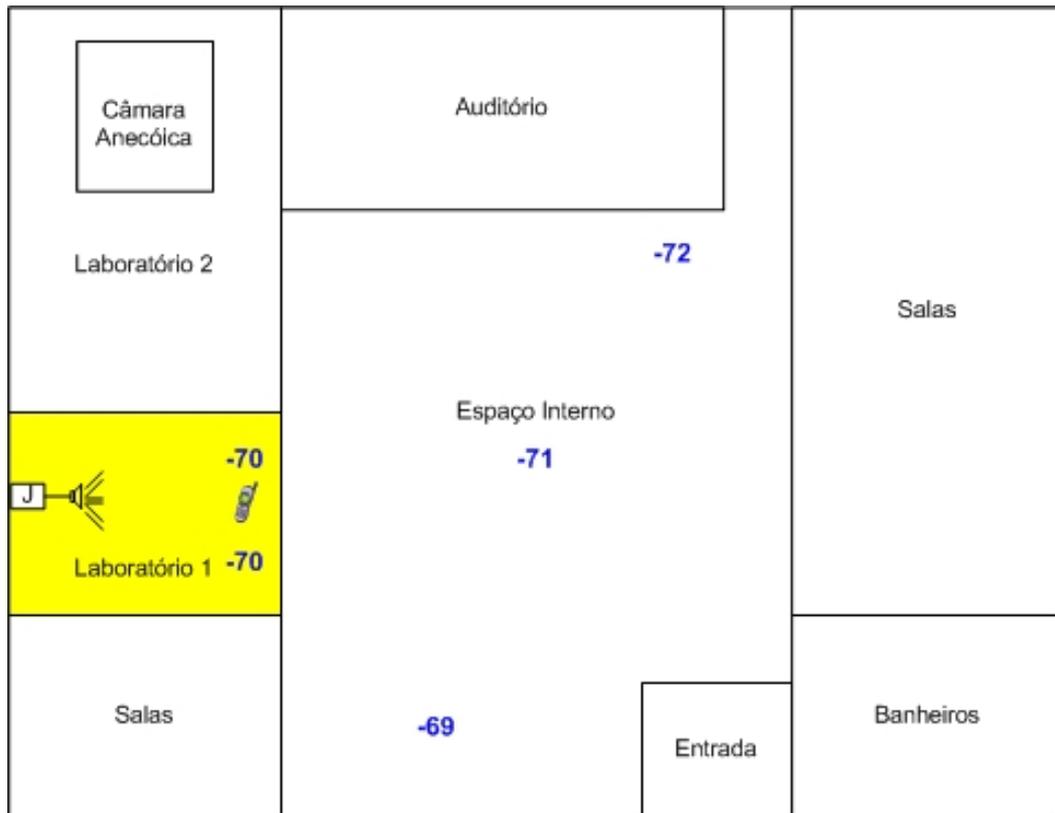


FIG. 6.9 - Mapeamento da potência do sinal recebido S (dBm).

6.3 EFETIVIDADE DO BLOQUEADOR SOBRE O SISTEMA DE TELEFONIA MÓVEL GSM

A área em destaque na FIG. 6.9 se refere ao local onde os testes sobre a efetividade do bloqueador foram realizados. Dentro desta área, com o dispositivo bloqueador operando, foi verificada a sua potência de saída. Para estimar a potência de bloqueio que chega ao celular foi calculada a perda de propagação no espaço livre, L . Segundo RAPPAPORT (1996), a perda de propagação aproximada no espaço livre é dada por:

$$L = 20\log_{10} f + 20\log_{10} d + 32,442dB \quad (6.1)$$

onde f é dado em MHz e d em km.

Para uma distância de 10 m e frequência central da faixa de *downlink* de 1845 GHz, a perda de propagação é aproximadamente de 58 dB.

Para todos os testes o bloqueador foi inicialmente configurado com uma potência mínima de saída de -7 dBm, podendo atingir a potência máxima de 20 dBm com *passos* de 1 dB.

A FIG. 6.10 apresenta a relação J/S medida dentro do Laboratório 1 para uma distância entre o bloqueador e a estação móvel de 10 m e os resultados da ação do bloqueador. A linha em vermelho representa o limite de bloqueio, ou seja, para valores de J/S acima da linha o sistema está bloqueado.

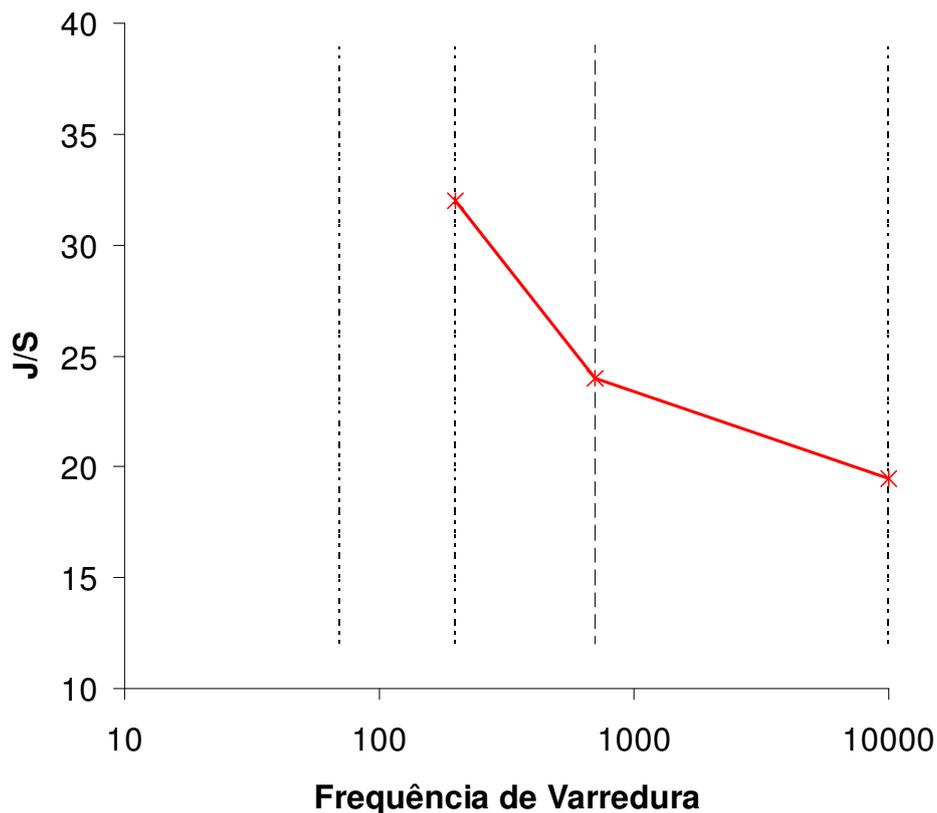


FIG. 6.10 - Resultados dos testes.

Analisando os resultados apresentados na FIG. 6.10, pode-se concluir que:

- Para a frequência de varredura de 70 Hz o bloqueio não foi eficiente e o celular operou normalmente para todas as relações de J/S .
- Aumentando a frequência de varredura do sinal de bloqueio para 200 Hz o celular operou normalmente até a relação J/S de 32 dB. A partir desse valor o sistema permaneceu sempre bloqueado.
- Configurando o sinal de bloqueio com varredura de 700 Hz o celular ficou em operação para relação J/S de 24 dB. A partir desse valor o sistema permaneceu sempre bloqueado.

- Por fim, o bloqueador foi configurado com varredura de 10 kHz. Com essa varredura o celular ficou em operação para relação J/S de 19 dB. A partir desse valor o sistema permaneceu sempre bloqueado.

Foram feitos testes nas seguintes condições:

- Telefone móvel desligado e dispositivo bloqueador ligado. Ao ligar o telefone móvel, o visor apresenta a mensagem “sem rede”.
- Telefone móvel ligado e dispositivo bloqueador desligado. Ao ligar o dispositivo bloqueador o telefone apresenta em seu visor a mensagem “sem rede”.
- Telefone móvel ligado e efetuando ou recebendo uma ligação. Ao ligar o dispositivo bloqueador o telefone apresenta em seu visor a mensagem “ligação perdida” e alguns segundos depois a mensagem “sem rede”.

Para validar as medidas dos níveis de potência de recepção do sinal S que foram medidos com o auxílio do celular Motorola V555 habilitado no modo campo de teste, foi montado um novo arranjo de medição, dividido em duas partes: para medir a potência de recepção do sinal S e para medir o valor da potência de bloqueio na entrada do receptor.

Para medir a potência de recepção do sinal S foi montado o arranjo da FIG. 6.11.

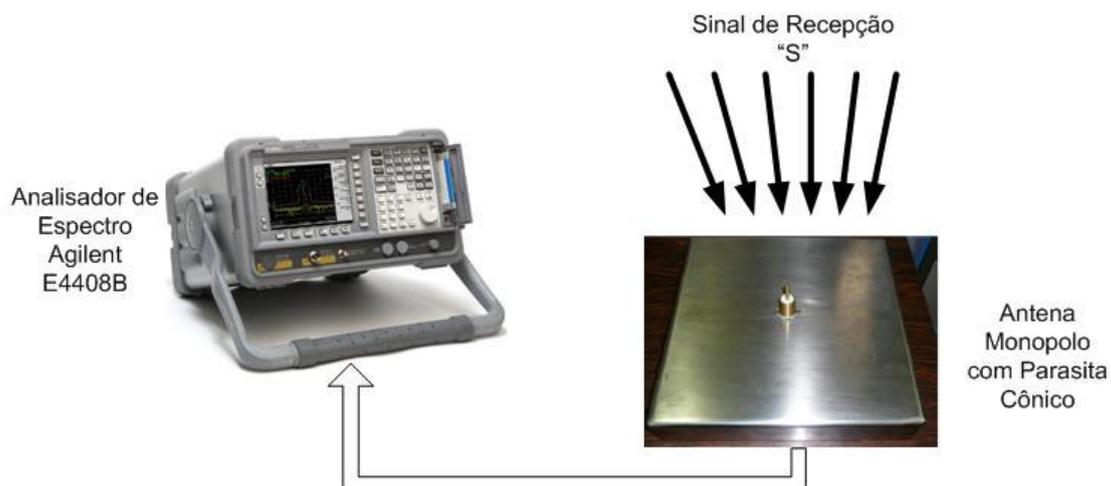


FIG. 6.11 – Arranjo de teste para medir a potência de recepção S .

