

UNIVERSIDADE FEDERAL DO PARÁ  
INSTITUTO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

# Processamento Digital de Sinais para Bloqueio de Telefonia Celular com Implementação de Protótipo em FPGA

Patrício Elvis Sousa Cordeiro

TD.XX/2014

UFPA / ITEC / PPGEE  
Campus Universitário do Guamá  
Belém-Pará-Brasil  
2014



UNIVERSIDADE FEDERAL DO PARÁ  
INSTITUTO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Patrício Elvis Sousa Cordeiro

Processamento Digital de Sinais para Bloqueio  
de Telefonia Celular com Implementação de  
Protótipo em FPGA

TD.XX/2014

UFPA / ITEC / PPGEE  
Campus Universitário do Guamá  
Belém-Pará-Brasil  
2014

UNIVERSIDADE FEDERAL DO PARÁ  
INSTITUTO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Patrício Elvis Sousa Cordeiro

# Processamento Digital de Sinais para Bloqueio de Telefonia Celular com Implementação de Protótipo em FPGA

Proposta de Tese de Doutorado para  
Exame de Qualificação submetida à  
Banca Examinadora do Programa de  
Pós-graduação em Engenharia Elétrica  
da Universidade Federal do Pará, como  
parte dos requisitos para a obtenção  
do Grau de Doutor em Engenharia  
Elétrica, ênfase em Telecomunicações.

UFPA / ITEC / PPGEE  
Campus Universitário do Guamá  
Belém-Pará-Brasil  
2014

UNIVERSIDADE FEDERAL DO PARÁ  
INSTITUTO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Processamento Digital de Sinais para Bloqueio de Telefonia Celular com  
Implementação de Protótipo em FPGA

**AUTOR: Patrício Elvis Sousa Cordeiro**

QUALIFICAÇÃO DE DOUTORADO SUBMETIDA À AVALIAÇÃO DA BANCA EXAMINADORA  
APROVADA PELO COLEGIADO DO PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA  
ELÉTRICA DA UNIVERSIDADE FEDERAL DO PARÁ A SER JULGADA PARA OBTENÇÃO DO GRAU  
DE DOUTOR EM ENGENHARIA ELÉTRICA NA ÁREA DE TELECOMUNICAÇÕES.

**JULGADA EM 28/11/2014**

**BANCA EXAMINADORA:**

.....  
.....

**Prof. Dr. Aldebaro Barreto da Rocha Klautau Júnior (ORIENTADOR - UFPA)**

.....  
**Prof. Dr. Adalbery Rodrigues Castro (MEMBRO-UFPA)**

.....  
**Prof. Dr. Carlos Aurélio Faria da Rocha (MEMBRO-UFSC)**

.....  
**Prof. Dr. Dionne Cavalcante Monteiro (MEMBRO-UFPA)**

.....  
**Prof. Dr. Johelden Campos Bezerra (MEMBRO-IESAM)**

**VISTO:**

.....  
**Prof. Dr. Evaldo Gonçalves Pelaes**

**COORDENADOR DO PPGEE/ITEC/UFPA**

# Resumo

A presente proposta consiste em apresentar sistemas inovadores para bloqueio de sinais de telefonia celular. Novos algoritmos e arquiteturas, assim como técnicas de processamento digital de sinais no processo da geração do sinal de bloqueio em banda base, combinado com técnicas de processamento analógico e de rádio frequência para gerar a versão do mesmo em RF, são propostos e explorados em experimentos simulados e práticos. Está no escopo do trabalho gerar um protótipo que permita validar os algoritmos na prática. Mais especificamente, são investigados bloqueadores do tipo A, os quais são dispositivos que visam interromper a comunicação entre um dispositivo móvel e sua estação de rádio base através da transmissão de um sinal de bloqueio nas mesmas frequências usadas pelos sistemas móveis para se comunicarem. Um protótipo baseado nos algoritmos e arquiteturas propostas, composto por uma unidade de lógica digital baseada em FPGA, o qual é flexível e reconfigurável, e um transmissor heteródino foram desenvolvido e devidamente testados em experimentos de geração do sinal de bloqueio em banda base e em RF, assim como sua aplicação em bloqueio dos sinais de telefonia celular. Resultados preliminares mostraram a eficiência do protótipo na geração do sinal para bloqueio de dois sistemas de telefonia móvel: LTE e GSM. Por fim, como planejamento para a pesquisa futura é proposta a implementação de novos algoritmos de classificação automática de tecnologias de acesso via rádio e sua incorporação no sistema do bloqueador, com o objetivo de identificar a RAT (em inglês *Radio Access Technology*) atuante em uma determinada área do espectro em situações onde as faixas de espectro são compartilhadas e, assim, gerar o sinal de bloqueio de maneira otimizada, de acordo com a RAT.

**PALAVRAS-CHAVES:** Bloqueadores de telefonia móvel, processamento de sinais, RAT, GSM, LTE, FPGA.

# Abstract

This proposal consists of researching innovative systems for jamming cell phone signals. New algorithms and architectures, as well as techniques of digital signal processing in the process of generating the baseband blocking signal, combined with techniques for analog and radio frequency processing to generate the RF version, are proposed and explored in simulation and practical experiments . Is in the scope of this work to generate a prototype that allows to validate the algorithms in practice. More specifically, type A jammers, which are devices that aim to disrupt communication between a mobile device and a radio base station by transmitting an RF signal in the same frequencies used by mobile systems to communicate are investigated. A prototype based on the proposed algorithms and architectures, consisting of an FPGA-based digital logic unit, which is flexible, reconfigurable, and an heterodyne-transmitter were developed and properly tested in experiments to generate baseband and RF jamming signal as well as its application in jamming mobile phone signals. Preliminary results show the efficiency of the prototype on generating signals for jamming two mobile phones: GSM and LTE. Finally, as planning for future research we propose implementation of new algorithms for automatic classification of radio access technologies and their incorporation in the jamming system, with the goal of identifying the active RAT in a particular area of the spectrum in situations of spectrum sharing and thus generate a jamming signal in a an optimized way according with the RAT.

**KEYWORDS:** Mobile jammers, signal processing, RAT, GSM, LTE, FPGA.

# Sumário

<b>Lista de Figuras</b>	<b>iii</b>
<b>Lista de Tabelas</b>	<b>vi</b>
<b>Glossário</b>	<b>vii</b>
<b>1 Tema e Proposta deste Trabalho</b>	<b>2</b>
1.1 Estrutura da Presente Proposta . . . . .	4
<b>2 Bloqueadores e Classificação de RAT: Conceitos e estado da arte</b>	<b>5</b>
2.1 Introdução . . . . .	5
2.2 Conceitos sobre Técnicas de Bloqueio para Telefonia Móvel . . . . .	6
2.3 Estado da Arte em Bloqueadores de Telefonia Móvel do Tipo A . . . . .	7
2.4 Conceitos de Sistemas de Telefonia Móvel: GSM e LTE . . . . .	10
2.4.1 Sistemas GSM . . . . .	10
2.4.2 Sistemas LTE . . . . .	13
2.5 Conceitos de Classificação de Tecnologia de Acesso via Rádio . . . . .	17
2.5.1 Estado da Arte em Classificação da Tecnologia de Acesso via Rádio . .	18
2.6 Conclusão . . . . .	19
<b>3 Sistema Proposto para Bloqueio de Telefonia Móvel</b>	<b>21</b>
3.1 Modelagem e Protótipo do Sistema Proposto . . . . .	21
3.2 Metodologia Proposta para Geração do Sinal em Banda Base . . . . .	23
3.2.1 <i>Peak-to-Average Power Ratio</i> para sinais multitom . . . . .	25
3.2.2 Razão sinal-ruído para sinais multitom . . . . .	26



3.3	Arquitetura para o Transmissor-Heteródino do Sistema de Bloqueador de Telefonia Móvel Proposto . . . . .	28
3.4	Ip-core para geração de sinais multitoom aplicados no bloqueio de sinais de telefonia móvel . . . . .	28
3.5	Introdução . . . . .	28
3.6	síntese digital direta . . . . .	28
3.6.1	Teoria de operação . . . . .	29
3.6.2	Metodologia para geração do sinal digital em banda base . . . . .	32
3.7	Protótipo Desenvolvido para o Bloqueador de Telefonia Móvel . . . . .	33
3.8	Conclusão . . . . .	39
<b>4</b>	<b>Resultados Preliminares</b>	<b>41</b>
4.1	Introdução . . . . .	41
4.2	Definição do Cenário Alvo de Bloqueio . . . . .	42
4.3	Determinação dos parâmetros para a geração do SB-BB . . . . .	43
4.4	Experimento 1: Resultados de Simulação em Matlab . . . . .	46
4.5	Experimento 2: Resultados da Implementação Prática . . . . .	51
4.6	Experimento 3: Bloqueio de sinais de LTE Em um Cenário Real . . . . .	56
4.7	Conclusão . . . . .	58
<b>5</b>	<b>Planejamento da Pesquisa Futura e Cronograma</b>	<b>61</b>
5.1	Cronograma Proposto . . . . .	64
<b>A</b>	<b>Classificação de Tecnologia de Acesso via Rádio Utilizando Weka</b>	<b>67</b>
A.1	Introdução . . . . .	67
A.2	Base de Sinais de Tecnologias de Acesso via Rádio . . . . .	67
A.3	Classificação de Tecnologias de Acesso via Rádio utilizando Matlab e Weka . .	68
A.3.1	Extração de Características . . . . .	68
A.3.2	Classificação de RAT utilizando o Weka . . . . .	68

# Lista de Figuras

2.1	Modelo de comunicação simplificado para BTM-A. . . . .	8
2.2	Esquema FDD com destaque das bandas UL e DL do sistema GSM800. . . . .	11
2.3	Ilustração de divisão de banda usando FDMA para GSM800. . . . .	12
2.4	Esquema de alocação de recursos tempo-frequência em sistemas GSM. . . . .	12
2.5	Esquemas de múltiplo acesso para DL e UL nos sistemas LTE. . . . .	14
2.6	Estrutura de recursos tempo frequência para DL nos sistemas LTE. . . . .	15
2.7	Diagrama em blocos simplificado representativo de um classificador de RAT. . .	18
3.1	Diagrama em blocos simplificado do sistema BTM. . . . .	22
3.2	ULD baseado em FPGA para geração do SBD-BB, $x[n]$ . . . . .	24
3.3	Diagrama em blocos simplificado do transmissor-heteródino. . . . .	30
3.4	PSD da cadeia do sinal no transmissor-heteródino. . . . .	31
3.5	Placa do protótipo de BTM desenvolvida para tese. . . . .	34
3.6	Esquema representativo em diagrama de blocos do protótipo do BTM: Destaque da estrutura <i>Top Level</i> do projeto HDL para a ULD. . . . .	35
3.7	Resposta em frequência de um FPB comercial típico. . . . .	37
3.8	Resposta em frequência de um filtro de RF empregado no canal 2 do protótipo do BTM para aplicações de LTE-B5. . . . .	38
3.9	Resposta em frequência de um filtro de RF empregado no canal 3 do protótipo do BTM para aplicações de GSM900. . . . .	39
4.1	LTE-B5: Ilustração do sinal na saída do <i>mixer</i> para $f_{LO} = 854$ MHz e $f_{LO} = 909$ MHz, respectivamente. . . . .	44
4.2	Ilustração do sinal na saída do <i>mixer</i> para $f_{LO} = 910$ MHz e $f_{LO} = 985$ MHz, respectivamente, para GSM900. . . . .	45

4.3	Resultado do SBD-BB computado com todos os valores do conjunto $\{\theta\} = 0$ . <b>superior</b> ) Sinal no domínio do tempo. <b>inferior</b> ) Sua magnitude da resposta em frequência. . . . .	47
4.4	Histograma da distribuição do SBD-BB para valores de $\{\theta\} = 0$ . . . . .	47
4.5	Comparação das características estimadas do SBD-BB com as teóricas (para $ \mathcal{K}  = 0$ até $ \mathcal{K}  = 1667$ ), computados com todos os valores do conjunto $\{\theta\} =$ 0: <b>superior</b> ) Potência do sinal. <b>médio</b> ) Potência do erro de quantização. <b>inferior</b> ) RSR. . . . .	48
4.6	Resultado do SBD-BB computado com com os valores do conjunto $\{\theta\}$ uniformemente distribuídos de $[-\pi, \pi]$ . <b>superior</b> ) Sinal no domínio do tempo. <b>inferior</b> ) Sua magnitude da resposta em frequência. . . . .	49
4.7	Histograma da distribuição do SB-BB para valores de $\theta$ aleatórios uniformemente distribuídos de $[-\pi, \pi]$ . . . . .	50
4.8	Comparação das características estimadas do SBD-BB com as teóricas (para $ \mathcal{K}  = 0$ até $ \mathcal{K}  = 1667$ ), computados com os valores do conjunto $\{\theta\}$ uniformemente distribuídos de $[-\pi, \pi]$ : <b>superior</b> ) Potência do sinal. <b>médio</b> ) Potência do erro de quantização. <b>inferior</b> ) RSR. . . . .	50
4.9	Top level do projeto de VHDL da ULD implementada para os dois canais do BTM. . . . .	51
4.10	A configuração dos componentes para o procedimento experimental. . . . .	52
4.11	PSD com medidas de potência do SB-BB para o LTE-B5 com zoom em seis canais. . . . .	53
4.12	PSD com medidas de potência do SB-BB para o LTE-B5 com zoom em seis canais.. . . .	54
4.13	PSD com medidas de potência dentro e fora da banda do SB-RF para o LTE-B5. . . . .	54
4.14	PSD com medidas de potência dentro e fora da banda do SB-RF para o GSM900. . . . .	55
4.15	Arcabouço para o experimento prático de bloqueio de sinais LTE. . . . .	57
4.16	Sinal do LTE recebido e decodificado no analisador do espectro. <b>superior</b> ) Constelação. <b>nferior</b> ) PSD. . . . .	58
4.17	Sinal do LTE recebido e (não decodificado) no analisador do espectro. <b>superior</b> ) Constelação. <b>Inferior</b> ) PSD. . . . .	59

5.1	Arcabouço proposto para um sistema integrado de classificação e bloqueio de RATs. . . . .	62
5.2	Exemplo ilustrativo de blindagem de sinais de RF em PCB. . . . .	63
5.3	Exemplo de uso de “cercas de vias” para proteger a trilha do sinal de RF. . . .	64
A.1	PSD dos sinais GSM LTE e WCDMA somados e modulados em IF. . . . .	69
A.2	Resultados obtidos no conjunto de teste do modelo criado pelo classificador. .	69
A.3	Resultados de acurácia obtidos no teste do modelo criado. . . . .	70
A.4	Matriz de confusão de confusão obtida nos teste do modelo criado. . . . .	70

# Lista de Tabelas

2.1	Resumo das principais características dos diferentes tipos de BTM. . . . .	8
2.2	Exemplo de bandas de frequência tipicamente usadas nos sistemas GSM. . . .	11
2.3	Exemplo de cinco bandas de operação e seus respectivos modos de duplexação para sistemas LTE. . . . .	13
2.4	Exemplos de parâmetros do LTE. . . . .	15
4.1	Parâmetros dos canais físicos dos STMs alvos: LTE-B5 e GSM900. . . . .	42
4.2	Sumário dos parâmetros especificados para a computação do do SB-BB. . . . .	46
4.3	Total do consumo do hardware do FPGA EP3C120F484C7 para implementação da ULD para dois canais . . . . .	51
5.1	Cronograma de execução das atividades futuras propostas. . . . .	66

# Glossário

3GPP	Third Generation Partnership Project
ARFCN	Absolute Radio Frequency Channel
BTM	Bloqueadores de Telefonia Móvel
CI	Circuito integrado
DAC	Digital to Analog Converter
DM	Dispositivo Móvel
EMI	Electromagnetic Interference
ERB	Estação de Rádio Base
ETSI	European Telecommunications Standards Institute
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
PAS	Processamento Analógico de sinais
PCI	Placa de Circuito Impresso
PDS	Processamento Digital de Sinais
PLL	Phase Locked Loop
RAT	Classificação de Tecnologias de Acesso via Rádio
RF	Rádio Frequência

ROM	Read-Only Memory
RSR	Razão Sinal-Ruído
SB	Sinal de Bloqueio
SB-RF	Sinal de bloqueio em Rádio Frequência
SBD-BB	Sinal de Bloqueio Digital em Banda Base
SMA	SubMiniature Version A
SPI	Serial Peripheral Interface
TDF	Transformada Discreta de Fourier
TH	Transmissor-Heteródino
ULD	Unidade Lógica Digital

# Capítulo 1

## Tema e Proposta deste Trabalho

A tese que é objeto da presente proposta consiste em pesquisar e gerar protótipos de sistemas inovadores para bloqueio de sinais de telefonia celular. A mesma tem por objetivo específico explorar técnicas de processamento digital de sinais para fazer o sensoriamento espectral e daí gerar o sinal de bloqueio (SB) em banda base, combinados com técnicas de processamento analógico e de rádio frequência (RF) para gerar a versão do mesmo em RF. Mais especificamente, no escopo dessa tese, o sensoriamento espectral consiste na classificação de tecnologias de acesso via rádio (RATc), de maneira a permitir que o sistema de bloqueio seja flexível e inteligente.

Nos últimos anos os telefones celulares tornaram-se ferramentas onipresentes em nossas vidas. Recentemente, esses dispositivos passaram de simples aparelhos de comunicação por voz para dispositivos inteligentes que permitem, em um único dispositivo, a transmissão de mensagens de texto, acesso à Internet, transmissão de vídeos e imagens e muito mais.

Amplamente usados, para simples conversas à transações comerciais, a importância do seu bloqueio em situações específicas aumenta, sejam por razões da garantia de um certo nível de silêncio e privacidade, tais como em salas de aula, igrejas, bibliotecas, cinema, teatro, etc; ou por questões de segurança, como prisões ou para evitar detonação de bombas improvisadas por terroristas por meio de dispositivos controlados via rádio.

Recentemente, os bloqueadores de telefonia móvel (BTM), que visam a interromper comunicação entre um dispositivo móvel (DM) e sua estação de rádio base (ERB), ganharam bastante popularidade como ferramenta de combate a utilização indesejável e/ou proibida de telefones móveis em locais e/ou situações específicas.

No Brasil, uma das aplicações mais promissoras dos BTM se encontra na área da segurança, mais especificamente, há uma grande demanda de bloqueio de telemóveis dentro



das prisões. O objetivo é evitar a comunicação via DMs entre prisioneiros e seus comparsas fora da prisão, fato que tem ocorrido com certa frequência nos presídios brasileiros nos últimos anos. Por este motivo vários BTMs vêm sendo instalados em diferentes prisões, em várias cidades do país, e legisladores vêm buscando modificar as regras, por exemplo, repassando às operadoras o dever de fazer o bloqueio. Existem várias categorias de BTM e uma classificação possível é baseada na técnica usada para interromper a comunicação do STM. Nesse caso, os mais simples e usados, transmitem um sinal de RF (ruído) nas mesmas frequências usadas pelos STM e, assim, bloqueiam a comunicação entre um dispositivo móvel e a sua ERB.

Geralmente, os BTMs que usam esta técnica são implementados mediante técnicas de processamento analógico de sinais (PAS), as quais fornecem pouca flexibilidade e seletividade espectral.

Nesta tese serão investigadas técnicas para se obter um sistema de BTM flexível e reconfigurável, o qual combine técnicas de processamento digital de sinais (PDS) e de PAS para gerar o sinal de bloqueio em banda base e em RF, respectivamente. O arcabouço do sistema proposto é formado por uma unidade lógica digital (ULD) e um transmissor-heteródino (TH) para gerar um sinal de bloqueio, onde este pode ser reconfigurado em tempo real para cobrir diferentes bandas do espectro.

Neste texto de qualificação, uma metodologia para gerar o SB digital em banda base (SBD-BB) é apresentada e avaliada em experimentos de PDS realizados no ambiente de simulação Matlab. Esta metodologia é estendida para uma implementação prática do mesmo. A parte da lógica digital é realizada usando um FPGA (*field programmable gate array*). Esse módulo é avaliado em experimentos práticos de geração de sinais em banda base.

Por fim é apresentado um protótipo do sistema BTM completo, desenvolvido na UFPA. O protótipo é testado em experimentos práticos de geração de SB em banda base e em RF.

As contribuições almejadas para a tese são:

- Propor novos algoritmos de processamento digital de sinais relacionados à geração do sinal de bloqueio e sensoriamento espectral.
- Desenvolvimento de um protótipo em hardware de maneira a validar a teoria, encontrar problemas práticos, rever os aspectos teóricos e obter benefícios desse ciclo virtuoso.
- Investigar técnicas para redução de custo computacional nas implementações de algoritmos em FPGA.
- Desenvolver e disponibilizar um conjunto de rotinas em software (“toolbox”) relacionados ao tema da tese.

- Publicar artigos científicos em periódicos qualificados.

Ressalta-se que as atividades práticas foram realizadas no Laboratório de Sensores e Sistemas Embarcados (LASSE) da UFPA. Parte desse trabalho foi financiado pela Brasilsat, empresa sediada em Curitiba, no âmbito de um projeto de pesquisa e desenvolvimento. Durante o projeto e a montagem de PCBs, o autor contou com a colaboração de alunos do LASSE.

## 1.1 Estrutura da Presente Proposta

O restante da presente proposta está organizado como segue.

No Capítulo 2 são introduzidos conceitos básicos sobre bloqueadores de telefonia móvel, com ênfase na descrição de diferentes técnicas usadas para bloqueio. Ainda, conceitos sobre sistemas GSM e LTE são apresentados e o capítulo é fechado com uma breve revisão sobre técnicas de classificação de tecnologias de acesso de rádio.

O Capítulo 3 ilustra o atual estágio da pesquisa através da apresentação da versão corrente de um sistema de bloqueio de telefonia celular baseado em técnicas de PDS e de RF.

No Capítulo 4 são apresentados os procedimentos e resultados experimentais obtidos pelo sistema atual, na geração de sinais digitais em banda base e em RF para BTMs, e na aplicação destes em cenário real, realizado no laboratório, de bloqueio de um sinal de telefonia.

Em seguida, no Capítulo 5 são apresentados comentários conclusivos, bem como as sugestões para a continuidade das pesquisas no escopo da tese proposta.

No apêndice A são apresentados alguns resultados preliminares em classificação de RAT usando os *softwares* matlab e Weka.

# Capítulo 2

## Bloqueadores e Classificação de RAT: Conceitos e estado da arte

### 2.1 Introdução

Este capítulo introduz conceitos e o estado da arte sobre BTMs, assim como conceitos introdutórios sobre duas RATs: LTE e GSM. O capítulo tem por objetivos específicos, explorar técnicas aplicadas em sistemas de BTM, com foco nos BTMs chamados de tipo “A” e, por outro lado, fornecer uma visão simplificada do funcionamento dos sistemas LTE e GSM, especificamente, no que se refere à estrutura da camada física dedicada à transmissão de dados, com ênfase nas técnicas de duplexação, bandas de espectro, métodos de acesso e canais de comunicação de dados. Tais conceitos são fundamentais para o desenvolvimento de estratégias, algoritmos e técnicas de bloqueio aplicados a estes sistemas.

Inicia-se o capítulo com a descrição de técnicas aplicadas em sistemas BTM para bloqueio de sinais de TM. Posteriormente, apresenta-se o estado da arte na área de BTMs, através de uma revisão bibliográfica detalhada, com ênfase nos BTM-A. Conclui-se o capítulo com a introdução de conceitos sobre as RATs, LTE e GSM.

## 2.2 Conceitos sobre Técnicas de Bloqueio para Telefonia Móvel

BTMs são dispositivos que visam interromper a comunicação entre um DM e sua ERB. A técnica usada para executar tal tarefa pode ser considerada inteligente, geralmente, quando o BTM usa técnicas sofisticadas para interagir com a ERB/DM, ou não-inteligente, quando não existe interação sofisticada entre o BTM e a ERB/DM.

Segundo [?], cinco tipos de BTM foram desenvolvidos ou já tiveram desenvolvimento planejado. Os cinco tipos foram classificados de “A” a “D”, baseados na técnica usada para bloquear os sinais dos SMs. Em seguida será descrito cada um dos tipos de BTM.

