Departamento de Ciências e Tecnologias de Informação

Estudo de Interferências nas Comunicações Móveis

Pedro Emanuel da Conceição Semedo

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Engenharia de Telecomunicações e Informática

Orientador
Prof. Dr. Francisco António Bucho Cercas, Professor Catedrático,
ISCTE-IUL

Co-orientador
Prof. Dr. Pedro Joaquim Amaro Sebastião, Professor Auxiliar,
ISCTE-IUL

Outubro, 2019

Resumo

As técnicas de espalhamento de espectro foram inicialmente desenvolvidas para sistemas militares e têm aplicações importantes no âmbito da segurança e confidencialidade das comunicações. Estas técnicas podem ser utilizadas em ambientes civis, como o caso da terceira geração que usam o *Code Division Multiple Access* (CDMA) ou *Long Term Evolution* (LTE), contudo é nas aplicações militares que podem ter o seu potencial.

Nesta dissertação vão ser utilizadas técnicas de sistemas de espalhamento de espectro com o objectivo de bloquer intencionalmente uma comunicação móvel de qualquer operador, usando as tecnologias 2G, 3G ou 4G, assim como uma rede WiFi, dado que as frequências de operação são muito próximas. As técnicas que permitem este tipo de ação são conhecidas por *jamming* e o dispositivo que gera os sinais potencialmente bloqueadores da comunicação é denominado de *jammer*.

As frequências utilizadas nos testes são as usadas pelas operadoras residentes em Portugal e serão intencionalmente afetadas para motivos de testes académicos, intencionalmente com potências muito baixas e dentro de uma sala afastada para não causar problemas nas comunicações vizinhas.

O *jammer* foi implementado numa plataforma de *hardware* BladeRFx40, juntamente com a ajuda de rotinas da biblioteca de *software* livre GNURadio que permite criar múltiplos sistemas de rádio sem a necessidade de *hardware* e que são vulgarmente conhecidas por *Software Defined Radio* (SDR).

Foram realizados alguns testes usando técnicas de espalhamento de espectro conhecidas de *jamming* e verificados os resultados numa comunicação com um telemóvel na rede móvel nacional.

Palavras chave: Sistemas de espalhamento de espectro, *jamming*, Software Defined Radio, Comunicações móveis.

Abstract

Spectrum spreading techniques have been applied to military systems and important applications in the field of security and confidentiality of communications. Some of these techniques can be used in civilian environments, such as the 3th Generation (3G) that uses Code Division Multiple Access (CDMA) or 4G, Long Term Evolution (LTE), but it is in military applications that can have their full potential.

In this dissertation, we will use spectrum spreading techniques in order to intentionally block mobile communication from any operator using 2G, 3G or 4G technologies, such as an WiFi network, since it can operate in the same frequency range. The communications operating in the intended frequency range can be blocked and the device that generates the potentially blocker signal is called a jammer.

The frequencies used in the tests are those used by telecom operators resident in Portugal and will be intentionally affected by laboratory tests, intentionally but with very low power and within a reserved room, not to cause any interference in the neighborhood communications.

The jammer was implemented on a BladeRFx40 hardware platform, which could be programmed by modified routines of the GNURadio open source library, allowing the creation of a hardware-free radio system that is commonly known by SDR (Software Defined Radio).

Some tests were conducted using spread spectrum techniques, whose results are reported for a communication using a mobile phone in the national mobile network.

Keywords: Spread Spectrum Systems, Jamming, Software Defined Radio, Mobile Communications.

Agradecimentos

Na realização da presente dissertação, contei com o apoio de múltiplas pessoas diretamente e indiretamente, pelo qual tenho de expressar os meus sinceros agradecimentos:

Aos meus orientadores Professor Doutor Francisco António Bucho Cercas e Professor Doutor Pedro Joaquim Amaro Sebastião, pela orientação prestada, esforço, disponibilidade e apoio que demonstraram durante o desenvolvimento da dissertação.

À minha família por toda a persistência e educação que me deram durante a minha vida académica.

A todos os meus colegas que me ajudaram e atenção que me deram durante o meu período académico.

A finalizar quero agradecer ao ISCTE-IUL e ao Instituto de Telecomunicações pelo equipamento disponibilizado.

Índice

Índice de figuras

Lista de Acrónimos

A/D – Analogic/Digital

ARFCN – Absolute Radio Frequency Channel Number

AT&T – American Telephone and Telegraph

BBN – Broadband Noise

CDMA – Code Division Multiple Access

DSSS – Direct Sequence Spread Spectrum

DSP – Digital Signal Processor

EARFCN – E-UTRA Absolute Radio Frequency Channel Number

FPGA – Field Programmable Gate Arrays

FDM – Frequency Division Multiplexing

FHSS – Frequency Hopping Spread Spectrum

FSK – Frequency Shift Keying

GPP – General Purpose Processors

GSM – Global System for Mobile

HSDPA – High Speed Downlink Packet Access

IEEE – Institute of Electrical and Electronics Engineers

LTE – Long Term Evolution

OFDM – Orthogonal Frequency Division Multiplexing

QAM – Quadrature Amplitude Modulation

QPSK – Quadrature Phase Shift Keying

RF – Radio Frequency

SDR – Software Defined Radio

ST – Single Tone

UARFCN – UTRA Absolute Radio Frequency Channel Number

UMTS – Universal Mobile Telecommunications System

UTRA – UMTS Terrestrial Radio Access

WCDMA – Wideband Code Division Multiple Access

Capítulo 1

Introdução

1.1 Motivação e Enquadramento

Os sistemas de comunicação de espalhamento de espectro foram inicialmente desenvolvidos para aplicações militares, especialmente devido às suas propriedades de baixa probabilidade de interceção, resistência a interferências e baixa densidade espectral, devido à grande largura de banda utilizada, o que lhes confere graus de segurança acrescidos, especialmente quando são usados códigos de espalhamento espectral muito robustos. Este conceito foi trazido para as comunicações civis, sendo o W-CDMA da terceira geração de comunicações móveis um dos exemplos mais comuns.

Sendo estas técnicas de espalhamento de espectro utilizadas para comunicações móveis, elas poderão facilmente ser objeto de estudo, nomeadamente para determinar a quantidade de potência de sinal necessária para bloquear intencionalmente um destes sinais, como poderá acontecer no âmbito de uma operação militar ou policial em que tal seja requisitado.

De modo a compreender em que medida estas comunicações poderão ser vulneráveis, é necessário interrogarmos como são afetadas as técnicas de espalhamento de espectro face ao *jamming* (termo usado para definir interferência para eliminar ou tornar inoperacional um determinado sinal numa banda de frequências) intencional, que tipos de sinais de espalhamento de espectro terão de ser gerados para ser efetivos neste propósito.

1.2 Objetivos

Para se conseguir gerar um sinal de espalhamento de espectro recorreu-se a uma plataforma de *hardware*, conhecida por *Software Defined Radio* (SDR), que é basicamente um sistema de comunicação rádio (emissor ou mesmo emissor/receptor) que pode operar numa determinada gama de frequências e cujo funcionamento é totalmente feito via *software*. Para o *software* recorreu-se à programação de módulos GNURadio.

O objetivo desta dissertação é o estudo da segurança das comunicações móveis em ambientes militares policiais, para verificar se é possível usar o conhecimento do efeito das técnicas de espalhamento de espectro de forma localizada, para diferentes serviços da rede móvel, nomeadamente para 3G e 4G. Igualmente é pretendido afetar todo o tipo de comunicações feitas por um dispositivo móvel portanto as comunicações GSM e WiFi também serão afetadas.

1.3 Estrutura

Esta dissertação encontra-se dividida em cinco capítulos, tal como se enumera a seguir.

O capítulo 1 destina-se a fazer uma introdução sobre o enquadramento, motivação e objetivos da mesma.

No capítulo 2 abordam-se alguns conceitos e técnicas que irão ser utilizados nesta dissertação.

No capítulo 3 é apresentado o *hardware* e *software* utilizados, em particular as especificações e o funcionamento, bem como frequências utilizadas para estabelecer um ambiente de teste.

No capítulo 4 descrevem-se as experiências realizadas e os seus resultados.

No capítulo 5 são apresentadas as conclusões desta dissertação.

Capítulo 2

Estado de Arte

As técnicas de espalhamento de espectro são há muito conhecidas e tanto podem ser usadas para tornar as comunicações extremamente robustas a interferências intencionais ou não, como também podem ser usadas exatamente para bloquear uma determinada comunicação [11][12][13][7]. Será este o objeto desta dissertação, apesar de o seu uso ser limitado à ação policial ou militar, como por exemplo, a hipótese de uma comunicação hostil que poderá colocar em perigo uma comunidade ou espaço e que poderia ser um telemóvel que poderia, por hipótese, acionar um explosivo. Para tal terá que ser desenvolvido um dispositivo capaz de fazer *jamming*, ou seja, um *jammer*, o qual irá abafar completamente aquela suposta comunicação hostil e assim devolver a segurança desejada a pessoas ou bens. [1][8][15]

Para tal é necessário conhecer em maior profundidade como funcionam os *jammers* e as técnicas mais utilizadas.

2.1 *Jammer*s

Os dispositivos que permitem fazer a disrupção de sinais rádio de forma deliberada são designados por *jammers* ou bloqueadores de sinais [1]. Estes conseguem fazer ataques *Denial of Service* (DoS) impossibilitando as comunicações de um telemóvel para uma estação base ou de um comando RF para um *drone*, numa determinada área ou numa gama de frequências específica. Estes foram criados durante a segunda guerra mundial para fazer *spoofing* dos sinais rádio (cópia falsa deliberada de um sinal para enganar um recetor), só durante o tempo da Guerra Fria começaram a fazer *jamming* dos

sinais rádio[15]. Mais tarde foram adaptados para comunicações móveis com o aparecimento da tecnologia 3G.

Na figura 1 é possível analisar que um *jammer* é facilmente implementado através de 3 blocos[44]:

- Uma fonte (*Power Supply*);
- Uma secção de geração do sinal desejado numa frequência intermédia (*IF Section*);
- Uma secção de RF que modula o sinal da secção anterior para a frequência da portadora RF desejada, sendo transmitido pela antena (*RF Section with Antena*).

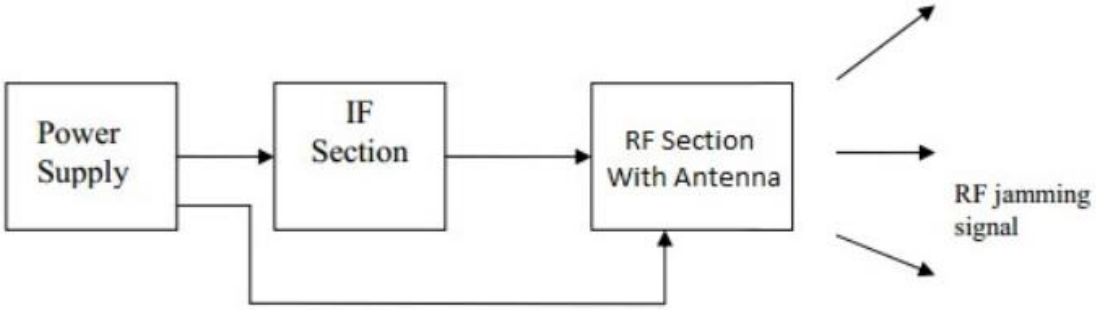

Figura 1– *Diagrama de blocos de um jammer* [Fonte: ELPROCUS].