Foi utilizada uma antena monopolo com parasita cônico, projetada por SAUNDERS (2009) para a faixa de 1 a 5 GHz. O analisador de espectro foi configurado para monitorar apenas a faixa de *downlink* do sistema GSM, frequência inicial 1,805 GHz e frequência final de 1,880 GHz. A função *MAX-HOLD* do espectro foi habilitada. Essa função detecta e armazena os picos de frequência recebidos. O resultado é apresentado na FIG. 6.12.

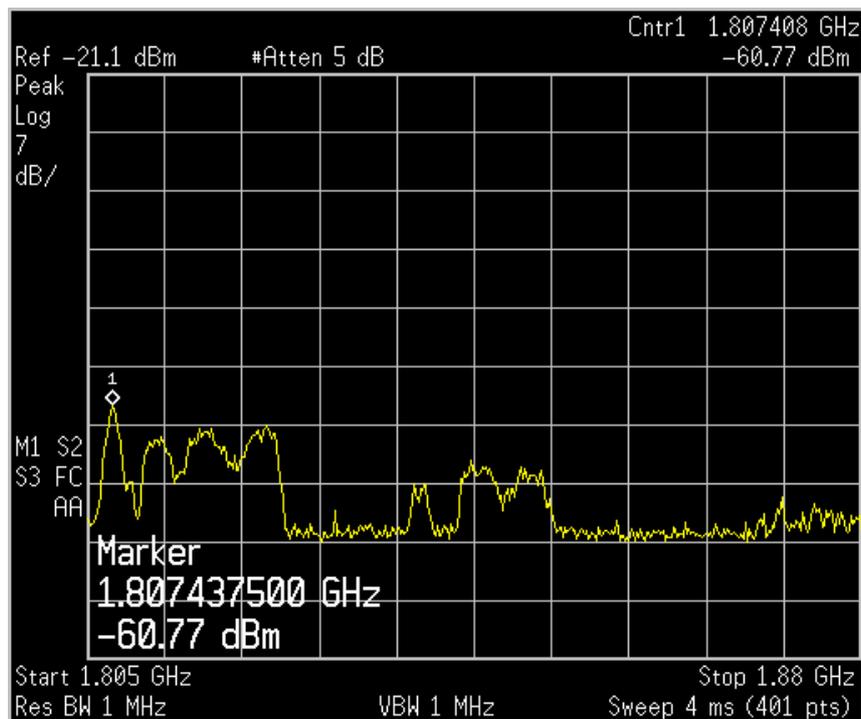


FIG. 6.12 – Potência de recepção S.

A potência máxima foi de $-60,77$ dBm e a potência mínima foi de $-72,43$ dBm. O Motorola V555 habilitado no modo campo de teste apresentava em seu visor o nível de potência recebida entre -65 dBm e -74 dBm. O valor utilizado nas medidas anteriores foi de -70 dBm. O celular Motorola V55 está apresentando a potência do sinal recebido da estação base próximo ao valor medido.

O próximo passo foi verificar a potência do sinal transmitido pelo bloqueador na entrada do receptor. Foi utilizado o arranjo da FIG. 6.8 e o bloqueador foi colocado a uma distância de 10 m do arranjo da FIG. 6.11. O analisador de espectro foi configurado para monitorar apenas a faixa de *downlink* do sistema GSM, frequência inicial 1,805 GHz e frequência final de 1,880 GHz. O propósito dessa medida foi verificar a perda de propagação e

consequentemente o nível de potência de bloqueio na entrada do receptor. A potência medida na entrada do receptor foi de -35 dBm.

As medidas foram refeitas para as frequências de varreduras de 70 Hz, 200 Hz, 700 Hz e 100 kHz. A FIG. 6.13 apresenta a relação J/S medida dentro do Laboratório 1. A linha em vermelho representa o limite de bloqueio.

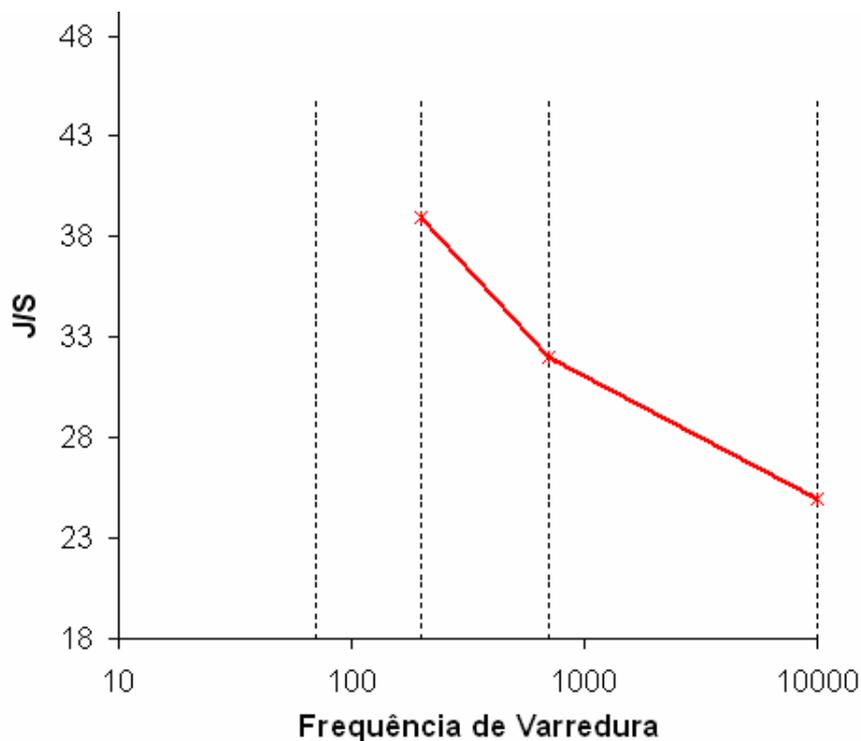


FIG. 6.13 - Resultados dos testes considerando os ganhos das antenas e perdas dos cabos.

Os resultados apresentados na FIG. 6.13 apresentaram uma diferença de aproximadamente 7 dB em relação aos resultados apresentados na FIG. 6.10. Essa diferença está correta porque nas novas medidas foram considerados os ganhos das antenas e as perdas dos cabos.

Analisando os resultados apresentados na FIG. 6.13, pode-se concluir que:

- Para a frequência de varredura de 70 Hz o bloqueio não foi eficiente e o celular operou normalmente para todas as relações de J/S .
- Aumentando a frequência de varredura do sinal de bloqueio para 200 Hz o celular operou normalmente até a relação J/S de 39 dB, diferença de 7 dB em relação às medidas da FIG. 6.10. A partir desse valor o sistema permaneceu sempre bloqueado.

- Configurando o sinal de bloqueio com varredura de 700 Hz o celular ficou em operação para relação J/S de 32 dB, diferença de 8 dB em relação às medidas da FIG. 6.10. A partir desse valor o sistema permaneceu sempre bloqueado.
- Por fim, o bloqueador foi configurado com varredura de 10 kHz. Com essa varredura o celular ficou em operação para relação J/S de 25 dB, diferença de 6 dB em relação às medidas da FIG. 6.10. A partir desse valor o sistema permaneceu sempre bloqueado.

6.4 VALORES SIMULADOS × VALORES PRÁTICOS

Para comparar os resultados medidos com os teóricos foram fixados três valores de BER, retirados das simulações do item 5.2.2. Nas simulações não foram considerados os ganhos das antenas e as perdas dos cabos. O limite de BER aceitável em todas as condições foi de 3,2%, conforme comentários acerca da TAB. 5.3. A TAB. 6.1 apresenta estas situações.

TAB. 6.1 – Valores J/S simulados para uma BER fixa.

BER	FREQUÊNCIA	J/S	EFEITO ESPERADO
2,1% (0,021)	70 Hz	30,2	Sistema Operando
	200 Hz	26,1	Sistema Operando
	700 Hz	22,3	Sistema Operando
	10 kHz	18,7	Sistema Operando
3,2% (0,032)	70 Hz	-	Sistema Operando
	200 Hz	29,12	Sistema Inoperante
	700 Hz	24,62	Sistema Inoperante
	10 kHz	20,52	Sistema Inoperante
4,8% (0,048)	70 Hz	-	Sistema Operando
	200 Hz	33,76	Sistema Inoperante
	700 Hz	26,5	Sistema Inoperante
	10 kHz	21,4	Sistema Inoperante

Os valores de J/S simulados para uma BER fixa, TAB. 6.1, foram plotados juntos com os valores práticos da FIG. 6.10. Os resultados estão ilustrados na FIG. 6.14. A linha em azul

representa o limite de bloqueio simulado para uma BER fixa de 4,8% (0,048), a linha em verde representa o limite de bloqueio simulado para uma BER fixa de 3,2% (0,032), a linha em laranja representa o limite de bloqueio simulado para uma BER fixa de 2,1% (0,021) e a linha em vermelho pontilhada representa o limite de bloqueio encontrado na prática.

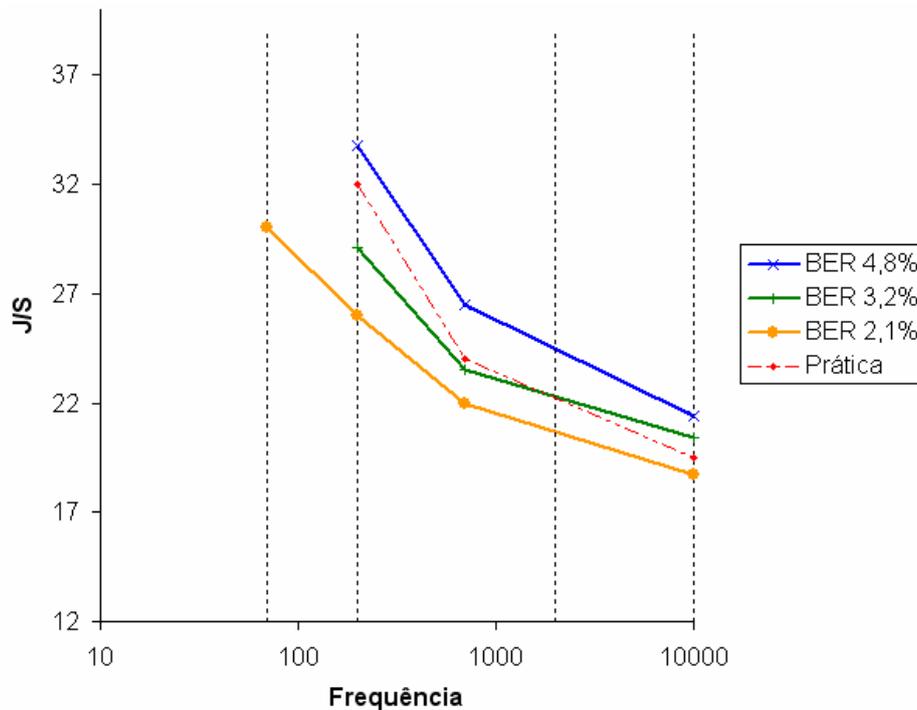


FIG. 6.14 – Resultados simulados e práticos.