- **BTMs do Tipo “A”** - BTM-A são relativamente simples quando comparados aos outros tipos. Sua técnica de bloqueio consiste na transmissão contínua de SB em RF (SB-RF) nas mesmas frequências usadas pelo(s) SM(s) alvo(s). Quando ativos em uma determinada área, são capazes de bloquear a comunicação entre os DM's e a ERB envolvidos na área. O alcance do bloqueio é dependente da potência de transmissão do BTM e da sua separação dos DM's alvos. Geralmente, estes dispositivos não interagem com a ERB e, portanto, sua implementação não requer cooperação com os provedores da telefonia celular, o que torna seu projeto e implementação relativamente simples. Porém, possuem pouca seletividade espectral e podem facilmente interferir nos sistemas de comunicação vizinhos. Ainda, a transmissão conjunta de vários dispositivos em uma determinada faixa do espectro, pode aumentar o ruído de fundo e impedir o funcionamento adequado dos sistemas vizinhos, além de um relativamente alto consumo de potência.
- **BTMs do tipo “B”** - Dispositivos do tipo “B” buscam superar as dificuldades citadas através de uso de técnicas inteligentes que não requerem transmitir continuamente SB-RF em vastas bandas. O bloqueio é baseado na interação entre o BTM e a ERB, onde o primeiro intercepta as mensagens de sinalização enviados pela ERB para um determinado MD e, em seguida, instrui a mesma de que o respectivo MD se encontra em uma “*área de silencio*” e, portanto, não pode se comunicar. Esta técnica permite a realização de chamadas emergências para usuários habilitados e sua implementação requer cooperação com as operadoras de telefonia celular.
- **BTMs do tipo “C”** - Atuam como *beacon* e, quando localizados em uma “*área silenciosa*”, instruem todos os MD compatíveis a desabilitarem a sua operação. Porém, chamadas de emergência são possíveis para usuários pré-designados, através do uso de

uma chave de acesso, a qual permite inibir a resposta ao *beacon*. Esta técnica não causa interferências e não requer nenhuma mudança nos STMs atuais. Por outro lado, tais dispositivos não são capazes de impedir o funcionamento de DMs não compatíveis, fato que inviabiliza em muitas aplicações o seu desenvolvimento efetivo .

- **BTMs do tipo “D”** - Este tipo de BTM comporta-se como uma ERB pequena, independente e portátil. Estes dispositivos podem interagir diretamente de forma, inteligente ou não-inteligente, com o funcionamento do STM alvo. O BTM funciona predominantemente no modo de recepção (passivo) e o SB é mantido ativo apenas enquanto o MD tenta estabelecer uma conexão com a ERB, caso contrário, o sinal é interrompido e o BTM volta para o modo passivo. Esta técnica tem a vantagem de menor poluição eletromagnética em termos de potência bruta transmitida e do espectro de frequência. Portanto, o sistema é menos prejudicial ao tráfego de sistemas vizinhos. Esta técnica pode ser implementada sem cooperação com as operadoras de telefonia móvel, mas pode impactar negativamente nestes. Esta técnica tem uma vantagem sobre o tipo “B” por não gastar tempo ou esforço negociando com o STM. Assim como o tipo “B”, esta técnica também permite a realização de chamadas emergenciais.
- **BTMs do tipo “E”** - Por último, os BTMs do tipo “E” usam a técnica de supressão de EMI (*electromagnetic interference*, ou interferência eletromagnética) para transformar uma determinada sala em uma *gaiola de Faraday*, a qual, essencialmente, bloqueia ou atenua significativamente as radiações eletromagnéticas e não as permite entrarem ou saírem da sala (ou gaiola). Esta técnica não permite a realização de chamadas emergenciais a menos que se providencie uma forma de receber e decodificar tais chamadas, e então, prover um cabo coaxial de dentro para fora da sala de forma a receber e re-transmitir o sinal.

Um resumo, em termos de principais aspectos de funcionamento dos BTM-A à “D”, é apresentado na Tabela 2.1.

## 2.3 Estado da Arte em Bloqueadores de Telefonia Móvel do Tipo A

Como explicado, embora existam muitos tipos de BTMs [?], o mais comum e simples são os do tipo “A”, no qual o BTM visa a interromper a comunicação do STM por poluição espectral, ou seja, transmitindo um SB-RF nas mesmas frequências usadas por este para se

Tabela 2.1: Resumo das principais características dos diferentes tipos de BTM.

Tipos de BTM	Complexidade de implementação	Exige cooperação com a OTC	Chamadas emergenciais
A	Baixa	Não	Não
B	Alta	Sim	Sim
C	Alta	Não	Sim
D	Média	Não	Sim
E	Alta	Não	Não

comunicar. O objetivo é deteriorar a razão sinal-ruído (RSR) do sistema alvo a níveis que tornem a comunicação impossível.

Um modelo simplificado de comunicação para BTM-A é apresentado na Figura 2.1.

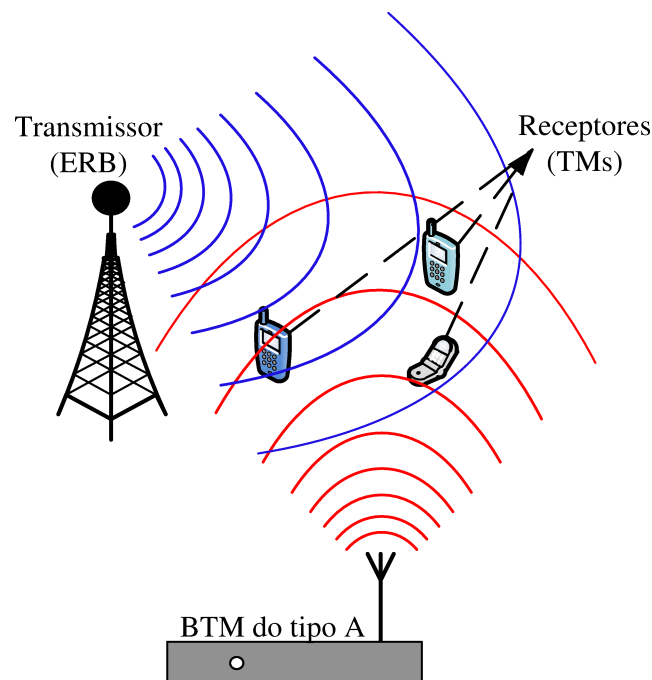


Figura 2.1: Modelo de comunicação simplificado para BTM-A.

O SB pode ser aplicado tanto na faixa de espectro reservado para o *downlink* (DL) (transmissão da ERB para DM), assim como no reservado para o *uplink* (UL) (transmissão do DM para ERB). No entanto, aplicar o bloqueio no DL é menos dispendioso em termos de potência total transmitida, devido ao BTM ser geralmente instalado próximo aos DMs alvos.

Para BTMs do tipo “A”, o uso de estratégias de múltiplo acesso pelo SM, como por exemplo, OFDMA e TDMA, são irrelevantes. Por exemplo, mesmo que a comunicação ocorra em intervalos de tempo (*timeslots*), o BTM gera o SB ininterruptamente. Assim, o canal de comunicação é representado aqui pela sua largura de banda  $B_c$  (por exemplo,  $B_c = 200$  kHz em um sistema GSM) e sua frequência da subportadora  $f_c^{RF}$ .

A faixa de frequência coberta pelo BTM-A pode variar significativamente de aplicação para aplicação [?]. O SB pode ser aplicado apenas nos canais de controle (por exemplo, no canal 0 com  $B_c = 200$  kHz de uma determinada célula de um sistema GSM [?]) ou em toda a banda (por exemplo, sobre 25 MHz para um sistema GSM com 124 canais). Desta forma, o BTM-A é subdividido aqui em BTM-Ac e BTM-Af, respectivamente.

BTM-Ac são descritos em [?, ?, ?] onde, em um cenário GSM, o SB é aplicado à canais de controle pré-selecionados. Esta técnica, por vezes referida como bloqueio inteligente, requer o conhecimento, a priori, das ARFCNs (*absolute radio frequency channel*) dos canais de controle e o bloqueio é normalmente restrito a alguma área específica. Por outro lado, este método reduz a poluição espectral e potência bruta transmitida, mas é dependente da RAT.

Em [?], o sistema de bloqueio monitora a potência recebida em um local fechado gerada por portadoras emitidas pelas ERB’s vizinhas. Em seguida, transmite o SB nas mesmas frequências e potência dos sinais de sinalização para perturbar o processo de controle e impedir a comunicação entre a ERB e os DMs. Em uma abordagem similar [?], o SB é transmitido apenas quando o a potência dos sinais de sinalização excede um limiar predefinido.

BTMs-Af foram investigados em [?, ?, ?], onde o SB é transmitido em todos os canais de um determinado sistema de comunicação.

A maioria dos trabalhos anteriores em BTM-A adotam processamento analógico para gerar o SB-BB, onde o processo é tipicamente realizado por meio de um oscilador controlado por tensão (VCO-*voltage controlled oscillator*, em inglês) a partir de uma forma de onda triangular ou por uma rampa. O SB gerado é um sinal de varredura em frequência, onde o tempo e o passo são geralmente controlados por um micro-controlador [?, ?, ?, ?, ?, ?].

Este método normalmente emprega circuitos integrados (CI) e/ou componentes discretos [?] no projeto do hardware do BTM. Desta forma, a precisão, em termos das componentes frequenciais geradas, é altamente dependente do desempenho de tais componentes. Por exemplo, resistores e capacitores são usados para definir a frequência de uma onda triangular usada para sintonizar o VCO [?]. A frequências de saída do VCO é controlada pelos valores de capacitância e resistência usadas. Porém, tais valores são geralmente definidos com tolerâncias (1%, 5%, etc) e também são sensíveis às mudanças de temperatura, o que pode causar variações significativas, imprevisíveis e incontroláveis nas frequência de saída do VCO.

Como resultado, o VCO pode produzir componentes em frequências fora da faixa desejada e, conseqüentemente, interferir com os sistemas de transmissão vizinhas.

Nota-se que o projeto de um BTM, seja este de que tipo for, exige conhecimentos específicos do STM alvo. Por exemplo, é necessário conhecer a largura de banda usada na transmissão, a faixa de espectro ocupada, as frequências das subportadoras, etc. Assim, para que esta proposta possa apresentar discussões concretas na próxima seção são introduzidos duas RATs: GSM e LTE, que são das mais importantes em termos comerciais. O objetivo é introduzir conceitos referentes às características básicas destes sistemas, principalmente no que se refere a estrutura da camada física para transmissão de dados.

## 2.4 Conceitos de Sistemas de Telefonia Móvel: GSM e LTE

Nesta seção são apresentados conceitos introdutórios sobre dois STMs: GSM e LTE. O objetivo é fornecer uma visão simplificada do funcionamento destes sistemas no que se refere a estrutura da camada física dedicada à transmissão de dados, com ênfase nas técnicas de duplexação, bandas de espectro, métodos de acesso e canais de comunicação de dados. Tais conceitos são fundamentais para o desenvolvimento de estratégias, algoritmos e técnicas de bloqueio aplicados a estes sistemas.

### 2.4.1 Sistemas GSM

GSM é um padrão digital de celular desenvolvido na Europa na década de 1980. O padrão GSM foi criado pela ETSI (european telecommunications standards institute) e atualmente é desenvolvido pela 3GPP (*Third Generation Partnership Project*). GSM é atualmente o padrão mais popular para telefonia móvel com mais de 4,4 bilhões de assinantes em mais de 200 países (junho de 2014)[?]. O GSM foi primeiramente desenvolvido para dar suporte a transmissão de voz e dados usando técnicas de modulação digital.

Os sistemas GSM utilizam FDD (*Frequency Division Duplex* ou duplexação por divisão de frequência). Devido ao FDD, o UL e o DL utilizam bandas de frequências distintas para comunicação. As bandas de UL e DL formam um par separado em frequência (*offset*), quer por 45 MHz, 80 MHz ou 95 MHz, dependendo do sistema GSM. Por exemplo, na Figura 2.2 é apresentado o esquema FDD do GSM800.

Os sistemas GSM usam faixas de espectro, *offsets*, e larguras de banda padronizadas.



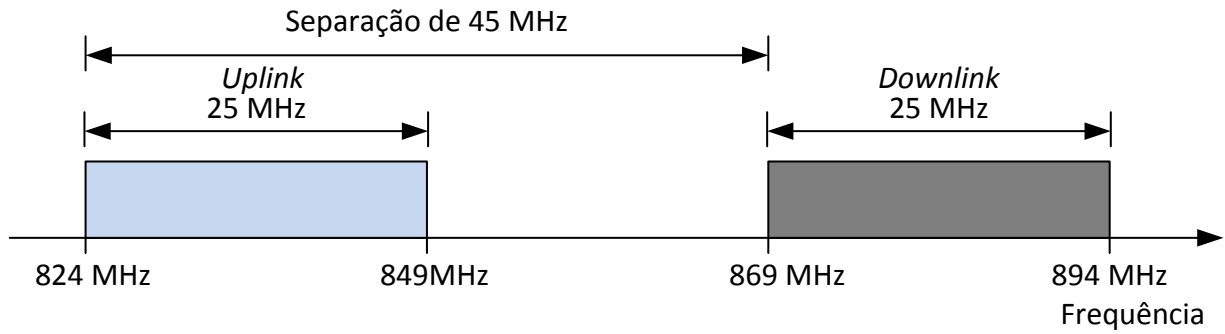


Figura 2.2: Esquema FDD com destaque das bandas UL e DL do sistema GSM800.

Algumas delas são listadas na Tabela 2.2.

Tabela 2.2: Exemplo de bandas de frequência tipicamente usadas nos sistemas GSM.

Sistema GSM	UL(MHz)	DL (MHz)	Largura de banda (MHz)	Separação (MHz)
GSM850	824 -849	869- 894	25	45
GSM900	890-915	935-960	25	45
GSM1800	1710-1785	1805-1880	75	95
GSM1900	1850-1910	1930-1990	60	80

Em termos de métodos de acesso ao canal, são usados dois métodos para permitir a comunicação simultânea de vários usuários com a ERB e, assim, aumentar a capacidade do sistema. O primeiro método é o FDMA (*frequency division multiple access*) ou acesso múltiplo por divisão de frequência, o qual consiste na divisão da banda total de frequência em  $n$  sub-portadoras ou canais espaçadas de  $\Delta_f^{GSM} = 200$  kHz com aproximadamente a largura de banda  $B_c = 200$  kHz cada, como apresentado na Figura 2.3.

O segundo método usado é o TDMA (*time division multiple access*) ou acesso múltiplo por divisão de tempo, o qual permite que vários usuários compartilhem o mesmo canal de frequência em intervalos de tempo (*timeslots*) diferentes. A estrutura básica de múltiplo acesso para um sistema GSM com largura de banda de 25 MHz é apresentada na Figura 2.4. Neste esquema, cada canal de frequência de 200 kHz é compartilhado por oito usuários, cujos dados são transmitidos em intervalos de tempo com duração de  $577\mu s$  (1 *slot*). Um conjunto de oito *slots* constitui um quadro (*frame*) TDMA, transmitido a cada 4.615 ms ( $8 \times 577\mu s$ ).

Os sistemas GSM usam uma variedade de canais para transmissão de informações. Estes canais são divididos em dois grupos: canais físicos e canais lógicos. Os canais físicos são determinados pelos *timeslots*, enquanto que os canais lógicos são caracterizados de acordo

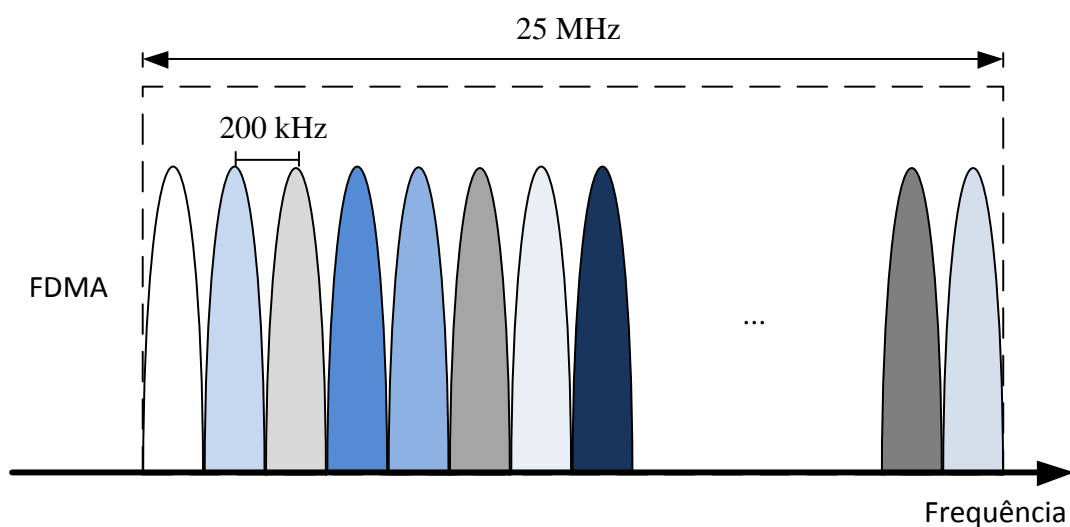


Figura 2.3: Ilustração de divisão de banda usando FDMA para GSM800.

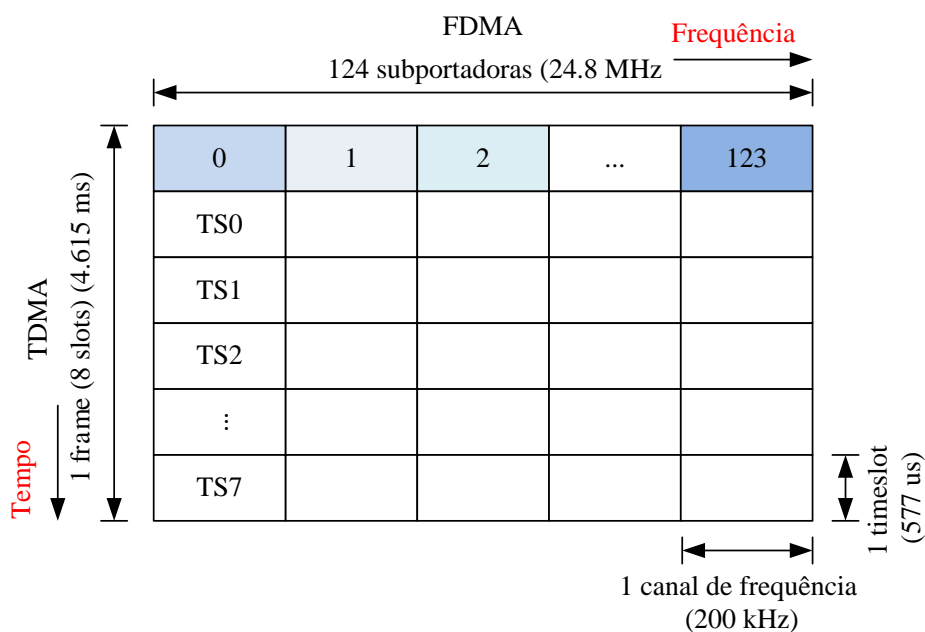


Figura 2.4: Esquema de alocação de recursos tempo-frequência em sistemas GSM.

com o tipo de informação transmitida nos canais físicos.

Os canais lógicos, por sua vez, são divididos em dois grupos: canais de tráfego (TCH - *traffic channels*) e canais de controle. Os TCH são canais destinados ao usuário para transmissão de voz ou de dados [?], enquanto que os canais de controle são usados para gerenciar toda a parte de sinalização para a gestão da mobilidade, controle de tráfego, etc [?].

## 2.4.2 Sistemas LTE

O LTE é a evolução do UMTS (*universal mobile telecommunication system* ou sistema universal de telecomunicações móveis) e constitui uma das mais recentes etapas de uma série de avanços de sistemas de telecomunicações móveis, juntamente com o LTE “Advanced” [?]. O desenvolvimento dos sistemas LTE pela 3GPP começou em 2004 e a primeira versão foi disponibilizada na versão 8 da série de especificações da 3GPP. O LTE é totalmente baseado em comutação de pacotes e seu objetivo é fornecer um desempenho superior aos das redes 3GPP anteriores baseadas em HSPA (*high-speed packet access* ou acesso a pacotes em alta velocidade), em termos de taxa máxima de dados, eficiência espectral, menor latência no plano do usuário e plano de controle e uma tecnologia de acesso de rádio otimizada e baseada em pacotes.

O LTE (por LTE assume-se aqui a versão 8) promete fornecer uma taxa máxima de dados de DL de 300 Mbps e de UL de 75 Mbps para uma alocação de espectro de 20 MHz.

LTE suporta tanto FDD como TDD e combina dois esquemas distintos de acesso múltiplo para DL e UL (Figura 2.5) [?]. Um exemplo de cinco bandas de operação e seus respectivos modos de duplexação para sistemas LTE é apresentado na Tabela 2.3

Tabela 2.3: Exemplo de cinco bandas de operação e seus respectivos modos de duplexação para sistemas LTE.

Banda Oper.	Uplink (MHz)	Downlink(MHz)	Modo de duplexação
1	1920-1980	2110-2170	FDD
2	1850-1910	1930-1990	FDD
5	824-849	869-894	FDD
33	1900-1920	1900-1920	TDD
34	2010-2025	2010-2025	TDD

No DL, o esquema de múltiplo acesso é o OFDMA (*orthogonal frequency division multiple access* ou acesso múltiplo por divisão ortogonal de frequência), onde a banda total é dividida em sub-bandas ou subportadoras ortogonais entre si e espaçadas de  $\Delta_f^{LTE} = 15$  kHz. Cada subportadora é atribuída a um usuário diferente, o que permite transmissão simultânea de vários usuários em frequências diferentes.

No UL, o esquema de múltiplo acesso é o SC-FDMA (*single carrier frequency division multiple access* ou acesso múltiplo por divisão de frequência e portadora única), onde a alocação

de banda é realizada de forma contígua de forma a possibilitar a transmissão de portadora única.

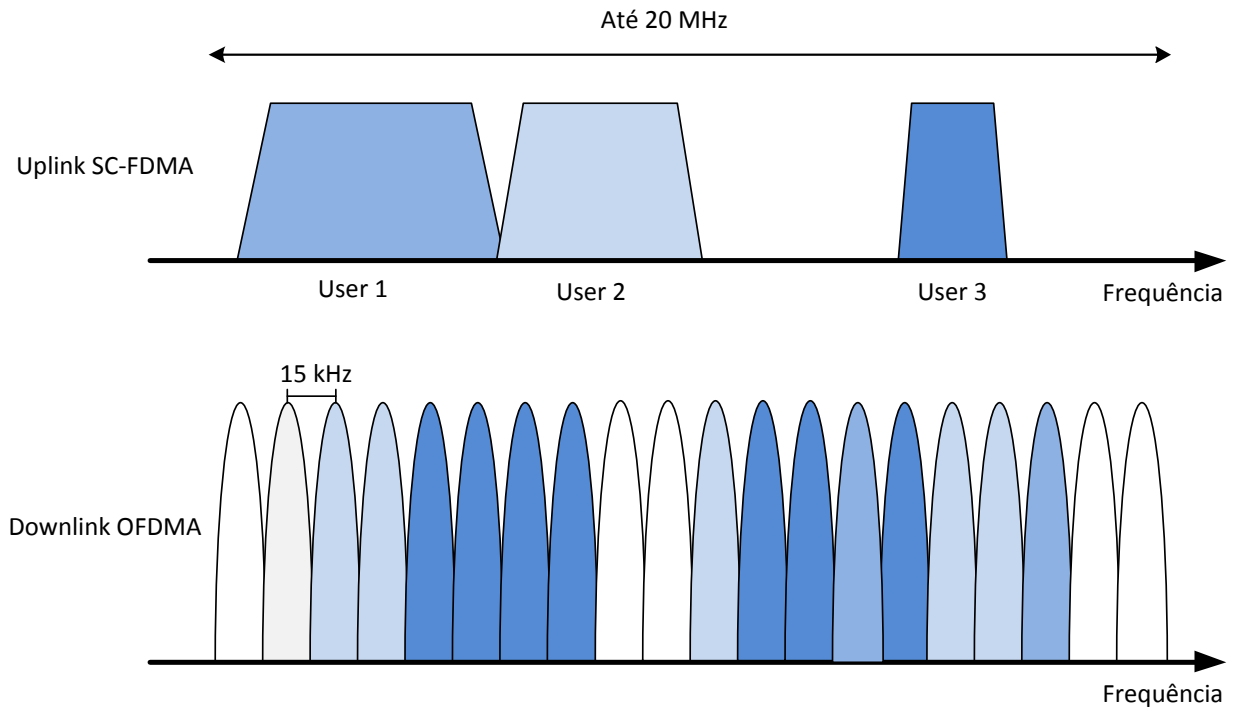


Figura 2.5: Esquemas de múltiplo acesso para DL e UL nos sistemas LTE.

O LTE foi projetado para suportar larguras de banda de transmissão diferentes, selecionadas dentre 1,4, 3, 5, 10, 15 e 20 MHz, dependendo da faixa do espectro disponível. Assim, a quantidade de recursos disponíveis depende da banda usada pelo sistema.

A estrutura detalhada dos recursos para DL (prefixo cíclico normal) para uma banda de 1,4 MHz é apresentada na Figura 2.6. Os recursos tempo-frequência para cada antena transmissora são divididos de acordo com a seguinte estrutura: No domínio de tempo, a maior unidade é o *frame* de rádio de 10 ms, o qual é subdividido em dez *subframes* de 1 ms cada. Cada *subframes* é dividido em dois *slots* de 0,5 ms e cada *slot* compreende sete símbolos OFDM.

