Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2011

Luís Miguel Vinhas Mendes

Medida e Análise de Atividade Espetral

Measurements and Analysis of Spectrum Activity

Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2011

Luís Miguel Vinhas Mendes

Medida e Análise de Atividade Espetral

Measurements and Analysis of Spectrum Activity

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia de Electrónica e Telecomunicações, realizada sob a orientação científica do Prof. Dr. Atílio Gameiro, Professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e Dr. Luís Gonçalves, Investigador (Pos-Doc) no Instituto de Telecomunicações da Universidade de Aveiro.

o júri / the jury

presidente / president

Prof. Dr. António Luís Jesus Teixeira
Professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

vogais / examiners committee

Prof. Dr. Carlos Miguel Nogueira Gaspar Ribeiro
Professor adjunto do Departamento de Engenharia Electrotécnica do Instituto Politécnico de Leiria (Arguente)

Prof. Dr. Atílio Manuel da Silva Gameiro
Professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro (Orientador)

Dr. Luís Carlos Carneiro Gonçalves
Investigador (Pos-Doc) no Instituto de Telecomunicações da Universidade de Aveiro (Co-Orientador)

agradecimentos/ acknowledgements

Ao Dr. Luís Gonçalves pela disponibilidade em esclarecer dúvidas partilhando o seu conhecimento. O espírito crítico e a paciência demonstrada revelaram-se importantes em todos os problemas encontrados no decorrer desta dissertação.

Ao Prof. Dr. Atílio Gameiro pela disponibilidade demonstrada em partilhar os seus conhecimentos com vista à execução desta dissertação.

Ao Instituto de Telecomunicações de Aveiro e a todos os seus colaboradores por terem fornecido todas as condições necessárias para o desenvolvimento desta dissertação.

Um agradecimento à ANACOM e VODAFONE Portugal por toda a informação disponibilizada.

À minha família por todo o suporte demonstrado, possibilitando o desenvolvimento desta dissertação.

palavras-chave

GSM, UMTS, Rádio Cognitivo, Modelos de Ocupação Espectral, Utilizadores Secundários, Estatistica, Setup de medidas.

resumo

Nesta dissertação são feitas medidas e a análise de ocupação de espectro em uma banda de GSM900, uma banda de DCS1800 e toda a largura de banda do UMTS. É apresentada uma modelização para potência analógica e para a potência binária quantizada. No caso da potência analógica são apresentados histogramas da distribuição de potência ao longo de um dia útil. No caso da potência quantizada as duas estatísticas, distribuição do período de tempo de oportunidades e distribuição do tempo entre oportunidades, são apresentadas, descritas e modeladas. O setup de medida encontra-se em linha de vista com a estação base. O setup é descrito e analisado em termos de máxima sensibilidade. A desocupação de espectro em termos de tempo total para a banda de GSM900 e para a banda DCS1800 é fornecida, para um dia de útil.

keywords

GSM, UMTS, Cognitive Radio, Spectrum Occupancy Models, Secondary Users, Statistics, Measurement Setup.

abstract

The dissertation deals with measuring and analyzing spectrum occupancy of a GSM900 band, DCS1800 band and all UMTS bandwidth. A modelization for analog power and binary quantized power is given. In the case of analog power, histograms of the power distribution during one working day are presented. In the case of quantized power the two time statistics, the time period of opportunities distribution and the time between opportunities distribution are presented, described and modeled. The measurement setup is standing in line of sight with the base station. Also, in terms of maximum sensitivity the measurement setup is described and analyzed. Spectrum non occupancy in terms of total time for the GSM900 band and the DCS1800 band is given, for a working day.

Table of Contents

Table List

Figure List

Acronyms and Abbreviations

2G	Second Generation
3G	Third Generation
ADSL	Asymmetric Digital Subscriber Live
AMR	Adaptive Multi-Rate
ANACOM	Autoridade Nacional de Comunicações
AWGN	Additive White Gaussian Noise
BCCH	Broadcast Control Channel
BLER	Block Error Ratio
BS	Base Station
BTS	Base Transceiver Station
CAMEL	Customized Application for Mobile network Enhanced Logic
CCBS	Completion of Cells to Busy Subscribers
CDMA	Code Division Multiple Access
CR	Cognitive radio
DCS	Digital Cellular Service
DETI	Department of Electronics, Telecommunications and Informatics
DL	Downlink
DS	Direct Sequence
DSSS	Direct Sequence Spread Spectrum
EDGE	Enhanced Data Rates for GSM Evolution
EDR	Enhanced Data Rate
EFR	Enhanced Full-Rate
EMI	Electromagnetic Interference
EOTD	Enhanced Observed Time Difference
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FCT	Fundação para a Ciência e Tecnologia
FDD	Frequency Division Duplexing
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform

FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
FOMA	Freedom of Mobile Multimedia Access
FR	Full Rate
GHz	Gigahertz
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile telecommunication
GMSK	Gaussian Minimum Shift Keying
HR	Half Rate
HSCSD	High-Speed Circuit-Switched Data
HSDPA	High-Speed Downlink Packet Access
Hz	Hertz
IEEE	Institute of Electrical and Electronics Engineers
IF	Intermediate Frequency
ILPC	Outer Loop Power Control
ITU	International Telecommunication Union
kbps	kilobit per second
LAN	Local Area Network
LOS	Line of Sight
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LPPF	Low Probability of Position Fix
LPSE	Low Probability of Signal Exploitation
MAC	Medium Access Control
Mbps	Megabit per second
Mbit	Megabit
MC	Multi-Carrier
Mcps	Mega chip per second
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MMS	Multimedia Messaging

MoU	Memorandum of Understanding
ms	milliseconds
MS	Mobile Station
MTS	Mobile Telephone Service
mW	Milliwatt
NF	Noise Figure
NLOS	Non-Line-Of-Sight
NMT	Nordic Mobile Telephone
OLPC	Outer Loop Power Control
PAGCH	Paging and Access Grant Channel
PC	Power Control
PDA	Personal Digital Assistant
PDTCH	Packed Data Traffic Channel
PN	Pseudo Noise
PSK	Phase-Shift Keying
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QoSMOS	Quality of Service and MObility driven cognitive radio Systems
QPSK	Quadrature Phase Shift Keying
RBW	Resolution Bandwidth
RF	Radio Frequency
RTMS	Radio Telephone Mobile System
RNC	Radio Network Controller
RRC	Radio Resource Control
R&S	Rohde & Schwarz
SA	Spectrum Analyzer
SACCH	Slow Associated Control Channel
SDCCH	Stand-alone Dedicated Control CHannel
SDR	Software-Defined Radio
SIM	Subscriber’s Identity Module
SIR	Signal to Interference Ratio
SMA	SubMiniature version A

SMS	Short Messaging Service
SNR	Signal-to-Noise Ratio
SS	Spread Spectrum
TACS	Total Access Communication System
TCH	Traffic Channel
TCH/F	Full Rate Traffic Channel
TCH/H	Half Rate Traffic Channel
TDMA	Time Division Multiple Access
TFO	Tandem Free Operation
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
ToA	Time of Arrival
TPC	Transmit Power Control
TSL	Timeslot
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunications System
U.S.	United States
UTRA	Universal Terrestrial Radio Access
VBW	Video Bandwidth
VSELP	Vector Sum Excited Linear Prediction
VSWR	Voltage Standing Wave Ratio
W	Watt
WCDMA	Wideband Code Division Multiple Access

1. Introduction

"A Cognitive Radio is a radio frequency transceiver designed to intelligently detect whether a particular segment of the radio spectrum is in use, and to jump into (and out of) the temporarily unused spectrum very rapidly, without interfering with the transmission of other authorized users."

Dr. Joseph Mitola III

1.1. Overview

This dissertation focuses on understanding the current spectrum usage, due to the fixed spectrum allocation in Portugal, and it also focuses on its utilization efficiency in the city of Aveiro in order to estimate the potential availability of spectral bands for Cognitive Radio (CR) through statistical analysis. These statistics are done according to power measurements, and they must be characterized in order to find channel occupational models. Spectrum is considered to be a scarce resource since all frequencies below 3GHz have been completed allocated to specific uses. However, actual measurements show that most of the allocated spectrum is vastly underutilized at any specific location and time [3]. In order to increase utilization of this spectrum, new approaches to spectrum sharing were made such as the operation of unlicensed devices using/exploring the spatially/temporally "unused" bands. These mentioned unlicensed devices are considered to be secondary users of the spectrum since they use the frequency bands only if the official user of the spectrum (primary system) is not using them.

1.2. Cognitive Radio and Secondary Users

According to Mitola [4], digital radios have some flexibility, but they don't have that much computational intelligence. When a network asks a device to count the number of distinguishable multipath components in the current location, two issues arise. The first one is that the network has no standard language to pose the question to the device. The second one is that the device, although having the answer in the structure of its time-domain equalizer taps internally, it cannot access this information. "*To be termed "cognitive," a radio must be self-aware of its surroundings*", in other words, it needs to know the basic facts of its outside world, observe it, and evolve to be able to communicate with other entities using that knowledge (Figure 1). With this, a comparison between hardware and software upgrade arises as a potential analysis category for nowadays communication technologies. Replacing hardware on communication technologies is expensive nowadays. With Software-Defined Radio (SDR), however it's possible to have new communication technologies by means of simple software upgrades. The fact that some of these upgrades can be done by direct wireless download, it reduces upgrading costs and allows immediate compatibility to be achieved among devices. This brings more flexibly when managing spectrum by time, frequency, space, power and coding of the transmitted wave form [5].

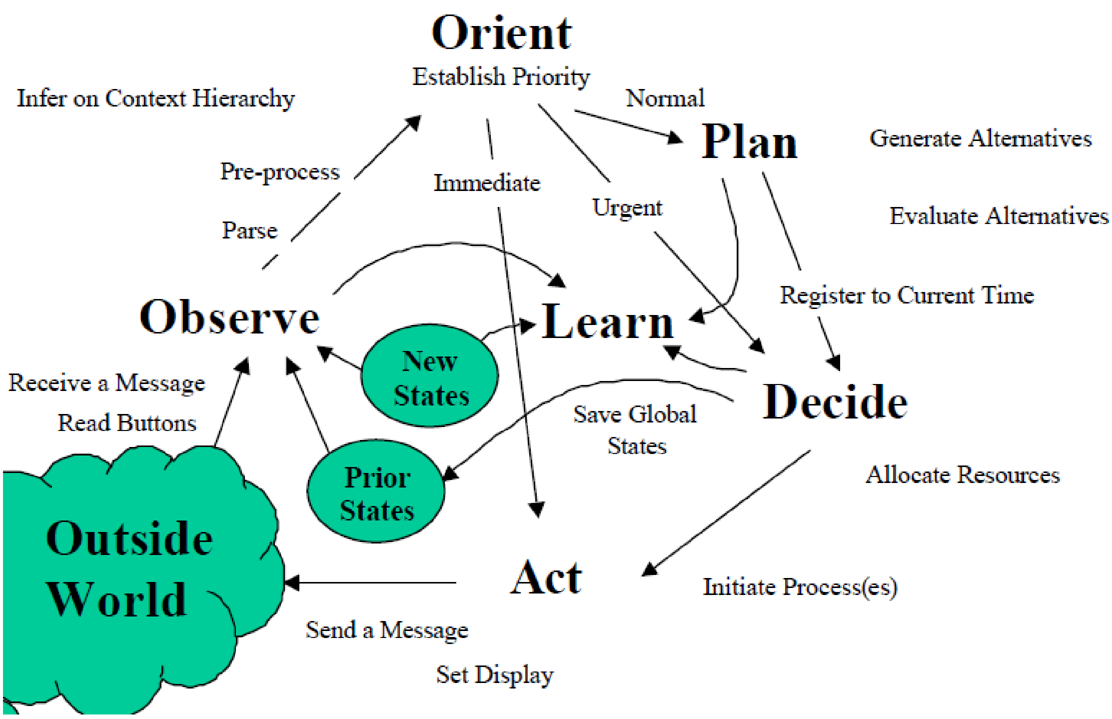


Figure 1 - Representation of a simplified Cognitive Cycle [4]

CR systems are considered to be a subset of SDRs. These are controlled by powerful microprocessors, programmed to search and analyze a number of radio channel parameters. Part of the main analysis is based on the ability of these devices to adapt to several specifications like the modulation technique, output power and frequency. Programming dynamically to accommodate different regulatory structures by adjusting frequencies, bandwidth, and directionality is going to allow a more effective use of the spectrum, instead replicating hardware and infrastructures (Figure 1) [5].