Para BER fixa de 2,1% era esperado nas simulações que o sistema permanecesse sempre em operação para todas as frequências de varredura do bloqueador, o que de fato ocorreu. A linha laranja do gráfico ilustra quais são os valores de J/S simulados que correspondem aos valores J/S práticos, considerando BER fixa de 2,1%. Comparando com as medidas práticas, a linha laranja ficou dentro dos limites de operações para todas as frequências de varredura de bloqueio.

Considerando o limite de BER de 3,2%, era esperado nas simulações que o sistema permanecesse sempre em operação para a frequência de varredura de 70 Hz e para outras frequências de varredura o sistema ficasse inoperante. A linha verde do gráfico ilustra quais são os valores de J/S simulados que correspondem aos valores J/S práticos, para BER fixa de 3,2%. Comparando com as medidas práticas, para a frequência de varredura de 200 Hz os valores práticos e simulados apresentaram comportamentos distintos. Nas simulações era esperado que o sistema ficasse inoperante para uma relação J/S de 29 dB e na prática o valor foi de 32 dB. Para as frequências de 700 Hz e 10 kHz, os pontos correspondentes na linha

verde do gráfico ilustram que o sistema ficou dentro dos limites de bloqueio. Para a frequência de varredura de 70 Hz o sistema permaneceu em operação nos dois casos, simulados e práticos.

Para BER fixa de 4,8% era esperado nas simulações que o sistema permanecesse em operação para a frequência de varredura de 70 Hz e para as outras frequências de varredura o sistema ficasse inoperante. A linha azul do gráfico ilustra quais são os valores de J/S simulados que correspondem aos valores J/S práticos, para BER fixa de 4,8%. Comparando com as medidas práticas, a linha azul ficou dentro dos limites bloqueio para todas as frequência de varreduras de bloqueio esperadas. Para a frequência de varredura de 70 Hz o sistema permaneceu em operação nos dois casos, simulados e práticos.

Considerando os ganhos das antenas, foram retirados três valores de BER fixos das simulações do item 5.2.2 (FIG. 5.12).

Os valores de J/S simulados para uma BER foram plotados juntos com os valores práticos da FIG. 6.13. Os resultados estão ilustrados na FIG. 6.15. A linha em azul representa o limite de bloqueio simulado para uma BER fixa de 4,8% (0,048), a linha em verde representa o limite de bloqueio simulado para uma BER fixa de 3,2% (0,032), a linha em laranja representa o limite de bloqueio simulado para uma BER fixa de 2,1% (0,021) e a linha em vermelho pontilhada representa o limite de bloqueio encontrado na prática.

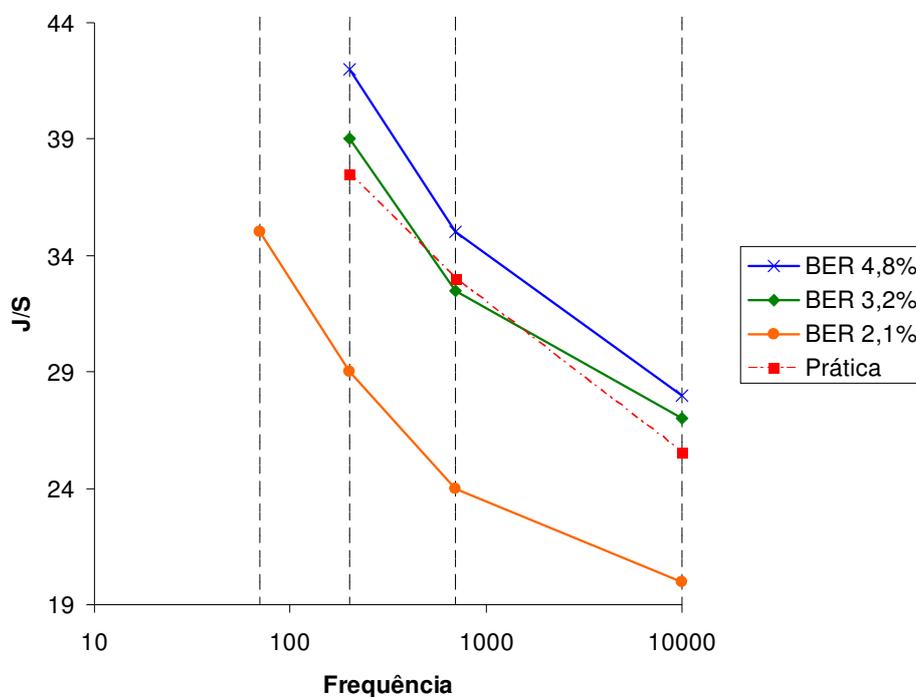


FIG. 6.15 – Resultados simulados e práticos, considerando os ganhos das antenas.

Para BER fixa de 2,1% era esperado nas simulações que o sistema permanecesse sempre em operação para todas as frequências de varredura do bloqueador, o que de fato ocorreu. Comparando com as medidas práticas, a linha laranja ficou dentro dos limites de operações para todas as frequências de varredura de bloqueio.

Considerando o limite de BER de 3,2%, era esperado nas simulações que o sistema permanecesse sempre em operação para a frequência de varredura de 70 Hz e para outras frequências de varredura o sistema ficasse inoperante. A linha verde do gráfico ilustra quais são os valores de J/S simulados que correspondem aos valores J/S práticos, para BER fixa de 3,2%. Comparando com as medidas práticas, para todas as frequências de varredura os valores práticos e simulados apresentaram valores com uma pequena diferença, que pode ser considerada normal. Para a frequência de varredura de 70 Hz o sistema permaneceu em operação nos dois casos, simulados e práticos.

Para BER fixa de 4,8% era esperado nas simulações que o sistema permanecesse em operação para a frequência de varredura de 70 Hz e para as outras frequências de varredura o sistema ficasse inoperante. A linha azul do gráfico ilustra quais são os valores de J/S simulados que correspondem aos valores J/S práticos, para BER fixa de 4,8%. Comparando com as medidas práticas, a linha azul ficou dentro dos limites bloqueio para todas as frequência de varreduras de bloqueio esperadas. Para a frequência de varredura de 70 Hz o sistema permaneceu em operação nos dois casos, simulados e práticos.

7 CONCLUSÕES E SUGESTÕES

Tendo como objetivo a análise da eficácia das técnicas de bloqueio sobre os principais sistemas de comunicações que operam com propagação no espaço livre, o presente trabalho apresentou estudo teórico, prático e experimental das principais técnicas de interferências e seus efeitos sobre os sistemas de comunicações CDMA, GSM e os baseados na norma militar MIL-STD-188-110B.

O trabalho abordou teoricamente as técnicas de modulações digitais e analógicas utilizadas pelos sistemas de comunicações, com foco nos sistemas CDMA e GSM e nos sistemas baseados na norma militar MIL-STD-188-110B, as técnicas de bloqueio do tipo CME, as técnicas de espalhamento espectral, o ganho de processamento de sistemas que utilizam técnicas de espalhamento espectral, a determinação da relação J/S e a margem de bloqueio M_J .

Para modulação analógica em amplitude o trabalho apresentou um estudo teórico e prático sobre sistemas que trabalham em altas frequências, sendo amostrados em banda base através do conceito de sub-amostragem. A modulação analógica foi o laboratório inicial do trabalho. Com a utilização desta técnica foi possível:

- Definir toda a formulação matemática envolvida, como a expressão geral para o sinal AM modulado, o espectro do sinal AM, a potência transmitida e a SNR na entrada do receptor AM;
- Aplicar o conceito de sub-amostragem; e
- Familiarizar-se com todas as ferramentas de trabalho aplicadas na dissertação, como por exemplo, a ferramenta computacional MatLab 7.0.

Dentre as técnicas de bloqueio do tipo CME, o trabalho abordou sucintamente as técnicas CME radar, CME infravermelho/laser e CME de comunicações. Foi dada ênfase à técnica CME de comunicações, por ser o foco principal do trabalho, sendo apresentadas formas para sua implementação.

Foi apresentado um estudo teórico sobre técnicas de espalhamento espectral DSSS, FHSS e THSS. Com o entendimento das técnicas de espalhamento espectral e das técnicas de bloqueio do tipo CME de comunicação, foram apresentados quais são as melhores técnicas de

bloqueio a serem utilizadas em sistemas com espalhamento espectral por sequência direta (DS), com salto em frequência rápido (FFH) e salto em frequência lento (SFH).

Para o sistema CDMA, o trabalho revisou o modelo de geração de bloqueio em terminais IS-95 apresentado por TOSCANO (2006), incluindo os seguintes passos:

- Abordagem teórica sobre o funcionamento do sistema CDMA, com o padrão IS-95;
- Determinação do valor do parâmetro sinal-bloqueio; e
- Apresentação de uma proposta para efetivação do bloqueio em parte da banda com um bloqueador PBN, em parte da banda com um bloqueador pontual com varredura e bloqueio sobre um único canal do sistema (canal 283).

Para o GSM foi realizada abordagem semelhante, incluindo os seguintes passos:

- Análise teórica sobre o funcionamento do sistema GSM, seguindo as normas internacionais definidas pelo Instituto Europeu de Padrões de Telecomunicações (ETSI);
- Determinação do valor do parâmetro sinal-bloqueio; e
- Apresentação de uma proposta para efetivação do bloqueio na faixa de downlink com um bloqueador PBN e um bloqueio na faixa de downlink com um bloqueador pontual com varredura.

Para sistemas militares baseados no padrão Militar STD-188-110B, foram realizadas abordagens semelhantes àquelas para os sistemas comerciais, incluindo os seguintes passos:

- Análise teórica sobre o funcionamento da norma MIL-STD-188-110B; e
- Apresentação de uma proposta para efetivação do bloqueio em toda banda com um bloqueador BBN, em toda banda com um bloqueador pontual com varredura e bloqueio sobre um único canal do sistema.

Através da ferramenta computacional Matlab 7.0 (Simulink), foram implementados diagramas de blocos das réplicas de:

- Técnicas de bloqueio do tipo CME de comunicação;
- Modelo do canal de tráfego do CDMA IS-95;

- Modelo do canal de tráfego do sistema GSM; e
- Modelo do canal de tráfego de sistemas militares baseados na norma MIL-STD-188-110B.