No domínio da frequência, os recursos são agrupados em unidades de 12 subportadoras (ocupando assim um total de  $B_c = 180$  kHz, com um espaçamento de subportadora de 15 kHz), de tal modo que uma unidade de 12 subportadoras para uma duração de um *slot* é denominado de bloco de recursos (BR). A menor unidade de recurso é o elemento de recurso (ER), que consiste em uma subportadora para a duração de um símbolo OFDM. Portanto, um BR compreende 84 ER. Na Tabela 2.4 são exemplificados esses parâmetros.

A alocação de recursos no domínio da frequência, tanto no UL como no DL, é realizada

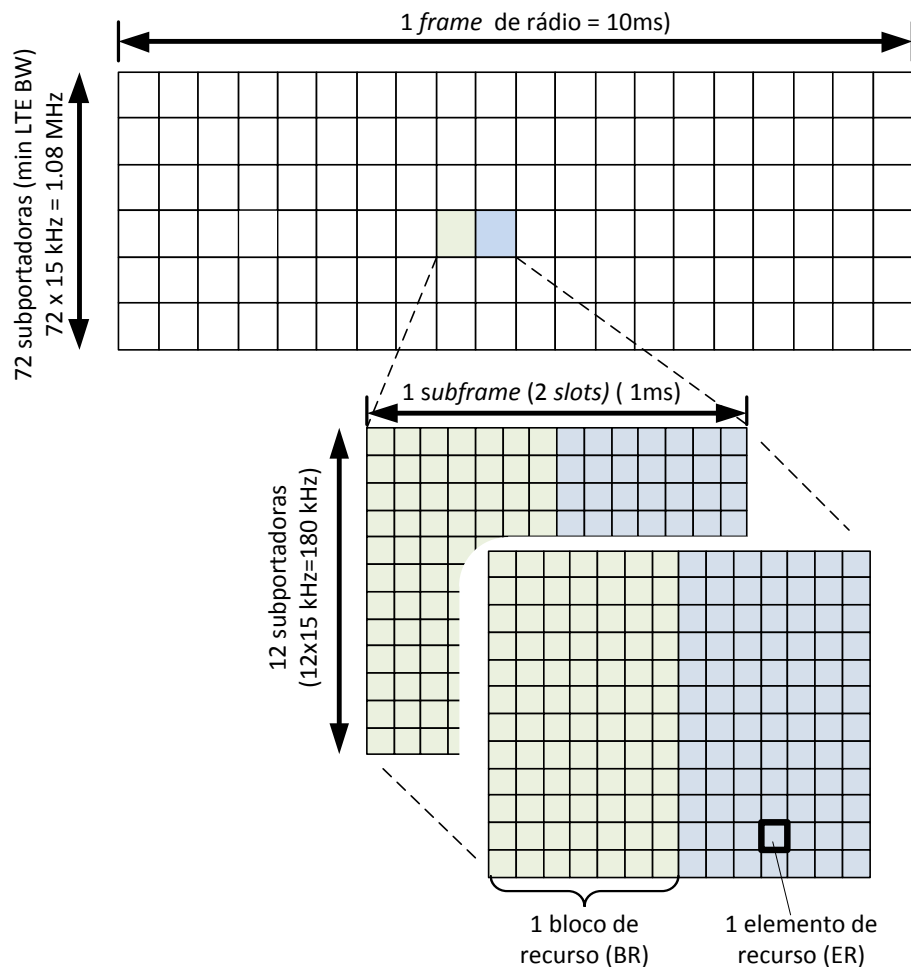


Figura 2.6: Estrutura de recursos tempo frequência para DL nos sistemas LTE.

Tabela 2.4: Exemplos de parâmetros do LTE.

BW do canal (MHz)	Num. de RBs	Num. de ER	BW ocupada (MHz)	Subportadoras
1.4	6	504	1.08	72
3	15	1260	2.7	180
5	25	2100	4.5	300
10	50	4200	9.0	600
15	75	6300	13.5	900
20	100	8400	18	1200

de forma dinâmica com resolução de 180 kHz. A alocação de recursos para um usuário específico é contíguo no UL para permitir a transmissão de portadora única, enquanto que no DL esta alocação é realizada de forma livre em diferentes áreas do espectro.

No que se refere à camada física de transmissão de dados, o LTE possui três canais de DL e dois de UL. Os canais físicos de dados de DL são [?, ?]: o PBCH (*physical broadcast channel*), o PDSCH (*physical downlink shared channel*) e PMCH (*physical multicast channel*). PBCH é o canal físico responsável pela transmissão da categoria MIB (*Master Information Block*) das informações do sistema (IS), necessários para o acesso dos dispositivos ao sistema. O MIB é o bloco de informação mais importante do sistema e consiste dos parâmetros essenciais para o acesso inicial da célula, como largura de banda de DL. O MIB é transmitido a cada 40 ms. Ao canal PBCH é sempre atribuída uma largura de banda de 1,08 MHz (72 subportadoras) independente da largura de banda do sistema e o mesmo é sempre alocado no centro da banda disponível do sistema.

O PDSCH é o principal canal de suporte de dados do DL. O PDSCH é usado para transmissão de todos os dados do usuário, bem como para a transmissão de ISs, os quais não são transmitidos no PBCH, e também para mensagens de *paging*. Por último, há o PMCH que é um canal projetado para transportar dados para MBMS (*multimedia broadcast and multicast services*) ou serviços de difusão e de multicast de multimídia.

Os canais físicos de dados de UL são: o PUSCH (*physical uplink shared channel*) e o PRACH (*physical random access channel*). O PUSCH é o canal mais importante de UL e sua principal tarefa é de transmitir os dados do usuário e informações de sinalização. O PRACH é o canal responsável pela sincronização e solicitação de recursos iniciais de UL e também pelo envio de resposta a mensagens de *paging*.

A taxa de dados momentânea de um usuário varia em função da alocação de recursos de UL dependendo da largura de banda momentaneamente alocada. O dobro da largura de banda resulta no dobro da taxa de dados. A largura de banda alocada varia entre 0 e 20 MHz em passos de 180 kHz.

Existem outros canais físicos adicionais para UL e DL, mas estes são usados apenas para controle de informações na camada física, suas descrições podem ser encontradas aqui [?, ?].

## 2.5 Conceitos de Classificação de Tecnologia de Acesso via Rádio

Nesta seção são introduzidos alguns conceitos básicos sobre classificação de tecnologias de acesso via Rádio (RATc) e uma breve revisão bibliográfica sobre o estado da arte é apresentada e discutida.

RATc é um conjunto de técnicas usadas para classificar padrões de RATs através de processamento de sinais aplicado à extração de características específicas de uma determinada RAT, seguida de um módulo de inteligência computacional que faz a classificação (usando, por exemplo, regras, árvore de decisão, redes neurais, etc.).

Através de RATc, o BTM pode se beneficiar para implementar um sistema eficiente capaz de adequar os seus parâmetros de geração e transmissão de SB de acordo com as RATs atuantes em uma determinada área do espectro em uma determinada área geográfica.

Com o avanço da tecnologia, a contínua inovação e a introdução de novas tecnologias de comunicação sem fio é inevitável o compartilhamento de espectro entre diferentes RATs. ERBs modernas estão se tornando cada vez mais multi-portadoras e multi-padrões para melhorar a eficiência e a capacidade de gerenciamento. O conceito de ERBs de múltiplo-padrão (MSR-ERB), cuja padronização está sendo desenvolvida pela 3GPP e especificada na serie 3GPP TS37 [?], já é uma realidade. Os MSR-ERBs transmissores e receptores irão suportar larguras de bandas maiores e incluir suporte não só para múltiplas portadoras de uma única RAT, mas também múltiplas RATs em um única ERB. Por exemplo, LTE, GSM e W-CDMA poderão ser transmitidas simultaneamente através de uma única MSR-ERB.

Por outro lado, em cenários de rádio cognitivo, o compartilhamento do espectro é realizado entre usuários licenciados e não licenciados, onde diferentes RATs podem assumir a mesma faixa de espectro para transmissão em momentos diferentes.

Neste contexto, torna-se importante projetar sistemas de BTM que sejam capazes de monitorar, identificar e classificar as RATs em uma determinada área geográfica e em seguida adaptar as suas características da geração e transmissão do SB de acordo com as RATs identificadas.

O sensoriamento espectral não apenas permitirá rastrear de forma dinâmica as mudanças no ambiente e habilitar o bloqueio de forma eficiente de todas as RATs licenciadas em uma determinada área geográfica, mas também permitirá identificar e potencialmente bloquear transmissões não autorizadas através de métodos pré-estabelecidos para geração e transmissão de SB para estes cenários.

Geralmente, a RATc é realizada através de análises das características espectrais ou temporais ou pela combinação de ambas do sinal da RAT. A classificação é beneficiada pelo fato dessas características serem geralmente pré-definidas e algumas delas serem únicas.

Um diagrama em blocos representativo de uma RATc é apresentado na Figura 2.7. O processo de classificação é realizado capturando o sinal de interesse em uma determinada área e banda do espectro através de uma antena. O sinal capturado é amostrado e processado usando algoritmos específicos para extração das características espectrais (por exemplo, PSD, largura de banda, frequência da portadora, etc.) ou temporais (prefixo cíclico, cicloestacionaridade, etc.), ou ambas do sinal da RAT. Em seguida, as características extraídas são processadas pelo classificador, que então sugere a RAT como a classe de saída. O classificador pode ser um simples comparador que contrasta os parâmetros de entrada com outros pré-armazenadas em uma base de dados, e então seleciona a RAT com maior semelhança. Outros tipos de classificadores (como redes neurais, por exemplo) incorporam a informação acerca das RATs em matrizes de pesos que são calculadas na fase de treino do classificador.

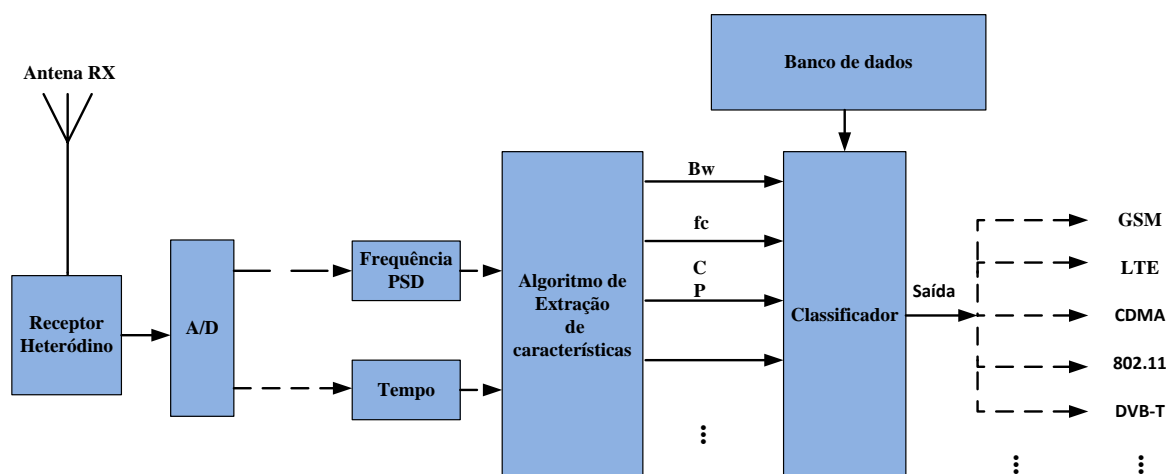


Figura 2.7: Diagrama em blocos simplificado representativo de um classificador de RAT.

### 2.5.1 Estado da Arte em Classificação da Tecnologia de Acesso via Rádio

Nos últimos anos vários trabalhos foram desenvolvidos e apresentados na literatura na área de RATc. Dentre os algoritmos apresentados, duas principais abordagens ganharam destaque: Abordagens baseadas nas características espectrais e outras baseadas nas características temporais do sinal da RAT.



No domínio da frequência a classificação da RAT é realizada, predominantemente, através da análise de características espectrais relacionadas ao formato e à largura de banda da PSD do sinal da RAT, beneficiando-se do fato de que, para a maioria das RATs, tais características são predefinidas e padronizadas de acordo com a RAT. Por exemplo, em [?] a RATc é realizada através de uma identificação “cega” baseada na largura de banda do canal, onde o algoritmo de classificação é baseado em redes neurais com funções de base radial (RBFNN) e a largura de banda da RAT é determinada através da comparação da PSD do sinal recebido com PSDs de referência pré-armazenadas para diferentes tipos de RATs (GSM, UMTS, etc.). Em seguida, escolhe-se a RAT com maior semelhança. O autor estudou a classificação de várias RATs, como por exemplo, UMTS, GSM, PDC, etc.

Em [?] o mesmo autor apresenta uma melhoria da técnica para diferenciar sinais com PSDs semelhantes, incluindo mais fatores de decisão como, por exemplo, o intervalo de guarda (GI) para discriminar entre sistemas de simples ou de multiportadoras.

Em [?] o mesmo método é aplicado e combinado com um algoritmo de identificação baseado em símbolos pilotos com o objetivo de identificar RATs com a mesma largura de banda, como por exemplo, DVB-T (digital video broadcasting-terrestrial) e DVB-T2.

Um algoritmo baseado na extração de características de medidas de PSD para diferentes RATs é apresentado em [?]. Neste caso, o algoritmo de classificação combina várias características genéricas como, por exemplo, distribuição de probabilidade de potência, transformadas wavelet, etc., para classificar as RATs (GSM, UMTS, DVB-T, Wifi, etc.).

Um *testbed* baseado em plataformas como Matlab e USRP (*Universal Software Radio Peripheral*) e ferramentas de SDR4all (*software defined radio*) é apresentado em [?] para implementação dos sistemas descritos em [?, ?].

Dois outros métodos baseados em PSD, os quais buscam ser insensíveis às imperfeições do receptor, tais como espúrios, ruídos não brancos e incertezas na potência do ruído (NPU-*noise power uncertainty*), são apresentados em [?].

Em [?] é apresentado um algoritmo de classificação para WiMAX e LTE, baseado numa extensa análise do preambulo, prefixo cíclico e cicloestacionariedade de sinais OFDM.

## 2.6 Conclusão

Neste capítulo foram apresentados conceitos sobre bloqueadores de telefonia celular, destacando-se os tipos e técnicas usadas para interromper a comunicação entre a ERB e o DM. Também foram apresentados conceitos referentes à estrutura da camada física dos sistemas

GSM e LTE. Por fim foi realizada uma revisão sobre diferentes técnicas de classificação de RATs, com o objetivo de reconhecer a RAT usada em uma determinada faixa de espectro em uma determinada área e, assim gerar a SB de acordo com as características predefinidas da referida RAT.

No capítulo seguinte é apresentado o estágio atual da tese através de uma proposta para o desenvolvimento de um sistema de BTM baseado em técnicas eficientes de PDS e de RF, aplicadas aos sistemas GSM e LTE.

## Capítulo 3

# Sistema Proposto para Bloqueio de Telefonia Móvel

Neste capítulo é apresentado o estágio atual da tese através da descrição de um sistema proposto para BTMs do tipo “Af”. Este sistema combina técnicas de PDS e PAD para gerar e transmitir o SB ininterruptamente e bloquear a comunicação dos SMs alvos.

Resgatando o já discutido, devido ao ritmo acelerado e à introdução contínua de novas tecnologias de acesso via rádio (RAT), o processamento analógico tem a desvantagem de fornecer menor flexibilidade, quando comparado com o processamento digital. Assim, o sistema BTM proposto, combina técnicas de PDS e PAS para constituir um sistema simples, eficaz e de relativo baixo custo. A parte do sistema proposto já desenvolvida implementa dois blocos: Um bloco é a unidade de lógica digital, responsável pela geração SBD-BB, e um bloco analógico de transmissor-heteródino, responsável pela transladação em frequência, filtragem amplificação e transmissão do sinal de BTM.

O terceiro bloco é o de RATc e está em desenvolvimento, não tendo ainda sido incorporado ao protótipo. Serão apresentados aqui resultados preliminares do mesmo e almeja-se ao final da tese integrá-lo ao protótipo para fins de validação e testes de desempenho.

### 3.1 Modelagem e Protótipo do Sistema Proposto

Um diagrama em blocos simplificado do sistema de BTM para bloqueio de múltiplas bandas é apresentado na Figura 3.1. O protótipo desenvolvido para esta tese adota essa arquitetura, mas a discussão será feita de forma mais genérica para indicar outras

possibilidades. Quando necessário será indicado o que foi efetivamente usado no protótipo.

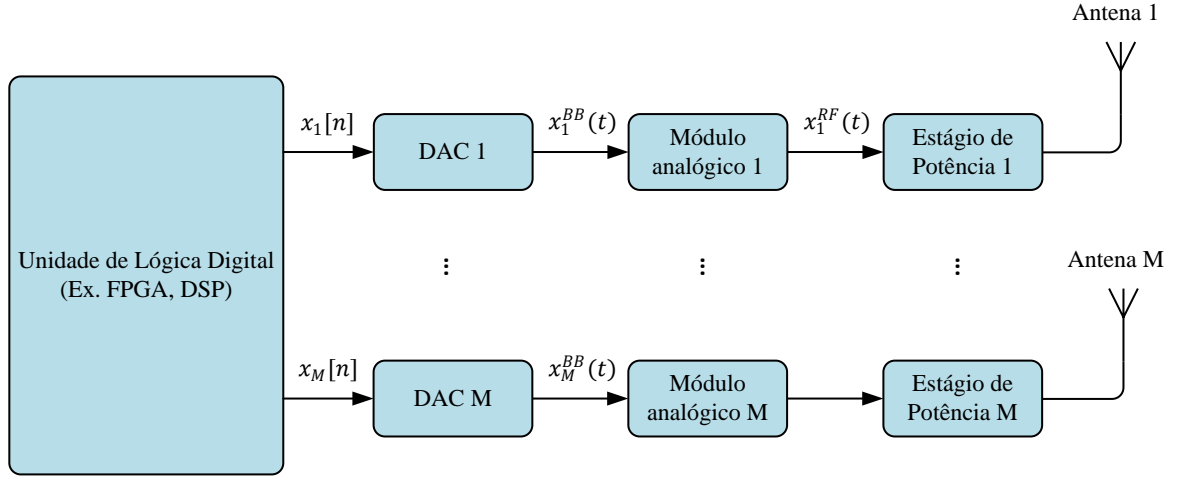


Figura 3.1: Diagrama em blocos simplificado do sistema BTM.

O sistema é basicamente composto por uma unidade de lógica digital, um módulo analógico e um estágio de potência.

O módulo digital implementa uma ULD, responsável pela geração do  $n$ -ésimo sinal digital  $x_M[n]$  para o  $n$ -ésimo canal do BTM.

O  $n$ -ésimo sinal digital  $x_M[n]$  é convertido para o sinal de tempo contínuo  $x_M^{BB}(t)$  pelo DAC (*digital to analog converter*, ou conversor de digital para analógico) .

O sinal na saída do DAC alimenta a entrada do módulo analógico que o translada, a partir da banda-base para uma RF, e gera o sinal  $x^{RF}(t)$ , o qual é amplificado no estágio de potência e enviado para uma antena para transmissão.

Se o BTM deve operar em bandas de frequências contíguas, pode ser benéfico usar um único  $x[n]$ . Porém, em outras situações, tais como quando se deseja bloquear múltiplas RATs, pode ser vantajoso usar  $M$  DACs e  $M$  módulos analógicos como indicado na Figura 3.1.

Nas duas próximas seções serão apresentados e descritos, com algum detalhe, as arquiteturas e seus principais componentes para a ULD e o TH.

## 3.2 Metodologia Proposta para Geração do Sinal em Banda Base

Nesta seção é proposta uma arquitetura da ULD baseada em FPGA para a geração do SBD-BB ( $x[n]$ ). O objetivo da ULD é de gerar o sinal digital  $x[n]$ , através do uso de técnicas eficientes de processamento digital de sinais.

Nos últimos anos, FPGA's se tornaram uma solução atraente para implementar sistemas de processamento digital de sinais. Dispositivos FPGAs consistem basicamente de componentes lógicos programáveis, portas lógicas e blocos de memória que podem ser configurados para operar em modos diferentes e implementar computações digitais complexas [?, ?]. FPGAs provêm uma arquitetura reconfigurável, programado via hardware mediante uma linguagem de descrição de hardware (HDL), o que possibilita sua reconfiguração para aplicações específicas, mesmo depois da instalação no campo. A natureza de processamento paralelo dos FPGAs possibilita a implementação em hardware de aplicações complexas e que exigem altas taxas de amostragem e de transmissão de dados. Esta flexibilidade é a principal vantagem do FPGA em relação aos chips DSP's.

A geração do sinal digital  $x[n]$  pode se beneficiar do paralelismo e taxas de amostragem altas oferecidos por FPGAs. Ainda, a possibilidade de reconfiguração oferece uma flexibilidade para alterar em tempo real a localização das portadoras e a largura de banda cobertas pelo SB do BTM.

Na Figura 3.2 é apresentada uma arquitetura para a ULD baseado em FPGA. A arquitetura é relativamente simples, composta por um PLL (*phase locked loop*),  $M$  ROMs (*read-only memory*) e  $M$  contadores. O PLL gera o *clock* do sistema através de um *clock* de referência externa e a frequência do clock gerado é controlado digitalmente. Cada ROM armazena as amostras de cada sinal  $y_M[n]$  pré-computadas. O contador interage sobre os endereços da ROM e as amostras são continuamente enviadas ao DAC.

O método proposto utiliza o processamento *off-line* para pré-computar um segmento  $y[n]$  com  $N$  amostras de  $b$  bits cada e gerar o sinal  $x[n]$  pela repetição de  $y[n]$ . Matematicamente  $x[n]$  é expresso como:

$$x[n] = \sum_{m=-\infty}^{\infty} y[n - mN] \quad (3.1)$$

Desta forma, a transformada discreta de Fourier (TDF) de  $x[n]$  é dada por

$$X(e^{j\omega}) = \frac{1}{2\pi} Y(e^{j\omega}) P(e^{j\omega}), \quad (3.2)$$

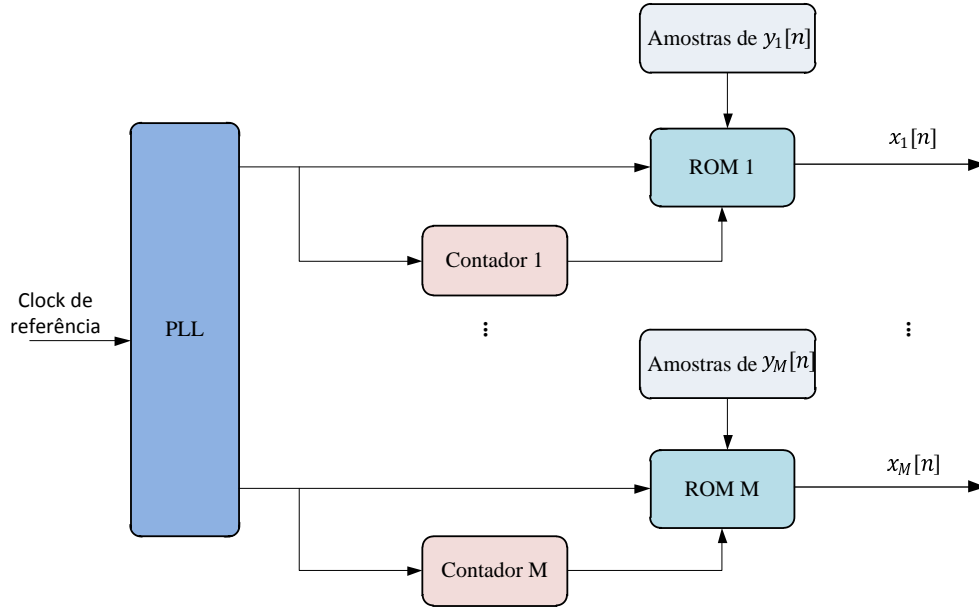


Figura 3.2: ULD baseado em FPGA para geração do SBD-BB,  $x[n]$ .

onde

$$P(e^{j\omega}) = \sum_{k=-\infty}^{\infty} \delta(\omega - k\Delta_{\omega}) \quad (3.3)$$

com  $\Delta_{\omega} = \frac{2\pi}{N}$ . Assim, apenas as frequências múltiplas de  $\Delta_{\omega}$  podem ser efetivamente usadas.

Assumindo que o DAC opera com  $F_s$  (Hz) amostras por segundo,  $\Delta_{\omega}$  em radianos corresponde a uma resolução em frequência  $\Delta_f = F_s\Delta_{\omega}/(2\pi) = F_s/N$  Hz, de tal forma que uma componente de  $x[n]$  com frequência  $k\Delta_{\omega}$  corresponda a  $k\Delta_f$  em  $x^{\text{BB}}(t)$ . A resolução  $\Delta_f$  (ou equivalentemente,  $F_s$  e  $N$ ) têm que ser escolhidos de acordo com a RAT alvo, as quais são representadas pelo conjunto de subportadoras  $\{f_c^{RF}\}$ , o espaçamento  $\Delta_f$  entre elas e a largura total do canal do sistema  $BW$  (UL ou DL).