CR Systems will be used in order to maximize the full potential of the allocated and unutilized spectrum of primary systems. However, the highest priority constraint for opportunistic secondary devices is to guarantee non-interference on the primary system. Given the density of interferer's transmissions, an area of use of the primary system is determined excluding the secondary users. A secondary user, inside this range, must be able to detect a primary signal accurately and stop transmission when it is present.

The study of the technology associated with these systems is at initial stage of despite several years of evolution and one already standard set (IEEE 802.22, for packet use in rural areas using the holes of TV spectrum).

1.3. Motivation and Objective

Wireless technology is advancing rapidly in nowadays society. Many social and individual benefits are brought by wireless computing and communications on recent devices. These devices, such as cell phones, PDAs and laptops receive a lot of attention by the consumer when the range of wireless technology is much greater than the narrowed view the consumer has. Sensor networks for safety applications and home automation, medical wearable and embedded wireless devices, and entertainment systems are only a few examples of how important this technology is [6].

The fact that wireless applications have been increasing in the last years, creates a big demand for more radio spectrum. The need for more capacity and cost effectiveness on transmission techniques that can exploit scarce spectral resources efficiently, is expected to continuously increase in the near and medium term future. Mobile users have access to voice, email, file transfer, and related services through mobile wireless technology. Fixed wireline networks offer similar services and they have greater bandwidth and availability than wireless networks, but on the other hand, wireless networks provide the services while the user is on the move [4]. Many studies have shown that some bands, used by these services, were significantly underutilized and lead to new researches on breakthrough radio technologies that can meet future demands in terms of spectrum efficiency and application performance.

CR [7], [8], [9] is considered to be one of the most promising solutions in terms of spectrum efficiency with its high dynamic in efficiency in the future of wireless communication systems.

Assembling a network based on CR technology, however, is a complex task. Latest researches shows that the need of understanding a wide range of issues like smart antenna technology, spectrum sensing and measurement, radio signal processing, hardware architectures including SDR, Medium Access Control (MAC), network discovery and self-organization, routing, adaptive control of mechanisms, policy definition and monitoring, and learning mechanisms, it is crucial when proceeding towards a CR system. This process takes into account a wide range of technologies and their specific applications which will enable understanding and properly controlling the behavior of the resulting system [6].

The main goal of this research is firstly to detect the spectrum behavior and then analyze its occupancy. This dissertation basically represents a study of temporal occupation of the spectrum in the bands of GSM900, GSM1800 and UMTS, so as to determine the power distribution of the primary signal. The underlying idea is to analyze statistically and model the previously mentioned bands, in terms of both occupancy and non occupancy. With this, a mathematical model can be obtained to describe the radio environment on the considered bands. This mathematical model can be used as information on CR devices, as a form of adaptation to the environment.

1.4. Scope of the dissertation

Cellular wireless network traffic has changed in terms of voice usage and it is developing fast in terms of data, streamed high-bandwidth video and digital TV. Since the network system itself was not prepared for these changes, mobile operators have to make decisions when it comes to upgrades. Changes like the release of some bands or even the television switching from analogue to digital leads to the potential usage of cognitive devices which share those bands, transmitting without any interference. The opportunistic user would require a cognitive device to sense its own spectrum occupancy and take advantage of other devices spectrum measurements, sharing on a dynamic temporal basis [10]. These opportunity windows can be used either for “congestion relief” during peak loads in the licensed spectrum, or for enhancing existing services and/or providing new services without the need for acquiring additional licensed spectrum. The usage of the spectrum could happen either upon instruction from a cognitive base station or autonomously by the device itself [10].

The work that is developed in this dissertation fits in the projects *Quality of Service and MObility driven cognitive radio Systems* (QoSMOS) [10] and AGILE with funding from *Fundação para a Ciência e a Tecnologia* (FCT). The main objectives of these projects are to research, develop, and validate concepts, mechanisms and architectures for cognitive radios and to demonstrate the advantages of opportunistic spectrum usage [11].
A system assembling is required for measuring the occupation of spectrum in the band from 25MHz to 6GHz, but also a software development in order to analyze the recorded data. This system has the purpose of identifying frequency bands that may prove advantageous to be used opportunistically by a secondary user in cognitive radio systems, and to statistically characterize its occupancy and non-occupancy.

This study complements the work presented in [12] which regards the period of time of opportunities distribution for a GSM900 band in a mobile situation and it goes beyond some other spectrum occupational articles [13] [14] in the way that it tries to model the spectrum occupancy.

1.5. Organization

This dissertation is organized as it follows. **Chapter 2** deals with several different aspects. It describes the way in which information is processed, which spread spectrum techniques are used in transmission and it also discusses many characteristics of spectrum sensing. These aspects are fundamental in the analysis for this dissertation, particularly in GSM and UMTS bands.

Chapter 3 describes the measurements setup used for the analysis and each of its components’ characteristics. Also, it presents all the software used and the program that was assembled for the purpose of running some statistical analysis on the collected data.

Chapter 4 represents analysis done on the collected data mainly exemplifying several tests done in varied frequencies for the purpose of enhancing the analysis. This chapter starts by analyzing the spectrum occupancy from 25MHz to 6GHz with different power levels of decision. Then it presents and discusses the results obtained in terms of occupancy and non occupancy of the selected frequencies.

Finally, **Chapter 5** makes conclusions on the grounds of the performed analysis and the results obtained.

2. Primary Systems and Cognitive Radio concepts

The purpose of this chapter is to give an overview of primary systems and a short overview of CR and its uses and constrains in the modern world. However, to fully understand how CR systems work, it is required an overview on how the signals are transmitted. Several concerns must be taken into account before regulators allow CR Systems to transmit opportunistically in already allocated bands. The most important constraint to be aware of is the non-interference on the primary receivers. With this said, the way information is used/transmitted is an important factor in nowadays studies. Starting from examples like, satellite television to garage door openers, emitting radiation through the electromagnetic spectrum can create valuable outputs. How can this natural resource be most efficiently used? Some techniques are used to enhance the communication/transmission between the emissary and the receiver, so that the spectrum can be used on its full potential [15].

The quest for efficiently use of nowadays wireless communications, leads to spectrum management, that provides a primary user the granted license and the exclusive exploitation rights for a specific frequency. Even though this process can ensure that excessive interference does not occur, it is not able to maximize its spectrum use.

With the search for improvements in spectrum management when it comes to topics like interference or spectrum efficiency, several technologies are considered for this work. GSM and UMTS are some of the primary systems taken into consideration in CR systems study. Several studies show that these technologies, and other technologies under 3GHz, have nearly no free frequencies with interesting propagation characteristics available [16]. Studies also revealed an under utilization of the allocated spectrum, and the claim for new frequency bands leads to new research about spectrum scarcity for new communication technologies [17].

CR systems study provides a better understanding on how to improve efficiency on spectrum usage. For example if a system possessing a license for a spectrum band, which is usually called primary user, and it does not use its spectrum allocation efficiently, secondary users may opportunistically access it, in an unlicensed way [3].

With this said, this chapter is structured in two big subchapters, and it is organized as it follows:

Primary systems

The First Generation was based on analogue technology, providing only simple voice telephony. The current Second Generation (2G) networks, based on the European digital GSM standard, provided a couple of additional data facilities, from Short Messaging Services (SMS) to narrow band ISDN under the latest Phase 2 standards.

The GSM standard was developed by European Telecommunications Standards Institute (ETSI) in the 80's as a digital mobile system that would replace the existing analog systems at the time (NMT, MTS, TACS, RTMS, ...). The purpose was to create a system with greater capacity while trying to unify a system that would enable the European mobile subscriber into having a terminal compatible in any country you are moving to (roaming). The standard was so successful it was adopted in different countries outside Europe such as the U.S. and several Latin American countries, a total of 130 countries that contain at least one GSM operator.

All of this was sufficient for basic data services like fax or electronic mail, but couldn't provide high resolution video or multimedia applications. UMTS, as the 3G of mobile telecommunications, brought mobile networks significantly closer to the capabilities of fixed networks, providing mobile users full interactive multimedia capabilities at data rates up to 2 Mbits/s, in addition to conventional voice, fax and data services. The improvements in coding and data compression technology also provided better speech quality and more reliable data transmission.

In order to understand some of these communication technologies and the way they can connect with CR systems (or secondary users), GSM and UMTS are some of the important bands to be study, when it comes to spectrum occupation and the possible use of these technologies with CR systems.

Secondary systems concepts

The first steps in the concepts of secondary users (CR systems) were first introduced by Mitola [4]. CR systems are able to sense their environment, to learn about their radio resources and user or even application requirements, but also to adapt their behavior by optimizing their own performance in response to user requests [18]. With this, CR systems are therefore a very powerful tool when it comes to solving the spectrum usage problem. The fact that these systems are capable of sensing spectrum occupancy, and, in conformity with the rules of the Federal Communications Commission (FCC), opportunistically adapting transmission to utilize empty frequency bands without disrupting other systems, makes them an important area in nowadays research.

2.1. Wireless networks

New communication systems with different sorts of functionalities, new coverage distances, and higher transmission rates are under development. In a future world where multiple communications systems interact between themselves, CR systems offer optimal communications strategies based not only on the surrounding communication conditions, but also the constraints of the application functions that needs to be served, and the user profiles and preferences [19].

Several systems are being proposed through several researches in order to achieve the cooperation and the coexistence of multiple communications systems. The following picture illustrates one proposal by [19], of the coexistence among several communication systems in a general scheme.