Com a elaboração das técnicas de bloqueio do tipo CME de comunicação e dos sistemas comerciais e militares no Matlab 7.0 (Simulink), o trabalho possibilitou:

- O entendimento do modelo de canal de tráfego dos sistemas CDMA IS-95, GSM e da norma MIL-STD-188-110B através de diversas simulações;
- A verificação do funcionamento dos sistemas na presença de bloqueadores do tipo CME de comunicação; e
- A determinação da relação J/S para efetivação do bloqueio em diferentes condições de operação.

Por fim, foi projetado e implementado um dispositivo bloqueador por varredura para a faixa de 1805 à 1880 MHz para realização de testes práticos sobre os sistema de telefonia móvel GSM, cujos resultados foram apresentados e comentados.

As simulações computacionais e os testes práticos mostraram que é possível, em condições bem definidas, bloquear sistemas que utilizam técnicas de espalhamento espectral.

Além das análises dos sistemas considerados, o trabalho deixa uma ferramenta computacional para simulação de sistemas bloqueadores, a qual pode ser usada para especificação das condições de funcionamento dos sistemas de bloqueio para os presentes e vindouros sistemas de comunicação com poucas adaptações, em múltiplas bandas de operação.

Como sugestões para trabalhos futuros, são apresentados os seguintes temas:

- Ampliação dos estudos teóricos e experimentais das técnicas de bloqueio seguidor e de bloqueio inteligente;
- Ampliação dos estudos sobre a norma MIL-STD-188-110B e desenvolvimento de um bloqueador para os rádios militares que utilizam essa norma;
- Simulações dos sistemas de comunicações considerando os efeitos de propagação para diferentes terrenos e ambientes urbanos;

- Realização de um estudo teórico e prático sobre um bloqueador por varredura que atue sobre múltiplas bandas de frequências; e
- Implementação de um algoritmo de salto em frequência para os sistemas GSM e para norma MIL-STD-188-110B, para avaliação mais realística das técnicas utilizadas.

8 REFERÊNCIAS BIBLIOGRÁFICAS

- ABU-RGHEFF, M. A. **Introduction to CDMA Wireless Communications**. Elsevier, 2007.
- ADAMY, D. L. **A Second Course in Electronic Warfare**, Artech House, 2004.
- ADAMY, D. L. **Introduction to Electronic Warfare Modeling and Simulation**, Artech House, 2003.
- AGUIAR, A. R. S. e DA SILVA, G. D. **Protótipo de um Oscilador Colpitts para Bloqueadores Multi-Faixa em Sistemas de Comunicação Wireless**. Projeto de Fim de curso, Instituto Militar de Engenharia - IME, Rio de Janeiro, Novembro 2004.
- BAUCH, G., FRANZ, V. **Iterative Equalization and Decoding for the GSM – System**, Munich University of Technology, 1998.
- BARROSO, M. M. **Radio communication and forest livelihoods in Brazilian Amazonian**. Tese de Doutorado, University of London, 2006.
- BITTENCOURT, **Técnicas de Modulação Digital, Correção de Desvios de Frequências e Sincronização de Relógio para Transmissão Digital em Canais de HF**. Projeto de fim de curso, Instituto Militar de Engenharia - IME, Rio de Janeiro, Dezembro 2008.
- BRASIL. Lei complementar nº. 97, de 9 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. **Diário Oficial da República Federativa do Brasil, Brasília**, 16 jun. 1999.
- DANTAS, M. B. T. **Desempenho de Protocolos TCP e de Camada de Enlace para Canal HF. Dissertação de Mestrado**, Instituto Militar de Engenharia, 2006.
- DILLINGER, M., MADANI, K., ALONISTIOTI, N. **Software Defined Radio; Architectures, Systems and Functions**. Wiley, 2003.
- FILHO, C. A. B. S., DE ANDRADE, D. V. e BISPO, F. A. B. **Protótipo de um Bloqueador de Celular para a Faixa de 800 a 900 MHz**. Projeto de Fim de curso, Instituto Militar de Engenharia - IME, Rio de Janeiro, Novembro 2003.
- GIT. **Basic EW Concepts. Apostila técnica sobre guerra eletrônica**, Georgia Institute Technology, 2001.

- GOODMAN, D. J. **Wireless Personal Communications Systems**. Addison-Wesley Wireless Communications Series, 1997.
- GSM 05.01, **Digital cellular telecommunications system (Phase 2+), Physical layer on the radio path, General description**. European Telecommunications Standards Institute, 2000.
- GSM 05.02, **3rd Generation Partnership Project, Technical Specification Group GSM/EDGE, Radio Access Network, Multiplexing and multiple access on the radio path**. European Telecommunications Standards Institute, 2001.
- GSM 05.03, **Digital cellular telecommunications system (Phase 2+), Channel coding**. European Telecommunications Standards Institute, 2005.
- GSM 05.04, **Digital cellular telecommunications system (Phase 2+), Modulation**. European Telecommunications Standards Institute, 2001.
- GSM 05.05, **Digital cellular telecommunications System (Phase 2+), Radio Transmission and Reception**. European Telecommunications Standards Institute, 2005.
- GSM 05.08, **Digital cellular telecommunications System (Phase 2+), Radio subsystem link control**. European Telecommunications Standards Institute, 2000.
- HARTE, L. **Introduction to Mobile Telephone Systems**, Althos Publishing, 2nd ed., 2006.
- HAYKIN, S. **Communication Systems**. John Wiley & Sons, Inc, 4th ed, 2001.
- JODALEN, V., EGGEN, A. e GRONNERUD, B. S. **Military Messaging in IP Networks Using HF Links**. IEEE Communications Magazine, p. 98–104, 2004.
- JODALEN, V., EGGEN, A., SOLBERG, B. e GRONNERUD, O. **Performance Testing Of Stanag 4406 (Military Messaging) Using IP Over HF**. Technical report, Norwegian Defense Research Establishment (FFI), 2005.
- JR, P. W. P. e G.PLONISCH, I. **Military Applications of Information Technologies**. Air & Space Power Journal, Volume XVIII,(Nr 1), 2004.
- LEE J. S., MILLER L. E. **CDMA Systems Engineering Handbook**, Artech House, 1998.

- LEE, W. C. Y. **Mobile Cellular Telecommunications - Analog and Digital Systems**. McGraw-Hill, Inc, 1995.
- Li, T. **Digital Signal Processing: Fundamentals and Applications**. Academic Press, 1 edition, 2007.
- LOPES, R. S. e BARBOSA, L. C. S. **Estudo de Conversores A/D - D/A com Aplicação no Rádio Definido por Software**. Projeto de Fim de curso, Instituto Militar de Engenharia - IME, Rio de Janeiro, Agosto 2006.
- MIL-STD-188-110B, **Interoperability And Performance Standards For Data Modems**.
- MILSTEIN, L. B., DAVIDOVIC S., SCHILLING, D. L. **The Effects of Multiple-Tone Interfering Signal on a Direct Sequence Spread Spectrum Communications System**, IEEE Transactions on Communication, p. 436-448 vol. COM-30, 1982.
- POISEL, R. A. Poisel, **Introduction to Communication Electronic Warfare Systems**. Artech House, Inc., 2002.
- POISEL, R. A.R. A. Poisel, **Modern Communication Jamming Principles and Techniques**. Artech House, Inc., 2004.
- PRASAD, R. JANSEN, M. **Near-far-effects on Performance of DS/SS CDMA Systems for Personal Communication Networks**, IEEE Transactions on Vehicular Technology Conference, p. 710-713, 1993.
- PROAKIS, J. G. **Communication Systems Engineering**, 2nd Edition Prentice-Hall, 2002.
- RAPPAPORT, T. S. **Wireless Communications Principles and Practice**. PrenticeHall PTR, 1996.
- SAUNDERS, G. A. B. **Projeto de Antenas de Banda Larga: Estudo de Caso de um Monopolo Carregado com Parasitas Cônicos e Cilíndricos**. Dissertação de Mestrado, IME, 2009.
- SILVA, E. P. **Análise do Software de Controle de Uma Plataforma Estabilizada de Um Equipamento de Medida de Ataque Eletrônico – Um Modelo OO**. Projeto de Fim de curso, Universidade Federal do Rio de Janeiro - UFRJ, Rio de Janeiro, Maio 2007.

- SOUZA, C. R. M., **Interferidores de GPS: Análise do Sistema e de Potenciais Fontes de Interferência**. Dissertação de Mestrado, IME, 2005.
- STAHLBERG, M. **Radio Jamming Attacks Against Two Popular Mobile**. Helsinki University of Technology, 2000. Disponível: http://www.tml.tkk._/Opinnot/Tik-110.501/2000/papers/stahlberg.pdf>
- STEELE R., HANZO L. **Mobile Radio Communications: Second and Third-generation Cellular and WATM Systems**, WileyBlackwell, 2nd Edition, 1999.
- STEELE R., LEE C., GOULD P. **GSM, cdmaOne and 3G Systems**, John Wiley & Sons, 2001.
- STEELE R., **Mobile Radio Communications**, John Wiley & Sons, 1992.
- TOSCANO, R. S. Toscano, **Bloqueador de Múltiplas Frequências: Concepção do Sistema e Estudo de Caso para Terminais IS-95**. Dissertação de Mestrado, IME, 2006.
- TSENG, Y., HWANG, W. **The Influence of Propagation Environment in a Live GSM Network**, National Koahsiung University of Applied Sciences, 2001.
- WIGARD, J., NIELSEN, T.T, MICHAELSEN, P.H., SKJAERRIS, S., MAGENSEN, P. **The influence of discontinuous transmission on equal statistics in GSM**, IEEE Vehicular Technology Conference, V: 3, p. 2505-2509 vol.3, 1999.

9 APÊNCICES

9.1 APÊNCICE 1: SISTEMA COMERCIAL GSM

A interface com o ar no GSM utiliza dois esquemas de técnicas de múltiplos acessos (FIG. 2.16): TDMA e FDMA. No GSM o espectro é dividido 200 kHz (FDMA), denominados ARFCN (*Absolute Radio Frequency Channel Number*). Cada canal é dividido em 8 *timeslot* (TDMA), que tem duração de 4,6 ms (577 μ s/*timeslot*).

O GSM separa o *uplink* e o *downlink* em bandas de frequência distintas, mostradas na TAB. 9.1. Dentro de cada banda, o esquema de numeração de canais usado é o mesmo. Na verdade, um canal do GSM é formado por um *uplink* e um *downlink* (GSM 05.01, 200).