2.2 Sistemas de espalhamento de espectro

Os sistemas de espalhamento de espectro existem desde 1942 e são utilizados para efeitos militares[38]. Com o avanço da tecnologia, as utilizações desses sistemas passaram a ter mais aplicações civis, nomeadamente comunicações pessoais e móveis, comunicações móveis por satélite entre outras, tornando-as mais seguras e mais resistentes a interceções, com a possibilidade de utilização da mesma largura de banda para múltiplos utilizadores (CDMA). Por definição, são sistemas que espalham o sinal numa largura de banda muitas vezes superior à largura mínima requerida para transmitir a informação, como exemplificado na Figura 2[12].

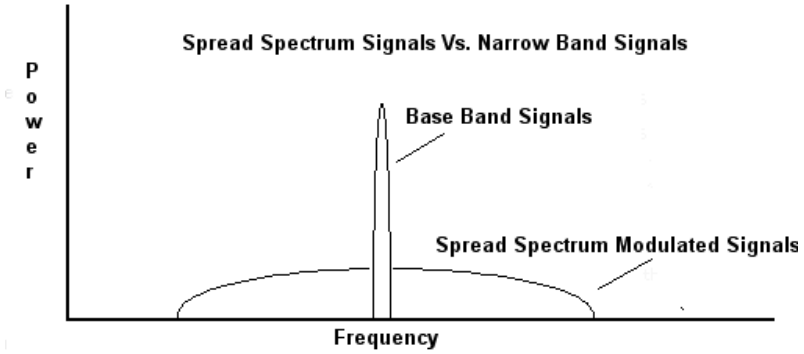

***Figura 2**– Exemplo do espalhamento de espectro*

Existem várias técnicas de espalhamento de espectro, sendo as duas mais importantes a sequência direta (*Direct Sequence*) e o salto na frequência (*Frequency Hopping*).

2.2.1 Ganho de processamento e Margem de interferência/*jamming*

Os sistemas de comunicação que utilizam técnicas de espalhamento de espectro são favorecidos na largura de banda ocupada pelo sinal modulado em comparação com o sinal de dados, embora isso também possa ser considerado uma desvantagem pelo fato de se usar muita largura de banda, apesar de se ter uma densidade espectral de potência muito baixa, tipicamente inferior à densidade espectral do ruído. Mas é precisamente o aumento da largura de banda que influencia o sinal em termos da resistência a interferências, e existe um ganho associado que é designado por ganho de processamento (G_p) e que pode ser definido pela razão entre largura de banda do sinal modulado (B_{RF}) e a largura de banda mínima para transmitir o sinal de dados (B_{Data}) [36].

$$G_p = 10 \log_{10} \frac{B_{RF}}{B_{Data}} \text{[dB]} \quad (1)$$

Também se pode definir a margem de *jamming* (M_j), que representa a capacidade do sistema resistir a interferências externas, e que é inferior ao ganho de processamento,

sendo calculado através da relação sinal-ruido à saída do sistema ($(S/N)_{out}$), perdas do sistema (L_{sys}) e ganho de processamento (G_p), pela seguinte expressão[36]:

$$M_j = G_p - \left[L_{sys} + \left(\frac{S}{N}\right)_{out}\right] \text{ [dB]} \qquad (2)$$

2.2.2 Técnicas de Espalhamento de Espectro

2.2.2.1 Sequência Direta (*Direct Sequence*)

Os sistemas de espalhamento de espectro baseado em sequência direta são os mais utilizados devido à sua simplicidade, e até do ponto de vista de implementação usando uma placa SDR é mais simples pois não exige muito processamento para produzir o sinal. Para obter um sinal num DSSS basta modular um sinal RF, já modulado de acordo com as técnicas convencionais, idealmente por *binary phase-shift keying* (BPSK) ou *differencial* PSK (DPSK), por uma simples sequência de um código pseudoaleatório de espalhamento, como se mostra na Figura 3[36]. Assumindo que o emissor e o recetor usam a mesma sequência de código é possível inverter o processo no recetor e recuperar o sinal original. Se um determinado sinal não usar o mesmo código de espalhamento, ele será simplesmente espalhado no recetor e completamente ignorado pois a sua densidade espectral será muito baixa à saída do filtro passa-banda. A banda do sistema estabelece um filtro de pós-correlação com a potência dos sinais rejeitados garantindo assim o ganho de processamento.

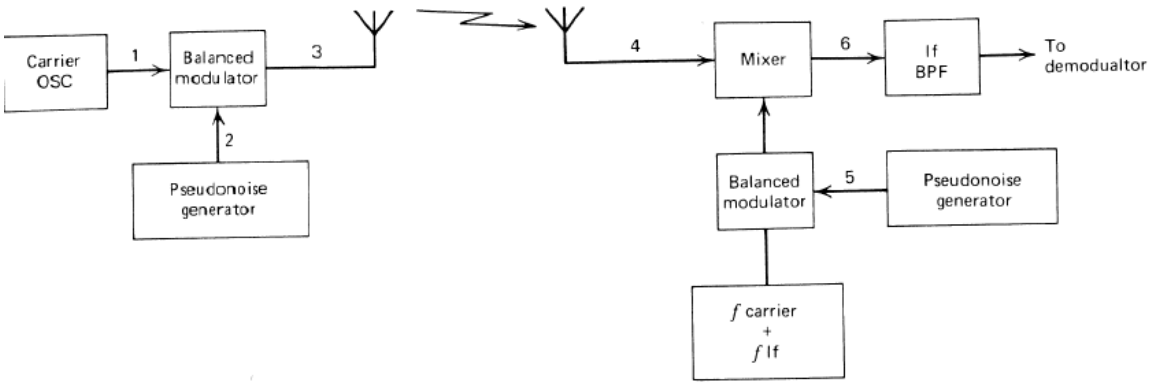

Figura 3– *Emissor e recetor de um DSSS[Spread Spectrum Systems]*

2.2.2.2 Salto na frequência (*Frequency Hopping*)

Os sistemas baseados no salto na frequência utilizam mais frequentemente a modulação FSK, o que lhes confere ainda mais espalhamento da banda [36]. Nesta técnica o sinal é emitido num grande número de frequências possíveis, de acordo com o código pseudoaleatório de espalhamento escolhido. Enquanto uma modulação FSK binária utiliza duas frequências, os FHSS poderão usar até 2^{10} frequências discretas de forma aleatória, com base no código usado. Os FHSS podem ser classificados em sistemas de salto de frequência com salto rápido ou com salto lento, de acordo com a velocidade com que comutam de frequência, isto é, de acordo com a velocidade de salto de frequência. [35] Os sistemas de espalhamento de espectro por salto de frequência a mais de 10 Hz já se consideram rápidos. O ganho de processamento nestes sistemas é simplesmente dado pelo número de canais ou frequências possíveis para emitir o sinal, uma vez que num sistema convencional bastaria uma.

2.3 Técnicas de interferência do sinal

Aqui vamos analisar as estratégias que permitem interferir com os sinais através de um *jammer[32]*. O objetivo do *jammer* é bloquear as comunicações e para o fazer precisa de obedecer à relação *Jammer to Signal* no qual o resultado é dado em dB (5) , pode ser definido pela proporção da potência do sinal interferente (P_J) com a potência do sinal da comunicação alvo (P_S) num determinado ponto como por exemplo uma antena de um terminal recetor (3). As fórmulas seguidamente apresentadas (3), (4) e (5) foram retiradas do livro *Electronic Warfare and Radar Systems Engineering* [45]:

$$\frac{J}{S} = \frac{P_j}{P_s} \tag{3}$$

Através da utilização da fórmula de Friis para o espaço livre temos:

$$p_{rec} = \frac{EIRP}{4\pi d^2} A_e = \frac{p_t g_t g_r \lambda^2}{(4\pi d)^2} \quad (4)$$

Onde *Equivalent Isotropically Radiated Power* (EIRP) é a potência necessária para transmitir um sinal de forma omnidirecional e λ é o comprimento de onda, ao substituirmos na equação (3) obtemos:

$$\frac{J}{S} = \frac{\frac{p_J g_{tJ} g_{rJ} \lambda_J^2}{(4\pi d_J)^2}}{\frac{p_S g_{tS} g_{rS} \lambda_S^2}{(4\pi d_S)^2}} = \left(\frac{EIRP_J}{EIRP_S}\right)^2 \frac{d_S^2}{d_J^2} \quad (5)$$

Onde p_J representa a potência do $jammer$, g_{tJ} é o ganho de transmissão da antena do *jammer*, g_{rJ} é o ganho de receção da antena do *jammer*, d_J é a distância a que o *jammer* encontra-se da antena do dispositivo alvo, d_S é a distância que o dispositivo encontra-se de uma estação base, p_S é a potência do dispositivo a comunicar, g_{tS} é o ganho de transmissão da antena do dispositivo, g_{rS} é o ganho de receção da antena do dispositivo.

Que depois traduzido para dB fica:

$$\left(\frac{J}{S}\right)_{dB} = EIRP_J - EIRP_S + 20\log d_S - 20\log d_J \quad (6)$$

É a margem de *jamming* que é o valor máximo da potência interferente (em média) relativo ao valor médio da potência da portadora de forma a que consiga cumprir um determinado desempenho. $\frac{R_p}{R_b}$ é o ganho de processamento G_p e é definido pela razão entre o ritmo de *chip* R_p e o ritmo binário R_b. J é a potência média do sinal interferente, C é a potência média da portadora, E_b é a energia de bit e J_0 é a densidade espectral de potência efetiva da interferência. As fórmulas (7) e (8) foram retiradas do Módulo 5 – *Spread Spectrum Techniques for satellites*, da unidade curricular Sistemas de Comunicações Digitais por Satélite [31]

$$j_M = \frac{J}{C} = \frac{\frac{R_p}{R_b}}{\frac{E_b}{J_0}} \quad (7)$$

Em dB fica:

$$J_M = G_p - \frac{E_b}{J_0}\,[\text{dB}] \tag{8}$$

Existem múltiplos métodos para afetar um sinal, cada um tem as suas vantagens e desvantagens. Irei aprofundar o tema com algumas técnicas de *jamming*.