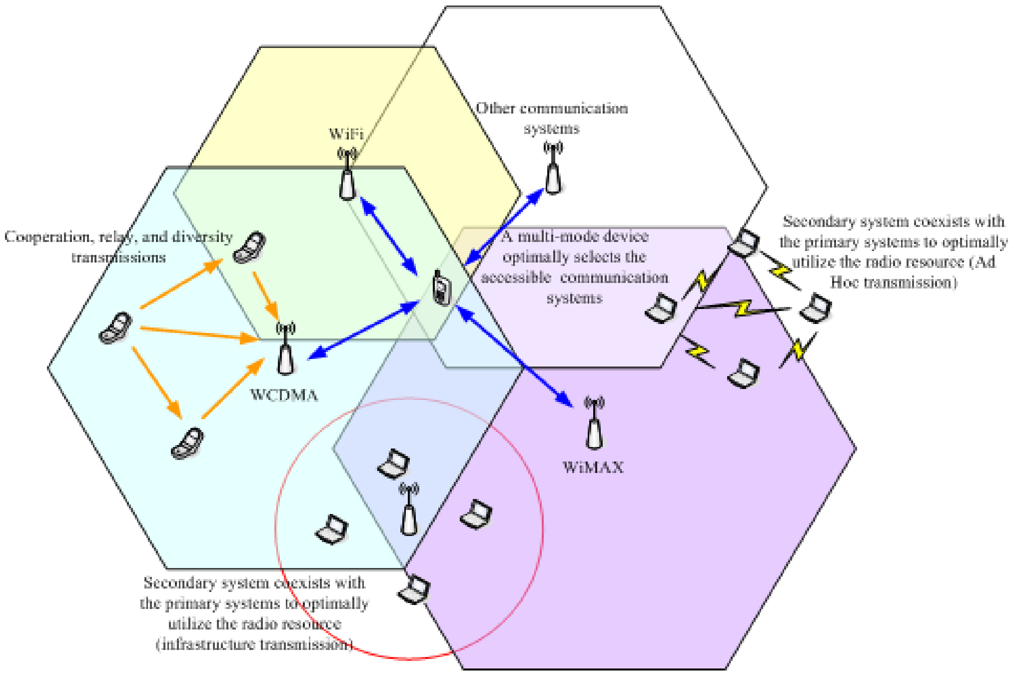


Figure 2 - Coexistence between several communication systems [19]

This scheme includes the coexistence of cognitive radio systems with the primary systems in order to optimally use the wireless radio resource, the multiple accessible communication systems selection and cooperation algorithms, and the transmissions diversity [19].

Some of these primary systems like GSM and UMTS are the target of studies when it comes to CR systems research. The possibility to use GSM or even UMTS bands for CR systems is the target of study of this dissertation, like previously mentioned. With this, the following sub-chapters will give an overview about them, and a description on how these technologies work and how are they structured.

2.2. Global System Mobile (GSM) Phased Approach

GSM as a cellular phone protocol was initially defined, by the International Telecommunication Union (ITU), in two frequency bands of 25 MHz for use by GSM (between 890 and 915 MHz, UL, and between 935 and 960 MHz, DL). Later on, a second band of frequencies around 1800 MHz was also used by GSM in Europe, while a band of frequencies around 1900 MHz was available for the U.S. [20].

The development of GSM specifications was split into two phases. Such a phased approach was developed and defined in order to ensure that the specifications followed a consistent set of features and services for *"multi-vendor of operation of GSM products, both on the terminal and the network sides"*[1].

In 1989, GSM responsibility was transferred to the ETSI, and Phase 1 of the GSM specifications was published in 1990. The first networks started commercializing their service in 1992. Some initial problems with network coverage, terminal type approval, echo, some control software problems, and others were gradually overcome, and Phase 1 GSM technology became stable and successfully established in a short time. The matrix of roaming agreements between GSM network operators quickly filled up, and the quality of service was accepted by the subscribers. Since the 900 and 1800 MHz bands provided more availability in terms of bandwidth, the additional cellular radio capacity for the new frequency allocations allowed become a positive market driver in several countries in Europe. Figure 3 represents the evolutionary steps of GSM until nowadays and its organization is described as it follows.

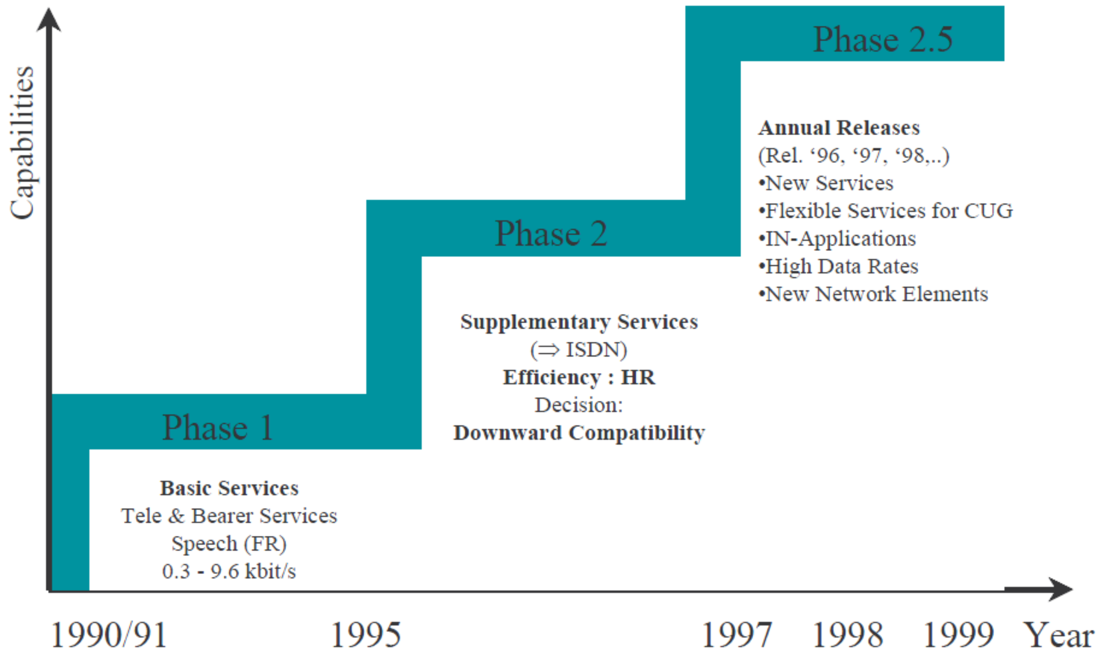


Figure 3 - GSM Evolutionary Concepts [21]

The introduction of Phase 1 services was initially restricted to voice telephony. Other features such as data services, available in some GSM networks since the start of 1995 were initially disappointing [20].

While the mentioned GSM Phase 1 networks were being deployed, GSM Phase 2 was being specified in ETSI SMG. The GSM Phase 2 specifications included a mechanism for cross phase compatibility and error handling to enable evaluation of the specifications. Other improvements concerning the technical part were made and they included several new supplementary services; line identification services, call waiting, call hold, advice of charge and multi-party call. Improvements in the speech area, however, consisted of a half-rate channel mode codec introduction, which functioned as a complement to the already specified speech codec for GSM full rate channel mode. Considering data support, the main improvement included group 3 fax service support [1]. The first phases of GSM provided relatively solid grounds for the GSM system evolution towards the 3G system requirements, also known as Phase 2+ items. The Phase 2+ was characterized by an introduction of General Packet Radio System (GPRS) network architecture, especially designed for Internet connectivity [1]. Also, similar enhancements, concerning both packet and circuit modes to provide higher bit rates and better network aptitude, were made on the radio access network. This phase also added to better speech quality, looking from the user´s perspective, as it mainly focused on enhancing capabilities in providing more efficient speech and data services. According to [1], the following list was presented, with the purpose to show an overview of the different work item categories:

- New bearer services and data-related improvements such as High-Speed Circuit-Switched (multislot) Data (HSCSD), 14.4-kbps (single-slot) data, GPRS and Enhanced Data Rates for Global Evolution (EDGE);
- Speech-related items such as Enhanced Full-Rate (EFR) speech codec, Adaptive Multi-Rate codec (AMR) with both narrow and wideband options, and Tandem Free Operation (TFO) of speech codecs;
- Mobile Station (MS) positioning–related items such as cell identity and timing advance, uplink Time of Arrival (ToA) and Enhanced Observed Time Difference (EOTD) methods based on measurements within the cellular network, and assisted Global Positioning System (GPS) method based on the GPS technology;
- Frequency band–related items such as GSM400, 700, and 850 MHz, unrestricted GSM multi-band operation, release independent support of frequency bands;
- Messaging-related items such as SMS concatenation, extension to alphabet, SMS interworking extensions, forwarding of SMSs and particularly Multimedia Messaging (MMS);
- New supplementary services such as call deflection, calling-name presentation, explicit call transfer, user-to-user signalling, completion of calls to busy subscriber and new barring services;
- Billing-related work items such as payphone services, provision for hot billing and support for home area priority;
- Service platforms such as Subscriber’s Identity Module (SIM) application toolkit and Customized Application for Mobile network Enhanced Logic (CAMEL).

2.2.1. GSM Phase 1

The aim of the Memorandum of Understanding (MoU) [22] to open a GSM system by July 1st 1991 was basically felt to be out of reach, in other words, it was seen that a system with full set of features could not possibly be opened on that date, but a limited one with only a

basic features could. The first Phase 1 network was an experimental one on July 1st 1991 in Finland, although its first set of specifications was released in 1990 with a total volume of 5000 pages. This set of specifications proved to be incomplete, moreover, it was inconsistent with many imperfections and errors.
Phase 1 contains the most common services including:

- Voice telephony
- International roaming
- Basic fax/data services (up to 9.6 Kbits/s)
- Call forwarding
- Call barring
- SMS

Phase 1 also incorporated features such as ciphering and SIM cards. Shortly after their release, Phase 1 specifications were frozen.

The GSM phase 1 specifications were unavailable for some time, but eventually their approval started in early 1992. In January 1994, in order to obtain a complete regulatory regime approval, this grant had to be based on the European Directive on telecommunication terminal equipment, and at the same time it had to include a more comprehensive set of tests. In GSM Phase 1 it was attempted to use a unique system simulator for all tests. This was a challenge in a way that the expertise on radio hardware and signaling protocol was in general located in different companies [22]. So, for GSM Phase 2, it was decided to use several machines. While still working on enhancing phase 1 set of specifications and implementation of features, the work on phase 2 was carried out at the same time.

2.2.2. GSM Phase 2

After the testing of pre-operational phase 1 networks in 1991, followed by their commercial opening in 1992, the work of the GSM group focused on the development of the phase 2 specifications which actually lasted until 1995. Several specifications had to be written; all the existing ones had to be reevaluated for correctness, consistency and completeness. The Phase 2 specifications and their official freezing, was in October 1995. Phase 2 work included the following main aspects [22]:

- Merging of GSM 900 and DCS 1800 specifications into single documents: a single document lists and describes the standards, the requirements, and the parameters for both systems;
- Adding new radio-related definitions (extended GSM frequency band and channel number allocations, lower transmit power control levels for mobiles, etc.);
- Standardization of additional supplementary services; call hold, call waiting, caller ID , multi-party call
- Standardization of the optional half-rate speech codec;
- Standardization of the optional enhanced full-rate speech codec (originally a Phase 2+ feature but moved into Phase 2);
- Improvements in SMS;
- Advanced SIM features.

Although the terminals that support Phase 2 features became available in 1996, the introduction of GSM Phase 2 service only took place in 1997 with significant results though.