A questão se resume em definir o sinal  $y[n]$  de tal forma que suas características permitam um bloqueio eficiente dos canais de comunicação dos SMs alvos.

Como apresentado nas Subseções 2.4.1 e 2.4.2, fisicamente, no domínio da frequência, os canais de comunicação dos sistemas apresentados são divididos em subportadoras espaçadas de  $\Delta_f$ , as quais são responsáveis pelo transporte da informação. Assim, um passo fundamental do processo é projetar  $y[n]$  de tal modo que pelo menos uma das suas componentes frequências caia dentro de cada subportadora do RAT de interesse, com potência suficiente para interromper a comunicação. Para simplificar, supõe-se aqui que um componente de frequência de  $y[n]$  é criada para cada subportadora  $\{f_c^{RF}\}$ . Com este objetivo, um conjunto  $\mathcal{K}$  de senóides com

frequências múltiplas de  $\Delta_\omega$  é selecionado e  $y[n]$  é dado por

$$y[n] = \sum_{k \in \mathcal{K}} \cos(k\Delta_\omega n + \theta_k), \quad (3.4)$$

onde  $\theta_k$  é a fase em radianos. O sinal  $y[n]$  é composto por soma de senoides com resolução em frequência igual  $\Delta_\omega$  e número total de senoides igual a  $|\mathcal{K}|$ . Assim,  $y[n]$  será referido como multitom, quando o  $|\mathcal{K}| > 1$ .

O sistema digital descrito tem vantagens sobre os analógicos, sendo as principais delas a flexibilidade de reconfiguração, em tempo real, da largura de banda e da localização no espectro do SB-BB. O procedimento é realizado de forma simples, através da atualização do conteúdo da ROM, mesmo depois da instalação do BTM em campo. Isso significa que, ao contrário da maioria dos sistemas BTM's analógicos, no sistema apresentado as bandas de frequências para cobrir e a largura de banda associada podem ser alterados em tempo real, sem qualquer alteração no hardware do sistema.

Uma importante tarefa no projeto de  $y[n]$  é manter o ruído de quantização em níveis toleráveis ou pré-especificados. Esta questão é relacionada a controlar o uso dos níveis de quantização do DAC, em especial a razão entre o pico e a média do sinal. Essas questões serão discutidas a seguir.

### 3.2.1 *Peak-to-Average Power Ratio* para sinais multitom

Embora a geração do sinal  $y[n]$  na Equação 3.4 seja relativamente simples, esta apresenta um desafio: Um potencial alto PAPR resultante da soma de amostras com altas amplitudes de senoides com frequências diferentes em um determinado instante de tempo. PAPR é uma medida da razão entre o máximo do módulo do sinal ao quadrado e sua potência média. Para o sinal  $y[n]$ , o PAPR é expresso matematicamente como

$$\text{PAPR} = \frac{\max\{|y[n]|^2\}}{E[|y[n]|^2]} \quad (3.5)$$

onde  $E[.]$  denota o operador do valor esperado.

No domínio discreto, valores altos de PAPR podem aumentar o ruído de quantização devido ao processo de arredondamento envolvido. Este problema pode ser contornado com o aumento de número de bits para representar o sinal, porém, isso exige mais hardware do FPGA e também um DAC com maior resolução e, portanto, mais custosos. Por outro lado, no domínio do tempo contínuo, um alto PAPR é potencialmente prejudicial aos amplificadores de potência (PAs) dos transmissores de RF, os quais são geralmente lineares apenas dentro de uma faixa dinâmica limitada. Assim, um sinal com alto PAPR produzirá excursões do sinal

na região de operação não-linear do amplificador de potência e, conseqüentemente, poderá sofrer distorções não-lineares causadas por *clipping*. Isto dá origem a emissões espúrias fora da banda e a distorção do sinal dentro da banda [?].

Várias técnicas foram apresentadas na literatura para combater altos PAPR [?]. Entretanto, um método simples e eficaz é baseado no uso de uma fase aleatória [?] e pode diminuir significativamente o PAPR, sem adicionar muita complexidade ao sistema. Tal método baseia-se em tomar um conjunto de valores aleatórios, uniformemente distribuídos para a fase  $\theta$ , a fim de evitar o alinhamento no tempo das amostras com altos valores de amplitude. Este método é adotado neste trabalho.

### 3.2.2 Razão sinal-ruído para sinais multitom

Ao gerar o SB-BB, podemos considerar duas fontes principais de ruído: O primeiro é o chamado ruído térmico, derivado da eletrônica do sistema, o qual tem uma densidade espectral de potência aproximadamente constante ao longo de todo o espectro (ruído branco). A segunda provem do DAC, como ruído de quantização e ruídos da distorção harmônica. Assumindo que a potência média do ruído térmico é muito menor que os ruídos provenientes do DAC, estes últimos então se tornam os principais limitantes do desempenho do sistema. Por isso, atenção especial deve ser tomada ao selecionar um DAC para atender às especificações em relação ao ruído de quantização, distorção harmônica, faixa dinâmica livre de espúrios (SFDR-Spurious-free dynamic range), etc. [?].

Busca-se a seguir obter uma expressão para a RSR (ou RSR de quantização  $RSR_q$ ) levando-se em conta apenas o ruído de quantização, pelo mesmo ser um dos fatores limitantes no desempenho do sistema e levando-se em conta que as demais imperfeições do DAC foram / serão combatidas através da escolha de um modelo adequado.

A expressão teórica da  $RSR_q$  de um DAC para uma única senoide é dada em função do número de bits  $b$  usados no processo de quantização das amostras como:

$$RSR_q = 6.02b + 1.76 \quad (\text{dB}) \quad (3.6)$$

Porém, esta expressão não é válida para sinais multitom, como é o caso da Equação 3.4, quando  $|\mathcal{K}| \gg 1$ . Assim, a expressão para multitom é deduzida a seguir.

Quando a cardinalidade  $|\mathcal{K}|$  do conjunto dos cossenos é suficientemente grande e o conjunto  $\theta$  assume valores aleatórios uniformemente distribuídos entre  $[-\pi, \pi]$ , a distribuição da amplitude de  $y[n]$  se assemelha ao envelope de uma Gaussiana com média zero, variância  $\sigma^2 = \frac{A^2}{2}|\mathcal{K}|$  e pode-se assumir que  $y[n] \in [-3\sigma, 3\sigma]$ , como será discutido a seguir.



Deve-se projetar um quantizador de  $b$ -bits para a faixa dinâmica do sinal e evitar (*overload*). Para tal, determina-se primeiramente a potência do sinal  $y[n]$ , que é dada por

$$P_s = E[|y[n]|^2] \quad (3.7)$$

$$= E \left[ \left| \sum_{k \in \mathcal{K}} A \cos(k\Delta_\omega n + \theta_k) \right|^2 \right] \quad (3.8)$$

$$\approx \frac{A^2}{2} |\mathcal{K}| \quad (3.9)$$

onde  $|\mathcal{K}|$  é o número total de senóides. A aproximação foi confirmada na prática e pode ser interpretada a partir do teorema do limite central.

Para um quantizador uniforme o passo de quantização  $\Delta$  é projetado de acordo com as estatísticas do sinal. Dois casos são observados abaixo:

1. Para um sinal com distribuição entre  $[-B, B]$

$$\Delta = \frac{2B}{2^b}, \quad (3.10)$$

onde  $b$  é o numero de bits.

2. Para um sinal com distribuição Gaussiana com média  $\mu$  e variância  $\sigma^2$ , uma decisão razoável é supor que a faixa dinâmica do sinal é  $[-3\sigma, 3\sigma]$ . Daí, se tem que:

$$\Delta = \frac{6\sigma}{2^b} \quad (3.11)$$

Devido às características de  $y[n]$ , adota-se a seguir a Equação 3.11. Assumindo que o erro de quantização é uniformemente distribuída com variância  $\sigma_q = \Delta^2/12$ , onde  $\Delta$  é o passo de quantização, a  $\text{RSR}_q$  da quantização é dada por

$$\text{RSR}_q = \frac{P_s}{\sigma_q} = \frac{P_s}{(6\sigma/2^b)^2/12} = \frac{2^{2b}}{3} \quad (3.12)$$

e pode ser aproximada por

$$\text{RSR}_q \approx 6b - 4,77 \quad (\text{dB}), \quad (3.13)$$

que é razoavelmente precisa para  $|\mathcal{K}| \geq 10$  e 6,5 dB abaixo da  $\text{RSR}_q$  para uma única senoide dada pela Equação 3.6.

### 3.3 Arquitetura para o Transmissor-Heteródino do Sistema de Bloqueador de Telefonia Móvel Proposto

### 3.4 Ip-core para geração de sinais multitoom aplicados no bloqueio de sinais de telefonia móvel

### 3.5 Introdução

### 3.6 síntese digital direta

A síntese digital direta (do inglês *direct digital synthesys*) é uma técnica que consiste na aplicação de técnicas e blocos de processamento digital de sinais para gerar um sinal com frequência e fase sintonizável referenciada a uma frequência fixa.

Today's cost-competitive, high-performance, functionally-integrated, and small package-sized DDS products are fast becoming an alternative to traditional frequency-agile analog synthesizer solutions. The integration of a high-speed, high-performance, D/A converter and DDS architecture onto a single chip (forming what is commonly known as a Complete-DDS solution) enabled this technology to target a wider range of applications and provide, in many cases, an attractive alternative to analog-based PLL synthesizers. For many applications, the DDS solution holds some distinct advantages over the equivalent agile analog frequency synthesizer employing PLL circuitry.

DDS advantages:

- Micro-Hertz tuning resolution of the output frequency and sub-degree phase tuning capability, all under complete digital control.
- Extremely fast hopping speed in tuning output frequency (or phase), phase-continuous frequency hops with no over/undershoot or analog-related loop settling time anomalies.
- The DDS digital architecture eliminates the need for the manual system tuning and tweaking associated with component aging and temperature drift in analog synthesizer solutions.
- The digital control interface of the DDS architecture facilitates an environment where systems can be remotely controlled, and minutely optimized, under processor control.
- When utilized as a quadrature synthesizer, DDS afford unparalleled matching and control of I and Q synthesized outputs.

### 3.6.1 Teoria de operação

In its simplest form, a direct digital synthesizer can be implemented from a precision reference clock, an address counter, a programmable read only memory (PROM), and a D/A converter (see Figure 1-1).

In this case, the digital amplitude information that corresponds to a complete cycle of a sine wave is stored in the PROM. The PROM is therefore functioning as a sine lookup table. The address counter steps through and accesses each of the PROMs memory locations and the contents (the equivalent sine amplitude words) are presented to a high-speed D/A converter. The D/A converter generates an analog sine wave in response to the digital input words from the PROM. The output frequency of this DDS implementation is dependent on 1.) the frequency of the reference clock, and 2.) the sine wave step size that is programmed into the PROM. While the analog output fidelity, jitter, and AC performance of this simplistic architecture can be quite good, it lacks tuning flexibility.

With the introduction of a phase accumulator function into the digital signal chain, this architecture becomes a numerically-controlled oscillator which is the core of a highly-flexible DDS device. As figure 1-2 shows, an N-bit variable-modulus counter and phase

register are implemented in the circuit before the sine lookup table, as a replacement for the address counter. The carry function allows this function as a phase wheel in the DDS architecture. To understand this basic function, visualize the sine wave oscillation as a vector rotating around a phase circle (see Figure 1-3). Each designated point on the phase wheel corresponds to the equivalent point on a cycle of a sine waveform. As the vector rotates around the wheel, visualize that a corresponding output sine wave is being generated. One revolution of the vector around the phase wheel, at a constant speed, results in one complete cycle of the output sine wave. The phase accumulator is utilized to provide the equivalent of the vectors linear rotation around the phase wheel. The contents of the phase accumulator correspond to the points on the cycle of the output sine wave. The number of discrete phase points contained in the wheel is determined by the resolution, N, of the phase accumulator. The output of the phase accumulator is linear and cannot directly be used to generate a sine wave or any other waveform except a ramp. Therefore, a phase-to-amplitude lookup table is used to convert a truncated version of the phase accumulators instantaneous output value into the sine wave amplitude information that is presented to the D/A converter. Most DDS architectures exploit the symmetrical nature of a sine wave and utilize mapping logic to synthesize a complete sine wave cycle from  $\frac{1}{4}$  cycle of data from the phase accumulator. The phase-to-amplitude lookup table generates all the necessary data by reading forward then back through the lookup table.

A arquitetura adotada para o TH é apresentada, em forma de diagrama em blocos, na Figura 3.3. A cadeia de processamento do TH é constituída de um filtro passa baixas (FPB) ou filtro de reconstrução (FR), um amplificador de frequência intermediária (AMP-IF), um míxer de conversão ascendente, um filtro de RF de banda passante (FBP), um amplificador de ganho variável (VGA), um sintetizador de PLL e um amplificador para o sinal da LO (AMP-LO).

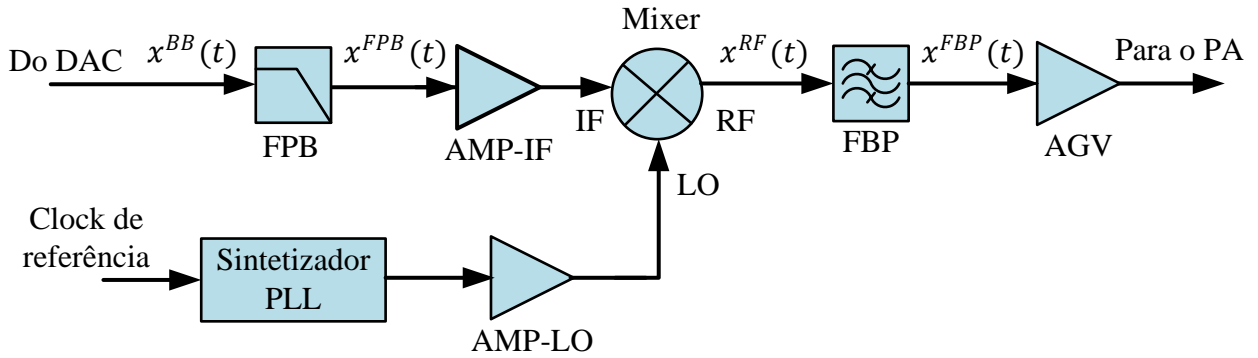


Figura 3.3: Diagrama em blocos simplificado do transmissor-heteródino.

O processamento do sinal pelo TH se inicia no FPB, que recebe o sinal  $x^{BB}(t)$ , proveniente do DAC, e o filtra para remover as imagens resultantes do processo de conversão. Em seguida, o sinal é enviado para AMP-FI, que adequa o seu nível para a entrada FI do *míxer*. A entrada LO do *míxer* é excitada por um sinal de onda senoidal ou quadrada, proveniente de um sintetizador PLL. O PLL, por sua vez, recebe um sinal de referência de um oscilador e gera o sinal de LO. A frequência de saída do PLL é controlada digitalmente e o seu nível é ajustado pelo AMP-LO, para adequá-lo à faixa de potência exigida na entrada LO do *míxer*. O *míxer* translada  $x^{FPB}(t)$  e gera o sinal de RF  $x^{RF}(t)$ . Em seguida, emprega-se o FBP no  $x^{RF}(t)$  para remover as imagens indesejadas na saída do *míxer*. Em seguida, emprega-se o VGA para adequar o sinal à níveis de potência mínima exigida pelo amplificador de potência (PA). Por último, o PA fornece a potência necessária e envia o sinal para antena para transmissão.

Uma ilustração, em termos da magnitude da resposta em frequência do sinal na saída de cada estágio do TH é apresentada na Figura 3.4.

A primeira ilustração, denominada de saída do DAC, apresenta um exemplo da resposta em magnitude do sinal na saída do DAC, sobreposta com a resposta em frequência ideal do FPB. Observa-se então que o espectro do sinal na saída do DAC é composto por várias imagens centradas em  $lF_s$ ,  $l \in \mathbb{Z} > 1$ . Estas imagens devem ser removidas pelo FPB, que, idealmente, deve ter uma magnitude da resposta em frequência,  $|H_{FPB}(f)|$ , dada por

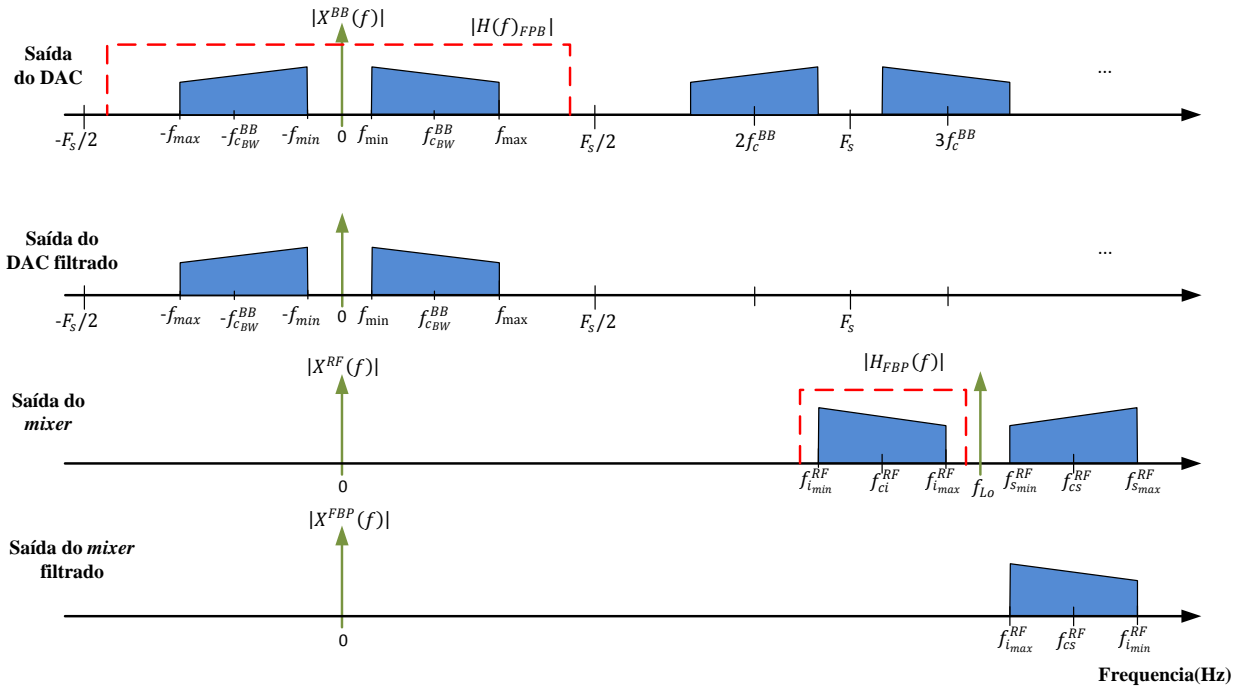


Figura 3.4: PSD da cadeia do sinal no transmissor-heteródino.

$$|H_{FPB}(f)| = \begin{cases} 1, & f_{\max} < f \leq F_s/2 \\ 0, & \text{outros valores,} \end{cases} \quad (3.14)$$

onde  $f_{\min}$  e  $f_{\max}$ , são as componentes de frequências mínima e máxima, respectivamente, do SB-BB.

A representação da resposta em frequência do sinal na saída do FPB é apresentada na segunda ilustração, denominada de “Saída do DAC filtrado”.

A terceira ilustração, denominada de “Saída do mixer”, apresenta a a magnitude da resposta em frequência do sinal na saída do *mixer*. A saída do mixer é composta por três componentes espectrais, o sinal da LO e duas imagens do sinal transladado, centradas em

$$\begin{aligned} f_{ci}^{\text{RF}} &= f_{\text{LO}} - f_{\text{cBW}}^{\text{BB}} \\ f_{cs}^{\text{RF}} &= f_{\text{LO}} + f_{\text{cBW}}^{\text{BB}}, \end{aligned}$$

onde  $f_{ci}^{\text{RF}}$  e  $f_{cs}^{\text{RF}}$  são as bandas inferior (imagem espelhada) e superior, respectivamente e  $f_{\text{cBW}}^{\text{BB}}$  é a frequência central da banda total (BW) do sinal em banda base. Geralmente, em aplicações onde se requer a recuperação das informações no sinal, é costume descartar a imagem espelhada juntamente com o  $f_{\text{LO}}$ . Porém, neste caso, não há a necessidade de recuperar nenhuma informação, então, qualquer uma das duas imagens podem ser usadas pelo BTM. A escolha de uma delas irá depender do FBP de RF disponível. Por exemplo, se

for escolhido filtrar a imagem centrada em  $f_{ci}^{RF}$ , então, o FPB aplicado deve ter um módulo da magnitude da resposta em frequência ideal dado por:

$$|H(f)_{FBP}| = \begin{cases} 1, & f < f_{LO} \cup f_{i_{\max}}^{RF} < f < f_{i_{\min}}^{RF} \\ 0, & \text{outros valores.} \end{cases} \quad (3.15)$$

onde  $f_{i_{\min}}^{RF}$  e  $f_{i_{\max}}^{RF}$  são, respectivamente, as frequências mínima e máxima da imagem centrada na banda inferior. O módulo da magnitude da resposta em frequência do sinal na saída do filtro da Equação 3.15 é apresentado na Figura 3.4.

Por outro lado, o mesmo procedimento se aplica quando a imagem escolhida para filtrar for a centrada em  $f_{cs}^{RF}$ , substituindo-se na equação o  $f_{i_{\min}}^{RF}$  e  $f_{i_{\max}}^{RF}$  por  $f_{s_{\min}}^{RF}$  e  $f_{s_{\max}}^{RF}$ , respectivamente.

Na prática, recomenda-se evitar ter  $x^{BB}(t)$  com potência significativa em frequências próximas ao nível DC e definir um deslocamento em frequência  $f_{min} \gg 0$  em relação ao DC (0 Hz), a fim de permitir o uso de um FBP menos seletivo no processo de filtragem para remoção das imagens indesejadas em RF.

Alguns *mixers* de conversão ascendente, chamados de *single-sideband mixers*, atenuam uma das imagens indesejadas e a portadora da LO. O uso deste tipo de *mixer* pode ajudar a relaxar as especificações do FBP. Porém, estes são tipicamente mais custosos que os tradicionais.

### 3.6.2 Metodologia para geração do sinal digital em banda base

Na sequência, resumimos uma metodologia para escolher os quatro parâmetros usados para gerar  $y[n]$ :  $F_s$ ,  $N$ ,  $\mathcal{K}$  and  $b$ .

---

**Metodologia de projeto**


---

**Input:** Defina as frequências centrais dos canais  $\{f_c^{RF}\}$  e suas larguras de banda  $\{B_c\}$

**Output:**  $F_s, N, \mathcal{K}, b, y[n]$  (Para cada canal do BTM)

```

1 A partir do conjunto de RATs de interesse, escolha  $M$ 
2 for  $i = 1, \dots, M$  (processa para cada um dos canais) do
3   Para cada RAT, determine  $\Delta_f, \{f_c^{RF}\}$  e  $BW$ 
4   Com base nas especificações do mixer, dos filtros de RF, e da máxima  $F_s$ 
   suportada/desejada pelo sistema, escolha  $f_{\min}$  e calcule  $f_{\max}$  para  $x_i^{BB}(t)$ 
5   Defina o  $n$ -th estágio de conversão ascendente, incluindo  $LO_i$ 
6   Com base nas características do FPB disponível, escolha  $F_s > 2f_{\max}$ 
7   Calcule  $N = \left\lceil \frac{F_s}{\Delta_f} \right\rceil$ 
8   if  $\frac{F_s}{\Delta_f}$  Não for um inteiro then
9     Recalcule  $F_s = N\Delta_f$ 
10  end
11  Calcule o grupo de  $\mathcal{K} = \{k\}$  índices de tal forma que  $f_k^{BB} = k\Delta_f$  são as componentes
   frequenciais em  $x_i^{BB}(t)$ 
12  Escolha o número de bits  $b$  para quantização. Como orientação,  $b \geq \lceil (RSR_q + 4.77)/6 \rceil$ 
   dado que, além do ruído de quantização, deficiências como SFDR também impactam na
   RSR e na PSD do transmissor
13  Calcule  $y[n]$  usando a Equação (3.4) e quantize-o com  $b$  bits, com o objetivo de utilizar
   toda a faixa dinâmica do DAC.
14 end

```

---

### 3.7 Protótipo Desenvolvido para o Bloqueador de Telefonia Móvel

Nesta seção é apresentado um protótipo de BTM-A, baseado nas arquiteturas e cadeias de processamento apresentadas na Seção 3.2 para geração do SBD-BB e na Seção 3.3 para a translação deste sinal para a RF.

O protótipo da BTM combina técnicas de PDS e PAS em um sistema modular composto basicamente por três partes principais: Uma placa digital, duas placas de

transmissor-heteródino e um módulo de controle.

O sistema completo do protótipo do BTM é apresentado na Figura 3.5, onde são destacadas as PCIs (placa de circuito impresso) que implementam cada um dos referidos módulos.