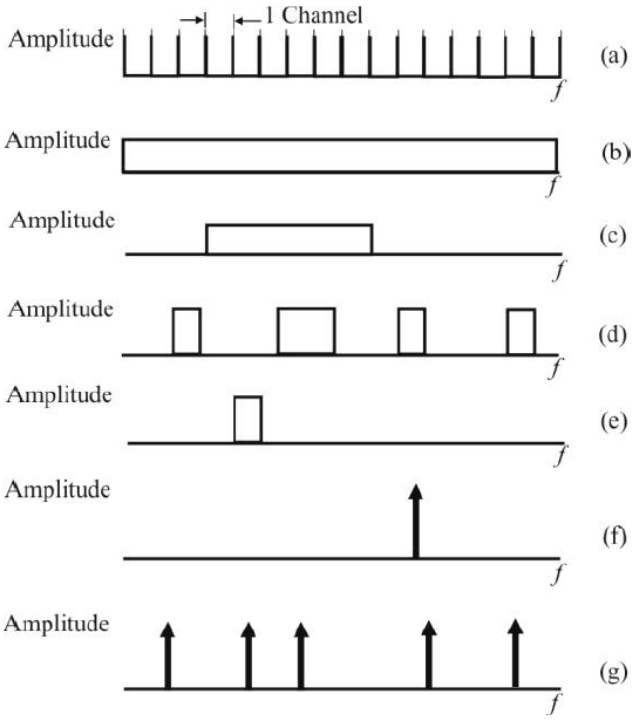

***Figura 4**– Exemplos de estratégias de jamming a) dedicadas a um canal(spot jamming), b) full-band jamming(BBN), c) partial-band jamming contagiosa(PBN), d) partial-band jamming não contagiosa, e) jamming de ruido de banda estreita (NBN), f) jamming de um tom(ST)* (Fonte: Modern Communications Jamming Principals and Techniques)

2.3.1 Broadband Noise jamming

*Broadband noise jamm*ing também conhecido por *barrage jamming* é um sinal que afeta toda a banda de frequências ideal para bloquear qualquer tipo de comunicação do recetor independente da sua localização prejudicando a energia do ruído derivado ao número de portadoras. (Figura 4-b)).[1]

2.3.2 Partial-band Jamming

Esta técnica tem as mesmas propriedades que o com simples diferenças, a energia é dividida por múltiplos canais não afetando toda a largura de banda e os canais podem ser todos seguidos ou separados em frequências separadas, como se pode ver na figura 4-c) e na figura 4-d).[1]

2.3.3 Narrowband Noise Jamming

A energia do ruído afeta unicamente a largura de banda de um canal ou apenas a largura do sinal de dados, indicado na figura 4-e).[1]

2.3.4 Tone jamming

Esta estratégia tem duas versões *single tone (ST)* e *multiple tone (MT)*, geralmente serve para aumentar o desempenho do *jammer*. A versão *single tone*, também conhecida por *spot jamming*, afeta uma única frequência, tendo melhor desempenho para sistemas DSSS, superando o ganho de processamento deteriorando o espectro, visto na figura 4-f).

A versão *multiple tone* pode emitir aleatoriamente ou pode emitir para um número específico de frequências. Mas se os tons forem em canais consecutivos é designado por *comb jamming*. Este tipo de estratégia é ideal se soubermos exatamente as frequências pois passa pelos filtros dos recetores sem distorção ou atenuação (Figura 4-g)).[1]

2.4 Dispositivo alvo de comunicação móvel

Atualmente o ser humano utiliza múltiplos meios para comunicar entre si, no qual o mais utilizado é o telemóvel. Este foi inventado nos anos 40 por engenheiros da AT&T, sendo estes rádios bidirecionais produzidos em massa em 1973 pela Motorola.[21][46] Na figura 5 podemos visualizar os principais blocos de um telemóvel. Este é composto por 5 blocos principais:

- Baseband;
- Back-End;
- IF Block;
- RF Front-End;
- Antenna and Propagation.

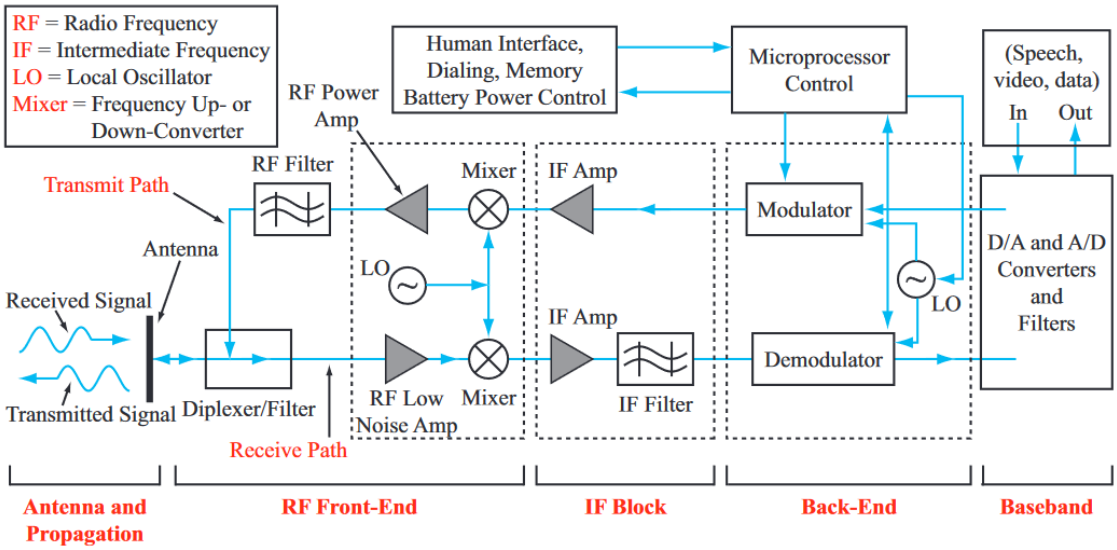

Figura 5- Diagrama de blocos do telemóvel [Fonte: *Cell-Phone Circuit Architecture - Oregon State University*]

Todos os sinais do telemóvel quando fazemos uma chamada ou vemos e ouvimos ficheiros multimédia para serem transmitidos e recebidos passam por alguns passos para chegarem a outro dispositivo móvel. No caso de sinais analógicos, como a voz, têm de ser convertidos para digital e vice-versa dependendo do estado do telemóvel se está a transmitir ou a receber. Os dados depois são modulados, neste caso em OFDM que é

usada desde a 4G, pois tem uma melhor eficiência espectral face às outras modulações. A portadora do sinal é amplificada e deslocada para uma frequência intermédia, e finalmente é colocada na frequência de emissão rádio para poder ser depois transmitida.

Quando um sinal é transmitido são-lhe atribuídos alguns canais dentro uma banda de frequências predefinidas pelas operadoras de cada país[47]. Como o país em causa é Portugal a figura 6 indica quais as bandas de frequência utilizadas, os canais referentes a cada operadora e o processo de transmissão no espectro de *downlink* e *uplink*.

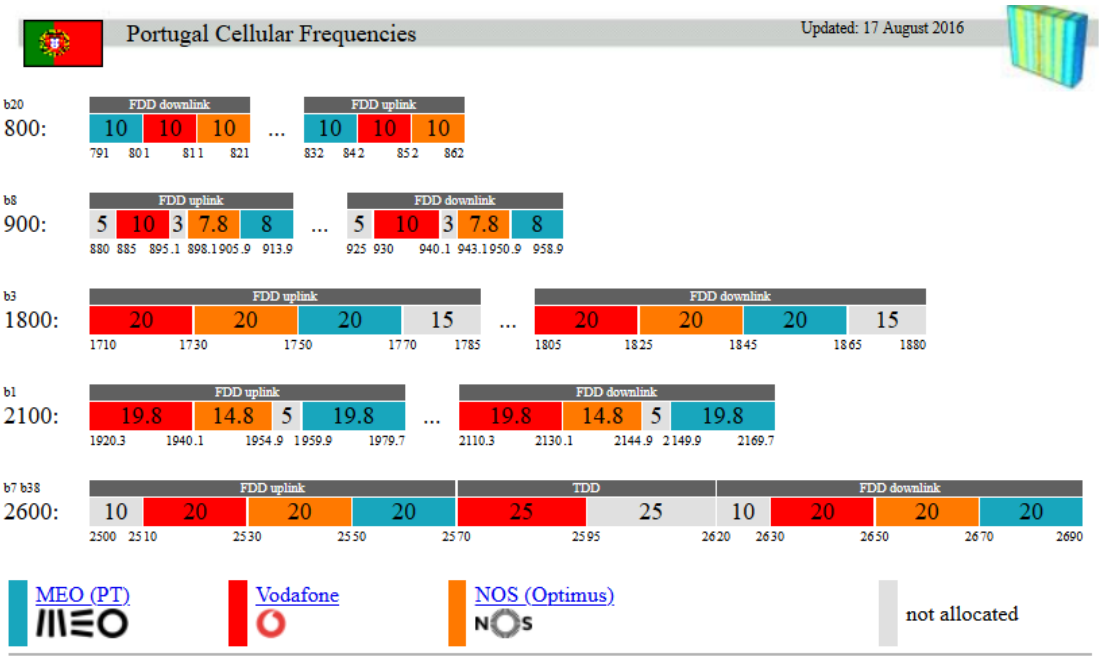

Figura 6 - Bandas de frequência presentes em Portugal [Fontes ANACOM e Frequency Check]

As bandas de frequências que Portugal usa são b20, b8, b3, b1, b7 e b38 e cada uma tem múltiplos canais. No caso da tecnologia 2G cada frequência é calculada através do ARFCN de *downlink* e encontram-se descritas na tabela 1 dos anexos[22]. Para as redes de terceira geração 3G ou UMTS, são usadas as equações (6) e (7) e para a quarta geração 4G ou LTE, as equações (8) e (9), sendo os *Absolute Radio Frequency Channel Number* (ARFCN) calculados respetivamente pelas seguintes fórmulas[24][25][26][27][28][29]:

$$DL_{Freq} = F_{DL_{Offset}} + 0.2 \times (DL_{UARFCN}) \quad (6)$$

$$UL_{Freq} = F_{UL_{Offset}} + 0.2 \times (UL_{UARFCN}) \quad (7)$$

$$F_{DL} = F_{DL_{LOW}} + 0.1 \times (N_{DL} - N_{DL\_Offset}) \quad (8)$$

$$F_{UL} = F_{UL_{LOW}} + 0.1 \times (N_{UL} - N_{UL\_Offset}) \quad (9)$$

Para obter os ARFCN de cada rede, os telemóveis precisam de aceder ao Modo de Serviço. Este indica a rede à qual o dispositivo encontra-se ligado, a banda e largura de banda, o ID da célula que está a prestar o serviço, o ARFCN e ritmos binários de *downlink* e *uplink*, entre outras informações.

Para aceder ao *Service Mode*, no caso do sistema Android é *#0011# e para o caso do iPhone é *3001#12345#*[23].

Figura 7 - Exemplos dos ARFCN e Frequências de Donwlink e Uplink

2.5 *Software* Defined Radio

O termo "*Software Defined Radio*" foi criado por Joseph Mitola III em 1911. Existem várias definições para SDR mas para simplificar o termo o Institute of Electrical and Electronics Engineers (IEEE) definiu SDR como *"Radio in which some or all of the physical layer fuctions are software defined"*, ou seja como sendo um conjunto de sub-sistemas rádio onde a maior parte das suas funções são definidas através de *software* podendo ser usados *Field Programmable Gate Arrays* (FPGAs), *digital signal processors* (DSP), *general purpose processors* (GPP), entre outras tecnologias que permitam a

implementação destas funcionalidades[3][4]. Desta forma existe uma enorme flexibilidade que permite que um mesmo dispositivo possa operar em diferentes modos e bandas do espectro em que opera, em custos adicionais.

No presente caso, foram adotadas os seguintes módulos disponíveis em http://wiki.gnuradio.org/index.php/List_of_Blocks , das fontes Signal Source e Noise Source, dos gráficos QT GUI Frequency Sink, QT GUI Tab Widget e dos controladores QT GUI Range, os módulos osmocom Source e osmocom Sink são externos e tiveram de ser instalados.

Capítulo 3

Estudo das Interferências

Para implementar as estratégias de *jamming* foi necessário recorrer a *hardware* e *software* que proporcionasse facilmente a manipulação do sinal transmitido bem como a sua potência de modo a atingir o objetivo de conseguir suprimir as comunicações do dispositivo móvel alvo.