However, there were some problems concerning Half Rate (HR) feature or a speech coding system for GSM, developed in the early 1990s. This system/feature operates at 5.6 Kbit/s, and requires half the bandwidth of the Full Rate (FR) codec. As a result, network capacity for voice traffic became doubled, at the expense of audio quality. It was recommended to use this codec when the battery is low, since it decreases energy consumption and thus saves 30% energy. The sampling rate is 8 kHz with resolution 13 bit, frame length 160 samples (20 ms) and subframe length 40 samples (5 ms). GSM HR is specified in ETSI EN 300 969 (GSM 06.20), and uses a form of the Vector Sum Excited Linear Prediction (VSELP) algorithm. The industry claimed to be able to support the HR feature in the networks and terminals, but the operators have remained reluctant to offer it due to its inferior voice quality in nonideal radio environments or in the presence of background noise [22]. Because of a bad performance of half rate features some companies in Germany were considering on notifying their customers on its poor quality. Other suggestions were to introduce lower tariffs for HR mode, or to provide HR mobile stations with a preferred access to the network or to make no distinction at all. Another possibility would also concern introducing HR in areas where voice quality is not yet an issue (where nobody has ever heard a better codec), and/or where the radio coverage is sufficient for adequate voice quality even when the HR codec is used. In any case, [22] points out, only a sufficient loading of the network with HR subscribers (something in the range of 30% to 50% of the network's traffic) will show reasonable network capacity benefits.

The EFR codec, which was initially specified by the North American market, has been used in handsets since late 1997, and enables most users to perceive GSM voice services in its EFR mode. Even though the EFR helps to improve call quality, this codec have higher computational complexity, which in a mobile device can result in an increase of energy consumption of 5% compared to 'old' FR codec. EFR was developed by Nokia and the University of Sherbrooke (Canada). In 1995, ETSI has selected the EFR voice codec as the industry standard codec for GSM/DCS [22].

Of great importance, apart from the above mentioned enhancements, was the decision to enable downward compatibility to the previous phases for all future GSM phases. Phase 2 specifications kept a compatibility with those from phase 1. This means that the Phase 1 terminals were able to function, within its original Phase 1 specifications, in a network supporting Phase 2 features. Similarly, a Phase 2 terminal could work in a Phase 1 network, even though its enhanced Phase 2 capabilities will not be exploited [22].

2.2.3. GSM Phase 2+

The phase of standardization of Phase 2+ discusses several issues. For as long as Phase 1 of the GSM implementation contained some basic teleservices, mostly voice communication, and Phase 2 standardization implemented other supplementary services in 1996, the topics of Phase 2+ deal with many aspects, ranging from radio transmission to communication and call processing. However, there is no complete revision of the GSM standard; only single subject areas are treated as separate standardization units, with the intent of allowing them to be implemented and introduced independently from each other.

As GSM Phase 2 defined a set of new supplementary services, so does Phase 2+ address in new bearers and teleservices. They significantly improve the GSM speech quality and make the utilization of available radio resources much more efficient. Furthermore, the new data services developed in this Phase seemed to be an important step towards wireless Internet access via cellular networks [23].

Since one of the most important services in GSM is voice service, Phase 2+ continued to develop in this field. Namely, the speech codecs of Phase 2, half rate and enhanced FR codec, have been replaced by AMR Codec in Phase 2+. The speech codecs used before used a fixed source/information bit rate that has been optimized for typical radio channel conditions. The problem with this approach was its inflexibility. Whenever the channel conditions were worse than usual, very poor speech quality resulted since the channel capacity assigned to the mobile station is too small for error free transmission. To overcome such problems, Phase 2+ developed a more flexible codec. The AMR codec can improve speech quality by adaptively switching between different speech coding schemes. In other words, AMR has two principles of adaptability: channel mode adaptation and codec mode adaption. These differ significantly mainly when it comes to independent usage. Channel mode adaptation selects the type of Traffic Channel (TCH) (either a FR (TCH/F) or a HR traffic channel (TCH/H) that a connection should be assigned to; moreover, it does it dynamically. Basically, the main idea is to adapt a user´s gross bit rate in order to optimize the usage of radio resources. For an example, if the traffic load in a cell is high, then, those connections that are using a TCH/F and having a good channel quality should be switched to a TCH/H. When the traffic load is low, however, the speech quality of several TCH/H connections can be improved by switching them to a TCH/F (GSM, Switching, Services and Protocols). The switching between full-rate and half-rate channels is realized by an intracell handover [23].

The task of codec mode adaptation is to adapt the coding rate according to the current conditions. In case of a bad radio channel, the encoder operates at low source bit rates at its input and uses more bits for forward error protection. On the other hand, when the channel´s quality is good, not so much error protection is needed. Phase 2+ also offers quite different features for group communication.

For example, group call or “push-to-talk” services with fast connection setup as known from private radio or digital trunked radio systems. Such services are crucial for most closed groups like the police, airport staff, taxi companies etc. The Phase 2+ introduces standardized teleservices that offer functionality for group communication such as the Voice Broadcast Service and Voice Group Call Service. In addition, the Enhanced Multilevel Precedence and Pre-emption Service are used to assign and control priorities to users and their calls (e.g. for emergency calls) [23].

Development was also continued with data services in Phase 2+. The desire for higher data rates in GSM networks was quite logical, since the maximal data rate of 9600bit/s data services in conventional GSM is rather low compared to fixed networks. Two new trends were developed: integration of packet services into GSM networks and a high-bit-rate bearer service with data transmission expected to go up to 10kbit/s, but this speed was not obtained in the end [23]. One of the GSM standardization groups specified the HSCSD service, which required a new generation of mobile stations with increased capabilities and since 1999 some networks started offering HSCSD regularly. Another addition in this field of development was the GPRS, which offered a genuine packet switched bearer service at air interface and was released, in its first phase of standardization, in 1997. Later releases enhanced the GPRS performance and its services, like for example the Release 99 when some new functions like point-to-multipoint services and prepaid services were added. Whereas HSCSD and GPRS can reach a higher data rates because a mobile station can use several time slots of the same Time Division Multiple Access (TDMA) frame and also because new coding schemes are employed, the new Enhanced Data Rates (EDR) for GSM Evolution (EDGE) system works even better. EDGE system replaced the Gaussian Minimum Shift Keying (GMSK) modulation scheme, which has been used in GSM, with an 8-Phase Shift Keying scheme, in order to achieve an approximately three times higher data rate per time slot and thus a higher spectral efficiency [23]. Furthermore, a link adaptation technique started to be used; a technique which dynamically chooses a modulation and coding scheme according to the current radio channel conditions [23]. Additionally, EDGE exists in two alternates for GSM: Enhanced Circuit Switched Data for HSCSD for an example, and Enhanced GPRS.

Concerning supplementary speech services, Phase 2+ brought about some changes and innovations. Some of those new services are for example mobile access hunting, short message forwarding, multiple subscriber profile, call transfer or Completion of Calls to Busy Subscribers (CCBS). The latter one, basically realizes “call back if busy” and if a subscriber does not momentarily accept a call due to an ongoing connection, the subscriber can active this supplementary service named CCBS which makes the network to notify him or her at the end of the called subscriber's ongoing call and automatically set up to the new connection. Moreover, one of the new services included the location service, in Release 99. This made it possible to determine the exact location of a mobile station down to a few meters. The reason for such a service to be developed is the law in the U.S. which demands to locate a person in case of an emergency call [23].

2.2.4. Enhanced Data rates for GSM Evolution (EDGE)

EDGE is a new wireless network technology offering third-generation data rates for the global evolution of GSM and TDMA to 3G. EDGE uses 8 Phase Shift Keying Modulation (8-PSK), rather than normal GSM GMSK, and therefore promotes higher data rates than GPRS. EDGE is designed to merge into existing GSM and TDMA networks, thus allowing operators to offer multimedia and other IP-based services at speeds of up to 384 Kbits/s (possibly 473 Kbits/s in the future) in wide area networks. The broadband internet connection, which EDGE develops for its users and enables them to exploit the multimedia services like emailing, Web infotainment and video conferencing, is easily accessible from wireless terminals. What can also be considered as one of the main advantages of EDGE technology is that it does not involve expense of additional hardware and software technologies. Introducing EDGE normally only requires a software upgrade of the existing GSM/GPRS network. It does not require any new sites or new spectrum, and has no impact on existing cell or frequency plans [24].

GSM operators can, with the help of EDGE's ability to achieve high geographic and population coverage in a short period of time, rapidly target all potential data users. As a result of such possibility, several hundred GSM networks have already upgraded to EDGE.

The performance of EDGE, as experienced by the end-user, depends on a variety of system characteristics. An example of web download may be taken into consideration according to [24]. It consists of multiple requests and downloads of objects and, as a result, the time it takes to download a page depends on the end-to-end round-trip time and user bit-rates in the system, which are the main performance indicators for any packet data system. Usually, performance is assessed by looking at a common set of subscriber applications. Today's state-of-the-art EDGE networks typically offer user speeds of

200kbps, with end-to-end round-trip time (latency) of 150ms. Features like advanced link quality control and persistent scheduling have improved performance significantly over standard GPRS and the first implementations of EDGE [24].

Evolved EDGE is an improved version of EDGE in a number of ways. To begin with, latencies are reduced by lowering the transmission time interval by half (from 20 ms to 10 ms). Bit rates are increased up to 1 Mbit/s peak bandwidth and latencies down to 80 ms using dual carriers, higher symbol rate and higher-order modulation (32QAM and 16QAM instead of 8-PSK), and turbo codes to improve error correction [25]. Lastly, by using dual antennas, improving average bit-rates and spectrum efficiency, signal quality is enhanced. EDGE Evolution can be, according to [25] gradually introduced as software upgrades, taking advantage of the installed base. With EDGE Evolution, end-users will be able to experience mobile internet connections corresponding to a 500 Kbit/s Asymmetric Digital Subscriber Line (ADSL) service. Furthermore and according to [24], different services may have varying performance requirements in different areas, but EDGE Evolution is expected to improve the perceived performance across all services by:

- Reducing latency to improve the user experience of interactive services and also to enhance support for conversational services such as multimedia telephony.
- Increasing peak and mean bit rates, to improve best-effort services such as web browsing or music downloads.
- Improving spectrum efficiency, which will particularly benefit operators in urban areas where existing frequency spectrum is used to its maximum extent – traffic volume can be increased without compromising service performance or degrading perceived user quality.
- Boosting service coverage, for example by reducing interference or allowing more robust services. Increased terminal sensitivity improves coverage in the noise limited scenario

2.2.5. GSM Radio System Description

After an historical context overview about GSM, this section is going to introduce some of the principles of GSM radio communication, its channel structure and basic functionality, such as frequency hopping and power control. These basic concepts for GSM radio communications, give a good understanding of GSM's structure that is required for this dissertation.

2.2.5.1. Channel Structure

The GSM standard is based on a Multi-Carrier, Time-Division Multiple Access and Frequency Division Duplex, MC/TDMA/FDD [26]. Table 1 represents the frequency bands that have been defined for GSM around the world.

GSM has a carrier spacing of 200 kHz allowing, for example, 124 and 374 radio frequency channels in the 900 and 1800 MHz bands respectively. Each radio frequency is time divided into TDMA frames of 4.615ms. Each TDMA frame is subdivided into eight full slots. Each of these slots can be assigned to a FR TCH, two HR TCHs or one of the control channels. A slot is equal to one timeslot (TSL) on one frequency [1]. Figure 4 represents the time and frequency structure mentioned above.