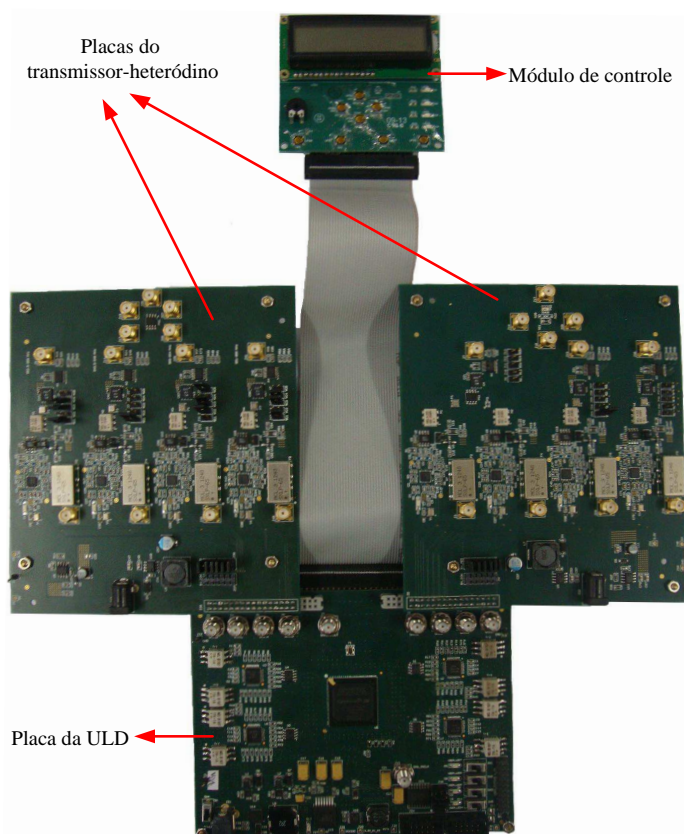


Figura 3.5: Placa do protótipo de BTM desenvolvida para tese.

Com o objetivo de apresentar de forma clara todos os aspectos constituintes do protótipo do BTM, apresenta-se na Figura 3.6 um esquema representativo em diagrama de blocos a estrutura detalhada do protótipo. Observa-se que a placa digital comporta a ULD implementada no FPGA EP3C120F484C7 da família Cyclone III da Altera [?] e, no que se refere à parte responsável pela geração do sinal digital, a mesma é baseada na arquitetura proposta na Seção 3.2 e ilustrada na forma de diagrama em blocos na Figura 3.2. Ainda, a placa digital é munida de 8 DACS (4 DACs duais) de 14 bits cada, compondo assim um sistema de  $M = 8$  canais independentes de transmissão. Cada canal é roteado para um conector SMA (*SubMiniature version A*) e disponibilizado para conexão com a placa analógica. Na mesma Figura é destacada a estrutura do nível mais alto (*Top level*) do projeto de HDL implementado no FPGA para a ULD, onde, basicamente, a ULD implementa três blocos principais que são



os seguintes:

1. **ROM** - armazena as amostras pré-calculadas do sinal digital;
2. **Controle de ganho** - ajusta os ganhos individuais de cada um dos canais em passos de 1 dB. Este bloco ainda tem a função de ligar ou desligar um determinado canal.
3. **Somador** - o somador fornece a opção de somar bandas menores em um único canal, em que cada uma das bandas irá possuir controle de ganho independente. Isso dá mais flexibilidade ao sistema, pois permite gerar e controlar duas bandas em um único canal. O somador pode ser ignorado caso se deseje gerar apenas uma única banda por canal.
4. **CPU** - responsável por rodar os programas que executam todo o processo de controle referente aos comandos de entrada via teclado, escrita no LCD e controle da frequência de saída do sintetizador PLL através da comunicação SPI (*serial peripheral interface*).

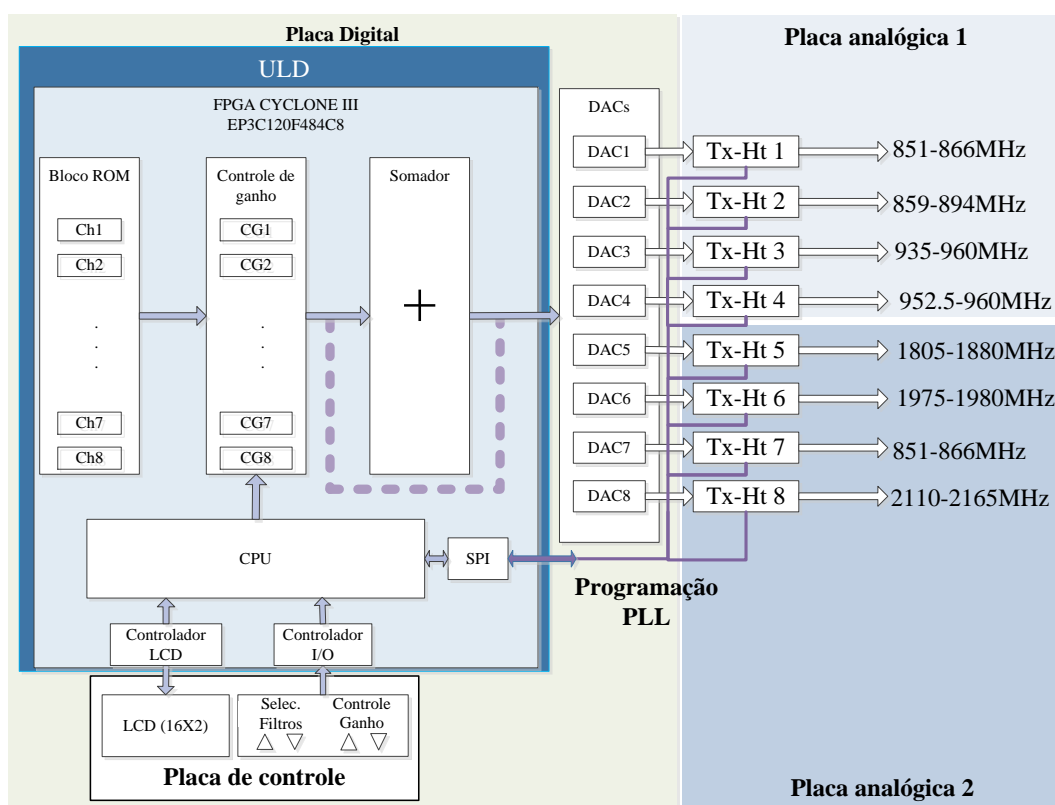


Figura 3.6: Esquema representativo em diagrama de blocos do protótipo do BTM: Destaque da estrutura *Top Level* do projeto HDL para a ULD.

A placa digital é um módulo independente e pode ser conectada a outros módulos de transmissor-heteródino ou pode ser usada para gerar sinais em banda base para efeitos de testes e avaliação da qualidade do SB-BB gerado digitalmente.

Ainda na Figura 3.6, referente à placa analógica para o transmissor-heteródino, ressalta-se que duas placas foram projetadas para permitir maior flexibilidade em termos de cobertura de diferentes áreas do espectro usados por STMs. Assim, a “placa analógica 1” compreende as frequências de 851-960 MHz dividida em 4 bandas, enquanto que a “placa analógica 2” compreende as frequências de 1805-2165 MHz (Figura 3.6) dividida em 3 bandas (duas bandas analógicas foram combinadas). As especificações para a divisão das bandas por canal foram baseadas na divisão de bandas para os STMs no Brasil [?]. Ressalta-se que bandas menores podem ser geradas, desde que estejam contidas na banda de passagem dos filtros de RF. Dentre as bandas possíveis estão envolvidos os sistemas como GSM850, GSM900, GSM1800, GSM1900, LTE, 3G, CDMA Nextel, etc. As duas placas ainda oferecem a possibilidade de combinar os canais para compor bandas maiores através de um combinador de sinais analógicos.

A arquitetura e cadeia de processamento dos THs de todos os canais nas duas placas são baseadas na apresentada na Seção 3.3 Figura 3.3, com exclusão do PA. Assim, o TH é constituído pelos seguintes componentes:

- **Filtro passa-baixas** - O filtro passa-baixas (FPB) ou filtro de reconstrução é o primeiro estágio pelo qual passa o sinal proveniente do DAC da placa digital e, como dito anteriormente, este filtro tem a função de atenuar as imagens do sinal resultantes do processo de conversão de digital para analógico, as quais são centradas em  $l \in \mathbb{Z} > 1$ . Na Figura 3.7 é apresentado a resposta em frequência do filtro passa-baixas empregado na reconstrução do sinal na saída do DAC de todos os canais do protótipo. Observa-se no entanto que este filtro tem uma banda de passagem de 65 MHz, onde a atenuação é menor que 1 dB. A frequência de corte é 71 MHz com atenuação de 3 dB. Na banda de rejeição, o filtro atenua mais que 20 dB na faixa de 86-96 MHz e mais que 40 dB para frequências maiores que 96 MHz.

As especificações do FPB foram levantadas levando em conta uma máxima largura de banda do sinal de 45 MHz com um  $f_{\min} = 10$  MHz o que resulta em um  $f_{\max} = 55$  MHz e, assim, um  $F_s > 110$  MHz. Por exemplo, nestas condições, se  $F_s = 150$  MHz, a imagem na segunda zona de Nyquist é centrada em 117.5 MHz e a sua mínima frequência é igual a 95 MHz, o qual será atenuado de mais de 20 dB e 40 dB após 1 MHz, que pode ser considerado bastante razoável nessas condições.

- **Amplificador de banda base** - Após a remoção das imagens do sinal na saída do

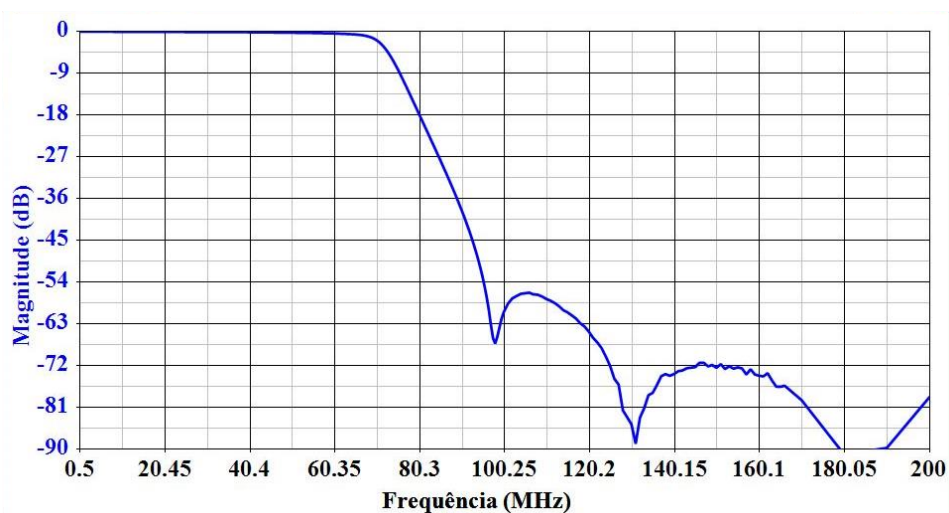


Figura 3.7: Resposta em frequência de um FPB comercial típico.

DAC pelo FPB, o sinal resultante necessita ser amplificado para compensar a perda imposta pelo filtro passa-baixas e da perda de conversão do mixer no próximo estágio. O amplificador de banda base é o responsável por realizar esta tarefa, provendo um ganho equivalente as perdas e diminuir a contribuição do ruído de fundo no sistema.

- **Mixer de conversão ascendente** - A translação do sinal proveniente do amplificador de banda base para RF é realizada através do mixer de conversão ascendente. O protótipo do BTM usa um mixer passivo comum (sem supressão de imagens) e sua faixa de atuação abrange as frequências centrais de todos os canais do BTM. Desta forma foi usado um único mixer em todos os canais do BTM.
- **Sintetizador de frequência PLL** - O sintetizador de frequência PLL é responsável por gerar o sinal para a LO do mixer. O BTM usa um sintetizador de banda larga com VCO (*voltage controlled oscillator* ou oscilador controlado por tensão) integrado. A geração do sinal é realizada alimentando o sintetizador com um clock externo de 40 MHz fornecido por um oscilador de cristal e a frequência do sinal gerado é controlada digitalmente, através de comunicação SPI controlado pela placa da ULD.
- **Amplificador de LO** - O amplificador de LO é usado para amplificar o sinal do LO e adequar a sua potência para o nível exigido na entrada LO do mixer. Neste caso, a potência do sinal gerado pelo sintetizador de frequência PLL varia entre -4 e 5 dBm (controlado digitalmente em passos de 3 dB), enquanto que a exigida na entrada LO do mixer varia entre 13 e 16 dBm. Usou-se então um amplificador com um ganho típico de aproximadamente 13 dBm para condicionar o sinal para a entrada LO do mixer.

- **Filtro banda-passante de RF** - Como discutido anteriormente, o sinal na saída de um mixer comum é composto por três componentes espectrais, duas imagens do sinal transladado e o sinal do LO. Porém, apenas uma das imagens transladadas é necessária e a outra, juntamente com o sinal do LO, devem ser removidas. O filtro banda-passante (FBP) de RF é o responsável pela remoção de tais componentes indesejados. No protótipo do BTM são usados diferentes FBP de RF, de acordo com a banda de interesse. Os filtros usados são da tecnologia SAW e são geralmente especificados de acordo com a aplicação. Por exemplo, na Figuras 3.8 e 3.9 são apresentadas as respostas em frequência dos filtros empregados, respectivamente, nos canais 2 e 3 do protótipo e os quais podem ser empregados nas aplicações de LTE banda 5 (LTE-B5) e GSM900, respectivamente.

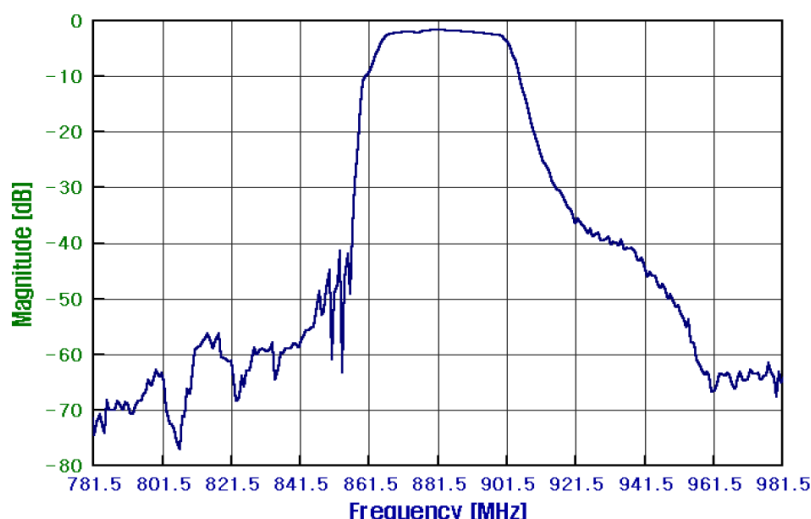


Figura 3.8: Resposta em frequência de um filtro de RF empregado no canal 2 do protótipo do BTM para aplicações de LTE-B5.

O filtro do canal 2 tem uma banda passante de 869-894 com perda por conversão de 2.2dB (típico) [?]. Este atenua, tipicamente, 47-60 dB em faixas de frequência de DC-849 MHz e 30-55 db em faixas de frequência de 914-2000 MHz. Já o filtro do canal 3 [?], possui uma banda de passagem de 935-960 MHz com perda por conversão de 1.8 dB (típico) atenua entre 38-40 dB nas frequências de 824-894 MHz e 42-45 dB nas frequências de 1020-1080 MHz.

- **Amplificador de RF** - O amplificador de RF constitui o último estágio do protótipo do BTM. O sinal proveniente do FBP deve ser amplificado para sua adequação aos níveis mínimos de potência exigidas na entrada do PA. Com o objetivo de fornecer maior flexibilidade no controle da potência que deve ser fornecida para o PA, o Amplificador

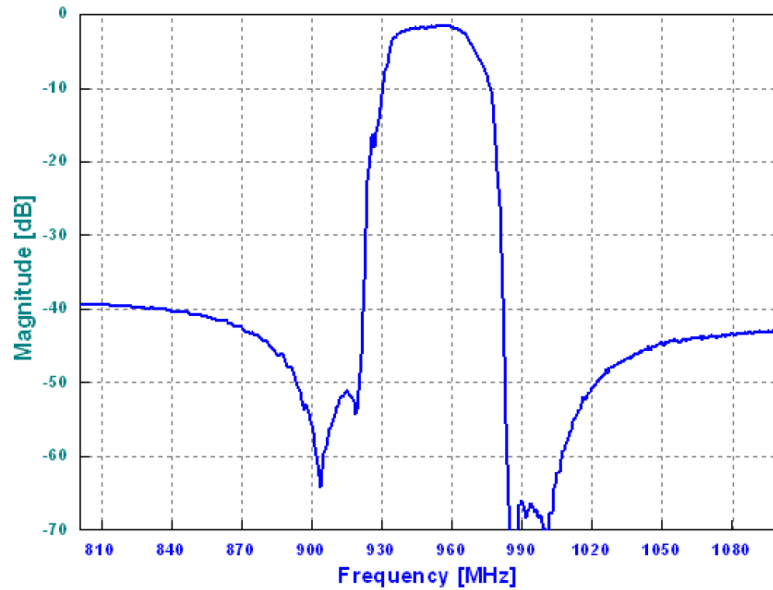


Figura 3.9: Resposta em frequência de um filtro de RF empregado no canal 3 do protótipo do BTM para aplicações de GSM900.

de RF foi combinado com um atenuador (não mostrado aqui) em um esquema em que o sinal é primeiramente amplificado e depois atenuado de acordo com a potência exigida na entrada de um determinado PA. Dois amplificadores de RF são empregados no protótipo para permitir a cobertura de todas as bandas usadas. O primeiro cobre as bandas de 851-960 MHz e o segundo cobre as bandas de 1805-2165 MHz. Ambos podem fornecer um ganho plano de aproximadamente 20 dB nas bandas de interesse.

## 3.8 Conclusão

Neste capítulo foi descrito o estágio atual do trabalho através do sistema proposto para bloqueio de telefonia móvel. Arquiteturas para os dois componentes principais que compõem o tal sistema foram apresentadas e discutidas.

Uma arquitetura para a ULD baseada em FPGA, o qual combina técnicas eficientes de PDS para gerar o SBD-BB foi apresentada e suas características principais detalhadas.

Uma expressão para a RSR de quantização foi derivada e a mesma permite escolher o DAC de forma flexível, o que é essencial ao projeto do sistema.

Por fim foi apresentado um protótipo desenvolvido para o BTM do tipo “A”, onde foram

apresentados, de forma detalhada, todos os componentes do sistema e suas especificações.

No próximo capítulo são apresentados resultados preliminares de simulação e validação da implementação prática.

# Capítulo 4

## Resultados Preliminares

### 4.1 Introdução

Para indicar concretamente o status do trabalho, neste capítulo são apresentados resultados de três experimentos sobre a geração de SBs e sua aplicação no bloqueio de sinais de telefonia celular.

O Experimento 1 explora o caso da geração do SB por simulação no Matlab e tem como objetivos: 1) A comprovação do método descrito na Seção 3.2.1 para redução do PAPR. Para tal, foram realizados experimentos por simulação no Matlab, através da comparação do PAPR. Tomando-se dois conjuntos de valores para o  $\{\theta\}$ , compara-se os mesmos através do PAPR e, conseqüentemente, as características temporais e frequenciais do SBD-BB gerado. 2) A comprovação da expressão da RSR teórica apresentada na Seção 3.2.2. Para tal foram realizados simulações no Matlab, as quais compararam os valores estimados e calculados de RSR para diferentes conjuntos de multitom.

O Experimento 2 mostra um caso prático de geração do SB mediante o protótipo apresentado na Seção 3.7. Os objetivos deste experimento são: 1) aplicar a metodologia apresentada na Seção 3.6.2 para especificação de parâmetros para geração do SB, aplicada a dois sistemas de telefonia celular: LTE-B5 e GSM900. 2) Gerar o sinal de bloqueio em banda base e em RF usando o protótipo do bloqueador e realizar análises das características espectrais levantadas por um analisador de espectro, tais como potência do sinal e do ruído dentro e fora da banda, para efeito de comparação da RSR levantada com a teórica.

O experimento 3 explora um caso prático que envolve um cenário real de transmissão, recepção e bloqueio dos sinais de LTE. O experimento tem como objetivo testar a eficiência do bloqueio de sinais de LTE pelo SB gerado e transmitido pelo protótipo, em um ambiente

real de transmissão e recepção realizada no LASSE.

## 4.2 Definição do Cenário Alvo de Bloqueio

Esta seção define o cenário no qual se enquadra a geração do SB-BB e SB-RF. O presente cenário constitui a base de todas os experimentos realizados, salvo quando alguma alteração nos parâmetros forem explicitamente informados. Tem-se como alvo dois STMs: LTE-B5 e GSM900, o que corresponde ao uso de  $M = 2$  na Figura 3.1. O objetivo é operar como BTM-Af, e transmitir o SB em todos os canais de DL, já que este, tipicamente, requer menos energia do que UL.

- **Parâmetros do LTE B5** - O LTE-B5 usa para o DL uma faixa de espectro compreendida entre 869-894 MHz, o que corresponde a uma largura de banda total de  $BW_{\text{LTE}} = 25$  MHz, centrada em  $f_{\text{cLTE}}^{\text{RF}} = 881.5$ , com  $|\mathcal{K}| = 1667$  subportadoras, espaçadas de  $\Delta_f^{\text{LTE}} = 15$  kHz.
- **Parâmetros do GSM900** - O GSM900, usa para o DL uma faixa de espectro compreendida entre 935.2-959.8 MHz, o que corresponde a uma largura de banda total de  $BW_{\text{GSM}} = 24.6$  MHz, centrada em  $f_{\text{cGSM}}^{\text{RF}} = 947.5$ , com  $|\mathcal{K}| = 123$  subportadoras, espaçadas de  $\Delta_f^{\text{GSM}} = 200$  kHz.

O resumo dos parâmetros dos canais físicos para ambos os sistemas é apresentado na Tabela 4.1.

Tabela 4.1: Parâmetros dos canais físicos dos STMs alvos: LTE-B5 e GSM900.

Parâmetro	LTE-B5	GSM900
$\Delta_f$ (kHz)	15	200
$f_c^{\text{RF}}$ (MHz)	$869:\Delta_f^{\text{LTE}}:894$	$935.2:\Delta_f^{\text{GSM}}:959.8$
Frequência central	881.5	947.5
$BW_{\text{DL}}$ (MHz)	25	24.6
Número total de subportadoras	1667	123

Em seguida são determinados os parâmetros principais para a geração da versão SB-BB para o atual cenário.



### 4.3 Determinação dos parâmetros para a geração do SB-BB

A computação do SB-BB foi realizada seguindo a metodologia proposta na Seção 3.6.2. Assim, com os  $\Delta_f$  e as  $BW$  conhecidos, o próximo parâmetro a determinar é o  $f_{\min}$ . De acordo com a metodologia proposta,  $f_{\min}$  deve ser escolhido de acordo com as especificações dos FBPs de RF e da  $F_s$  máxima suportada pela ULD e o DAC, já que valores altos de  $f_{\min}$  resultam em valores altos de  $f_{\max}$ , para uma mesma  $BW$ . Após a escolha do  $f_{\min}$ , determina-se o  $f_{\max}$  e  $F_s$ . Em seguida, calcula-se o  $N$  a partir do  $F_s$  e  $\Delta_f$ . Por fim, escolhe-se o valor de  $b$ , de acordo com a RSR desejada ou DAC disponível.

- **Determinação dos parâmetros para o LTE-B5** - O LTE-B5, compreende a faixa de frequência do canal 2 do protótipo de BTM. A especificação do filtro de RF aplicado neste canal, assim como sua magnitude da resposta em frequência, foram apresentadas e descritas na Seção 3.7, Figura 3.8. Assim, com aplicação do referido filtro e tendo em vista o *trade-off* entre  $f_{\min}$  e a  $F_s$ , um valor razoável seria adotar  $f_{\min} = 15$  MHz, o que resulta em  $f_{\max} = 40$  MHz e  $f_{cBW}^{BB} = 27.5$  MHz. Neste caso, a  $f_{LO}$  será dada por:

$$f_{LO}(\text{MHz}) = 881.5 \pm 27.5 = \begin{cases} 854 \text{ MHz} \\ 909 \text{ MHz} \end{cases}$$

Para  $f_{LO} = 854$  MHz, o sinal na saída do *mixer* será constituída de duas imagens centradas em 826.5 e 881.5 MHz. Por outro lado, se  $f_{LO} = 909$  MHz, estas serão centradas, respectivamente, em 881.5 e 936.5 MHz. Como exemplo, as duas situações são ilustradas na Figura 4.1.