3.1 *Hardware*

3.1.1 Blade RF

Nesta dissertação foi utilizada uma BladeRF x40 da Nuand como plataforma de SDR. Esta foi desenhada para universitários e entusiastas que exploram as comunicações RF pode funcionar através do *software open source* GNURadio, Photos via SoapySDR, entre outros *softwares* de SDR, igualmente também funciona com o Mathworks MATLAB.

A BladeRF possui circuitos separados para receber e transmitir sinais RF e pode fazê-lo em modo bidirecional e em simultâneo. A conversão A/D e D/A é feita através do chip LMS6002D que é um emissor/recetor capaz de manipular qualquer sinal desde áudio FM até 4G LTE.

A gama de frequências que esta placa permite estende-se dos 300MHz até aos 3.8GHz e com largura de banda de 1.5MHz até 28MHz. Como supracitado a placa realça o fator de ser utilizada para comunicações RF com múltiplas aplicações desde o desenvolvimento de ondas rádio a simulação e receção de ADSB (*Automatic dependent surveillance broadcast*) o qual determina a posição de uma aeronave via satélite.

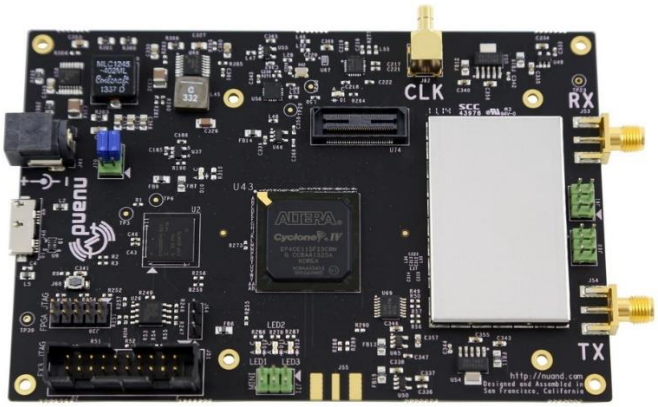

Figura 8 *- BladeRF x40*

3.1.2 Telemóvel

O dispositivo móvel utilizado como alvo para conduzir as experiências mais abaixo descritas é um Samsung Galaxy S6 Edge+, contém o sistema Android *Nougat* 7.0 e consegue funcionar nas seguintes tecnologias: GSM, *High Speed Packet Access* (HSPA) / WCDMA e LTE.

Dentro deste conhecimento o telemóvel consegue ter acesso às seguintes bandas:

2G GSM	3G UMTS	4G LTE
GSM 850	HSDPA 850	Banda 1 (2100)
GSM 900	HSDPA 900	Banda 2 (1900)
GSM 1800	HSDPA 1900	Banda 3 (1800)
GSM 1900	HSDPA 2100	Banda 4 (1700/2100)
		Banda 5 (850)
		Banda 7(2600)
		Banda 8 (800)
		Banda 12 (700)

Banda 17 (700)
Banda 18 (800)
Banda 19 (800)
Banda 20 (800)
Banda 26 (850)

3.1.3 Antenas

Nesta dissertação foram usados dois tipos de antenas: uma omnidirecional e uma yagi-uda.

A antena omnidirecional é uma antena bastante versátil derivado ao seu diagrama de onda permitindo transmitir e receber em qualquer direção cobrindo uma área circular, tem um ganho de 0 dB. Esta antena irá ser ligada à porta Rx da bladeRF servindo assim de recetor para as experiências do capítulo 4.

A antena yagi-uda é uma antena mais diretiva e consequentemente com um melhor ganho face à antena omnidirecional. Esta antena será ligada à porta Tx da bladeRF com a finalidade de ser o *jammer* a emitir o sinal intercorrente.

3.2 *Software*

3.1.2 GNURadio

O GNURadio é uma ferramenta *open source* que permite o processamento de blocos de rádio através de *software*, licenciado pela GNU *General Public License* (GLP). As aplicações são escritas em Python e o processamento dos sinais é feito através da linguagem de programação C++. Pode ser utilizado imediatamente com *hardware* RF para criar *software defined radios*, ou sem *hardware* num ambiente de simulação.

Consegue suportar comunicações sem fios e sistemas de rádio utilizados em todo o mundo (Figura 9).

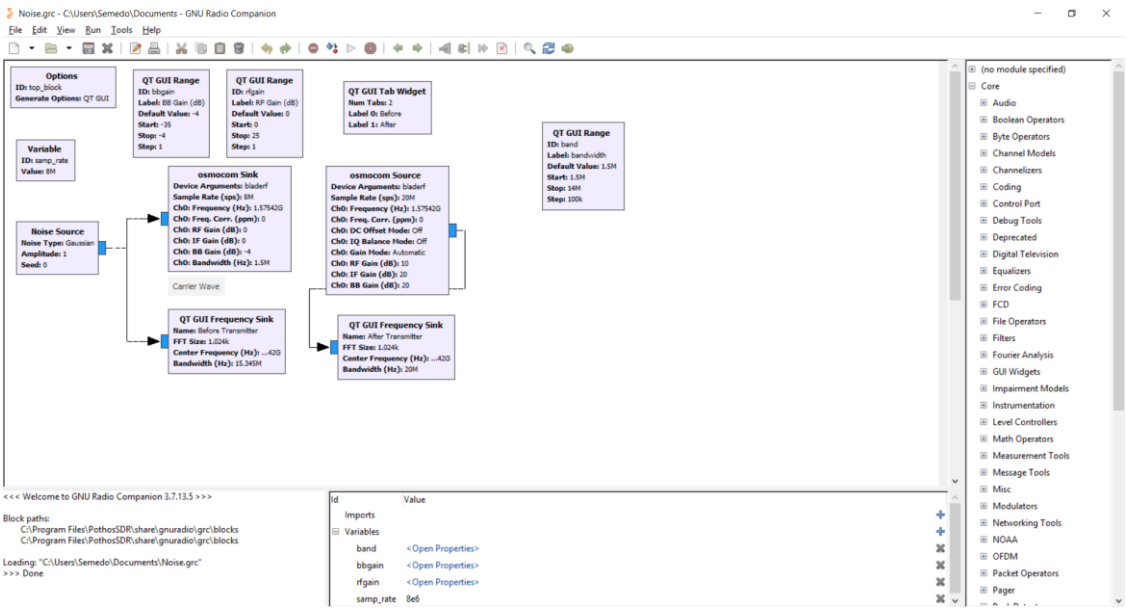

***Figura 9** - Ambiente de trabalho do GNURadio*

Os blocos escolhidos para realizar a parte experimental desta dissertação foram os seguintes:

- Noise source;
- Signal Source;
- QT GUI Range;
- osmocom Sink;
- osmocom Source;
- QT GUI Tab Widget;
- QT GUI Frequency Sink.

Cada componente é importante para gerar os sinais pretendidos, as duas GUI Range permitem aumentar o ganho do *jammer* e o ganho da banda base e mostrar a largura de banda do sinal; o ruído branco gaussiano é gerado através do bloco Noise source, o bloco Signal Source gera uma onda sinusoidal com a função de ser a fonte de ruido utilizada na segunda experiência. A QT GUI Frequency Sink concede a visualização do sinal antes e depois de ser aplicado às interferências intencionais, os blocos osmocom Sink e osmocom Source fazem a ligação à bladeRFx40 sendo a Source o recetor e o Sink o emissor. Por último o bloco QT GUI Tab Widget estabelece a janela usada com dois separadores um

para ver o sinal antes da aplicação das interferências e outro para a observação após as interferências feitas pelo *jammer*.

3.3 Frequências Utilizadas

Como mencionado na secção 2.4 existem várias bandas de frequências para Portugal, as quais dependem da capacidade da estação base para poderem transmitir e receber nessas mesmas bandas, da operadora (MEO, NOS e Vodafone).

Neste caso o telemóvel é da operadora MEO restringindo a gama de frequências a ser utilizada para poder efetuar os cálculos para o *downlink* de modo a sabermos qual a frequência a ser afetada pelo sinal de *jamming* a gerar. A ativação do modo "SERVICEMODE" no terminal permitiu obter os dados que se representam nas figuras 10 a 12.

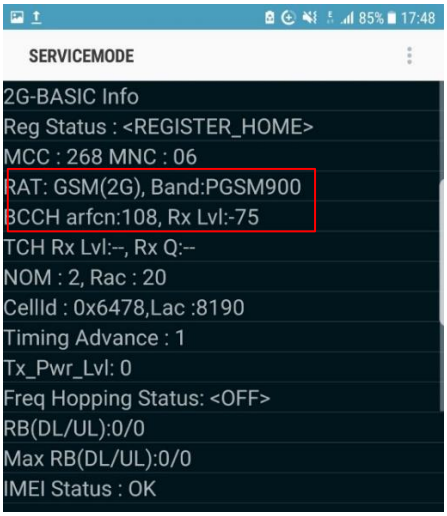

Figura 10 - ARFCN do GSM

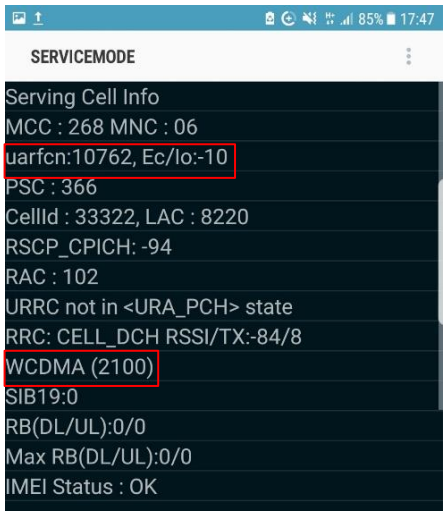

Figura 11 - ARFCN do UMTS

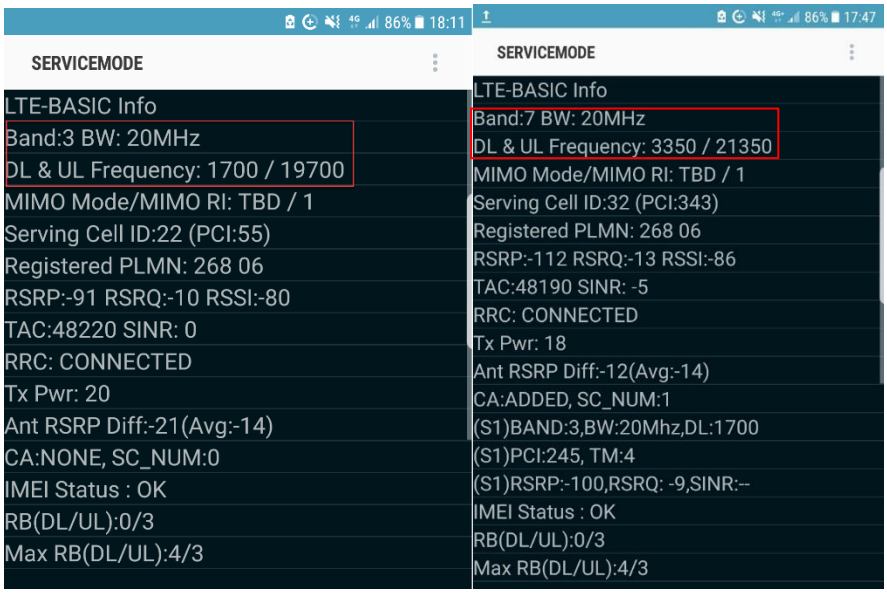

Figura 12 - ARFCN do LTE

Neste caso o telemóvel é da operadora MEO. Podemos assim restringir a gama de frequências de acordo com a figura 6, a qual será utilizada para poder efetuar os cálculos para o *downlink* de modo a sabermos qual a frequência a ser afetada. Durante o processo de captura dos ARFCN do LTE, o telemóvel alternava entre a banda 3 e a banda 7 (Figura 12). Isto acontece devido à distância que o telemóvel se encontra em relação à estação base com melhor qualidade de sinal, o qual apresenta flutuações ao longo do tempo.