Table 1 - GSM standardised frequency bands [1]

GSM frequency band	*Available Frequencies*	*Where available*
400 MHz	450.4-457.6 MHz paired with 460.4-467.6 MHz or 478.8-486 paired with 488.8-496MHz	Europe
800 MHz	824-849 MHz paired with 869-894 MHz	America
900 MHz	880-915 MHz paired with 925-960 MHz	Europe, Asia Pacific, Africa
1800 MHz	1710-1785 paired with 1805-1880 MHz	Europe, Asia Pacific, Africa
1900 MHz	1850-1910 paired with 1930-1990 MHz	America

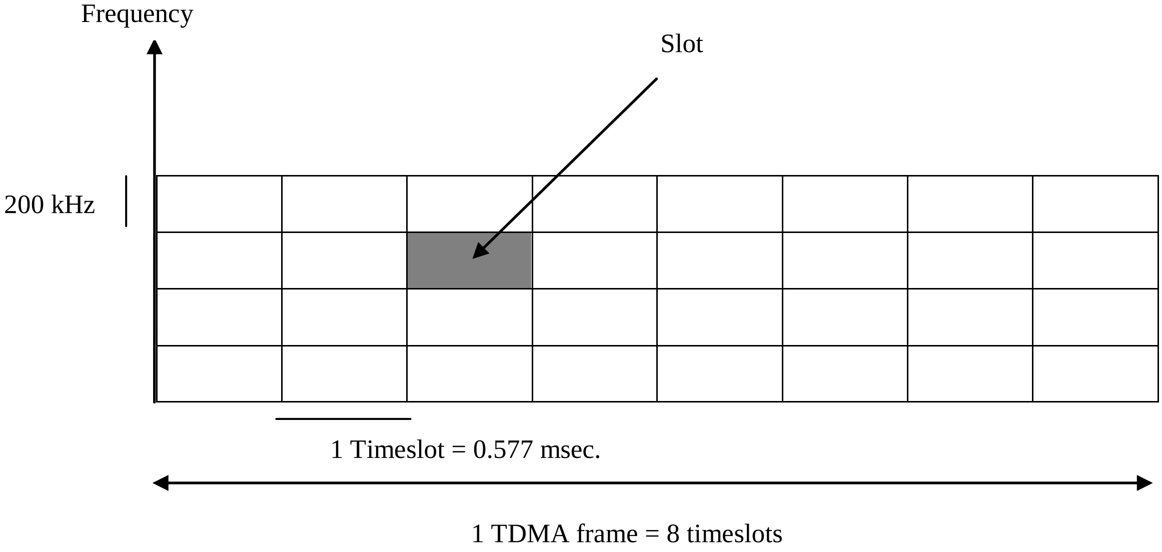
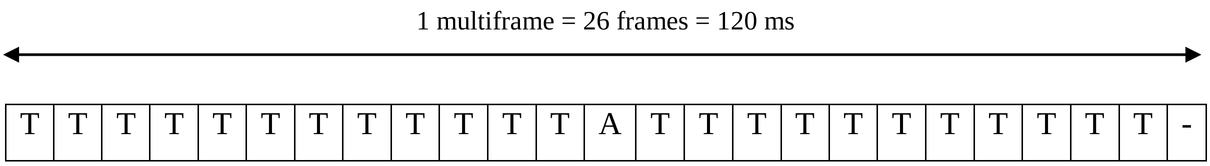


Figure 4 - The multiple access scheme in GSM [1]

The data transmitted in one of the slots is designated as a burst. According to [2] there are five different types of bursts: the normal burst, the access burst, the frequency correction burst, the synchronization burst and the dummy burst.

Channels can be described at two levels, the physical and the logical level, which confine the format and information of the individual bursts depending on the type of channel that it belongs to. When it comes to the physical channel, this one corresponds to one timeslot on one carrier, while a logical channel refers to the specific type of information carried by the physical channel. Different logical channels carry different kind of information, being then mapped or multiplexed on physical channels. According to [1] logical channels can be divided into two groups: control channels and TCHs. User data is carried by traffic channels that can be either speech or data. A logical TCH for speech and circuit-switched data in GSM is designed by TCH that can be either full rate (TCH/F) or half rate (TCH/H). A logical TCH for packet-switched data is called as Packet Data Traffic Channel (PDTCH). In order to support speech and data communication the TCH channels support bi-directional transmission. A PDTCH/F corresponds to the resource allocated to a single mobile station on one physical channel for user data transmission and a PDTCH/H correspond to the resource allocated to a single mobile station on half a physical channel for user data transmission. Hence the maximum instantaneous bit rate for a PDTCH/H is half than for a PDTCH/F. When it comes to uplink (PDTCH/U), for a mobile-originated packet transfer or downlink (PDTCH/D) for a mobile-terminated packet transfer, all packet data traffic channels are unidirectional. One of the logical channels type, the control channel, carries signaling and controlling information and in GSM, there are common as well as dedicated control channels. Several combinations of the different channels are possible. Figure 5 presents the organization of the TCH/F speech channel and the corresponding Slow Associated Control Channel (SACCH). This 26-frame multiframe organization considers one timeslot per TDMA frame and of the 26 frames, 24 are used for traffic. One of those 26 frames is used for the SACCH channel, and the last one is an idle frame. This idle frame considers a time interval period where a mobile can receive other control channels and measure the received signal level from neighboring cells.



T: TDMA frame for TCH

A: SACCH frame for TCH

-: idle frame

Figure 5 - Organization of TCH and the corresponding control channels [2]

Figure 6 represents the complete GSM frame, timeslot and burst structure. This structure is mainly based on Multiframes. Multiframes are frames that are grouped or linked together in order to perform specific tasks. On GSM system, Multiframes are used to established schedules for specific purposes, such as coordinating with frequency hopping patterns. Multiframes used in the GSM system include two important frames, the 26 traffic multiframe and the 51 control multiframe [27].

Traffic Multiframe Structures - The 26 traffic multiframe structure is used to send information on the traffic channel. The 26 traffic multiframe structure is used to combine user data (traffic), slow control signaling (SACCH), and idle time period. The idle time period allows a mobile device to perform other necessary operations such as monitoring the radio signal strength level of a beacon channel from other cells.

Control Multiframe Structures - The 51 control multiframe structure is used to send information on the control channel. The 51 frame control multiframe is sub divided into logical channels that include the frequency correction burst, the synchronization burst, the Broadcast Control Channel (BCCH), the Paging and Access Grant Channel (PAGCH), and the Stand-alone Dedicated Control Channel (SDCCH).

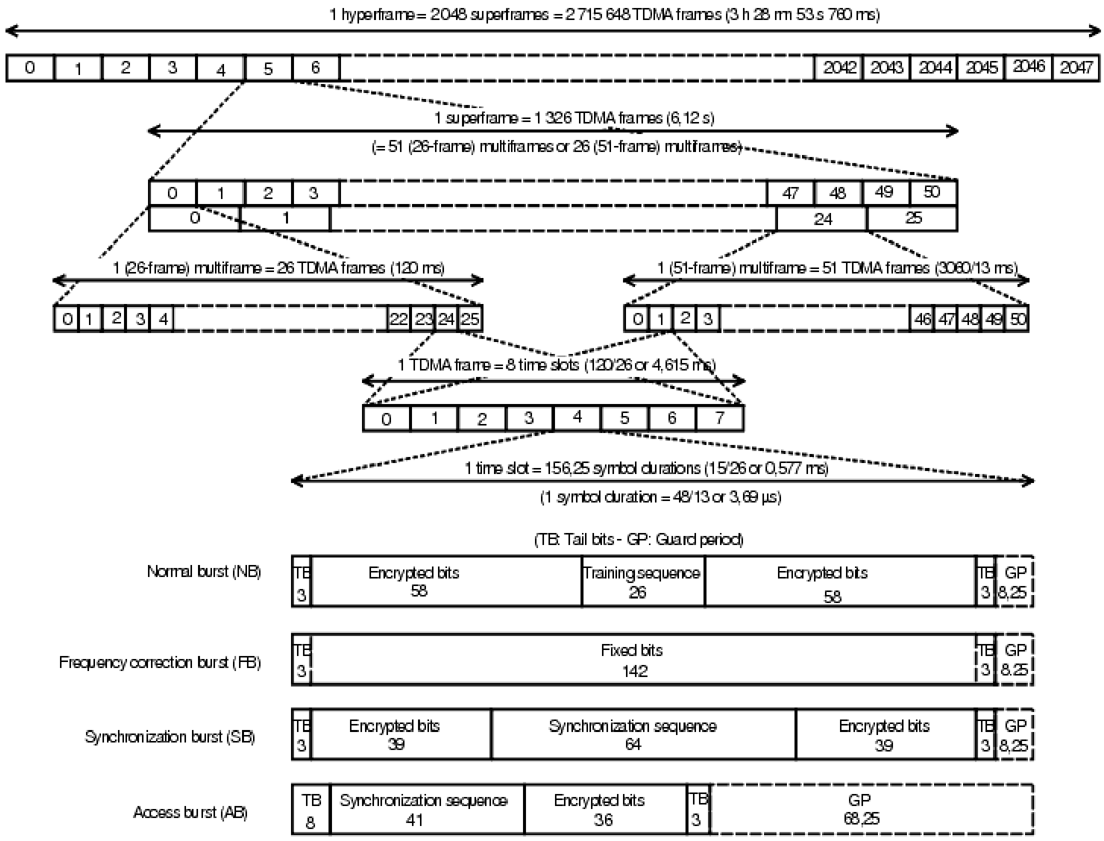


Figure 6 - Time Frames, Time Slots and Bursts in GSM [28]

2.2.5.2. Transmitting and Receiving Chain

After presenting the main GSM structure, the transmission and receiving processes are an important factor to consider in this dissertation. Several processes from the data preparation, to the data transmission and to the receiving data treatment, have to be performed in order to convert a speech signal into a radio signal and back. Figure 7 shows the transmitting and receiving chain of a GSM receiver. According to [29] some operations take place on the transmitting side:

- Source coding. Converts speech from an analogue signal into a digital equivalent.
- Channel coding. Redundancy is introduced by adding extra bits into the data flow, increasing its rate by adding information calculated from the source data, in order to allow detection or even correction of bit errors that may be introduced during transmission.
- Interleaving. Induces a mixing up the bits of the coded data blocks. The main purpose of this is to have adjacent bits in the modulated signal spread out over several data blocks.