Neste caso, foi escolhido o valor de  $f_{LO} = 854$  MHz, devido o filtro de RF oferecer maior atenuação nas faixas de frequência que envolvem a imagem centrada em 826.5 MHz.

Com os valores de  $f_{\min}$  e  $f_{\max}$  definidos, o próximo passo é escolher o valor de  $F_s$ , o qual deve facilitar o processo de reconstrução do sinal, permitindo o uso de FBPs menos seletivos e menos custosos, e diminuir o nível de ruído de quantização da PSD, enquanto a relação  $F_s > 2 \times 40 > 80$  é obedecida. As características e a resposta e a magnitude da resposta em frequência do FPB usado em todos os canais do protótipo foi apresentado na Seção 3.7. O referido filtro atenua aproximadamente 60 dB nas frequências acima de 110 MHz (referir-se à Figura 3.7).

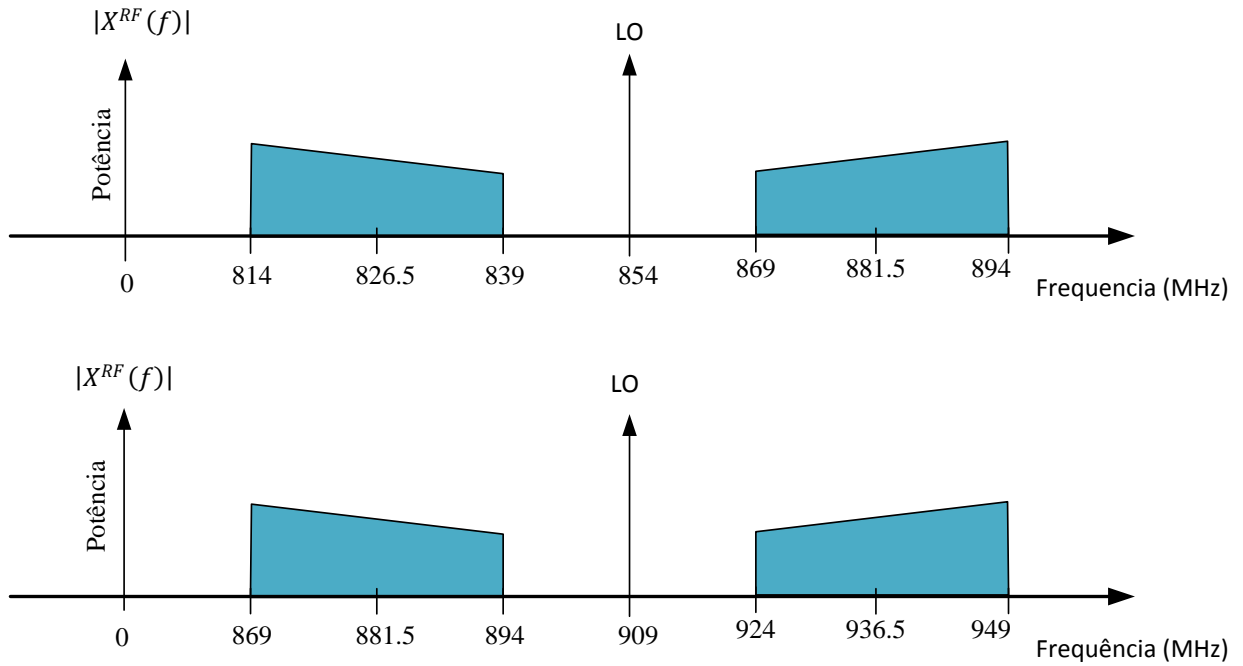


Figura 4.1: LTE-B5: Ilustração do sinal na saída do *mixer* para  $f_{LO} = 854$  MHz e  $f_{LO} = 909$  MHz, respectivamente.

Assim, foi adotado um valor de  $F_s = 150$  MSPS. Isso resulta em uma banda de transição de 70 MHz com a imagem na segunda zona de Nyquist centrada em 122.5 MHz, com uma frequência mínima de 110 MHz, a qual pode ser facilmente filtrada.

Com  $F_s$  definido calcula-se o valor de  $N$ , a partir da relação  $N = F_s/\Delta_f$ , o que resulta em  $N = 10000$  amostras.

Finalmente o número mínimo de bits  $b$  do DAC é escolhido. Isso em grande parte depende das especificações do DAC e da RSR desejada. No projeto atual, foi adotado uma  $RSR_q = 55$ dB, o que resulta em  $b = 10$ -bits, de acordo com a etapa 12 da metodologia de projeto apresentada.

- **Determinação dos parâmetros para GSM900** - O canal do protótipo do BTM dedicado a aplicações de GSM900 é o 3 (Figura 3.6). As especificações do FPB e do FBP aplicados neste canal, assim como suas magnitude da resposta em frequência, foram apresentadas e devidamente comentadas na Seção 3.7, Figuras 3.7 e 3.9.

Após uma análise detalhada da resposta em frequência dos dois filtros, chegou-se à conclusão de que um valor razoável seria adotar  $f_{\min} = 25.2$ , o que resulta em

$f_{\max} = 49.8$  MHz e  $f_c^{BB} = 37.5$  MHz. Daí, a  $f_{LO}$  será dada por

$$f_{LO}(\text{MHz}) = 947.5 \pm 37.5 = \begin{cases} 910 \text{ MHz} \\ 985 \text{ MHz} \end{cases}$$

Se  $f_{LO} = 910$  MHz, as imagens são centradas em 872.5 e 947.5 MHz, respectivamente. Por outro lado, se  $f_{LO} = 985$  MHz, as imagens são centradas, respectivamente, em 947.5 e 1022.5 MHz. Como exemplo, as duas situações são ilustradas na Figura 4.2.

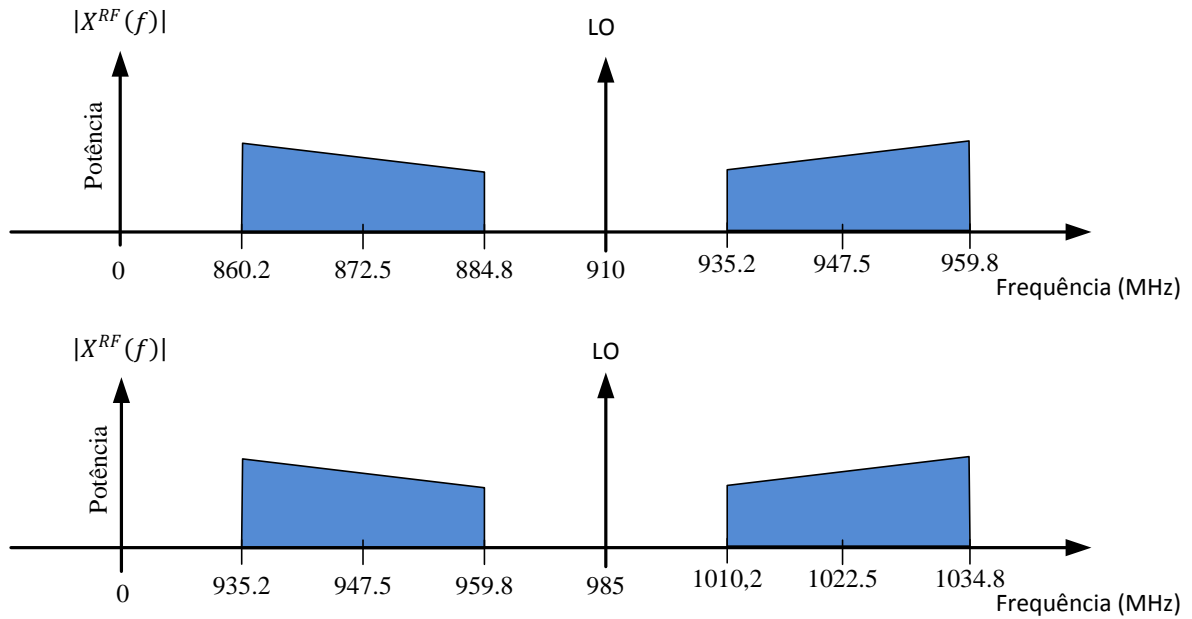


Figura 4.2: Ilustração do sinal na saída do *mixer* para  $f_{LO} = 910$  MHz e  $f_{LO} = 985$  MHz, respectivamente, para GSM900.

Neste caso, também foi adotado um valor de  $F_s = 150$  MHz, o que resulta em uma banda de transição de 50.4 MHz e uma imagem na segunda zona de Nyquist centrada em 112.5 MHz, com uma frequência mínima de 100.2 MHz, o qual também pode ser facilmente filtrado pelo FPB do canal 3 do protótipo do BTM.

Com  $F_s$  escolhido, calcula-se finalmente o  $N = 750$  amostras e escolhe  $b = 10$  bits.

O resumo dos parâmetros escolhidos e calculados para a computação do SB para os dois sistemas alvos é apresentado na Tabela 4.2.

Tabela 4.2: Sumário dos parâmetros especificados para a computação do do SB-BB.

Parameters	LTE Banda 5	GSM900
$f_{\min}$ (MHz)	15	25.2
$f_{\max}$ (MHz)	40	49.8
$f_c^{BB}$ (MHz)	$15 : \Delta_f^{LTE} : 40$	$25.2 : \Delta_f^{GSM} : 49.8$
$f_c^{BB}$ (MHz)	27.5	37.5
$F_s$ (MHz)	150	150
$b$	10	10
N	10000	750

## 4.4 Experimento 1: Resultados de Simulação em Matlab

Nesta seção são apresentados os resultados preliminares de simulações realizadas no ambiente Matlab para geração do SBD-BB. Esta etapa tem como objetivos: 1) Analisar a influência da escolha de diferentes conjuntos de  $\{\theta\}$  nos valores de PAPR e RSR; 2) Validar a expressão da RSR proposta na Subseção 3.2.2, através do levantamento das RSRs para diferentes conjuntos de Multitom. Desta forma, a simulação foi dividida em duas etapas:

Na primeira etapa,  $\theta = 0$  para todos os elementos do conjunto  $\{\theta\}$ , enquanto que na segunda,  $\theta$  assume valores aleatórios uniformemente distribuídos entre  $[-\pi, \pi]$ .

A computação do SBD-BB se deu através da Equação (3.4), com  $A = 1$  e o restante dos parâmetros, especificados de acordo com os valores dispostos na Tabela 4.2, referentes ao LTE-B5. Após a computação, o SBD-BB foi quantizado em ponto fixo com 10-bits mediante o quantizador descrito na Seção 3.2.2.

Resultados da primeira etapa, com o conjunto  $\{\theta\} = 0$ , são apresentados na Figura 4.3. Onde observa-se que o sinal no domínio do tempo (**parte superior da Figura**) apresenta altos picos em relação à média, principalmente nas duas extremidades. Como resultado, obteve-se um valor alto do PAPR, aproximadamente 10 dB. No domínio da frequência, o resultado é uma PSD altamente distorcida (**parte inferior da Figura**), dentro e fora da banda de interesse.

Estes resultados se devem ao fato de que para este conjunto de valores de  $\{\theta\}$ , a faixa dinâmica do sinal é maior que  $[-3\sigma, 3\sigma]$  e sua distribuição não mais segue uma Gaussiana. Isso é comprovado pelo histograma da distribuição do sinal, apresentado na Figura 4.4 (A amplitude

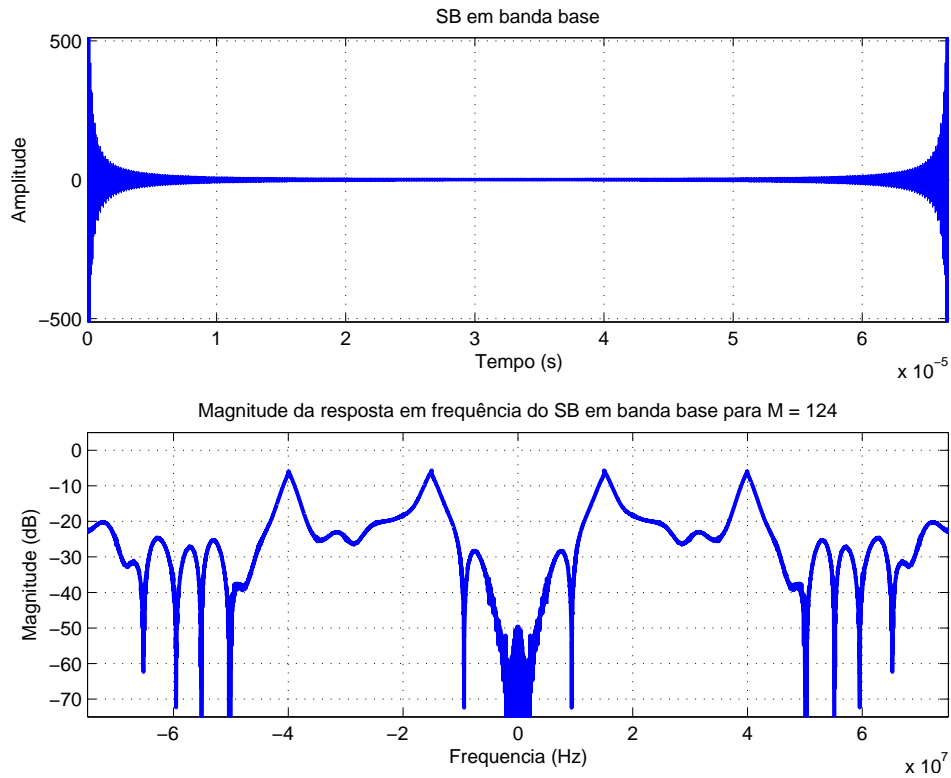


Figura 4.3: Resultado do SBD-BB computado com todos os valores do conjunto  $\{\theta\} = 0$ . **superior**) Sinal no domínio do tempo. **inferior**) Sua magnitude da resposta em frequência.

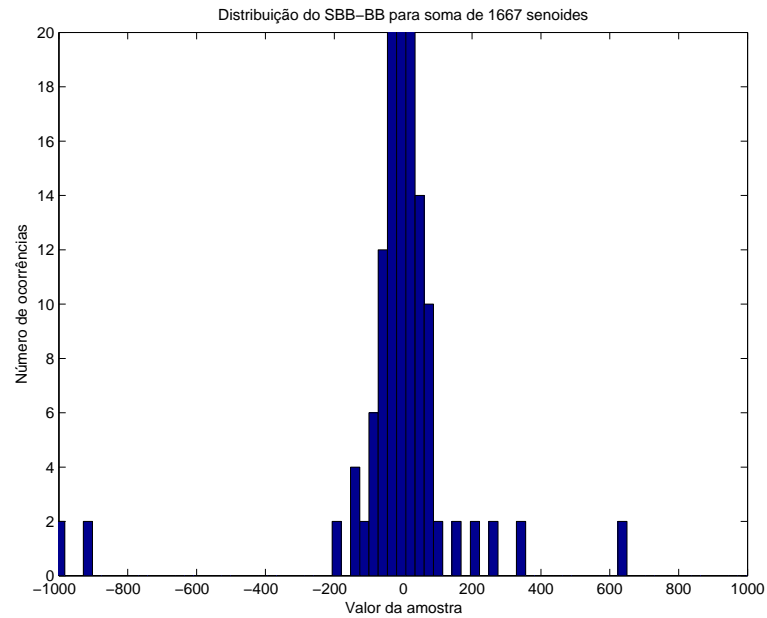


Figura 4.4: Histograma da distribuição do SBD-BB para valores de  $\{\theta\} = 0$ .

foi cortada para caber no texto) (para  $|\mathcal{K}| = 1667$ ), onde observa-se que a variação máxima do sinal foi de aproximadamente  $[-1000, 1000]$ , para uma variância do sinal de  $\sigma_s^2 = \frac{A^2}{2} |\mathcal{K}| = 834$ ,

o qual é muito maior que 90% da faixa dinâmica ( $[-86.6, 86.6]$ ). Em termos de quantização, os valores fora da faixa dinâmica esperada, provocam um *overload* no quantizador e o erro de quantização cresce.

Na Figura 4.5 são apresentados os resultados comparativos (para cada conjunto multitom) entre os valores teóricos e estimados da potência, do erro de quantização e da RSR. Ainda na mesma Figura, observa-se que a potência teórica e estimada coincidem, porém a potência do erro de quantização estimada não segue a teórica, o que resultou em diferença de RSR de aproximadamente 54 dB.

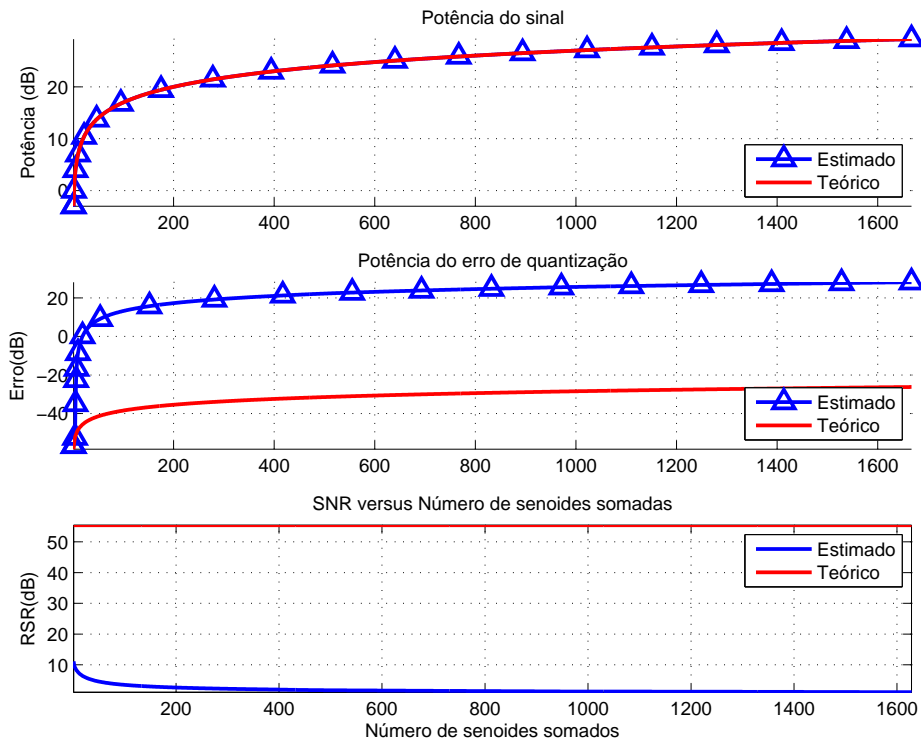


Figura 4.5: Comparação das características estimadas do SBD-BB com as teóricas (para  $|\mathcal{K}| = 0$  até  $|\mathcal{K}| = 1667$ ), computados com todos os valores do conjunto  $\{\theta\} = 0$ : **superior**) Potência do sinal. **médio**) Potência do erro de quantização. **inferior**) RSR.

Para o segundo caso, tomou-se um conjunto de valores de  $\{\theta\}$  uniformemente distribuídos de  $[-\pi, \pi]$ . Para garantir que a faixa dinâmica do sinal fique contido entre  $[-3\sigma, 3\sigma]$ , são executadas várias realizações com diferentes conjuntos de valores de  $\theta$ , para cada conjunto de Multitons. Em seguida são escolhidos os sinais resultantes com menor amplitude.

O SBD-BB resultante, no domínio do tempo e a sua magnitude da resposta em frequência são respectivamente apresentadas na Figura 4.6. Observa-se que o sinal no domínio do tempo não apresenta picos altos em relação a média. O resultado foi um valor baixo de

PAPR, aproximadamente  $-10.2$  dB.

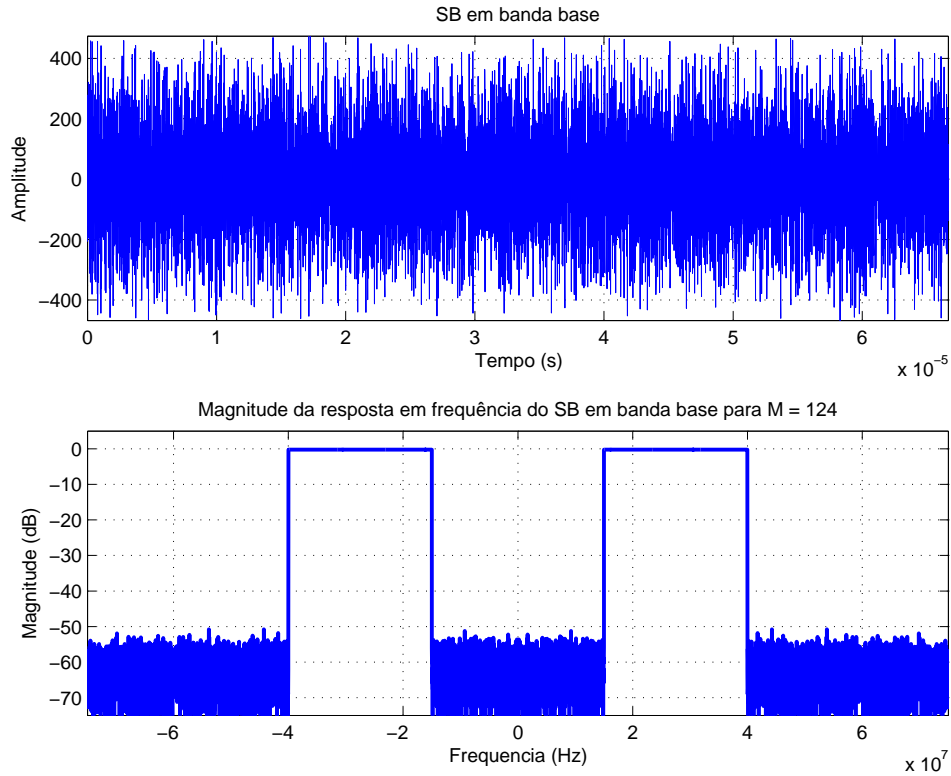


Figura 4.6: Resultado do SBD-BB computado com os valores do conjunto  $\{\theta\}$  uniformemente distribuídos de  $[-\pi, \pi]$ . **superior**) Sinal no domínio do tempo. **inferior**) Sua magnitude da resposta em frequência.

Na Figura 4.7 é apresentado o histograma do SBD-BB para  $|\mathcal{K}| = 1667$ . Observa-se então, que neste caso a distribuição do sinal é aproximadamente Gaussiana e sua variância é  $\sigma_s^2 = \frac{A^2}{2}|\mathcal{K}| = 834$ . A variação máxima do sinal foi de aproximadamente  $[-80, 80]$ , 90% da faixa dinâmica de  $[-86.6, 86.6]$ , como esperado.

A comparação dos valores teóricos e estimados (para cada conjunto multiton) da potência, do erro de quantização e da RSR são apresentados na Figura 4.8. Observa-se então que para este caso as RSRs estimadas seguem o teórico, com uma máxima variação de aproximadamente  $\pm 0.05$  dB.

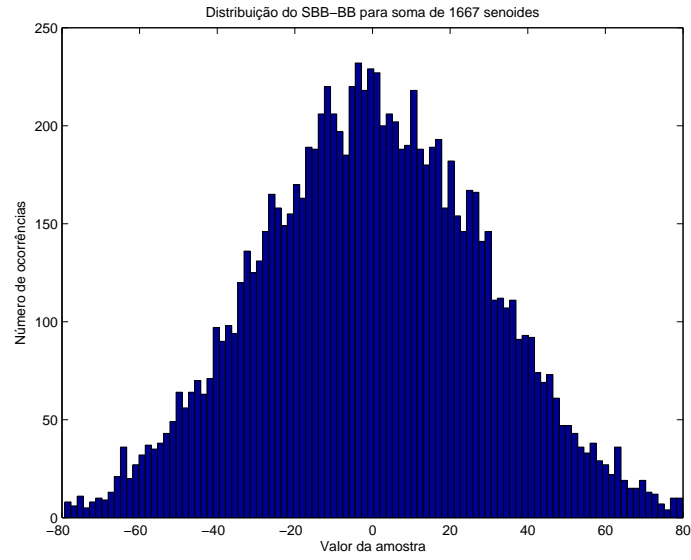


Figura 4.7: Histograma da distribuição do SB-BB para valores de  $\theta$  aleatórios uniformemente distribuídos de  $[-\pi, \pi]$ .