Para os casos supracitados, pudemos deduzir os ARFCN de cada rede para o cálculo das frequências, de acordo com as fórmulas descritas no capítulo anterior e com o auxílio das tabelas em anexo:

2G GSM		3G UMTS		4G LTE	
Uplink [MHz]	Downlink [MHz]	Uplink [MHz]	Downlink [MHz]	Uplink (banda 3 e banda 7) [MHz]	Downlink (banda 3 e banda 7) [MHz]
911.6	956.6	1962.4	2153	1760/2560	1855/2680

Tabela 1 - Frequências dos ARFCN

Para além das bandas 2G, 3G e 4G, os telemóveis conseguem aceder à rede WiFi para fazer *Voice over IP*(VoIP) e para fazer outros tipos de aplicações. Isto implica que é necessário conhecer com ela é distribuída.

Na rede WiFi, os routers têm 14 canais separados por 5MHz cada um [Anexos: Tabela 4] na qual podem acomodar os utilizadores. Por omissão os routers transmitem no canal 6, mas podem deslocar a sua operação para os canais 1 e 11 de modo a que não existam problemas de sobreposição de canais, devido a interferências, o que iria resultar na redução do *throughput* do sistema. Os routers podem ser configurados para emitirem nos outros pares de canais e que são: 2,7,12 ou 3,8,13 ou 4,9,14 ou 5,10,14. O canal 14 é um caso particular pois só é compatível com routers que funcionam na norma 802.11b e a FCC baniu o acesso ao mesmo canal, uma vez que a frequência central deste canal, que é 2.48GHz, é também conhecida por Industrial Scientific and Medical (ISM) podendo ser acedida mundialmente. Crê-se que também possa ser utilizada para uso militar e para comunicações com satélites. Para localizar e visualizar as alterações do router foi necessário aceder a uma aplicação externa chamada de WiFi *Analyzer*, que indica as redes disponíveis, os protocolos que utilizam e a potência do sinal em dBm(Figura 13).

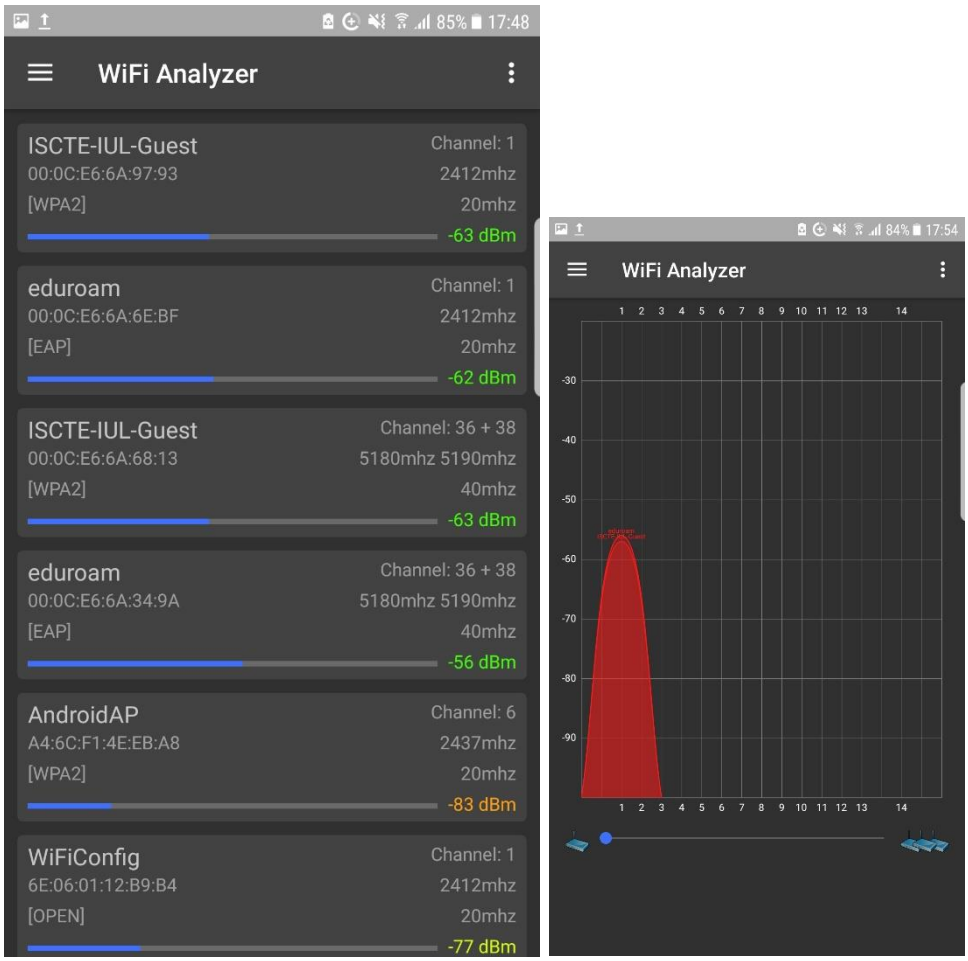

Figura 13 - WiFi Anayzer do ISCTE

As frequências anteriormente calculadas irão ser utilizadas nas experiências do capítulo 4, permitindo examinar melhor a resistência do espalhamento do espectro perante a criação de ruido intencional, e para tal foram usadas duas estratégias de *jamming* anteriormente descritas, nomeadamente BBN e ST.

Capítulo 4

Resultados e Discussão

As experiências realizadas nesta secção dispõem de uma breve descrição que relata a experiência em causa e os seus resultados após a exibição das figuras 19 e 20. Ambas as experiências executadas foram para as redes de dados 2G, 3G e 4G.

A técnica de *jamming* utilizada para a experiência 1 é o *Broadband Noise Jamming* (BBN) e para experiência 2 a técnica usada é o *Single Tone Jamming* (ST).

Experiência 1:

A primeira estratégia a ser aplicada é bloquear toda a banda de frequências usada na comunicação (idealmente seria desde a frequência 791MHz até à frequência 2.690GHz pois para casos reais não sabemos quais as frequências presentes nos telemóveis de cada operadora existente, com tal não pode ser possível devido aos limites da largura de banda da BladeRF, daí que se optou por ter abordagem mais direta ao centrar nas frequências presentes na tabela 1 do capítulo anterior), ou seja, aplicar um *broadband jammer* a um sistema de telecomunicações. Inicialmente é necessário definir o GNURadio (Figura 14) para transmitir o sinal de ruído através do bloco *osmocom Sink* e *osmocom Source* para receber o sinal para depois ser processado e visto pela QT GUI *Frequency Sink* para garantir a visualização do sinal na frequência correta existe um campo na configuração do QT GUI Frequency Sink (Figura 16), igualmente este bloco permite fazer a transladação do sinal para a frequência indicada na figura 16. As definições do *osmocom Sink* e *osmocom Source* tem a mesma janela de configuração e encontram-se presentes na Figura 15. Na janela de configuração altera-se unicamente o valor do campo *Ch0: Frequency (Hz)* para a frequência que se quer transmitir e receber, descritos na tabela 1 do capítulo 3.

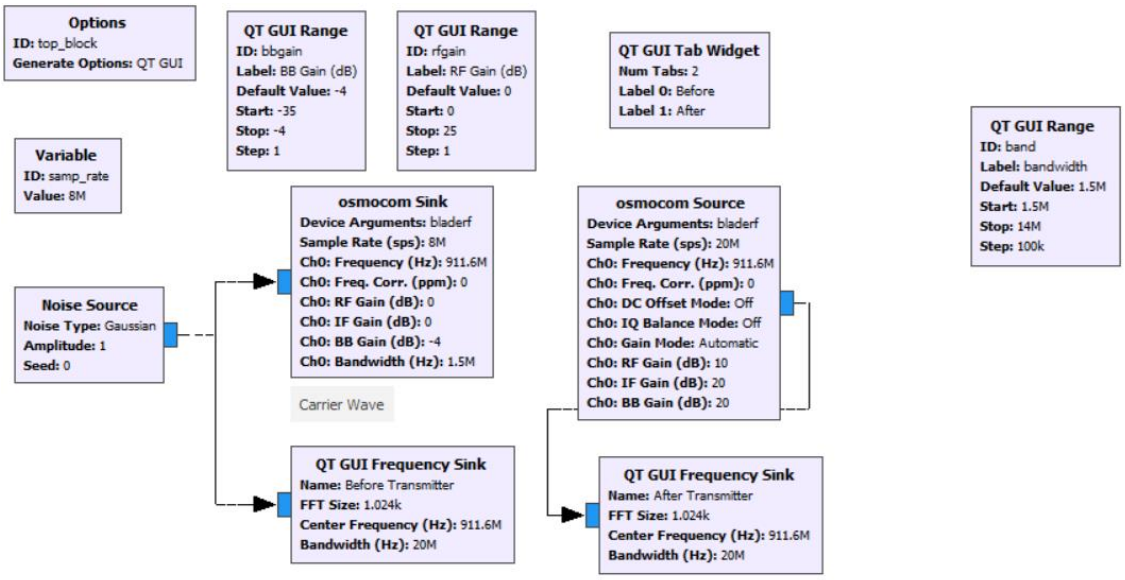

***Figura 14** - Experiência 1 BroadBand Jammer para GSM*

Na figura 14, observa-se os blocos utilizados e suas as ligações no GNURadio para o teste do GSM na frequência 911.6 MHz.