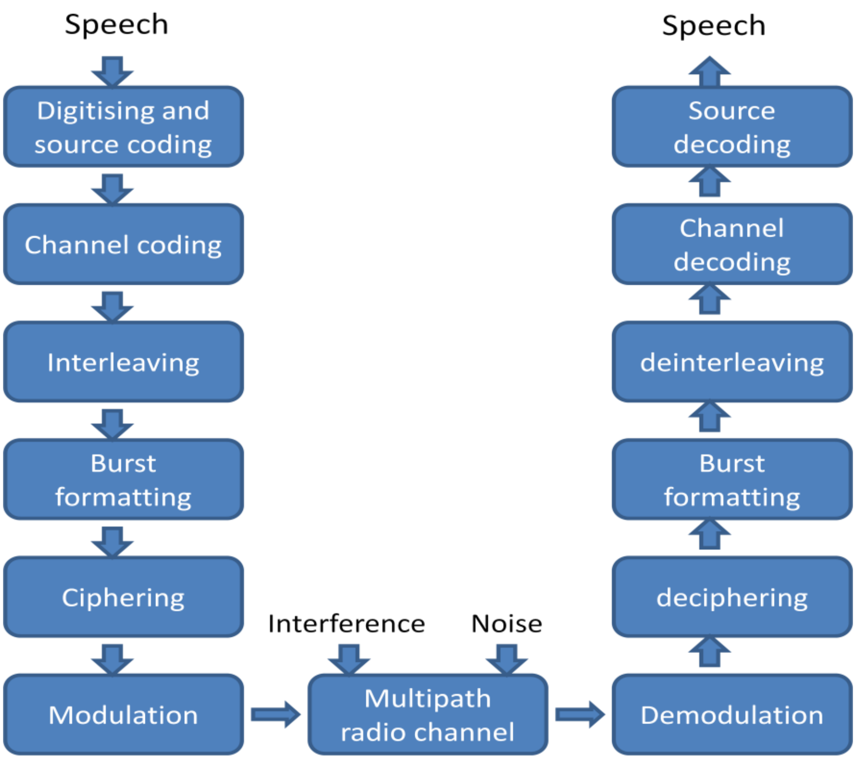


Figure 7 - Flow diagram of the link operations according to [1]

The fact that error probability of successive bits in the modulated stream is typically highly correlated, and the channel coding performance is better when errors are decorrelated, according to [1], interleaving improves the coding performance by decorrelating errors and their position in the coded blocks. With this, the following blocks represent important processes in order to best perform when transmitting the intended data.

- Ciphering. Changes the contents of these blocks by having a secret code which is known only by the mobile station and the base station.
- Burst formatting. Adds synchronization and equalization information to the ciphered data.
- Modulation. Transforms the binary signal into an analogue signal at the right frequency so that the signal may be transmitted as radio waves.

When it comes to the receiver side, this one performs the reverse operations as follows [1]:

- Demodulation. Transforms the radio signal received at the antenna into a binary signal.
- Deciphering. Modifies the bits by reversing the ciphering code known.
- Deinterleaving. Puts the bits of the different bursts back in order to rebuild the original code words.
- Channel decoding. Tries to reconstruct the source information from the output of the demodulator, using the added coding bits to detect or correct possible errors, caused between the coding and the decoding.
- Source decoding. Converts the digitally decoded source information into an analogue signal to produce the speech that was initially produced.

The reordering and interleaving process mixes the encoded data block of 456 bits, and groups the bits into eight sub-blocks (half bursts). The eight sub blocks are transmitted on eight successive bursts [1]. Figure 8 represents the channel coding process and Figure 9 represents the reordering and interleaving process.

The mistakenly received bits tend to have a bursty nature due to multipath propagation. With this, the convolutional code provides the best performance for random positioned bit errors, and therefore reordering and interleaving is introduced in the GSM signal transmission flow. However, the reordering/interleaving only improves the coding performance if the eight successive bursts carrying the data information of one speech block are exposed to uncorrelated fading. This can be ensured either by spatial movement (high user speed) or by frequency hopping [30].

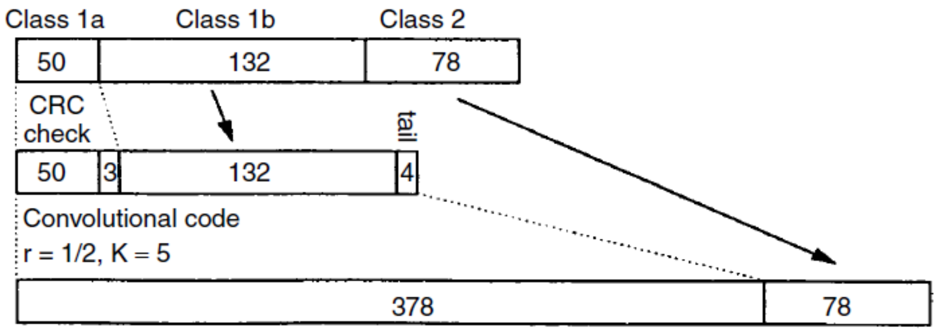


Figure 8 - Channel coding process

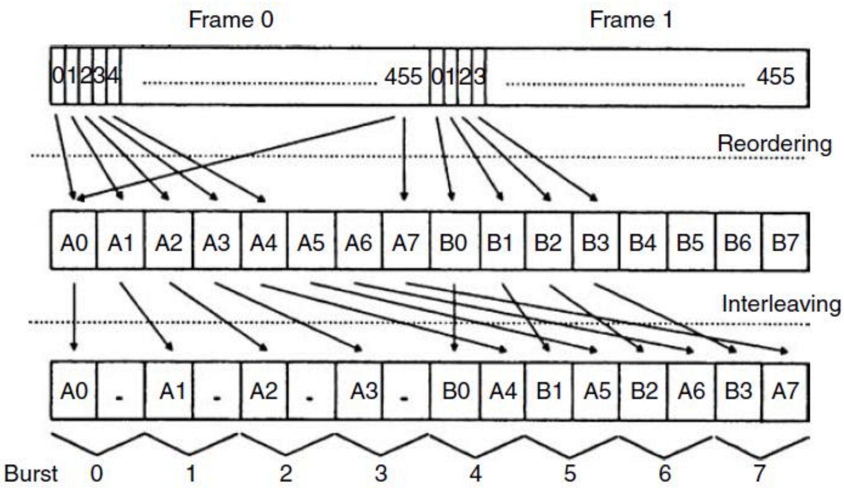


Figure 9 - Reordering and interleaving process

2.2.6. GSM Power Control

Power control (PC) is a set of strategies or techniques required, that allows the adjustment of the transmitted power. Power control adjusts the transmitted power in order to achieve the desired signal strength. The main question asked is: Why do we need to control the power level? There are several reasons for power control in GSM. The increasing battery life of the mobile phones is one of them, and enabling power control generally decreases interference in a network.

If a mobile finds itself far away from a base station, it will require a stronger transmitted signal than a mobile close to a base station. One way of improving the quality of the system is by decreasing the signal strength for one mobile, if it has speech quality better than necessary, hence an interference reduction will be stated. With this, the mobile will also experience a decrease in battery consumption when transmitting to the base station. PC is used in uplink and in downlink between base station and mobile and for both, the principles are similar. Figure 10 presents a common scenario in nowadays mobiles, where each mobile receives a carrier signal power C and interference I. The transmission power p from the base station to the mobile should be controlled to optimize the power transmitted. The power needs to be high enough to achieve a sufficient carrier signal power C at the mobile station and low enough to minimize interference I at other mobiles. Each GSM network has its own power control algorithm, to control the transmitted powers from the base stations to the mobiles [31].

GSM defines five classes of mobile stations, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 W. In order to minimize co-channel interference and to conserve power, both the mobiles and the Base Transceiver Station (BTS) transmits at the lowest power level but with an acceptable signal quality. Power levels can be stepped up or down in steps of 2 dB from the peak power for the class, to a minimum of 13 dBm (20 mW) [32].

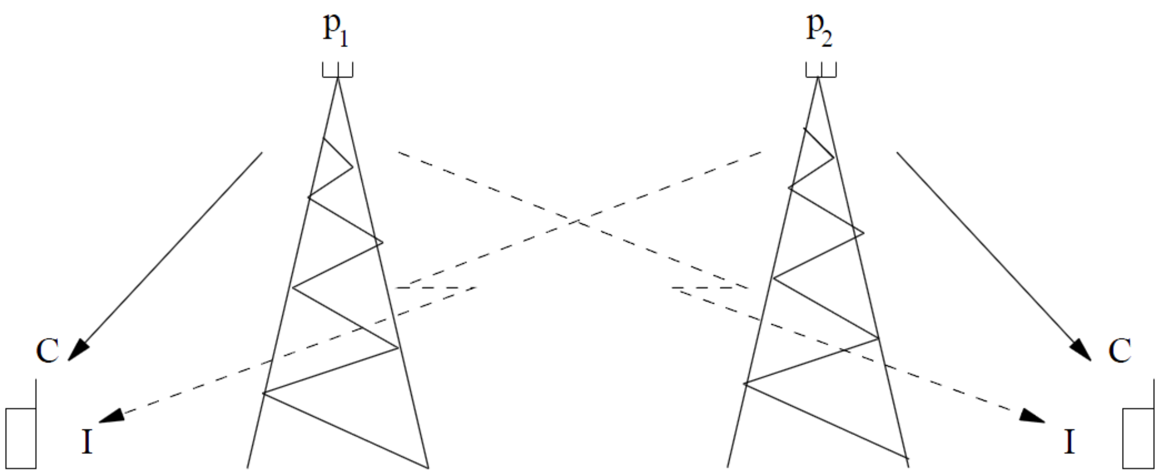


Figure 10 - Transmission power p1 and p2 from base stations to mobile stations [31]

In order to make use of available resources in cellular radio systems the control of the transmitted powers, as mentioned above, is required. Maintaining a certain quality, in other words an acceptable C/I, throughout the lifetime of a connection is the main goal. Power control optimizes the transmitted power, hence increasing the number of satisfied users if traffic is maintained or even if the traffic is increased [33]. The use of power control reduces the total amount of radiated power compared to when it is not used [31].

With this, the maintenance of an acceptable level of quality is possible, despite the variation of channel conditions and interference from other users. When it comes to quality, the existing power control algorithm only considers the system quality and not the quality for individual mobile users as the main regulating factor. This implies that some mobiles have to assume slightly worse quality in order to improve the total system quality. However, when applying power control to real systems, some challenges are defined. Available information in measurement reports is basic, highly quantized and constrained to physical limits. So one challenge is to issue relevant power levels and based on this information to obtain an acceptable quality [34].

2.3. Universal Mobile Telecommunication System (UMTS)

UMTS is a 3G mobile systems broadband, a packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps) [35]. This system based on Wideband Code Division Multiple Access (WCDMA) radio technology, has the following modes Frequency Division Duplex (FDD) and Time Division Duplex (TDD) for Europe, and in the EUA the cdma2000 is also based on CDMA. This technology shows some advantages has a technology and when comparing it with GSM. Some of these advantages are, adaptive antennas (already used in 2G technology), diversity when transmitting with space-time codes receiving, multi-user detection, greater spectral efficiency and higher bandwidth than GSM.

All in all, UMTS brings new considerations in terms of study, since its transmission is done in a different way from GSM. The following sub chapters provide an overview about UMTS transmission and why is it important for this dissertation.

2.3.1. Spread Spectrum

The demand for new and efficient communication is leading system planners to use several techniques that can bring an extra advantage to nowadays “old” technology. One of these techniques is called spread spectrum. Security, multipath rejection and multiple accessing capabilities are some attributes of the spread spectrum waveform design, making spread spectrum very competitive for a variety of commercial applications, in particular, for mobile units.

Spread Spectrum (SS) techniques are considered to be methods in which energy generated at a narrow band is spread over a wide bandwidth. Figure 11 represents a basic spread spectrum technique. This technique is used to achieve transmission, robust against channel impairments, to be able to resist natural interference or jamming and to prevent hostile detection. The techniques are said to be spread spectrum if transmission bandwidth is much greater than minimum bandwidth needed for transmitting information. According to Bernard Sklar, to achieve spread spectrum, the system needs to fulfill the following requirements [36]:

- Signal occupies higher bandwidth than the minimum bandwidth necessary to send information.
- Spreading is accomplished by means of spreading code signal which is independent of the data.
- At the receiver, despreading is accomplished by the correlation of the received spread signal with a synchronized replica of the spreading code used to spread information.