TAB. 9.1 – Bandas de Operações para o GSM.

Sistema	Downlink	Uplink
GSM900	935-960 MHz	890-915 MHz
DCS1800	1805-1880 MHz	1710-1785 MHz

Os oito *timeslots* juntos formam o frame do GSM, FIG. 9.1, que podem ocupar um dos 125 canais para o GSM 900 ou um dos 375 canais para o DCS1800.

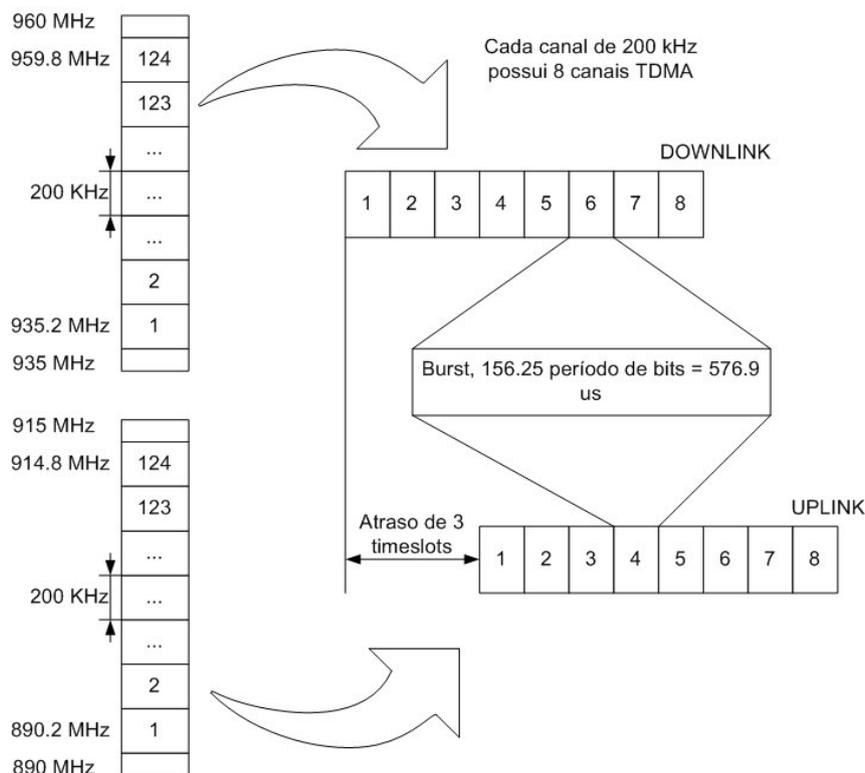


FIG. 9.1 - Frame do GSM 900.

O frame do TDMA da faixa de *uplink* é transmitido com um atraso de 3 *timeslots* com relação à faixa de *uplink*, FIG. 9.1. Esse atraso é utilizado para que a estação móvel não transmita e receba dado ao mesmo tempo, não necessitando de uma unidade duplexadora. Cada frame de TDMA utiliza uma rajada (*burst*) normal de 156,25 períodos de bits e cada *timeslots* possui uma duração de 576,9 μ s. Portanto, os oitos *timeslots* têm duração de 4,615 ms.

Segundo a norma GSM 05.02 (2001), a rajada (*burst*) de RF dos *timeslots* é dividido em (FIG. 9.2), (BAUCH, 1998):

- Bits finais (*tail bits*) - são grupos de três bits nulos colocado no início e no fim do fragmento de rajada útil;
- 57 bits codificadores – informação a ser enviada;
- 1 bit sinalizador de roubo (*stealing flag*) – indica ao receptor que tipo de dados é transportado pela rajada. Quando há necessidade de envio de informações urgentes ao usuário, os bits sinalizadores possibilitam “roubar” a rajada de tráfego para que sejam enviadas mensagens de controle;
- 26 bits de treinamento (*bits training*) – utilizado para sincronizar o receptor com a informação de chegada;
- 1 bit sinalizador de roubo (*stealing flag*);
- 57 bits codificadores;
- 3 bits finais (*tail bits*);
- Tempo de guarda (*guard time*) que tem comprimento de 8.25 bits e é utilizado para evitar a colisão de duas estações móveis.

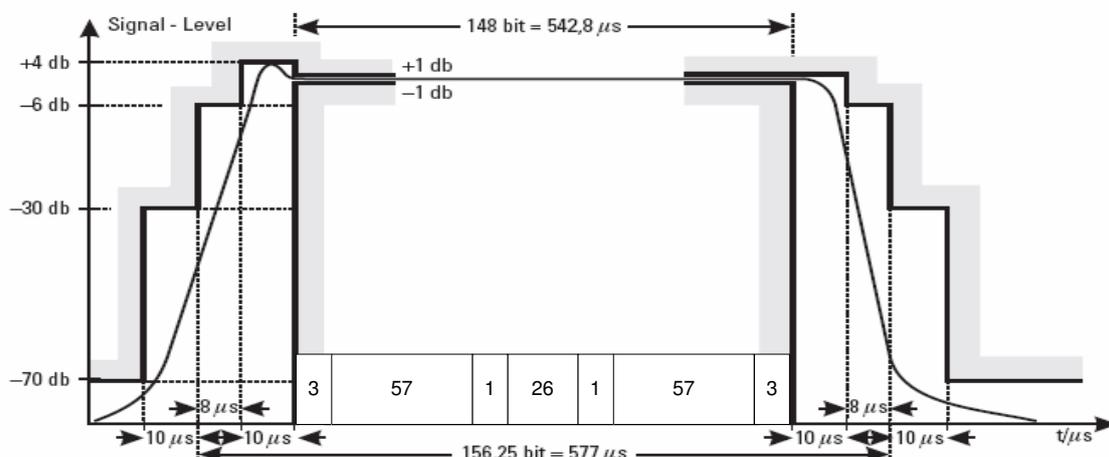


FIG. 9.2 - Rajada do sistema GSM.

O sistema GSM é um sistema de multiplexação por divisão de tempo. Um timeslot tem um período equivalente a 156,25 destes bits de dados. Como há 8 usuários em cada frequência, há 8 timeslots por quadro. Este padrão é repetido, dando aos usuários outros timeslots nos outros quadros. O intervalo do quadro é 4,615 ms. Os quadros são agrupados em estruturas maiores, denominadas multiquadros. Há dois tamanhos de multiquadros, os multiquadros de 26 quadros e os multiquadros de 51 quadros. O TCH usa multiquadros de 26 quadros, enquanto que o canal de radio fusão BCH usa pares de multiquadros de 51 quadros, um colocado após o outro para formar uma sequência de 102 quadros. Um superquadro é formado por 51 ou 26 multiquadros e um hiperquadro é formado por superquadros, FIG. 9.3.

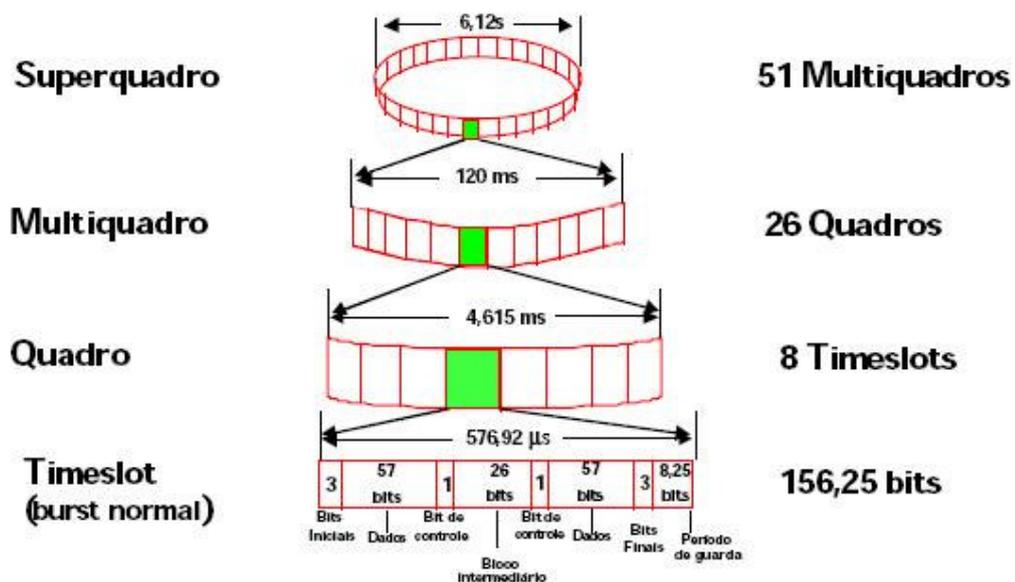


FIG. 9.3 – Timeslot, Quadro, Multiquadro e Superquadro do sistema GSM.

Além do canal de tráfego TCH, o GSM possui canais de controle e sinalização (GSM 05.02, 2001), FIG. 9.4.

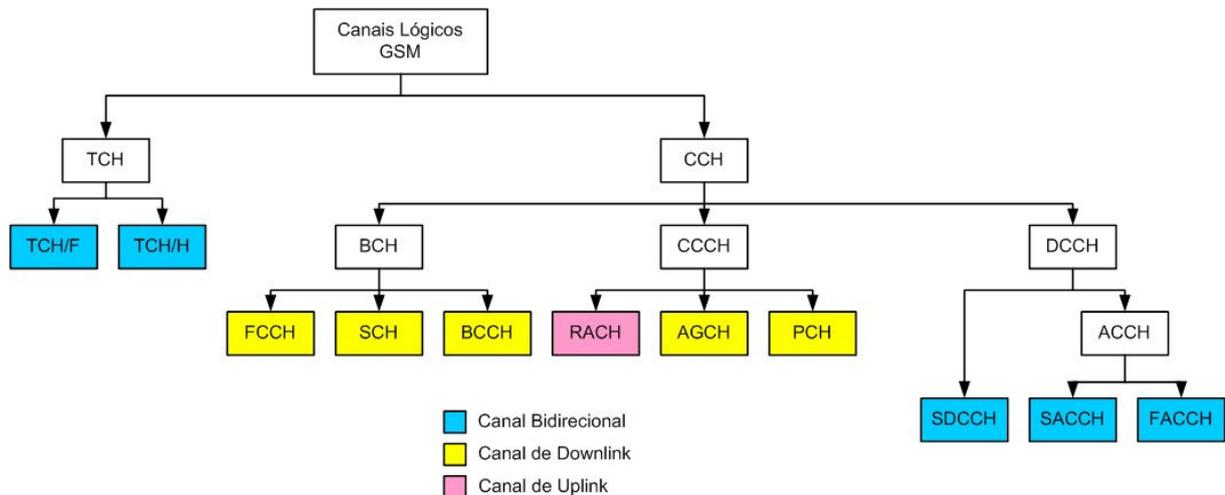


FIG. 9.4 – Canais lógicos do sistema GSM.