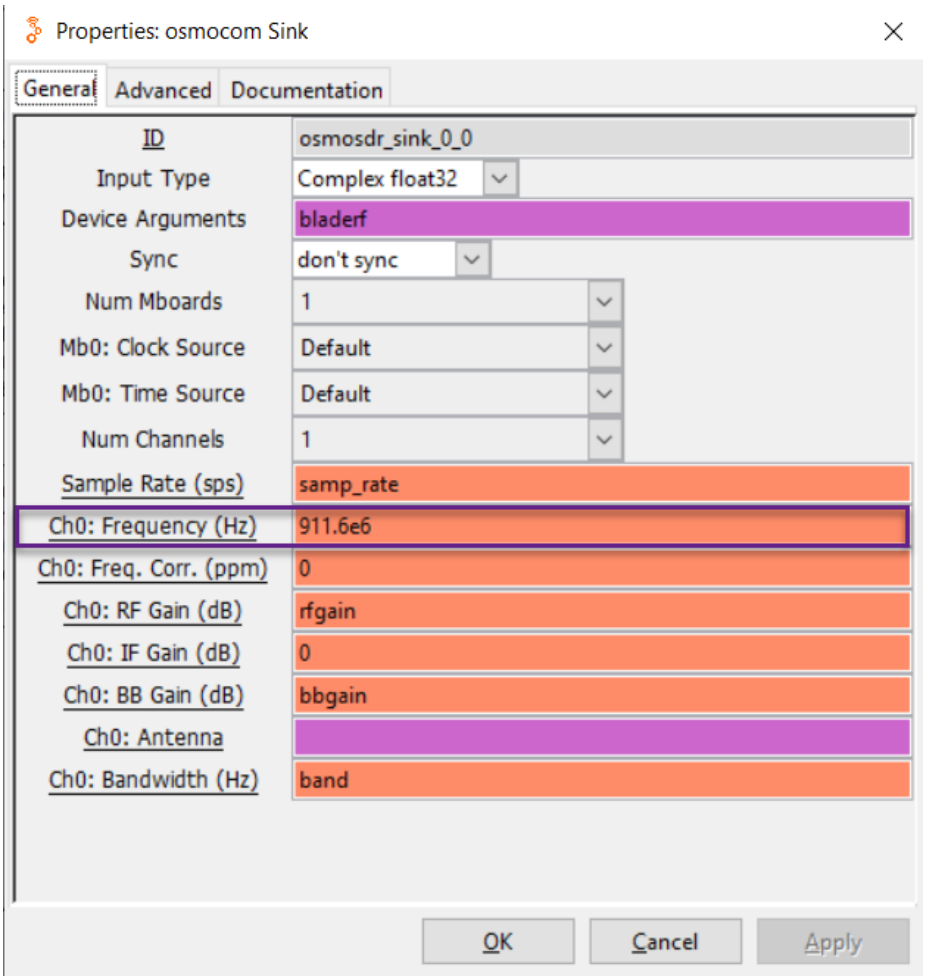

***Figura 15** - Definições do osmocom Sink*

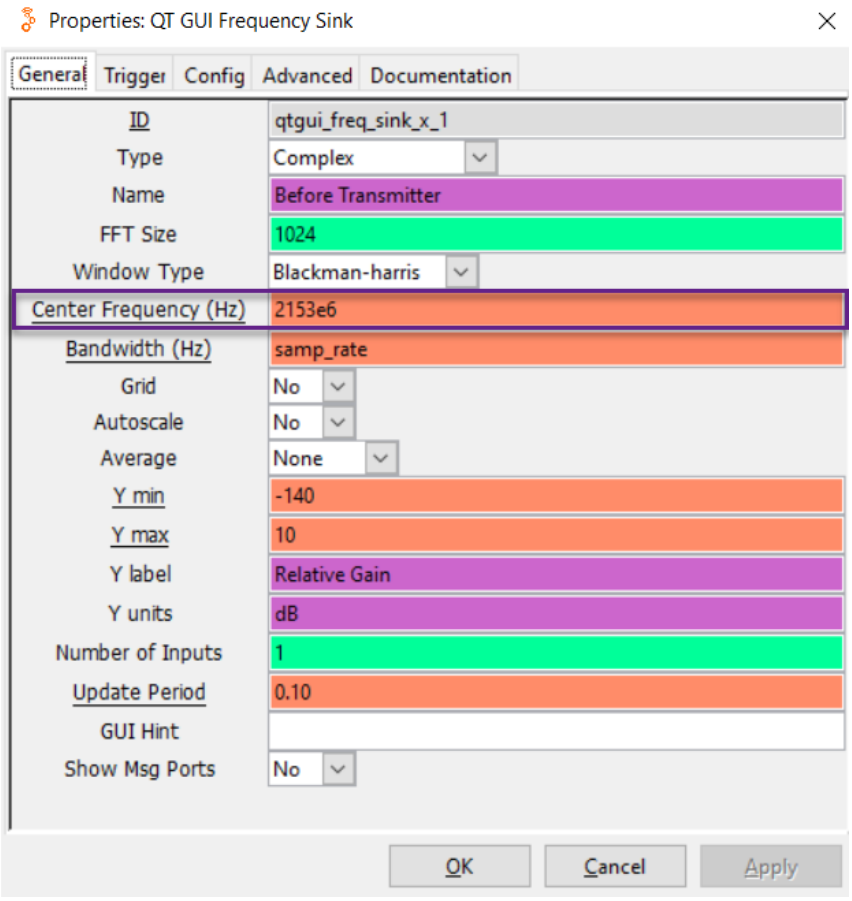

Figura 16 -Propriedades do QT GUI Frenquency Sink

Experiência 2:

O segundo ensaio foi executar um *single tone jammer* para todas as gamas de frequências que a operadora MEO fornece, para tal o GNURadio foi redefinido para aplicar uma onda sinusoidal como fonte do ruído em vez da *Noise source* (Figura 17).

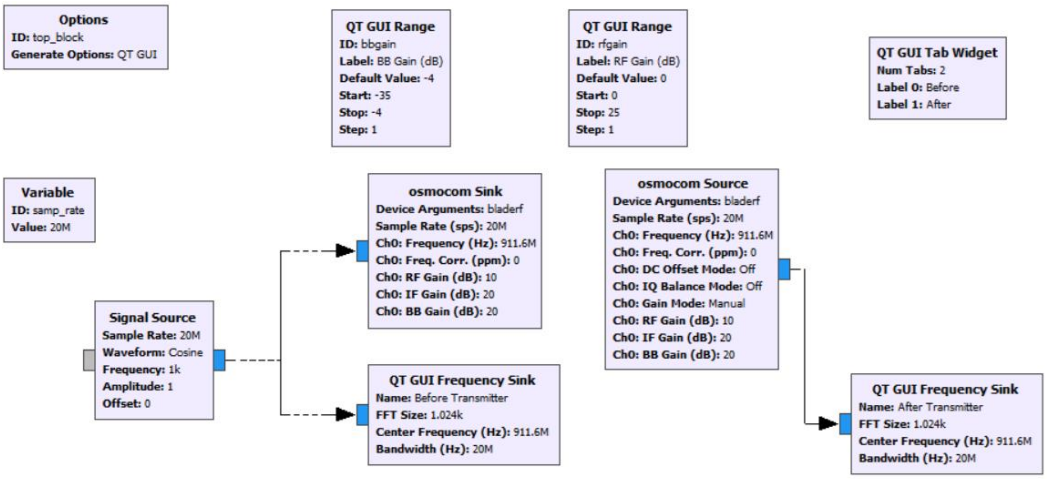

Figura 17 *– Experiência 2 Tone Jamming GSM*

Resultados da experiência 1:

Ao observarmos a experiência 1, antes de ser aplicado o *jammer* o espectro encontra-se com algumas interferências na ordem dos -40 dB podendo executar todo o tipo de comunicações (Figura 18).

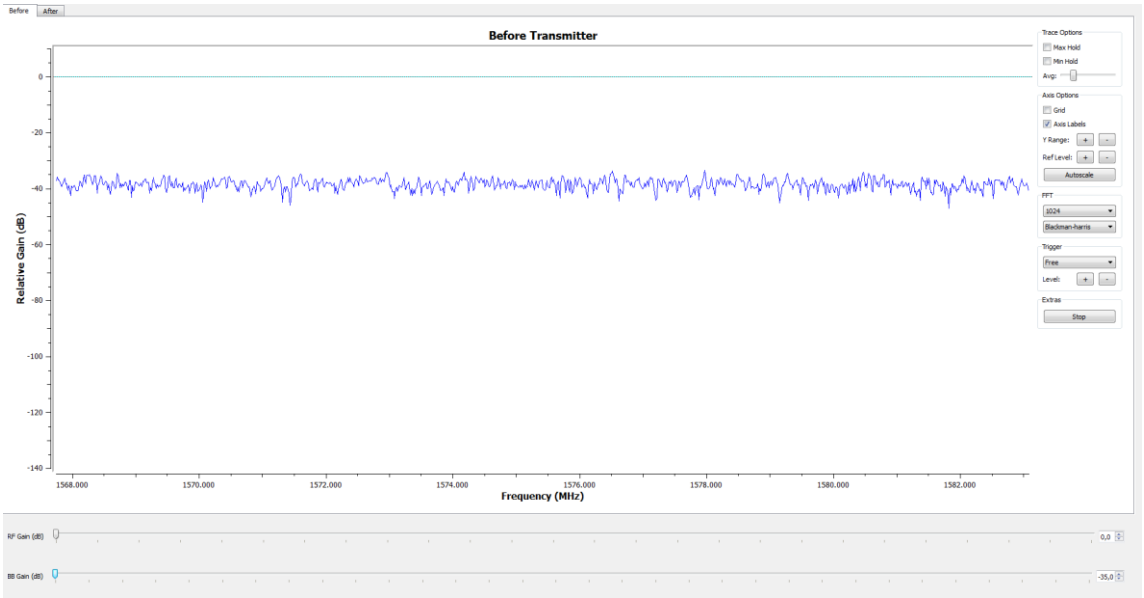

Figura 18 *- Espectro antes da aplicação do jammer*

Mas quando aplicamos o *jammer*, o espectro produzido revela uma ligeira aproximação para os 0 dB (Figura 20), embora exista a prevalência da portadora. É de notar que existe um pico na frequência central, isso é denominado de DC Offset. Este pode ser causado no conversor analógico-digital através de um erro de deslocamento do Least Significant Bit (LSB), ou à saída dos filtros passa-baixo pois deixam propagar qualquer polarização DC, ou no *mixer*, nomeadamente no oscilador local (LO) que se encontra no centro da frequência desejada passando assim o *DC Offset* para o recetor. Este acontecimento é frequente em todas as gamas de frequências testadas.

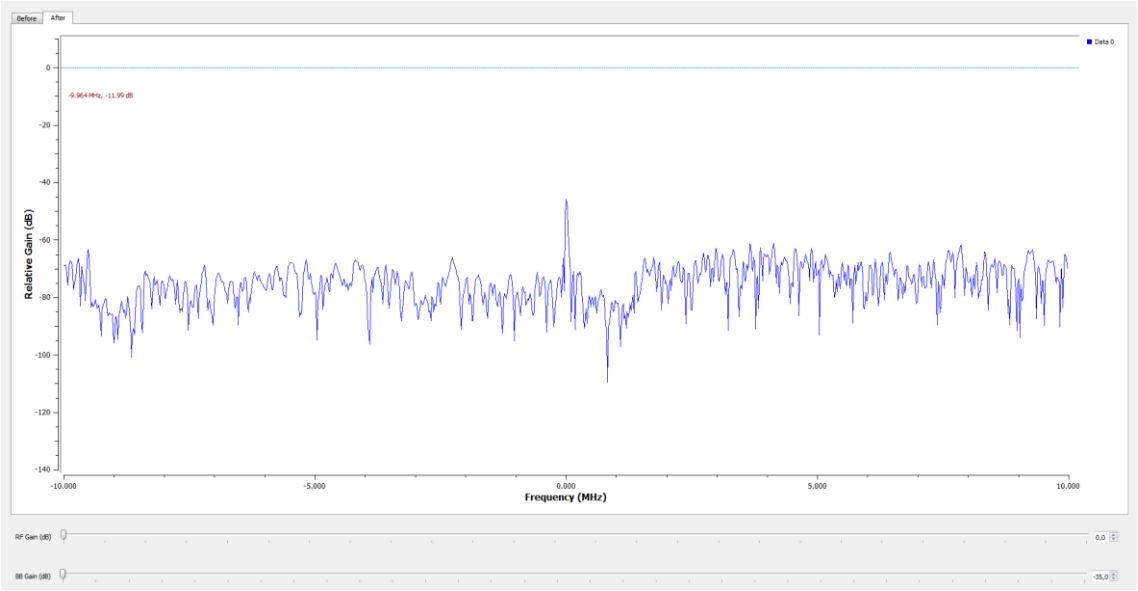

Figura 19 - Espectro após a aplicação do jammer BBN sem aplicação dos ganho de processamento