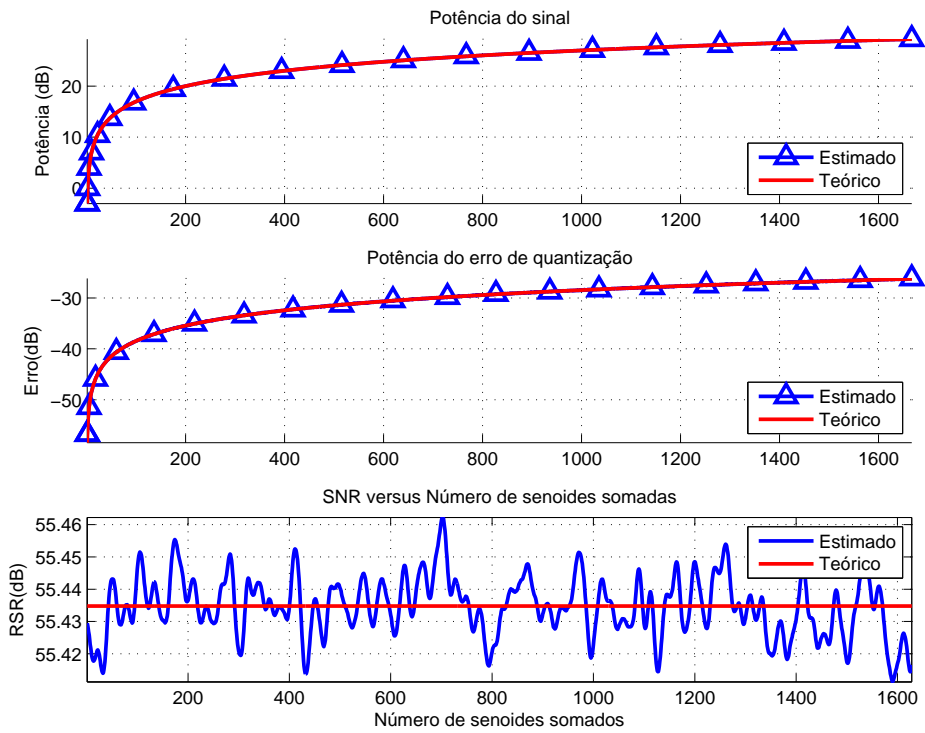


Figura 4.8: Comparação das características estimadas do SBD-BB com as teóricas (para  $|\mathcal{K}| = 0$  até  $|\mathcal{K}| = 1667$ ), computados com os valores do conjunto  $\{\theta\}$  uniformemente distribuídos de  $[-\pi, \pi]$ : **superior**) Potência do sinal. **médio**) Potência do erro de quantização. **inferior**) RSR.



## 4.5 Experimento 2: Resultados da Implementação Prática

Nesta seção são apresentados resultados de implementação prática da geração do SB-BB e SB-RF para os sistemas LTE-B5 e GSM900. Os experimentos foram realizados com o protótipo da BTM apresentado na Seção 3.7.

O projeto de hardware do FPGA para a ULD foi desenvolvido no software da Altera, Quartus II e o esquemático do nível mais alto (Top level) é apresentado na Figura 4.9.

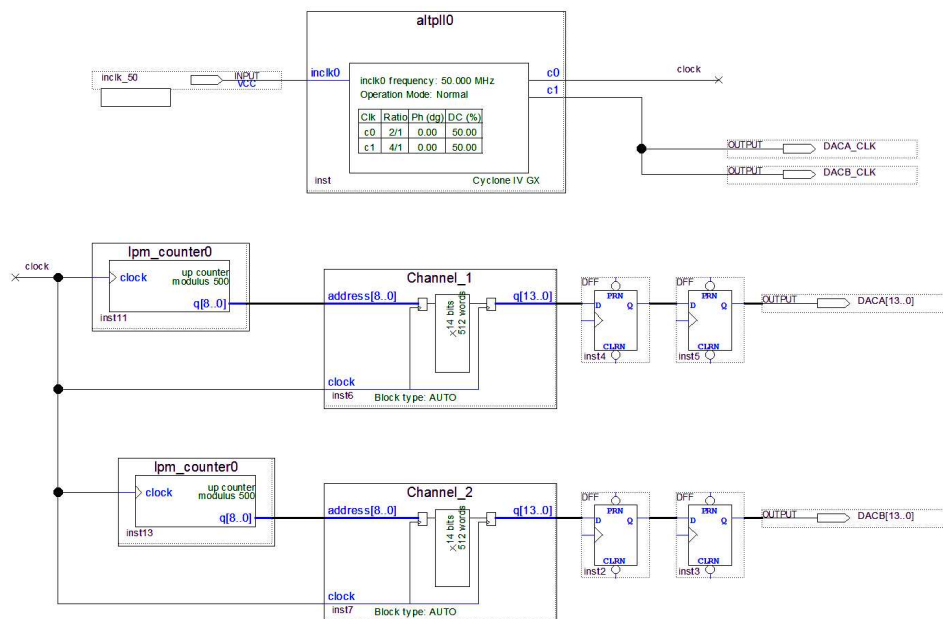


Figura 4.9: Top level do projeto de VHDL da ULD implementada para os dois canais do BTM.

O sumário do consumo total do hardware do FPGA para ambos os sistemas é apresentado na Tabela 4.3.

Tabela 4.3: Total do consumo do hardware do FPGA EP3C120F484C7 para implementação da ULD para dois canais .

Tipo de recurso	Quantidade usado	Porcentagem dos recursos disp/usados
Elementos Lógicos (LEs)	14	1 %
Memória (bits)bits	16,000	1 %

Verifica-se então que o sistema consome pouco hardware devido a lógica simples

implementada. De fato o consumo se concentrou nos bits de memória usados no armazenamento das amostras pré-processadas. Isso mostra que a técnica de pré-processamento é extremamente vantajoso, em termos de consumo de hardware, eficiência e velocidade do sistema.

O arcabouço experimental é apresentado na Figura 4.10, onde o protótipo da BTM é conectado a um analisador de espectro via conectores SMA para o levantamento das PSDs de interesse.

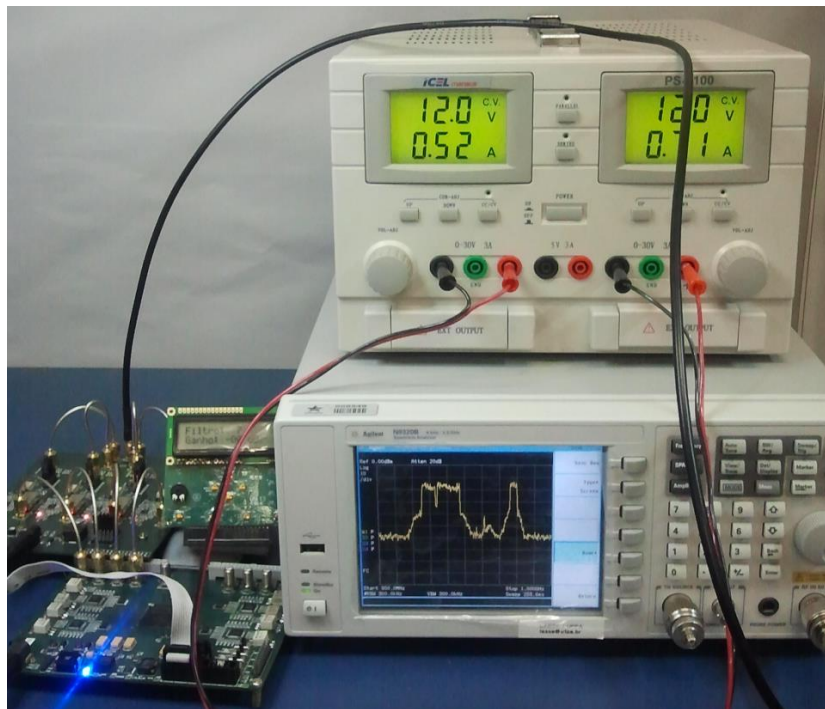


Figura 4.10: A configuração dos componentes para o procedimento experimental.

O programa para a geração do sinal é carregado no FPGA da ULD, que gera e transmite de forma contínua as amostras digitais para o DAC. Em seguida, o SB-BB, na saída do DAC, é enviado para a placa do TH, que o converte e gera o SB-RF. Em seguida o SB-RF é enviado para o analisador do espectro para análise.

Desta forma, primeiramente foi realizada a análise do SB-BB e em seguida do SB-RF.

A PSD capturada no analisador de espectro dos SB-BBs, na saída do DAC filtrado (com destaque em quatro canais), para o LTE-B5 e GSM900 são apresentadas na Figuras 4.11 e 4.12, respectivamente. Como esperado, a PSD de ruído medido do DC para  $F_s/2$  é aproximadamente plana para ambos os SB-BBs. Para o LTE, a PSD do ruído medido foi  $\mathcal{N}_0 \approx -135$  dBm/Hz, o que corresponde a uma potência total de ruído de  $\approx -56$  dBm/75 MHz. A potência medida do

sinal foi de  $\approx -4.3$  dBm/25 MHz, isso resulta em uma  $RSR_q \approx 52$  dB, que é aproximadamente igual a  $RSR_q$  especificada.

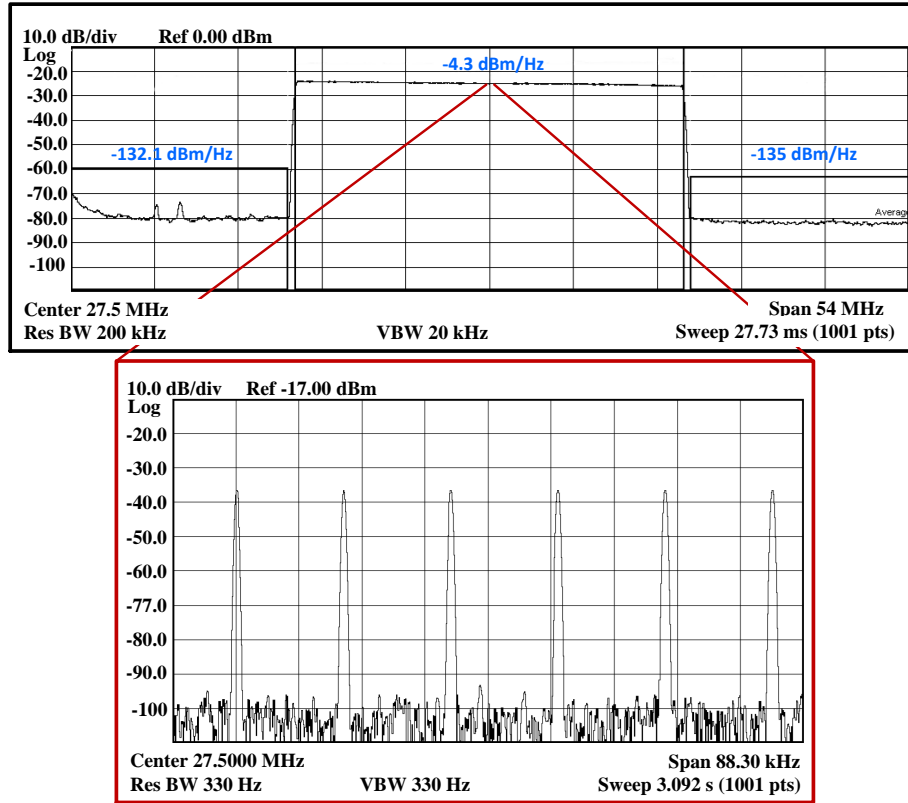


Figura 4.11: PSD com medidas de potência do SB-BB para o LTE-B5 com zoom em seis canais.

No caso do GSM, a PSD do ruído medido foi  $\mathcal{N}_0 \approx -136.7$  dBm/Hz, o que corresponde a uma potência de ruído total de  $\approx -58$  dBm/75 MHz. A potência medida do sinal foi de  $\approx -5.2$  dBm/24.6 MHz, isso resulta em uma  $RSR_q \approx 53$  dB, que também é aproximadamente igual a  $RSR_q$  especificada.

Nas Figuras 4.13 e 4.14, são apresentadas, respectivamente, as PSDs dos SB-RFs da saídas filtradas dos *mixer* para o LTE-B5 e o GSM900.

No caso do GSM, mediu-se uma potência do sinal de  $\approx 4.28$  dBm/24.6MHz e a potência do ruído medido em uma banda de 76 MHz (fora da banda), abaixo e acima da banda de interesse foi de, respectivamente,  $-128.2$  dBm/Hz e  $-120$  dBm/Hz, ou seja, a  $RSR_q$ , é aproximadamente 53 dBm e 45 dBm, respectivamente.

Para o LTE-B5, foi medida uma potência de sinal de 4.2 dBm/25MHz e as potências do ruído abaixo e acima foram, respectivamente,  $-113.1$  dBm/Hz e  $-122$  dBm/Hz, o que resulta

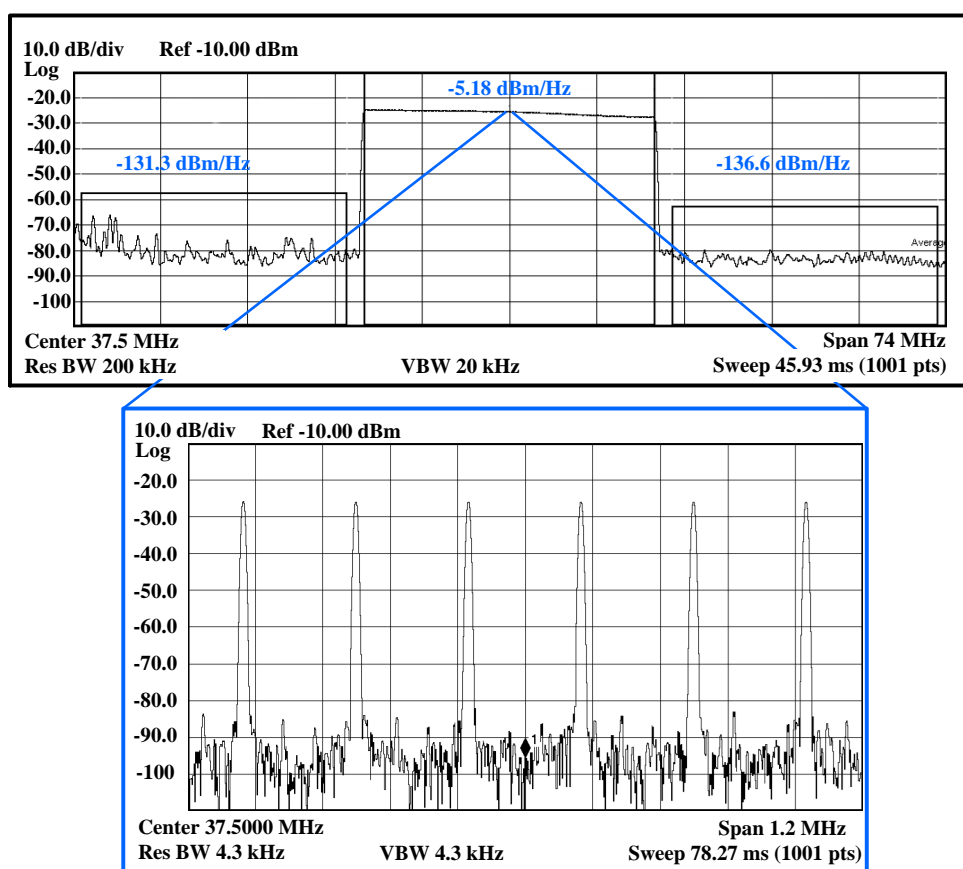


Figura 4.12: PSD com medidas de potência do SB-BB para o LTE-B5 com zoom em seis canais..

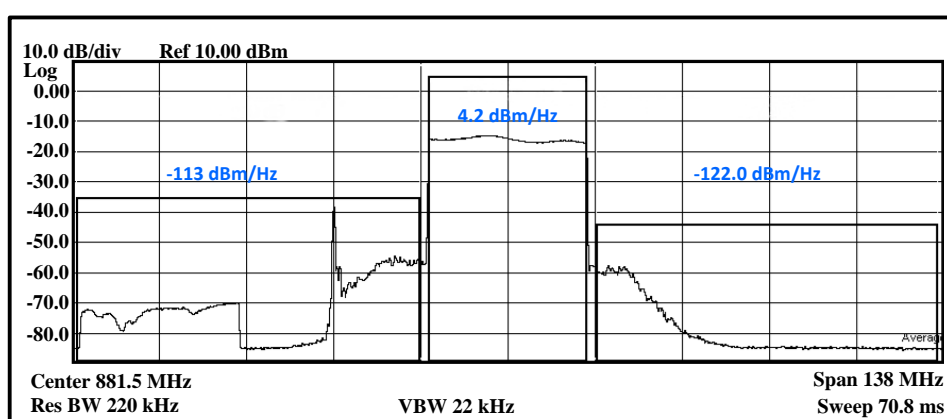


Figura 4.13: PSD com medidas de potência dentro e fora da banda do SB-RF para o LTE-B5.

em RSRs de aproximadamente 38 dBm e 47 dBm, respectivamente.

A potência do ruído na banda abaixo tem a contribuição do sinal remanescente da

imagem filtrada e do LO. Isso pode ser melhorado aplicando FBP com maiores atenuações e também o uso de *mixer* de frequência que requerem LO com potências menores.

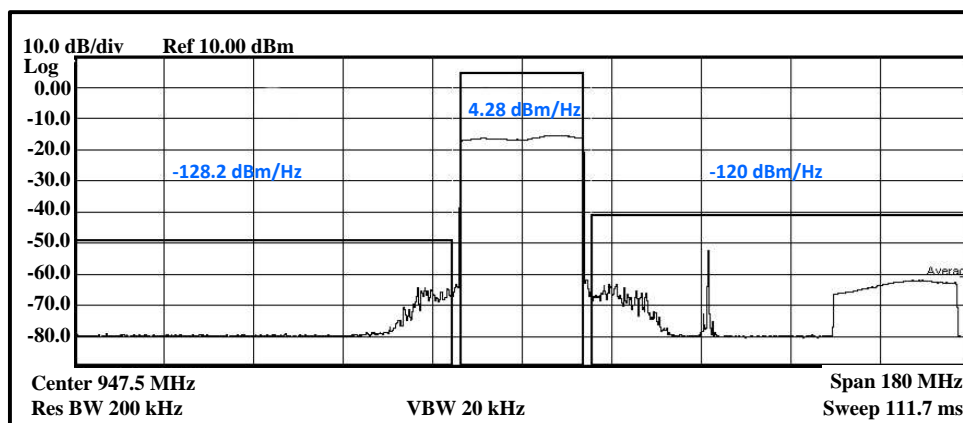


Figura 4.14: PSD com medidas de potência dentro e fora da banda do SB-RF para o GSM900.

## 4.6 Experimento 3: Bloqueio de sinais de LTE Em um Cenário Real

Nesta seção são apresentados resultados de experimentos de bloqueio de sinais LTE. O experimento é conduzido em um cenário real de transmissão, recepção e bloqueio de sinais LTE.

O sucesso ou não do bloqueio se caracterizou de forma binária, baseado na decodificação ou não do sinal recebido na presença do SB. Neste caso, o sinal foi considerado bloqueado quando o receptor foi incapaz de decodificar o sinal recebido e apresentar a sua constelação.

O experimento consiste em gerar e transmitir um sinal de LTE na direção DL com largura de banda do canal igual a 10 MHz, centrada na frequência 947.6 MHz. Em seguida, executar o bloqueio deste sinal, mediante a transmissão de um SB com a mesma largura de banda,  $\Delta_f = 15$  kHz e centrada na mesma RF do LTE. A transmissão do SB-RF se deu pelo canal 1 do protótipo da BTM.

- **Arcabouço Experimental** - O arcabouço experimental para o cenário de bloqueio é apresentado na Figura 4.15. O arcabouço é constituído de um computador com o software da Agilent (agora Keysight) Systemvue, um gerador de forma de ondas arbitrárias (transmissor) um analisador de espectro (receptor) e o BTM do bloqueador. O computador com o Systemvue é conectado ao analisador via Ethernet para transmissão de amostras. A transmissão e recepção dos sinais é feita mediante as antenas TX e RX.
- **Geração dos sinais** - O processo de geração do sinal do LTE começa no Systemvue, que computa as amostras do sinal e as envia para o gerador através de uma interface Ethernet. O gerador então processa as amostras e gera o sinal da LTE.
- **Transmissão e recepção** - A transmissão do sinal se deu através de uma antena VERT900 (para aplicações de 900 MHz) conectada ao gerador. No outro lado, o analisador de espectro funcionou como um receptor, capturando o sinal também através de uma antena VERT900. A decodificação do sinal é realizada no software de análise VSA instalado no próprio analisador de espectro. Devido à baixa potência de transmissão envolvida, as antenas do transmissor e do receptor foram posicionadas próximas o suficiente para permitir a decodificação do sinal do LTE na ausência do SB. Já a posição do BTM foi determinada empiricamente, e este foi posicionado um pouco afastado do receptor.
- **Resultados** - A realização do experimento se deu em duas etapas: Na primeira etapa,

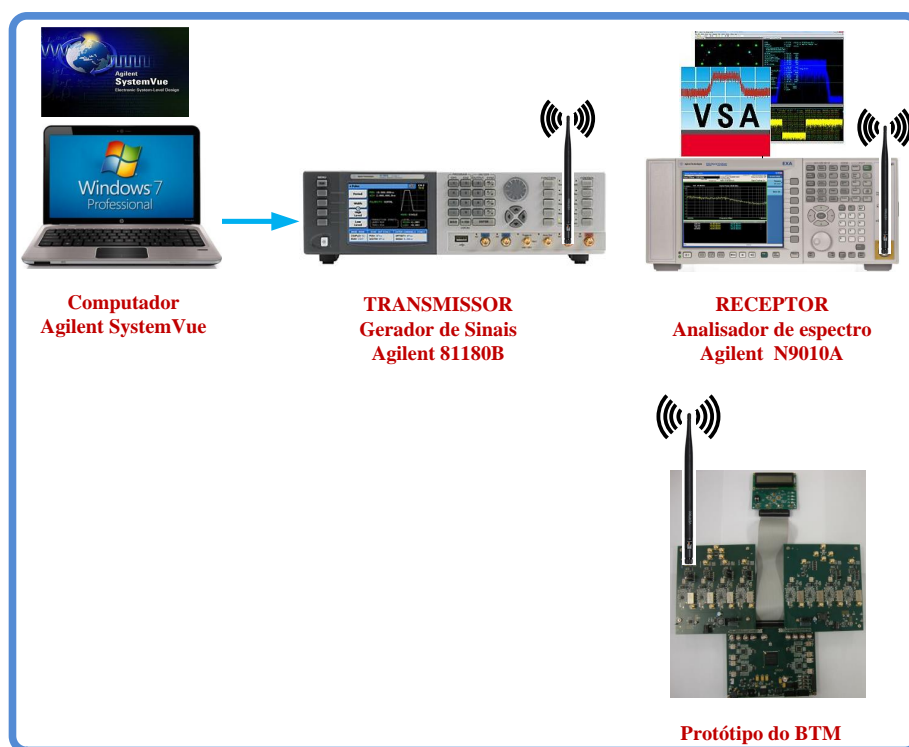


Figura 4.15: Arcabouço para o experimento prático de bloqueio de sinais LTE.

apenas o sinal do LTE foi transmitido e o SB foi desligado. Já na segunda etapa ambos os sinais foram transmitidos e recebidos ao mesmo tempo.

Nas condições de transmissão e recepção descritas, a potência do sinal de LTE e do SB, medidas no receptor foram de aproximadamente -18 dBm e -17.3 dBm, respectivamente. Em relação à primeira etapa do experimento, esta tem por objetivo, verificar a decodificação do sinal pelo receptor, na ausência de qualquer interferência. Os resultados desta etapa são apresentados na Figura 4.16, em termos de PSD e da constelação do sinal recebido. Para este caso, o sinal foi decodificado, como mostra a constelação dos símbolos recebidos. A PSD do sinal recebido, para este caso, assim como a constelação decodificada são apresentadas na Figura 4.16.

Na segunda etapa, o sinal do LTE e o SB foram transmitidos ao mesmo tempo. Como resultado, o receptor não foi capaz de sincronizar e nem tão pouco decodificar o sinal recebido (Figura 4.17). Neste caso foi considerado que o sinal foi devidamente bloqueado.