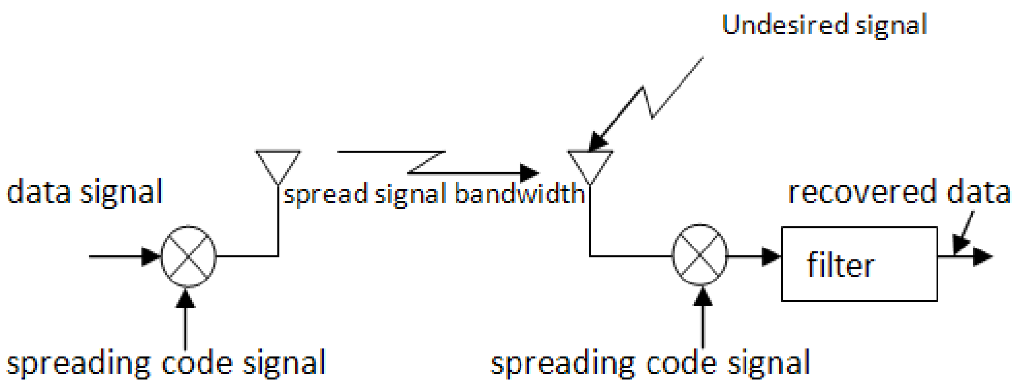


Figure 11 - Model of basic spread spectrum technique [36]

The fact that SS signals present gain in SNR at the end of the system (before the filter in Figure 11), allows SS signals to be transmitted at a much lower power density than narrow band transmitters. The lower transmitted power density characteristic is a great advantage for SS signals. The main interest in spread spectrum comes from the fact that SS and narrowband signals can occupy the same band, with little or no interference. SS signals are hard to detect on narrow band equipment because the signal's energy is spread over a bandwidth of N times the information bandwidth [37]. The SS signals are able to resist interference and jamming and the bottom center behind interference rejection capability of SS is achieved by [36]:

- Multiplying signal by spreading signal once spreads the signal bandwidth.
- Multiplying signal by spreading signal twice recovers original signal.
- Desired signal gets multiplied twice and interference gets multiplied only once, and that makes interference as spread noise and the signal of interest as narrowband with much more power density.

Conventional modulation schemes such as frequency modulation and pulse code modulation also spread the spectrum of an information signal, but they do not qualify as SS systems since they do not satisfy all the conditions as outlined. SS techniques are implemented where transmission has to be operated without information being detected by anyone other than the intended receiver. Communications systems designed for this task is known as Low Probability of Detection (LPD) or Low Probability of Intercept (LPI) filter. SS systems that are designed to present LPI may also be designed to expose Low Probability of Position Fix (LPPF), even if the presence of the signal may be perceived, direction of the transmitter is difficult to pinpoint. Afterwards they can present Low Probability of Signal Exploitation (LPSE) which means that identification of the source is hard to determine. The main idea of these systems is, by using minimum signal power and optimum signaling scheme, results in a minimum probability of being detected, intercepted or demodulated. SS uses wide band, noise-like signals and because the signals are noise-like, they are hard to detect. Spread spectrum techniques use spreading code signals, called pseudorandom or pseudonoise codes to perform spreading and despreading on the signal itself. Pseudorandom codes are called like this because they are not random at all. They are deterministic periodic signals that are known to both transmitter and receiver. Even though these mentioned signals are said to be deterministic, they present randomness properties and that appear random to common users [36].

2.3.2. Spreading Techniques

In terms of spread spectrum transmission, the original information signal, which occupies a bandwidth of B Hz, is transmitted after spectral spreading to a bandwidth N times higher, where N is known as the processing gain [38]. Figure 12 presents the frequency-domain spreading concept representing the idea behind spread spectrum transmission. The power of the transmitted spread spectrum signal is spread over N times the original bandwidth, while its spectral density is correspondingly reduced by the same amount. Hence, the processing gain is given by [39]:

$$N = \frac{B_s}{B}$$

Equation 1

where B_s is the bandwidth of the spread spectrum signal while B is the bandwidth of the original information signal.

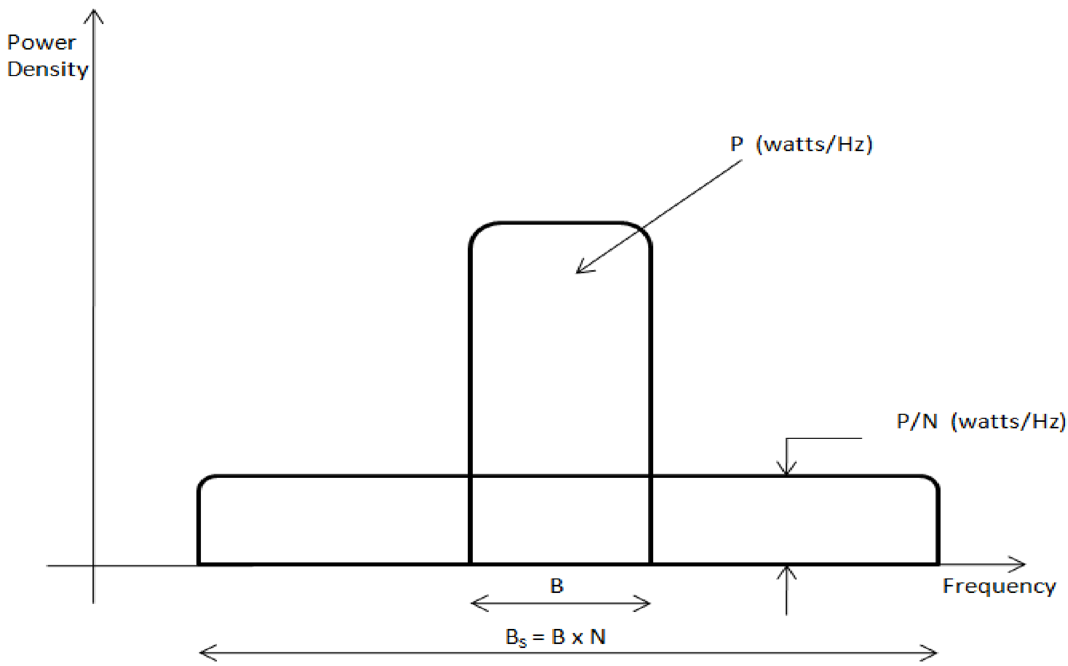


Figure 12 - Power spectral density of signal before and after spreading

The spreading technique consists basically of a series of spreading and modulating operations with a defined initial data, using a spread-spectrum code, getting the energy of the initial signal to lower significantly (Figure 13). Afterwards the data is transmitted through a proper channel with an RF carrier.

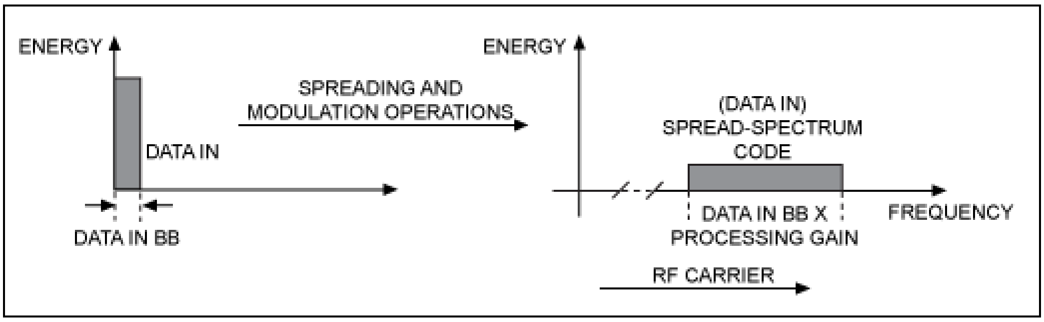


Figure 13 - Spreading operation spreads the signal energy over a wider frequency bandwidth [40]

The despreading operation consists of reversing the system. The signal received is returned to its initial form with the spread-spectrum code which involves a series of operations for despreading and demodulating the signal (Figure 14).

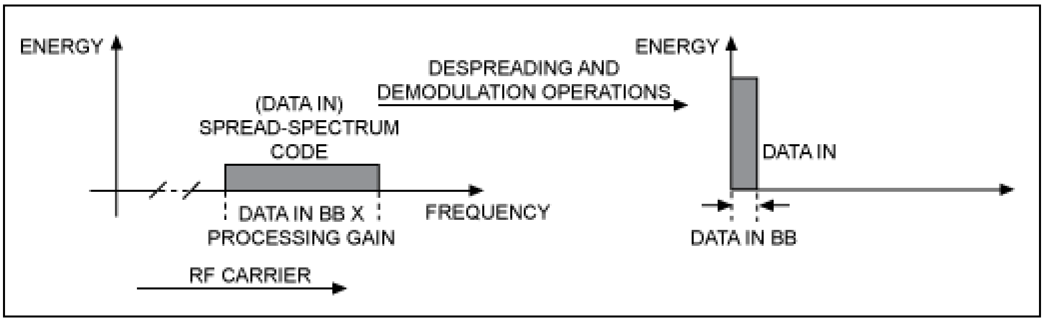


Figure 14 - The despreading operation, recovering the original signal [40]

Spread spectrum techniques can be classified into two main categories namely frequency hopping spread spectrum, direct sequence spread spectrum and the combination of two of the two techniques.

- **Frequency Hopping** (FH) SS systems
- **Direct Sequence** (DS) SS systems

FH and DS are the most commonly used, even though there are variations of these two. The following sub chapters will give an overview of these techniques.

2.3.2.1. Frequency Hopping

Frequency Hopping Spread Spectrum (FHSS) technique is based on sending its transmissions through a different carrier frequency at different times. The FHSS carrier is going to hop on a predetermined, pseudo random pattern previously defined [41].

FHSS radios have the limitation of being able to send only small amounts of data on each channel for a selected time period before the need to hop to the next channel in the sequence. Upon each "hop", the device must re-synchronize with the other radio before it can resume any data transmission. The purpose of the pseudo-random hopping pattern use is to avoid interfering signals by not spending very much time on any specific frequency and to define each "hop" done. Even if interference is found on any of the channels in the hopping pattern, the small amount of time spent transmitting on that frequency will minimize the interference done on the transmission [41].