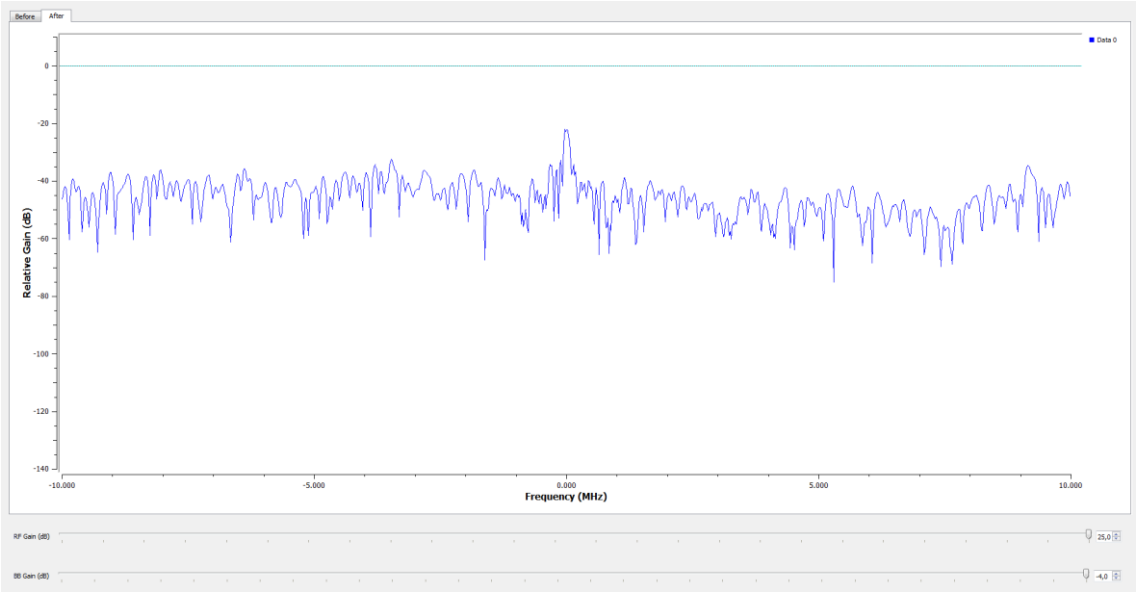

***Figura 20** - Espectro após a aplicação do jamme BBN com aplicação dos ganhos de processamento*

Na figura 20 podemos afirmar que a nível de comunicações ainda foi possível fazer chamadas, mas na utilização de dados através da rede 2G(911.6MHz) foi quase completamente interrompida, se estivermos a transmitir unicamente em 3G ocorre o mesmo que na rede 2G. Passando para um modo entre 3G/2G, o telemóvel muda para a rede com melhor qualidade, ou seja vê a frequência da 3G sendo atacada ele(o telemóvel) muda para rede 2G. No caso do 4G não foi possível testar unicamente somente essa rede pois o telemóvel dispunha o acesso às restantes verificando o comportamento do caso 3G/2G. Mesmo assim as comunicações de dados foram afetadas, embora com impacto diminuto devido à necessidade de amplificação do sinal emitido pelo *jammer* (máximo obtido: -60dB).

Resultados da experiência 2:

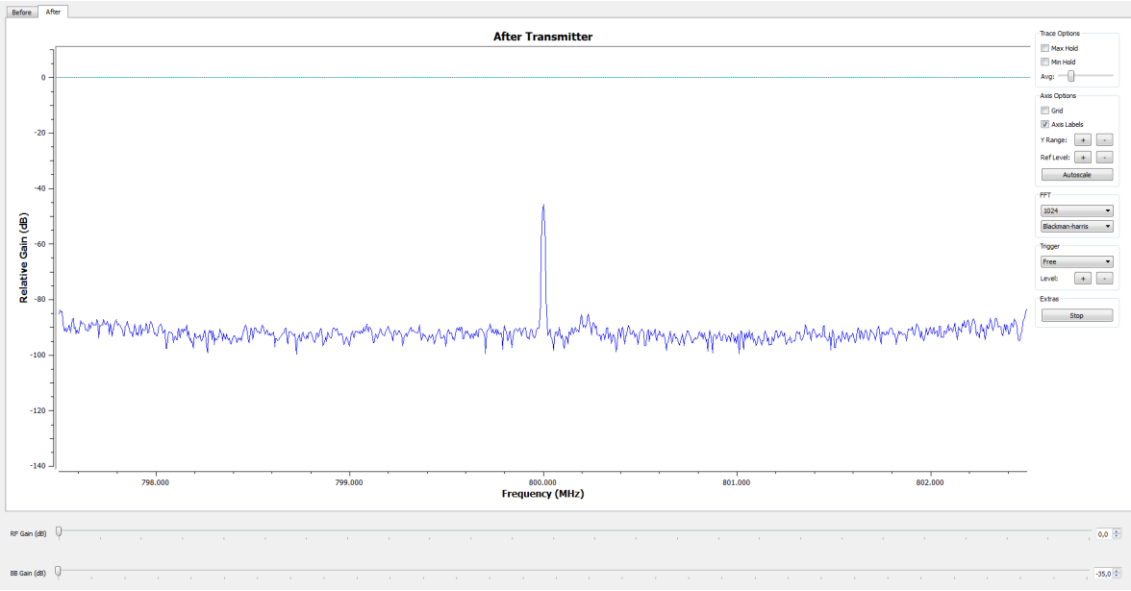

Figura 21 *- Espectro após a aplicação do jammer Single Tone*

Ao analisar os resultados da experiência 2 foram bastante interessantes, as comunicações mais uma vez não foram interrompidas, mas a rede de dados 2G como as restantes não foram interrompidas. Provavelmente se a experiência fosse com *multiple tone jamming* teria quase os mesmos resultados que a experiência 1.

Capítulo 5

Conclusões

Ao desenvolver esta dissertação era pretendido estudar a influência que as técnicas de espalhamento de espectro têm quando usadas para fins de *jamming*, nomeadamente sobre as comunicações móveis em vigor em Portugal, o que foi concluído com sucesso.

As tecnologias usadas nas comunicações móveis são bastantes resistentes e provaram resistir a alguns testes de interferência externa intencional. Apesar de se ter usado a amplificação disponível a nível de software, o sinal gerado não foi muito influente dado que a única antena disponível tinha um ganho de aproximadamente zero dB, pois era omnidirecional. Outro fator que influenciou o modo como a comunicação foi afetada, foi a distância à estação base a que o telemóvel alvo estava ligado, uma vez que se essa estivesse muito perto, e isso até é plausível dado existirem antena das operadoras no telhado do edifício onde as experiências decorreram, então seria mais difícil interferir na comunicação, especialmente devido à baixa potência gerada pela placa usada nos testes. Verificou-se também que o método mais eficaz para anular as comunicações numa zona foi a utilização de *broadband jamming* pois qualquer dispositivo de comunicação móvel tem tecnologia *fail safe* (no caso da rede de dados) que pode transmitir numa das quatro tecnologias 2G, 3G, 4G e Wi-Fi.

Contudo é possível referir que existem estratégias de *jamming* mais complexas e mais localizadas para interferir no espectro de forma mais eficiente. No entanto, o uso desta BladeRF mostrou alguma limitação não apenas devido às técnicas usadas, mas também devido à baixa potência de emissão, que não se conseguiu melhorar pois não se dispunha de uma antena de ganho elevado. Ainda assim foram observadas alterações e algumas disrupções, nomeadamente na comunicação de dados, que demonstram o objetivo desta dissertação.

Trabalho Futuro

As comunicações são um universo em constante expansão que necessita de cuidados adicionais, quer para se protegerem de ataques intencionais, quer para obter informações ou bloquear os sinais de uma determinada comunicação móvel em casos estritos e devidamente identificados. Os sistemas de espalhamento de espectro têm muitas potencialidades a explorar e que podem ser utilizados para proporcionar aos sinais transmitidos a redução destes efeitos nocivos para a comunicação. Para trabalho futuro, uma das possibilidades poderá ser a utilização destas técnicas quer como ferramentas de *jamming*, quer como ferramentas de *anti-jamming* de forma mais precisa, para afetar seletivamente apenas uma determinada comunicação ou então para a proteger, segundo as necessidades. Para cumprir este objetivo será necessário estudar não apenas os métodos mencionados nesta dissertação, mas também os métodos de modulação e codificação específicos da comunicação em causa, assim como as demais características específicas, de forma a aumentar a eficácia do efeito pretendido.

Referências

[1] R. A. Poisel, “Modern Communications Jamming Principles and Techniques,” , 2003. [Online]. Available: https://amazon.com/communications-jamming-principles-techniques-information/dp/158053743x. [Acedido em 29 9 2019].

[2] J. A. Mahal, “Analysis of Jamming-Vulnerabilities of Modern Multi-carrier Communication Systems,” , 2018. [Online]. Available: https://vtechworks.lib.vt.edu/handle/10919/83570. [Acedido em 29 9 2019].

[3] A. L. G. Reis, A. F. Barros, K. G. Lenzi, L. G. P. Meloni e S. E. Barbin, “Introduction to the Software-defined Radio Approach,” *IEEE Latin America Transactions,* vol. 10, nº 1, pp. 1156-1161, 2012.

[4] D. . Valerio, “Open Source Software-Defined Radio: A survey on GNUradio and its applications,” , 2008. [Online]. Available: https://pdfs.semanticscholar.org/90cd/fd630dabf4ea75aea53bbc9c22ae2367e737.pdf. [Acedido em 29 9 2019].

[5] S. . Zoican, “Frequency hopping spread spectrum technique for wireless communication systems,” , 1998. [Online]. Available: https://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=726253. [Acedido em 29 9 2019].

[6] D. L. Schilling, L. B. Milstein, R. L. Pickholtz, M. . Kullback e F. . Miller, “Spread spectrum for commercial communications,” *IEEE Communications Magazine,* vol. 29, nº 4, pp. 66-79, 1991.

[7] J. . Stephens e D. . Norman, “Direct-sequence spread spectrum system,” , 1991. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a223021.pdf. [Acedido em 29 9 2019].

[8] L. . Pap, “A general jamming model of spread-spectrum systems,” , 1993. [Online]. Available: http://ieeexplore.ieee.org/document/397309. [Acedido em 29 9 2019].

[9] C. E. Cook e H. S. Marsh, “An introduction to spread spectrum,” *IEEE Communications Magazine,* vol. 21, nº 2, pp. 8-16, 1983.

[10] Q. . Ling e T. . Li, “Modeling And Detection Of Hostile Jamming In Spread Spectrum Systems,” , 2007. [Online]. Available:

https://scholars.opb.msu.edu/en/publications/modeling-and-detection-of-hostile-jamming-in-spread-spectrum-syst. [Acedido em 29 9 2019].

[11] Y. . Chen, W. . Xu, W. . Trappe e Y. . Zhang, "Jamming Attacks and Radio Interference," , 2009. [Online]. Available: https://link.springer.com/chapter/10.1007/978-0-387-88491-2_10. [Acedido em 29 9 2019].

[12] D. . Torrieri, "Principles of Spread-Spectrum Communication Systems, 2nd Edition," , 2011. [Online]. Available: https://dl.acm.org/citation.cfm?id=2050043. [Acedido em 29 9 2019].