Existem três principais canais de controle CCH (*Control Channel*) no sistema GSM. São eles:

a) Canais de radiodifusão BCH (*Broadcast Channel*) – Os canais que o compõem são:

- Canais de correção de frequência FCCH (*Frequency Correction Channel*) - provê referências de frequências do sistema para a estação móvel;
- Canal de sincronização SCH (*Sincronization Channel*) - carrega as informações da BTS para a sincronização do frame;
- Canal de controle de radiodifusão BCCH (*Broadcast Control Channel*) - informar os parâmetros específicos para o móvel identificar a rede e ou ganhar acesso a ela, identificar o operador, as frequências de células vizinhas, os parâmetros de acesso e a sequência de saltos de frequências;

b) Canais de Controle Comum CCCH (*Common Control Channel*) – Formado por canais que trabalham nos enlaces direto e reverso no estabelecimento de chamadas. Os canais que o compõem são:

- Canal de Controle PCH (*Paging Channel*) - Utilizado pela BTS para anunciar as chamadas;
- Canal de concessão de acesso AGCH (*Access Grant Channel*) - anuncia o canal designado para o estabelecimento de chamada, podendo ser o canal de tráfego TCH;

- Canal de acesso randômico RACH (Random Access Channel) - utilizado quando a estação móvel identifica o número no canal PCH, reconhecendo que deve responder com uma solicitação de serviço, também enviada por este canal.

c) Canais de Controle Dedicados DCCH (*Dedicated Control Channel*) – Formado por canais associados a uma única MS, é responsável por validar a MS e estabelecer as chamadas. Os canais que o compõem são:

- Canais de Controle Dedicados Independentes SDCCH (Stand-Alone Dedicated Control Channel) - É um canal de controle alocado exclusivamente para uma estação móvel, que executa diversas operações como: registro do móvel, autenticação, atualização da localização, medidas do enlace, controle de potência, entre outros;
- Canal Lento de Controle Associado SACCH (*Slow Associated Control Channel*) - é usado para enviar lentamente, mas regularmente, informações de controle à unidade móvel. Por exemplo, a unidade móvel pode ser instruída a alterar a potência de transmissão ou avanço de *timing*.
- Canal Rápido de Controle Associado FACCH (Fast Associated Control Channel) - é usado para mensagens de eventos, como informações sobre handover e autenticação.

O canal de tráfego TCH é responsável pelo envio de voz e dados codificados tanto no downlink quanto no uplink. Para transmissão de voz o canal TCH pode ser utilizado de duas maneiras distintas, TCH/F (taxa de 13 kbit por segundo) e TCH/H (taxa de 6,5 kbit por segundo). O presente trabalho utiliza um canal de tráfego TCH/F, que fornece 260 bits por bloco de conversação de 20 ms (GSM 05.03, 2005), resultando na taxa de 13 kbit por segundo. Os bits de saída são ordenados, conforme a sua importância, em grupos de classe Ia, classe Ib e classe II.

A natureza da interface aérea GSM resulta na introdução de alguns erros de bit. Os bits são manipulados de forma que haja uma maior probabilidade de que os erros ocorram onde prejudiquem menos. A qualidade do som é mais afetada pelos bits de coeficientes mais significativos do que pelos bits menos significativos. Os bits de menor importância, ou bits de tipo II, não têm correção ou detecção de erros. Os bits mais importantes, de tipo Ia, têm

detecção de erro, com a inclusão de bits de CRC. No tipo Ia e o tipo de importância média Ib, há a inclusão de bits de correção de erro convolucional.

O processo de codificação do GSM consiste em: adição de 3 bits de paridade aos 50 bits da classe Ia, código de blocos, adição de 4 bits '0' aos 132 bits da classe Ib mais a saída do código de blocos, resultando em 189 bits. O código convolucional recebe os 189 bits e gera 378 bits codificados. A saída do codificador é somada com os 78 bits não protegidos da classe II, totalizando 456 bits codificados.

Os 456 bits de dados de conversação são divididos em 8 blocos de 57 bits codificadores, *interleaving*. Cada *rajada* do TCH transporta dois blocos de 57 bits codificadores de dados provenientes de dois segmentos diferentes de 20 ms de conversação com 456 bits.

Com os dois blocos de 57 bits codificadores o sistema adiciona os bits restantes e monta a *rajada* do GSM como ilustrado na FIG. 9.2.

Os níveis de potências transmitidos pelo sistema GSM são apresentados na TAB. 9.2, (GSM 05.05, 2005).

TAB. 9.2 - Níveis de potência no GSM.

		MAX	MIN
GSM900	MS	39 dBm	5 dBm
	BTS	58 dBm	9 dBm
DSC1800	MS	30 dBm	0 dBm
	BTS	46 dBm	17 dBm

Segundo a norma GSM 05.04 (2001), o GSM utiliza a modulação GMSK com índice de modulação de 0,5 e velocidade de modulação de 270 kbps. A largura de banda normalizada (WT_b) do filtro gaussiano utilizado depois do estágio de modulação é de 0,3. A modulação GMSK foi detalhada no item 2.1.2.2.

O salto em frequência no GSM tem como objetivo a redução do desvanecimento rápido causado pela movimentação dos assinantes. A sequência de saltos pode utilizar mais de 64 frequências diferentes, que é um número muito menor comparado aos sistemas militares com FH desenvolvidos para evitar bloqueios e escutas.

9.2 APÊNCICE 2: NORMA MIL-STD-188-110B

A norma MIL-STD-188-110B é aplicável para a concepção e desenvolvimento de sistemas operando a uma taxa de transmissão de 2400 baud (símbolos por segundo) e velocidade de transmissão de 75, 150, 300, 600, 1200, 2400 e 4800 bps.

O diagrama em blocos representativo da sequência para estruturação de quadros prevista na norma é ilustrado na FIG. 9.5

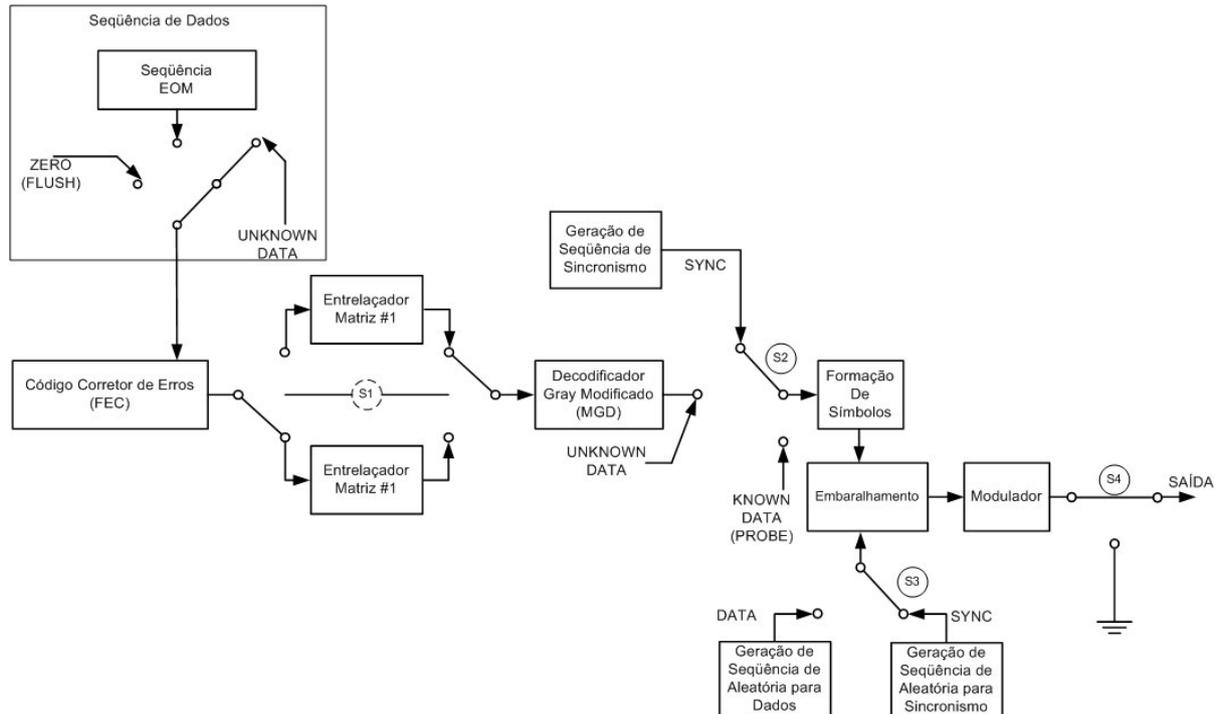


FIG. 9.5 - Diagrama do transmissor definido pela norma MIL-STD-188-110B.

A seguir são descritos os blocos do esquema da FIG 2.20.

9.2.1 BLOCO DE SEQUÊNCIA DE DADOS

As seqüências pseudo-aleatórias de dados são geradas no Bloco de Seqüência de Dados, as quais seguem uma distribuição uniforme, *UNKNOWN DATA*. A esses dados deverão ser justapostos bits de fim de mensagem (EOM). Oitos números hexadecimal representam a seqüência EOM, 4B65A5B2, e devem ser representados da esquerda para direita.

9.2.2 BLOCO DE CÓDIGO CORRETOR DE ERROS (FEC)

A norma MIL STD-188-110B recomenda o emprego de um código convolucional de taxa 1/2 e memória igual a 7 para as velocidades de transmissão 600, 1200 e 2400 bps, que geram fluxo de dados codificados a 1200, 2400 e 4800 bps, respectivamente. Os polinômios geradores são dados por: $T_1(x) = 1 + x + x^3 + x^4 + x^6$ e $T_2(x) = 1 + x^3 + x^4 + x^5 + x^6$.

O diagrama em blocos da FIG. 9.6 ilustra o codificador especificado pela norma.