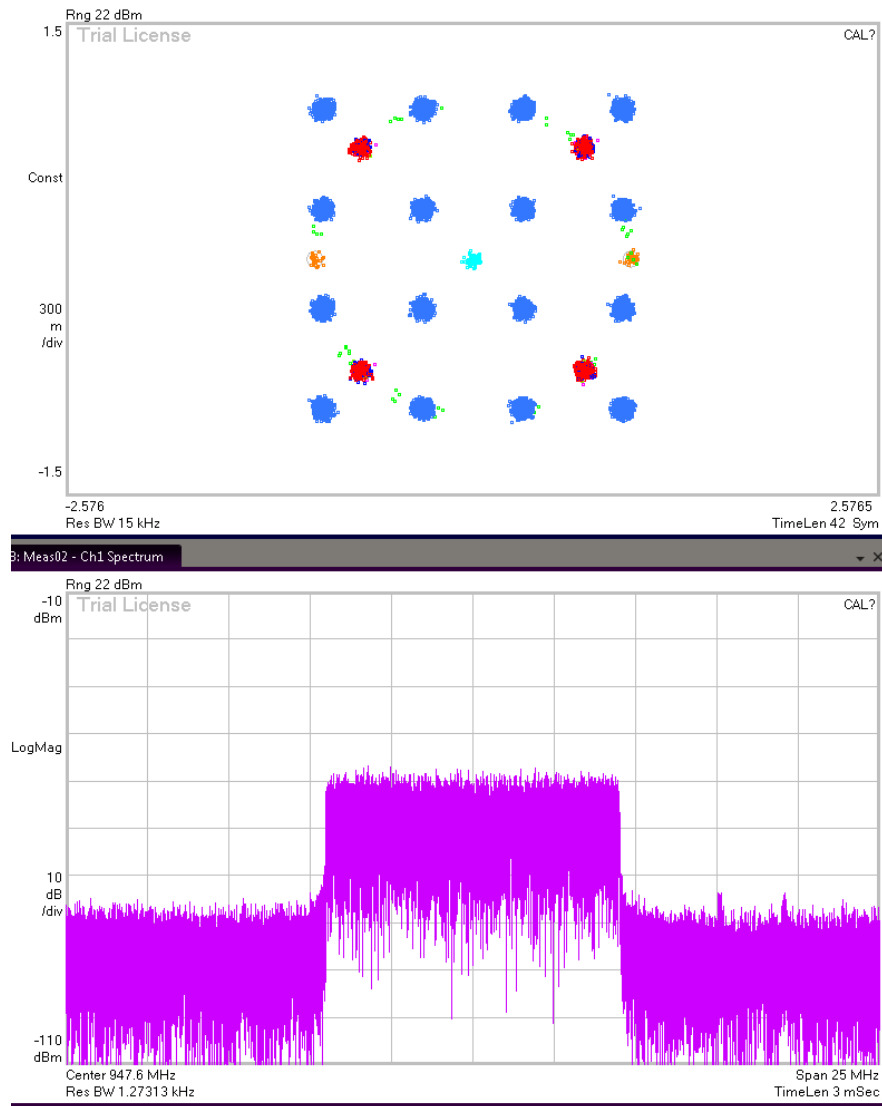


Figura 4.16: Sinal do LTE recebido e decodificado no analisador do espectro. **superior**) Constelação. **inferior**) PSD.

## 4.7 Conclusão

Este capítulo apresentou resultados de três experimentos na geração de SB e sua aplicação no bloqueio de sinais de telefonia celular.

No Experimento 1 foram obtidos resultados, mediante simulações realizadas no matlab, os quais validaram o método proposto na Seção 3.2.1 para redução do PAPR. Verificou-se que tomando um conjunto de valores de  $\theta$  uniformemente distribuídos entre  $[-\pi, \pi]$ , o PAPR



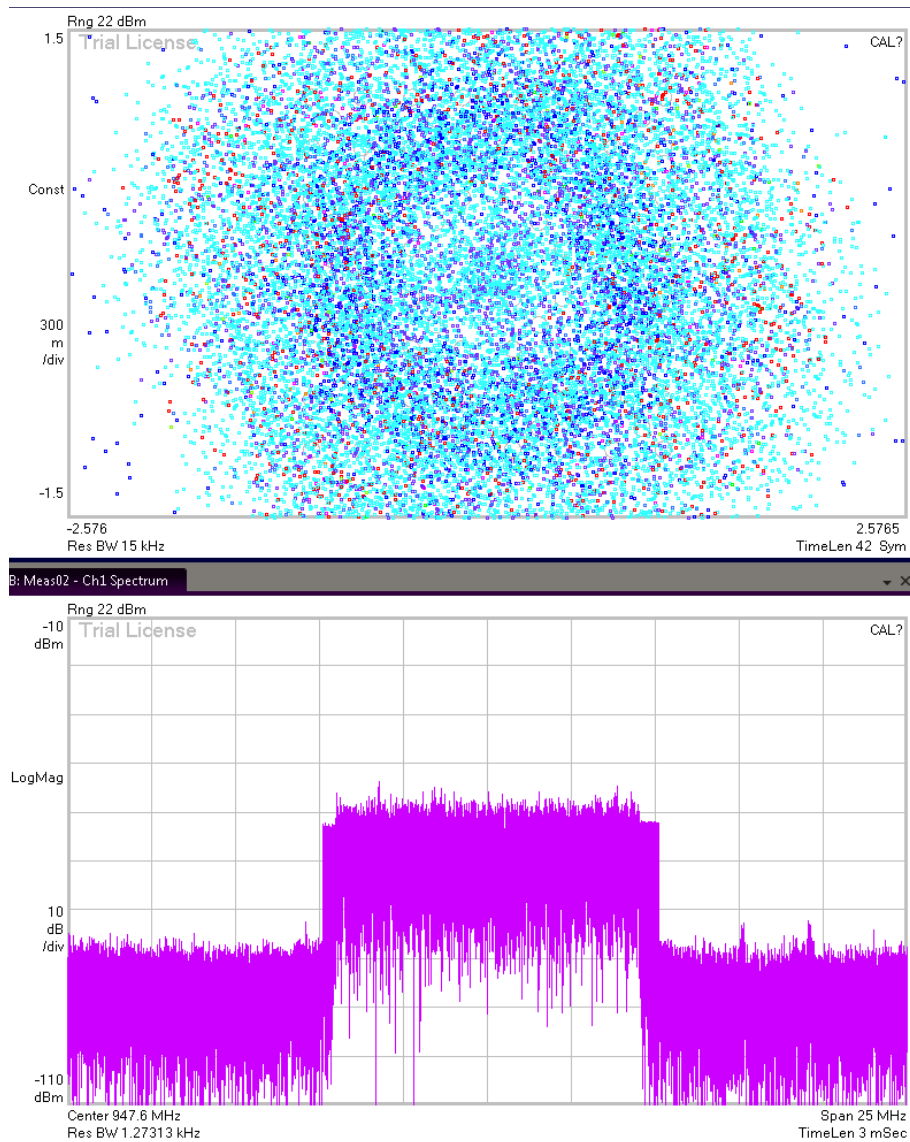


Figura 4.17: Sinal do LTE recebido e (não decodificado) no analisador do espectro. **superior)** Constelação. **Inferior)** PSD.

é significativamente menor, quando comparado com o PAPR resultante de um conjunto de valores de  $\theta = 0$ , como esperado. Ainda, resultados comparativos entre  $RSR_q$  teórica e estimada, foram praticamente iguais aos teóricos. Isso validou a metodologia e mostra que o protótipo do BTM tem condições de obter o desempenho projetado em termos do SB-BB e SB-RF.

Por fim, O experimento 3 explorou um caso prático que envolve um cenário real de transmissão, recepção e bloqueio dos sinais de LTE. Resultados obtidos mostraram que o sinal

gerado pelo BTM é capaz de realizar a tarefa.

O protótipo ainda será aperfeiçoado no decorrer dessa pesquisa, mas o mesmo já se mostrou apto a validar os algoritmos. O estudo de RATc tem um viés acadêmico forte, e os algoritmos derivados no escopo do mesmo poderão ser avaliados em condições realísticas de operação.

## Capítulo 5

# Planejamento da Pesquisa Futura e Cronograma

Nesta proposta foram investigadas técnicas para se obter um sistema de BTM flexível e reconfigurável, o qual combina técnicas de (PDS) e de PAS para gerar o sinal de bloqueio em banda base e em RF, respectivamente. O arcabouço do sistema proposto é formado por uma (ULD) e um (TH) para gerar um sinal de bloqueio, onde este pode ser reconfigurado em tempo real para cobrir diferentes bandas do espectro.

Uma metodologia de projeto para gerar o SBD-BB e uma expressão para a RSR de quantização para sinais multitom foram derivadas, avaliadas e validadas em experimentos de PDS realizados no ambiente de simulação Matlab. A metodologia foi estendida para uma implementação prática para a geração do SBD-BB.

A parte da lógica digital foi realizada usando um FPGA. Esse módulo foi avaliado e validado em experimentos práticos de geração de sinais em banda base.

As técnicas e arquiteturas investigadas formaram a base que derivou um protótipo de BTM completo, o qual tem a vantagem de ser reconfigurável e usar poucos recursos de hardware no processo de geração do SB. O protótipo foi testado em experimentos práticos de geração de SB em banda base e em RF com resultados satisfatórios.

A proposta desta tese é de continuar o trabalho já desenvolvido para incluir um módulo de RATc no sistema do BTM. A tarefa principal focaliza: investigar e desenvolver novos algoritmos que sejam eficientes e de fácil implementação para classificação de RATs; prover uma arquitetura baseada em FPGA, focada na redução de recursos de hardware e processamento rápido, para implementação em hardware dos algoritmos desenvolvidos; investigar e desenvolver novos algoritmos para a geração automática, em tempo real, do

SBD-BB; prover um arcabouço que integre classificação e geração dos SBs, com capacidade de monitorar o espectro, identificar atividades e classificar as RATs atuantes em uma determinada faixa de espectro, em uma determinada área. A partir dos RATs classificados, o BTM deverá adequar os seus parâmetros de geração e transmissão do SB de acordo com os parâmetros pré-estabelecidos para cada RAT.

O diagrama em blocos do arcabouço proposto é apresentado na Figura 5.1. Este sistema é composto por um módulo de receptor-heteródino, um módulo de RATc, um módulo gerador e um módulo de transmissor-heteródino.

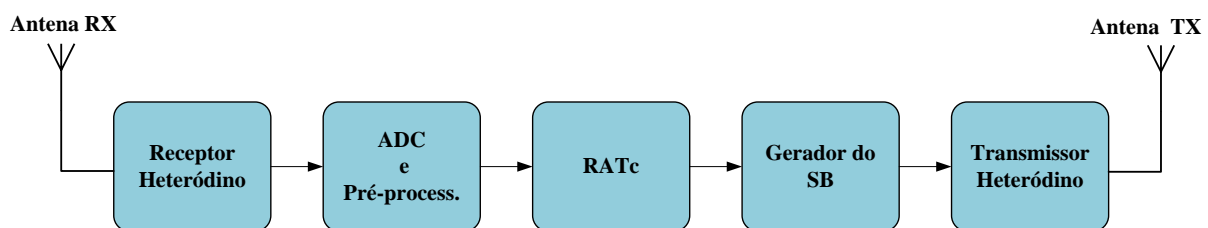


Figura 5.1: Arcabouço proposto para um sistema integrado de classificação e bloqueio de RATs.

A função de cada um dos módulos é descrito a seguir:

- **Receptor-heteródino**— Tem a função de receber o sinal de RF da antena, transladá-lo para uma FI e enviar para o conversor de AD.
- **Pré-processador digital** - A função deste módulo é de receber digitalizar e condicionar o sinal para pós-processamento. Este módulo será implementado em FPGA.
- **RATc**— A função deste módulo é de extrair as características (temporais ou frequenciais) pré-determinadas do sinal pré-processado, realizar a classificação da RAT através de algoritmos rápidos e eficientes implementados em FPGA e gerar uma etiqueta (rótulo ou classe) de acordo com a RAT determinada.
- **Gerador**— Este módulo recebe do classificador a etiqueta da RAT identificada e gera o SBD-BB de acordo com as características ( $\Delta_f$ ,  $BW$ , etc.) pré-estabelecidas para aquela RAT específica. Em seguida o SBD-BB é convertido para SB-BB e enviado para o transmissor.
- **Transmissor-heteródino**— Tem a função de transladar o SB-BB para SB-RF e enviar para antena para transmissão.

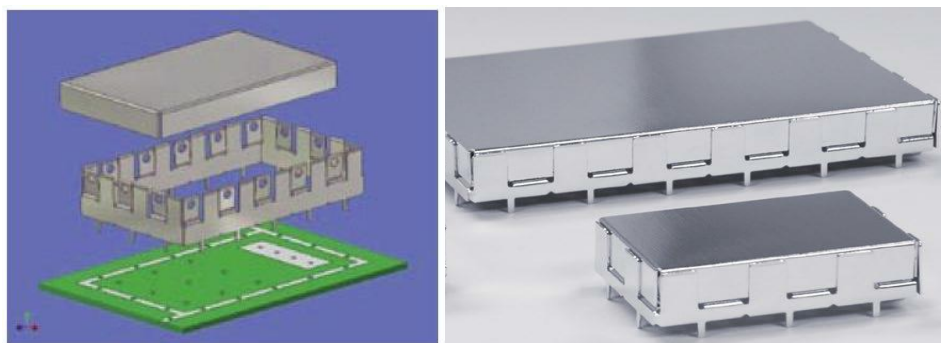


Figura 5.2: Exemplo ilustrativo de blindagem de sinais de RF em PCB.

O principal objetivo da tese é avançar o processamento digital de sinais para BTMs, focando por exemplo em problemas como RATc. Mas o protótipo tem sua importância pois será usado para validação. Assim, além da pesquisa de novos algoritmos em si, serão feitas melhorias no protótipo, as quais serão financiadas pela empresa Brasilat, que colabora com a UFPA nesta pesquisa.

Com o objetivo de melhorar a qualidade do sinal gerado, em termos de emissão de espúrios fora da faixa e de filtragem, propõe-se as seguintes mudanças e melhorias para o protótipo Beta do BTM:

- **Amplificador de banda base** - Selecionar um amplificador com menor ganho e menos distorção na banda desejada, de modo a preservar o espectro do sinal em banda base, em termos de emissão de espúrios fora da faixa.
- **Mixer** - Selecionar mixers de nível 3 ou 4, com o objetivo de diminuir a potência exigida na entrada do LO. Talvez seja necessário usar mixers ativos ou de supressão de banda, para atenuar os sinais do LO e da imagem não desejada do sinal.
- **Amplificador de RF** - Selecionar um novo amplificador com menor ganho e menor distorção nas frequências de interesse em RF, com o objetivo de diminuir as emissões fora da faixa em RF.
- Adotar implementação modular onde cada canal possui sua própria placa de transmissor heteródino de modo a evitar o vazamento do sinal de RF de um canal para outro.
- Prover blindagem usando módulos de blindagem de RF de modo a evitar a interferência deste em outros sistemas e de outros sistemas neste. Um exemplo de esquema de blindagem de PCB com uso de módulos de metal é apresentado na Figura 5.2

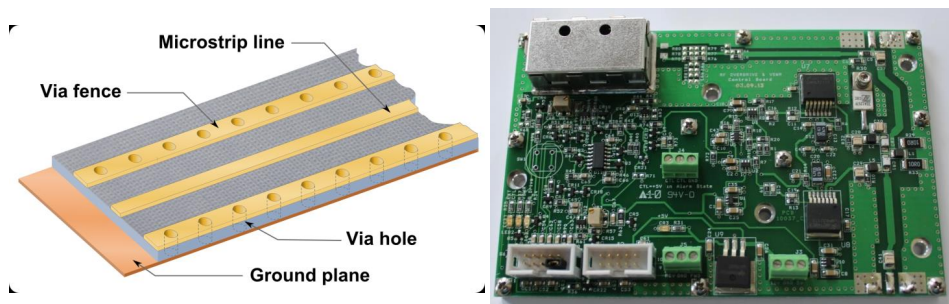


Figura 5.3: Exemplo de uso de “cercas de vias” para proteger a trilha do sinal de RF.

- Projetar a PCB para prover isolamento nas trilhas, principalmente aquelas que conduzem os sinais de RF.
- Isolar trilhas do sinal de RF com “cercas de vias” para evitar interferência eletromagnética entre os sinais. Um exemplo desta técnica é apresentado na Figura 5.3
- Isolar as partes de frequência mais baixas das de frequências mais altas com blindagem metálica.

## 5.1 Cronograma Proposto

As principais atividades para a continuação deste trabalho estão resumidas no cronograma seguinte:

1. Aperfeiçoar e manter atualizada a revisão bibliográfica e estado da arte em classificação de RATs.
2. Investigar algoritmos de classificação de RATs propostos na literatura e contrastar os baseados nas características espectrais com os baseados nas características temporais. Selecionar, implementar e simular em Matlab os algoritmos de maior relevância.
3. Propor novos algoritmos de classificação de RATs, voltadas para sistemas GSM e LTE. Simular os algoritmos em ambiente Matlab e usar o Weka para classificação.
4. Implementar os algoritmos propostos em VHDL e testar em ambiente de simulação Multisim.
5. Propor uma arquitetura baseada em FPGA para um classificador de RATs, baseado nos algoritmos desenvolvidos.

6. Investigar algoritmos e técnicas de PDS baseados em FPGA propostos na literatura para a geração automática de sinais multiton.
7. Propor algoritmos eficientes, baseados em VHDL para geração automática de sinais multiton. Simular os algoritmos nas plataformas Quartus II e Modelsim.
8. Implementar em FPGA, mediante plataformas de desenvolvimento da Altera, um sistema para geração automática de sinais multiton, baseado nos algoritmos desenvolvidos.
9. Implantar as melhorias sugeridas no protótipo Beta do BTM.
10. Realizar testes de verificação de qualidade do sinal na saída de cada canal do BTM
11. Selecionar novos componentes para o protótipo beta do BTM
12. Projetar um novo circuito para o BTM beta
13. Projetar a PCB do BTM beta
14. Montar e testar o BTM beta
15. Publicação de artigos
16. Escrita e defesa da tese

Tabela 5.1: Cronograma de execução das atividades futuras propostas.

[illegible]



# Apêndice A

## Classificação de Tecnologia de Acesso via Rádio Utilizando Weka

### A.1 Introdução

Este apêndice apresenta alguns resultados básicos em classificação de RATs utilizando o *software* livre Weka, o qual é uma coleção de algoritmos de aprendizado de máquina feitos em linguagem de programação Java, com o objetivo de executar tarefas de Mineração de Dados. O Weka possui um conjunto de ferramentas para pré-processar dados, além de ferramentas de classificação, regressão, clusterização e associação. Uma delas, o *radial basis function neural network* (RBF-NN) é bastante usado em classificação de RATs e será adotado aqui.

Ressalta-se que os resultados apresentados neste apêndice são para simples conferência do estado da pesquisa atual no âmbito da tese em si.

### A.2 Base de Sinais de Tecnologias de Acesso via Rádio

Uma base de dados é um conjunto de exemplos (instâncias) descritos por um conjunto de atributos e uma classe de saída. Deste modo, cada exemplo possui um conjunto de atributos (ou características) que definem perante o classificador a sua classe.

A base das simulações realizadas possui 532 instâncias, 13 atributos de entrada e um atributo de saída denominado classe. Os atributos de entrada são todos numéricos e representam as PSDs de sinais gerados no SystemView. Os atributos de saída (atributos classe) são as RATs, que podem ser LTE , GSM ou WCDMA. Deste modo o classificador

criará um modelo que analise as PSDs e classifique o sinal em LTE, GSM ou WCDMA.

## A.3 Classificação de Tecnologias de Acesso via Rádio utilizando Matlab e Weka

Qualquer processo de classificação pode ser dividido em duas etapas:

1. Extração de características, onde são obtidos os parâmetros e
2. Algoritmo de classificação.

Assim, usa-se o Matlab para computar a extração das características e geração de dados, os quais são usados pelo Weka no processo de classificação de RATs.

### A.3.1 Extração de Características

Como já dito, este processo é realizado no Matlab através de um pacote de códigos que implementam diferentes algoritmos de extração de características e geram arquivos de entrada para o Weka. Neste caso, se extraiu os parâmetros dos sinais envolvidos e dois arquivos no formato ARFF foram criados. Os arquivos serviram de base nas tarefas de treino e teste do classificador. Cada arquivo contém um cenário o qual é composto por um receptor e um subconjunto de RATs ou modulações definidos na simulação.

Cada transmissor envia um sinal com uma RAT através do seu canal, na frequência central especificada neste cenário específico, a saída é o envelope complexo de um sinal multiplexado representando a banda  $BW_{IF}$ . Cada um dos sinais é convertido no domínio da frequência através do algoritmo de estimação da PSD *pwelch* e escrito em arquivos binários. Sintonizando a frequência de um LO, elas podem corresponder a diferentes larguras de banda de RF. Cada cenário tem uma única descrição especificada. Cada cenário pode ter várias instâncias, cada instância é descrita por um *arquivo.m*. Assim os arquivos criados pelo Matlab possuem as PSDs (A.1) das RATs na banda base e um rótulo identificando cada instância.

### A.3.2 Classificação de RAT utilizando o Weka

Após a geração dos cenários e fornecidas as características, utilizou-se os arquivos de treino e teste. O Weka utiliza os dados de treino para produzir uma rede neural artificial (um modelo) o qual será utilizado para testar o conjunto de testes.

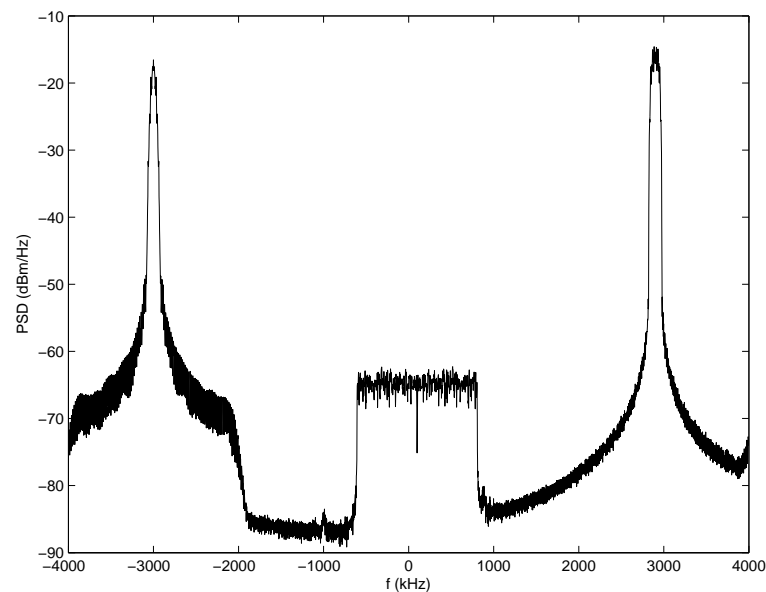


Figura A.1: PSD dos sinais GSM LTE e WCDMA somados e modulados em IF.

Os relatórios abaixo exemplificam as estatísticas dos testes feitos com o modelo criado pelo Weka:

Os resultados dos testes produzidos no Weka são apresentados nas Figuras A.2 - A.4.

Os primeiros parâmetros (Figura A.2) mostram quantas amostras de teste foram corretamente classificadas. O *kappa statistic* mede a concordância entre a predição do modelo de treino e a verdadeira classe. Um valor igual a 1, significa que a predição do modelo foi totalmente correta. Neste caso *kappa* foi igual a 0.8734.

```
Time taken to build model: 0.35 seconds

=== Evaluation on test set ===
=== Summary ===

Correctly Classified Instances      506      95.1128 %
Incorrectly Classified Instances    26       4.8872 %
Kappa statistic                    0.8734
Mean absolute error                 0.0479
Root mean squared error             0.1516
Relative absolute error             18.6168 %
Root relative squared error         42.3261 %
Total Number of Instances          532
```

Figura A.2: Resultados obtidos no conjunto de teste do modelo criado pelo classificador.

O relatório inclui também testes de precisão, onde tem-se os parâmetros TP (*true positive Rate*) mostra a proporção de exemplos corretamente classificados em uma classe x. O TP é equivalente ao parâmetro *recall* e pode ser calculado pela divisão do elemento da linha

relevante pela diagonal principal. O fator FP (*false positive Rate*) nos mostra a proporção de elementos que foram classificados como a classe x, porém pertencem a outra classe. FP pode ser calculado com a ajuda da matriz de confusão, utilizando a soma dos elementos da classe x menos o elemento da matriz x na diagonal principal, dividido pela soma das linhas das outras classes. A precisão representa a proporção de exemplos de uma classe que foram classificadas corretamente sobre todos os outros exemplos, na matriz de confusão este elemento pode ser obtido dividindo-se o elemento da classe na diagonal principal, pela soma dos elementos nesta mesma coluna. O parâmetro *F-Measure* faz uma média combinada dos fatores precisão e recall e pode ser obtido pela seguinte expressão:

$$F\text{-Measure} = 2 \left( \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \right). \quad (\text{A.1})$$

A *ROC Area* explicita a área sob a curva ROC como a estatística de Wilcoxon-Mann-Whitney, como mostrado abaixo.

```
=== Detailed Accuracy By Class ===
```

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.688	0.013	0.88	0.688	0.772	0.989	GSM
	0.933	0.04	0.747	0.933	0.83	0.993	LTE
	0.995	0.008	0.998	0.995	0.996	1	WCDMA
Weighted Avg.	0.951	0.012	0.955	0.951	0.951	0.998	

Figura A.3: Resultados de acurácia obtidos no teste do modelo criado.

A matriz de confusão é uma matriz quadrada de ordem igual ao número de classes de saída, onde o número de amostras corretamente classificadas é igual a soma dos elementos da diagonal principal e as outras amostras são elementos da classe coluna que foram classificados como coluna, como por exemplo na figura abaixo, 44 elementos da classe GSM foram corretamente classificados, 19 elementos pertencentes a classe GSM, foram classificados como LTE e 1 elemento pertencente a GSM foi classificado como WCDMA (linha 1 da matriz de confusão abaixo).

```
=== Confusion Matrix ===
```

a	b	c	<-- classified as
44	19	1	a = GSM
4	56	0	b = LTE
2	0	406	c = WCDMA

Figura A.4: Matriz de confusão de confusão obtida nos teste do modelo criado.