[13] K. . Zigangirov, "Introduction to Spread Spectrum Communication Systems," , 2004. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/047165549x.ch2/summary. [Acedido em 29 9 2019].

[14] L. . Xiao, "Spread Spectrum-Based Anti-jamming Techniques," , 2015. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-24292-7_2. [Acedido em 29 9 2019].

[15] K. . Lathief, "Mobile Jammers in Educational Institutions," *International Journal of Research in Engineering and Applied Sciences,* vol. 5, nº 4, pp. 1-6, 2015.

[16] "bladeRF – USB 3.0 Software Defined Radio," , . [Online]. Available: http://www.kickstarter.com/projects/1085541682/bladerf-usb-30-software-defined-radio. [Acedido em 29 9 2019].

[17] E. G. Ström, T. . Ottosson e A. . Svensson, "An Introduction to Spread Spectrum Systems," , 2002. [Online]. Available: http://ieee.hr/_download/repository/introduction to spread spectrum systems.pdf. [Acedido em 29 9 2019].

[18] P. . Baier e M. . Pandit, "Spread Spectrum Communication Systems," *Advances in electronics and electron physics,* vol. 53, nº , pp. 209-267, 1980.

[19] G. L. Stüber, J. R. Barry, S. W. Mclaughlin, Y. G. Li, M. A. Ingram e T. G. Pratt, "Broadband MIMO-OFDM wireless communications," *Proceedings of the IEEE,* vol. 92, nº 2, pp. 271-294, 2004.

[20] B. . Engström e C. . Östberg, “A system for test of multiaccess methods based on OFDM,” , 1994. [Online]. Available: https://doi.org/10.1109/vetec.1994.345418. [Acedido em 29 9 2019].

[21] uSwitchTech, “History of mobile phones | What was the first mobile phone?,” 21 Fevereiro 2019. [Online]. Available: https://www.uswitch.com/mobiles/guides/history-of-mobile-phones/. [Acedido em 2 Outubro 2019].

[22] “List of Mobile Frequencies by Country (GSM, CDMA, UMTS, LTE, 5G),” [Online]. Available: https://spectrummonitoring.com/frequencies/#Portugal. [Acedido em 2 Outubro 2019].

[23] Stelladoradus, “Finding my mobile frequency on my Iphone or Android phone (fieldtest mode) - Stelladoradus,” 24 Outubro 2016. [Online]. Available: https://www.stelladoradus.com/finding-my-frequency-on-my-iphone/. [Acedido em 5 Outubro 2019].

[24] “GSM ARFCN to frequency calculator | ARFCN to frequency conversion,” [Online]. Available: https://www.rfwireless-world.com/Terminology/GSM-ARFCN-to-frequency-conversion.html. [Acedido em 7 Outubro 2019].

[25] “UMTS frequency bands UARFCN | UMTS tutorial,” [Online]. Available: https://www.rfwireless-world.com/Tutorials/UMTS-frequency-bands-UARFCN.html. [Acedido em 7 Outubro 2019].

[26] “UMTS UARFCN to frequency calculator | frequency to UARFCN equation | WCDMA,” [Online]. Available: https://www.rfwireless-world.com/Terminology/UMTS-UARFCN-to-frequency-conversion.html. [Acedido em 7 Outubro 2019].

[27] “LTE EARFCN to frequency calculator | frequency to EARFCN equation,” [Online]. Available: https://www.rfwireless-world.com/Terminology/LTE-EARFCN-to-frequency-conversion.html. [Acedido em 7 Outubro 2019].

[28] “LTE frequency band,” [Online]. Available: http://niviuk.free.fr/lte_band.php. [Acedido em 7 Outubro 2019].

[29] “Wi-Fi Channels, Frequency Bands & Bandwidth » Electronics Notes,” [Online]. Available: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php. [Acedido em 7 Outubro 2019].

[30] C. Hoffman, “Why Wi-Fi Channels 12, 13, and 14 Are Illegal in the USA,” 18 Fevereiro 2019. [Online]. Available: https://www.howtogeek.com/402142/why-wi-fi-channels-12-13-and-14-are-illegal-in-the-usa/. [Acedido em 15 Outubro 2019].

[31] F. Cercas, *Sistemas de Comunicações Digitais por Satélite Módulo 5,* 2015/2016.

[32] N. Thakur, “Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks,” *IRACST - International Journal of Computer Science and Information Technology & Security,* vol. Vol. 3, pp. 202-207, 2013.

[33] D. Torrieri, Principles of Spread-Spectrum Communication Systems, 2015.

[34] C. A. Bruce, P. B. Crilly e J. C. Ruthledge, Communication Systems: An Introduction to Signals and Noise in Electrical Communication, 2002.

[35] P. Affairs, S. Aly e W. Mohamed, “Improved Jamming-Resistant Frequency Hopping Spread Spectrum Systems,” 2014.

[36] R. C. Dixon, Spread spectrum systems, Wiley-Interscience, 1984.

[37] “Jamming and Anti-jamming Techniques in Wireless Networks: A Survey,” *Int. J. Ad Hoc and Ubiquitous Computing.*

[38] R. A. Scholtz, “The Origins of Spread-Spectrum Communications,” *Ieee Transactions on Communications,* vol. C, nº 5, pp. 822-854, 1982.

[39] T. Ulversoy, “Software defined radio: Challenges and opportunities,” *IEEE Communications Surveys and Tutorials,* vol. 12, nº 4, pp. 531-550, 2010.

[40] L. B. MILSTEIN, “Interference Rejection Techniques in Spread,” *PROCEEDINGS OF THE IEEE,* vol. 76, nº 6, pp. 657-671, 1988.

[41] R. P. J. M. L. R. V. M. J. H. R. Marc Lichtman, *LTE/LTE-A Jamming, Spoofing, and Sniffing:Threat Assessment and Mitigation.*

[42] R. Krenz, “Jamming LTE signals,” em *IEEE International Black Sea Conference on Communications and Networking*, 2015.

[43] J. A. D. García, “Software Defined Radio for Wi-Fi Jamming”.

[44] “Mobile Jammer - How Cell Phone Jammer Works,” 26 7 2016. [Online]. Available: https://www.elprocus.com/mobile-phone-jammer-working/. [Acedido em 22 Setembro 2019].

[45] E. Defense e E. W. Support, “Chapter 26 : Electronic Warfare”.

[46] C. Terminology, “Cell-Phone Circuit Architecture 1-1 Historical Timeline”.

[47] “Portugal Wireless Frequency Bands and Carriers,” [Online]. Available: https://www.frequencycheck.com/countries/portugal. [Acedido em 2 Outubro 2019].

Anexos

Tabela 1 – ARFCN

Banda GSM	ARFCN(N)	Frequência Uplink	Frequência Downlink
GSM 450	259-293	450.6+0.2*(N-259)	F_{UL}(N)+10
GSM 480	306-340	479+0.2*(N-306)	F_{UL}(N)+10
GSM 750	438-511	747.2+0.2*(N-438)	F_{UL}(N)+30
GSM 850	128-251	824.2+0.2*(N-128)	F_{UL}(N)+45
P-GSM	1-124	890+0.2*N	F_{UL}(N)+45
E-GSM	975-1023	890+0.2*(N-1024)	F_{UL}(N)+45
GSM-R	955-1023	890+0.2*(N-1024)	F_{UL}(N)+45
DCS 1800	512-885	1710.2+0.2*(N-512)	F_{UL}(N)+95
PCS 1900	512-810	1850.2+0.2*(N-512)	F_{UL}(N)+80

Tabela 2 – UARFCN

Banda da Frequência UMTS	Frequência da Portadora (MHz)	UARFCN
Banda 1	1922.4-1977.6(F_{UL}), 2112.4-2167.6(F_{DL})	9612-9888(UL), 10592-10838(DL)
Banda 2	1852.4-1907.6(F_{UL}), 1932.4-1987.6(F_{DL})	9262-9538(UL), 9662-9938(DL)
Banda 3	1712.4-1782.6(F_{UL}), 1807.4-1877.6(F_{DL})	937-1288(UL), 1162-1513(DL)
Banda 4	1712.4-1752.6(F_{UL}), 2112.4-2152.6(F_{DL})	1312-1513(UL), 1537-1738(DL)
Banda 5	826.4-846.6(F_{UL}), 871.4-891.6(F_{DL})	4132-4233(UL), 4357-4458(DL)
Banda 6	832.4-837.6(F_{UL}),	4162-4188(UL),

	877.4-882.6(F_{DL})	4387-4413(DL)

Tabela 3 – EARFCH

	Downlink			Uplink		
Banda	F_{DL_low} (MHz)	$N_{Offs-DL}$	N_{DL} Range	F_{UL_low} (MHz)	$N_{Offs-UL}$	N_{UL} Range
1	2110	0	0-599	1920	18000	18000-18599
2	1930	600	600-1199	1850	18600	18600-19199
3	1805	1200	1200-1949	1710	19200	19200-19949
4	2110	1950	1950-2399	1710	19950	19950-20399
5	869	2400	2400-2649	824	20400	20400-20649
6	875	2650	2650-2749	830	20650	20650-20749
7	2620	2750	2750-3449	2500	20750	20750-21449
8	925	3450	3450-3799	880	21450	21450-21799
9	1844.9	3800	3800-4149	1749.9	21800	21800-22149
10	2110	4150	4150-4749	1710	22150	22150-22749
11	1475.9	4750	4750-4949	1427.9	22750	22750-22949
12	729	5010	5010-5179	699	23010	23010-23179

13	746	5180	5180-5279	777	23180	23180-23279
14	758	5280	5280-5379	788	23280	23280-23379
…						
17	734	5730	5730-5849	704	23730	23730-23849
18	860	5850	5850-5999	815	23850	23850-23999
19	875	6000	6000-6149	830	24000	24000-24149
20	791	6150	6150-6449	832	24150	24150-24449
21	1495.9	6450	6450-6599	1447.9	24450	24450-24599
22	3510	6600	6600-7399	3410	24600	24600-25399
23	2180	7500	7500-7699	2000	25500	25500-25699
24	1525	7700	7700-8039	1626.5	25700	25700-26039
25	1930	8040	8040-8689	1850	26040	26040-26689
26	859	8690	8690-9039	814	26690	26690-27039
27	852	9040	9040-9209	807	27040	27040-27209
28	758	9210	9210-9659	703	27210	27210-27659
292	717	9660	9660-9769	N/A		–
31	462.5	9870	9870-9919	452.5	27760	27760-27809
…						–

33	1900	36000	36000-36199	1900	36000	36000-36199
34	2010	36200	36200-36349	2010	36200	36200-36349
35	1850	36350	36350-36949	1850	36350	36350-36949
36	1930	36950	36950-37549	1930	36950	36950-37549
37	1910	37550	37550-37749	1910	37550	37550-37749
38	2570	37750	37750-38249	2570	37750	37750-38249
39	1880	38250	38250-38649	1880	38250	38250-38649
40	2300	38650	38650-39649	2300	38650	38650-39649
41	2496	39650	39650-41589	2496	39650	39650-41589
42	3400	41590	41590-43589	3400	41590	41590-43589
43	3600	43590	43590-45589	3600	43590	43590-45589
44	703	45590	45590-46589	703	45590	45590-46589

Tabela 4 – WiFi 2.4GHz canais e frequências

Canais	Frequência inferior [MHz]	Frequência central [MHz]	Frequência superior [MHz]
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433

4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495