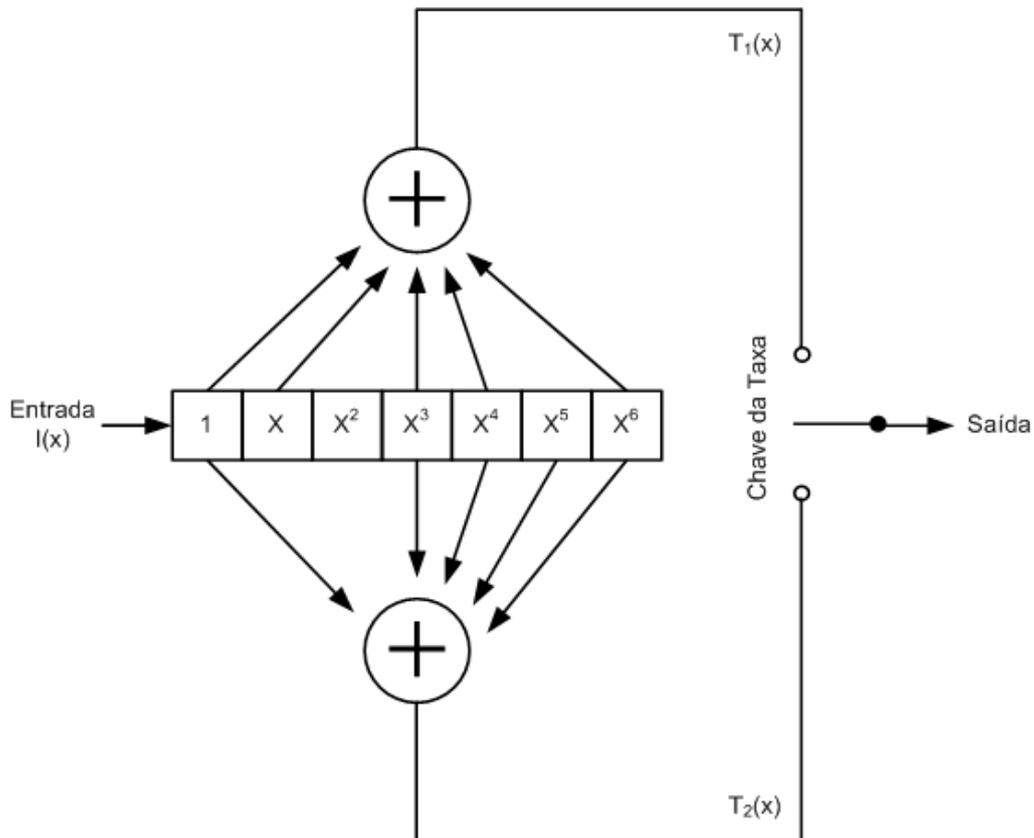


FIG. 9.6 - Diagrama do codificador convolucional.

Para taxas de transmissão de 150 e 300 bps, combina-se o código convolucional com o código de repetição, gerando correção de erro com taxas 1/4 e 1/8, ou seja, os bits da saída do codificador devem ser repetidos o número de vezes necessário para gerar um fluxo de dados codificados a 1200 bps.

A norma estabelece o código de repetição como sendo uma alternância dos polinômios geradores na treliça do codificador tantas vezes quantas forem indicadas nas taxas efetivas do código, TAB. 9.3.

TAB. 9.3 - Relação entre taxa de transmissão e taxas do código com código de repetição.

Taxa de informação (bps)	Taxa efetiva do código	Método para cálculo da taxa do código
4800	Sem código	Sem código
2400	1/2	Taxa 1/2
1200	1/2	Taxa de código 1/2
600	1/2	Taxa de código 1/2
300	1/4	Taxa de código 1/2 repetido 2 vezes
150	1/8	Taxa de código 1/2 repetido 4 vezes

9.2.3 BLOCO ENTRELAÇADOR

O algoritmo padronizado pela norma consiste em carregamento e esvaziamento de matrizes por bits de informação seguindo determinados padrões. Os bits de entrada são armazenados em matrizes de entrelaçamento cujas dimensões são dependentes da taxa de informação empregada e do tipo de entrelaçador adotado pelo usuário, sendo duas as possibilidades previstas na norma (TAB. 9.4): longo (4,8 segundos) ou curto (0,6 segundos)

TAB. 9.4 - Dimensões da matriz de entrelaçamento.

Taxa de Bit (bps)	Entrelaçador longo		Entrelaçador curto	
	Nº. Linhas	Nº. Colunas	Nº. Linhas	Nº. Colunas
2400	40	576	40	72
1200	40	288	40	36
600	40	144	40	18
300	40	144	40	18
150	40	144	40	18

Para o carregamento destas matrizes, o primeiro bit de informação é armazenado na posição (1,1) da matriz, o segundo bit é inserido na posição (10,1) e assim sucessivamente aumentando a posição dos bits dentro da mesma coluna. Faz-se esse processo até que todas as 40 linhas desta coluna estejam carregadas e então o processo se repete para as demais colunas até que toda a matriz esteja carregada com os bits de informação. Para a taxa de 4800 bps não se adota código corretor de erro.

Depois de carregada, deve-se esvaziar a matriz a fim de restabelecer um vetor contendo os bits de informação embaralhados. Para tal, retira-se o primeiro bit da posição (1,1), a posição do próximo bit é determinada incrementando em 1 o número da linha e decrementando em 17 o número da coluna. Ou seja, para uma taxa de 2400 bps com

entrelaçador longo, o segundo bit advém da posição (2,560), o terceiro bit de (3,543) e assim sucessivamente, até que toda a matriz tenha sido esvaziada.

Os bits obtidos do processo de entrelaçamento devem ser agrupados em um, dois ou três bits, para formar um símbolo, TAB. 9.5.

TAB. 9.5 - Numero de bits necessários para formação de um símbolo.

Velocidade de Transmissão (bps)	Número de bits
2400	3
1200	2
600	1
300	1
150	1

9.2.4 BLOCO DECODIFICADOR GRAY MODIFICADO (MGD)

A norma recomenda que cada um, dois ou três bits seguidos sejam mapeados em pontos das constelações das estratégias de modulação previstas na norma. A decodificação Gray para as taxas de 2400 e 4800 bps deve seguir a TAB. 9.6 e para as taxas de 75 bps (frequência fixa) e 1200 bps, a TAB. 9.7.

TAB. 9.6 - Decodificador Gray para 2400 bps e 4800 bps.

Bit de Entrada			Saída decodificada do MGD
Primeiro Bit	Bit do Meio	Último Bit	
0	0	0	000
0	0	1	001
0	1	0	011
0	1	1	010
1	0	0	111
1	0	1	110
1	1	0	100
1	1	1	101

TAB. 9.7 - Decodificador Gray para 75 bps (frequência fixa) e 1200 bps.

Bit de Entrada		Saída decodificada do MGD
Primeiro Bit	Último Bit	
0	0	00
0	1	01
1	0	11
1	1	10

9.2.5 BLOCO DE FORMAÇÃO DE SÍMBOLOS

A etapa de formação de símbolos consiste em mapear um, dois ou três bits oriundos da saída do MGD ou da sequência de sincronismo em “tribits” (sequência constituída por três bits), usando o esquema 8-PSK.

Para cada um dos dados transmitidos nas sequências de transmissão, o mapeamento é realizado de forma diferenciada. O Unknown Data, os símbolos devem ser tomados na saída do entrelaçador apenas enquanto o modem está transmitindo dados do usuário e o Probe é utilizado durante o período em que os dados de treinamentos são transmitidos

9.2.5.1 UNKNOWN DATA

Para todas as taxas de transmissão, cada um dos símbolos de um, dois ou três bits deve ser mapeado diretamente em um dos 8 tribits, como mostrado na FIG. 9.7. Para taxas de 150, 300 e 600 bps o tribit deve ser 0 ou 4. Na taxa de 1200 bps, o símbolo é formado por um “dibit”, que deve ser mapeado nos tribits 0, 2, 4 ou 6. Nas taxas de 2400 e 4800 bps, todos os tribits são usados na formação de símbolo.

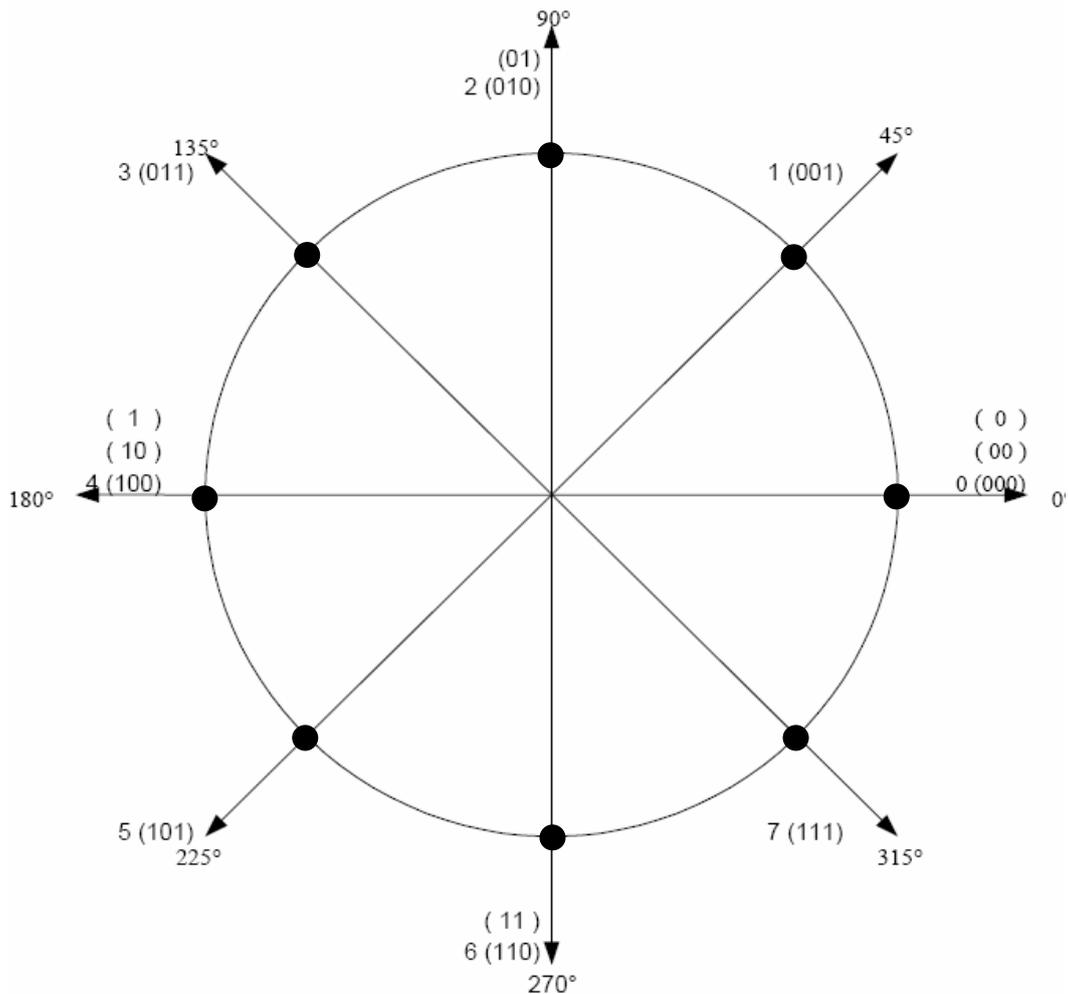


FIG. 9.7 - Constelação da modulação 8-PSK.

9.2.5.2 PROBE – SEQUÊNCIA DE TREINAMENTO

Durante os períodos em que dados de treinamento são transmitidos, a saída do formador de símbolos de canal deve ser sempre 0 (000), exceto para as duas sequências de símbolos que precedem a transmissão de um novo bloco de entrelaçamento, composto de 1440 símbolos para dados provenientes do entrelaçador curto e 11520 símbolos para o entrelaçador longo. Quando as duas sequências de símbolos que precedem a transmissão de um novo bloco de entrelaçamento são transmitidas, os 16 símbolos devem ser configurados por D1 e D2, respectivamente, como definido na TAB. 9.8.

TAB. 9.8 - Sequência de treinamento D1 e D2.

Taxa de Bit (bps)	Entrelaçador longo		Entrelaçador curto	
	D1	D2	D1	D2
4800	7	6	-	-
2400 (Voz Segura)	7	7	-	-
2400 (Dados)	6	4	4	4
1200	6	5	4	5
600	6	6	4	6
300	6	7	4	7
150	7	4	5	4
75	7	5	5	5

Estes dois padrões de símbolos são repetidos como indicado na TAB. 9.9. Nos casos onde a duração da sequência de treinamento seja de 20 símbolos, os últimos 4 tribits devem ser configurados como zero (000).

TAB. 9.9 - Mapeamento das sequência D1 e D2.

Símbolo	Tribits
000	(0000 0000) repetido 2 vezes
001	(0404 0404) repetido 2 vezes
010	(0044 0044) repetido 2 vezes
011	(0440 0440) repetido 2 vezes
100	(0000 4444) repetido 2 vezes
101	(0404 4040) repetido 2 vezes
110	(0044 4400) repetido 2 vezes
111	(0440 4004) repetido 2 vezes

Quando o tamanho do entrelaçador é configurado como zero, o padrão de treinamento que deve ser associado é o de 0,6 segundos.

9.2.6 BLOCO DE GERAÇÃO DA SEQUÊNCIA DE SINCRONISMO

A sequência de sincronismo é basicamente a mesma para todas as taxas de transmissão, dependendo do tamanho do entrelaçador (se zero, curto ou longo). Cada segmento que constitui a sequência consiste de 15 símbolos de canal: 0, 1, 3, 0, 1, 3, 1, 2, 0, D1, D2, C1, C2, C3, 0. Os valores de D1 e D2 devem ser configurados segundo o tamanho do entrelaçador e a taxa de transmissão do modem, TAB. 2.11. Os símbolos de canal C1, C2 e C3 representam a contagem do número de segmentos que foram enviados. Os valores de cada símbolo (C1, C2,

C3) devem ser lidos como uma palavra de 6 bits, onde C1 contém os 2 bits mais significativos. Os dois bits de cada símbolo C (C1, C2 e C3) devem ser convertidos a três bits adicionando o bit 1 como o bit mais significativo. Por exemplo, o número 23 é transformado no binário 010111. O passo seguinte é dividir a sequência binária em pares de bits, 01|01|11. Por fim é adicionado o bit 1 em cada par de bit, 101|101|111 (5|5|7). Então C1, C2 e C3 é igual a 5, 5, 7, respectivamente. Esta conversão está mostrada na TAB. 9.10.

TAB. 9.10 - Mapeamento de dois a três bits na sequência de sincronismo.

2 bits	Tribits mapeado
00	4 (100)
01	5 (101)
10	6 (110)
11	7 (111)

O mapeamento do símbolo de canal deve ser realizado conforme a TAB. 9.11.

TAB. 9.11 - Mapeamento das sequência C1, C2 e C3.

Símbolo	Tribits
000	(0000 0000) repetido 4 vezes
001	(0404 0404) repetido 4 vezes
010	(0044 0044) repetido 4 vezes
011	(0440 0440) repetido 4 vezes
100	(0000 4444) repetido 4 vezes
101	(0404 4040) repetido 4 vezes
110	(0044 4400) repetido 4 vezes
111	(0440 4004) repetido 4 vezes

9.2.7 BLOCO DE EMBARALHAMENTO

O algoritmo de embaralhamento consiste de uma soma entre o tribit proveniente do processo de formação de símbolos e o tribit fornecido pelo gerador de sequências aleatórias (dados ou sincronismo).

9.2.7.1 GERADOR DE SEQUÊNCIA ALEATÓRIA PARA DADOS

O gerador de sequências aleatórias é um registro de deslocamento de 12 bits, cujo diagrama funcional encontra-se na FIG. 9.8. No início da fase de envio de dados, o registro deve ser configurado com o valor de 101110101101, e devem ser deslocados 8 ciclos. São tomados três bits do registro e fornecidos ao bloco de embaralhamento em um valor de 0 a 7. A cada vez que um novo número é requerido, o registro deve ser deslocado em 8 ciclos e os novos bits são tomados do registro e fornecidos ao bloco de embaralhamento. A cada 160 transmissões de símbolo, o registro deve ser reiniciado com seu valor original.

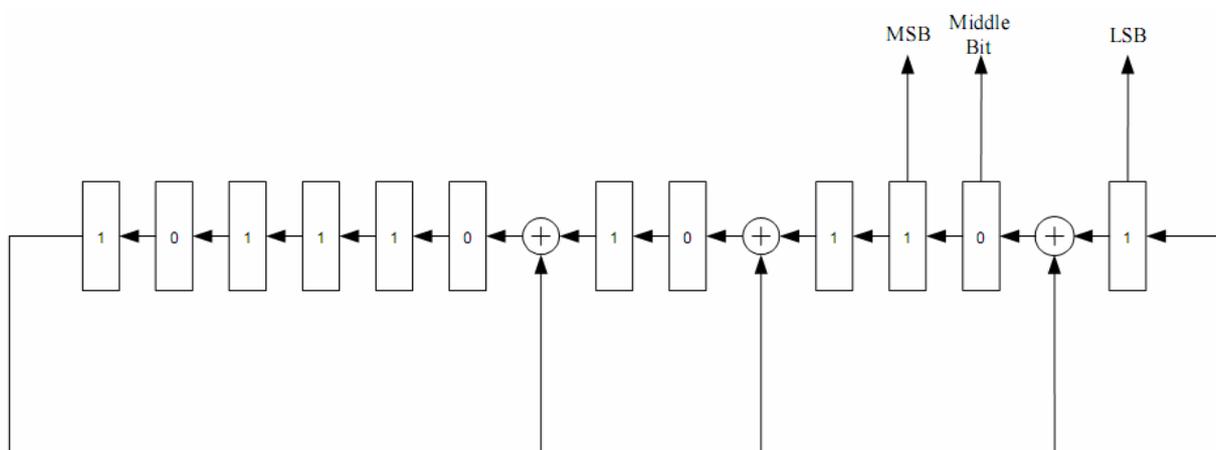


FIG. 9.8 - Registro de deslocamento para embaralhamento.

9.2.7.2 GERADOR DE SEQUÊNCIAS ALEATÓRIAS PARA O SINCRONISMO

A sequência 74305150221157435026216200505266 é utilizada para embaralhar os símbolos de sincronismo. Esta sequência deve ser repetida a cada 32 símbolos transmitidos.

9.2.8 BLOCO MODULADOR

Toda a estrutura de quadros que fora embaralhada é mapeada numa constelação 8-PSK, independente de qual tipo de modulação havia sido escolhida anteriormente na formação do símbolo.

A modulação 8-PSK deve ser realizada atribuindo os números de três bits (tribits) da saída do embaralhador a um sinal senoidal (portadora) com incremento de 45°. Desta forma tem-se: 0 (000) corresponde a 0 grau; 1 (001) corresponde a 45°; 2 (010) corresponde a 90°, etc.

9.2.9 BLOCO RECEPTOR

Uma vez tendo passado pelo canal, o sinal chega ao receptor. Neste precisa ser realizada uma amostragem para que os símbolos produzidos no transmissor possam ser recuperados.

Na primeira fase do processo de recepção é realizado o sincronismo de início de quadro. Nesse sincronismo, todo o sinal que chega ao receptor passa por um processo de correlação com uma parte do preâmbulo conhecida pelo receptor. Para sincronizar, o receptor precisa saber a taxa e o tipo de embaralhamento utilizado pelo transmissor, pois o preâmbulo é função desses dados. O Sincronismo correto significa a amostragem no momento ideal.

Após a fase de sincronismo, o sinal é recuperado e pode-se estimar a valor da BER do sistema.

Livros Grátis

(<http://www.livrosgratis.com.br>)

Milhares de Livros para Download:

[Baixar livros de Administração](#)

[Baixar livros de Agronomia](#)

[Baixar livros de Arquitetura](#)

[Baixar livros de Artes](#)

[Baixar livros de Astronomia](#)

[Baixar livros de Biologia Geral](#)

[Baixar livros de Ciência da Computação](#)

[Baixar livros de Ciência da Informação](#)

[Baixar livros de Ciência Política](#)

[Baixar livros de Ciências da Saúde](#)

[Baixar livros de Comunicação](#)

[Baixar livros do Conselho Nacional de Educação - CNE](#)

[Baixar livros de Defesa civil](#)

[Baixar livros de Direito](#)

[Baixar livros de Direitos humanos](#)

[Baixar livros de Economia](#)

[Baixar livros de Economia Doméstica](#)

[Baixar livros de Educação](#)

[Baixar livros de Educação - Trânsito](#)

[Baixar livros de Educação Física](#)

[Baixar livros de Engenharia Aeroespacial](#)

[Baixar livros de Farmácia](#)

[Baixar livros de Filosofia](#)

[Baixar livros de Física](#)

[Baixar livros de Geociências](#)

[Baixar livros de Geografia](#)

[Baixar livros de História](#)

[Baixar livros de Línguas](#)

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)