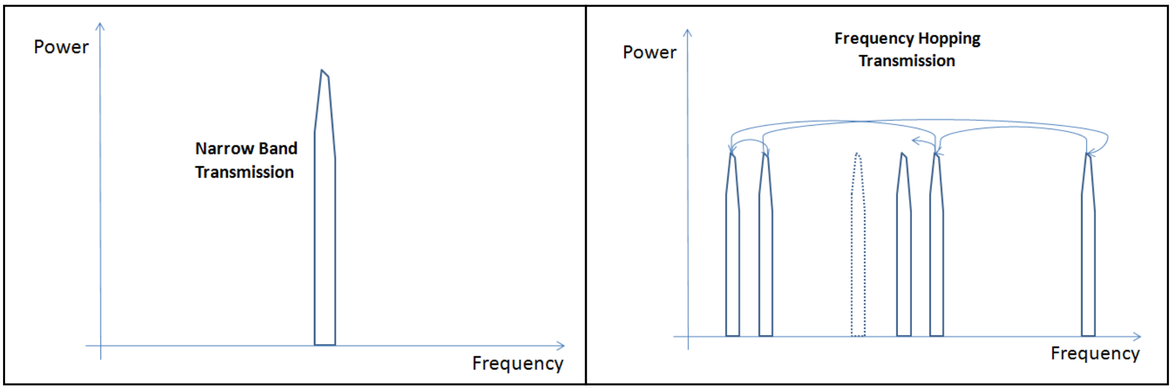


Figure 15 - Frequency Hopping technique

2.3.2.2. Direct Sequence Modulation

Direct Sequence Spread Spectrum (DSSS) uses a carrier which remains fixed to a specific frequency band. Instead of the data signal being transmitted on a narrow band, this one is spread on a much larger range of frequencies (RF bandwidth) using a specific code (Figure 16). This code is designated as Pseudo-Noise (PN) sequence. The narrowband signal and the spread spectrum signal both use the same amount of transmit power and carry the same information. However, the power density of the spread spectrum signal is much lower than the narrowband signal, which results in a hardest detection on the presence of the spread spectrum signal. Hence DSSS devices provide a secure communications link [41].

A pseudo-random number multiplied with the symbol information from the data stream results in a signal which is spread over a much larger amount of bandwidth than would normally be used for data transmission but with a much lower power level. A gain factor is present in this type of systems, transmitting many fully redundant copies, as the number of chips of the pseudo-random number, of the initial data at the same time. This factor provides resistance to interference from other signals. Even though the signal is emitted multiple times, the equipment must receive only one of the signals. The existence of interference in the band will make the DSSS system to take partial transmissions from any number of the redundant transmission and assemble them together properly. This comes has a very valuable and reliable advantage of the DSSS systems [36].

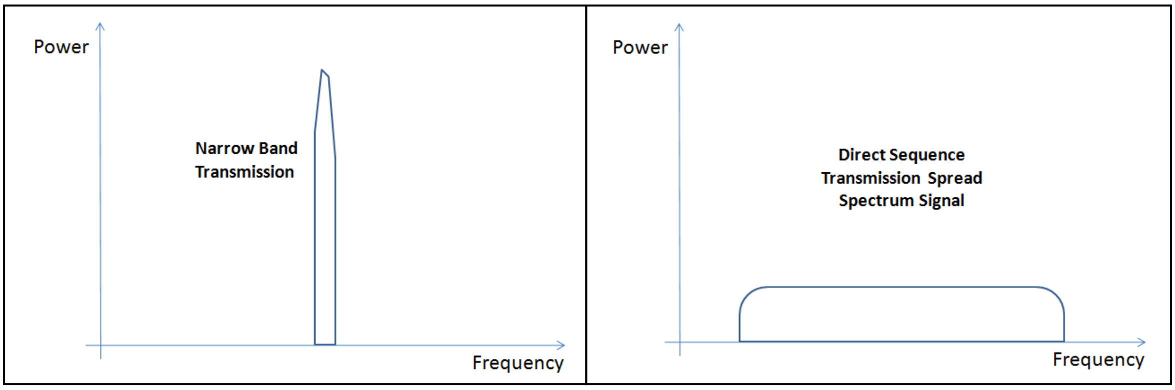


Figure 16 - Direct Sequence technique (Spreading Operation)

The presence of an interfering signal in the same band, it will usually show as a higher power, narrow band signal. Besides the processing gain of the DSSS devices, the interference will be spread out during the de-spreading process. The despreading process causes a dramatic reduction of the power density of the interference (Figure 17) [36].

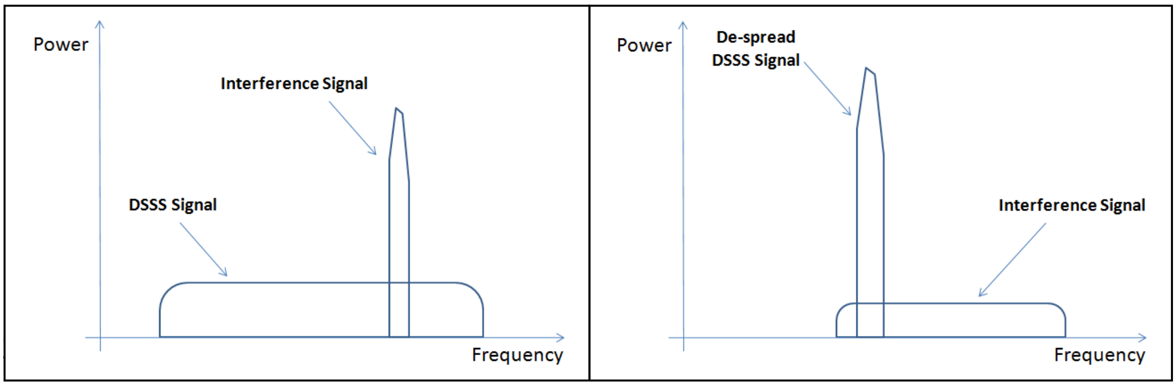


Figure 17 - Direct Sequence technique (De-spreading Operation)

The selection of multiple access schemes arises as an important issue when designing and standardizing cellular systems. Multiple access comprises three basic principles, FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access), and CDMA (Code Division Multiple Access). The three principles enable multiple users to share the same physical channel. However, the two competing technologies differ in the way user shares the common resource. TDMA enables users to share the same frequency channel by dividing the signal into different time slots in order to increase the amount of data that can be carried for transmitting and receiving over the channel. CDMA uses a spread spectrum technology which involves spreading the information contained in a particular signal of interest over a much greater bandwidth than the original signal. In TDMA, users can only transmit in their respective time slot. Unlike TDMA, in CDMA each user can transmit their spread signal superimposed on others over the channel, at the same time and frequency [42].

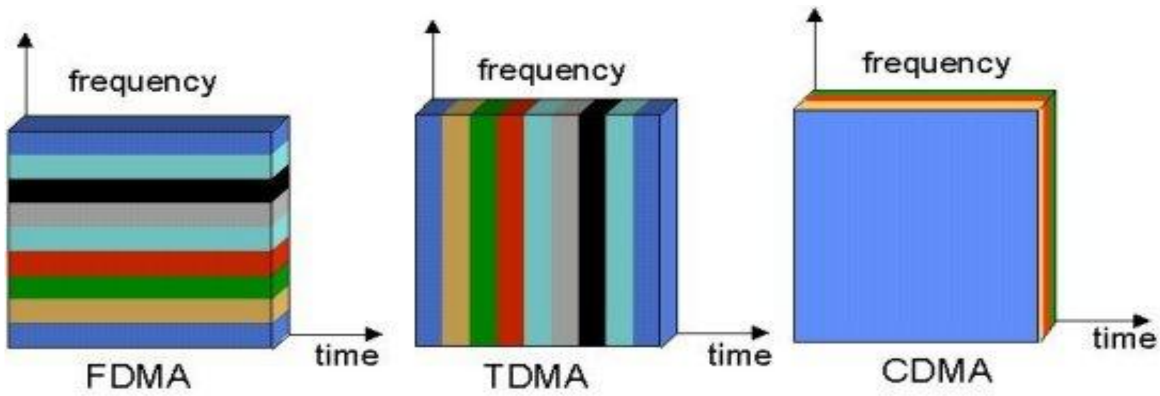


Figure 18 - Multiple Access Schemes [43]

All users can transmit at the same time, and each is allocated the entire available frequency spectrum for transmission.

In CDMA each user:

- Has its own PN code
- Uses the same RF bandwidth
- Transmits simultaneously (asynchronous or synchronous)

CDMA as a method of multiplexing (wireless) users by distinct (orthogonal) codes, uses unique spreading codes to spread the baseband data before transmission. That way the signal is transmitted in a channel, which can be below noise level at the reception. The receiver then uses a correlator, or in equivalently a Matched Filter to dispread the wanted signal. This operation corresponds to multiplying the signal with the Spreading Sequence, with the Integrator and with the Symbol Sampler, represented on the receptor in Figure 19. The superimposed signal will not be despread.

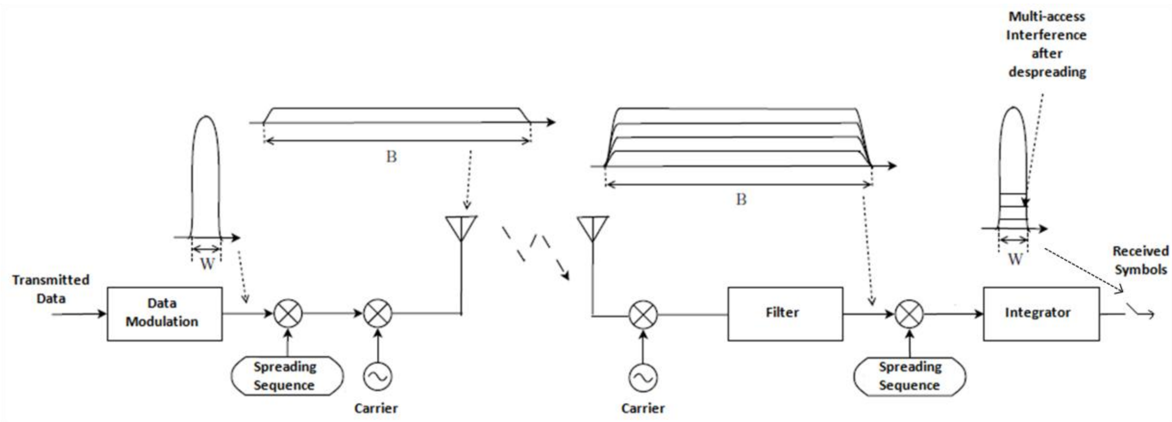


Figure 19 - Simplified CDMA system [44]

CDMA is also regarded as interference limited multiple access system. Since all users transmit on the same frequency, internal interference generated by the system is the most significant factor in determining system capacity and call quality according to [43]. Although the transmit power for each user must be reduced to limit interference, it should still have enough power to maintain the required SNR for a satisfactory call quality.

One of the main advantages of CDMA systems is their ability of using arriving signals in the receivers with different time delays. This is regarded as multipath. Unlike CDMA, FDMA and TDMA are narrow band systems and they cannot discriminate between the multipath arrivals, but they opt for using equalization to mitigate the negative effects of multipath. On the other hand, CDMA uses the multipath signals and combines them to make an even stronger signal at the receivers.

WCDMA is one of the main technologies for the implementation of 3G cellular systems. It is the multiple access method selected by ETSI as basis for UMTS air interface technology. Wideband CDMA is an extension of CDMA architecture using a large bandwidth of at least 5 MHz, and it has more advanced characteristics than the second generation CDMA systems. For example according to [45], some of the WCDMA features are:

- Radio channels are 5MHz wide.
- Chip rate of 3.84 Mcps
- Supports two basic modes of duplex: frequency division and time division. Current systems use frequency division, one frequency for uplink and one for downlink. For time division, Freedom of Mobile Multimedia Access (FOMA – 3G System in Japan) uses sixteen slots per radio frame, whereas UMTS uses fifteen slots per radio frame.
- Employs coherent detection on both the uplink and downlink based on the use of pilot symbols and channels.
- Supports inter-cell asynchronous operation.
- Variable mission on a 10 ms frame basis.
- Multicode transmission.
- Adaptive power control based on SIR (Signal-to-Interference Ratio).
- Multiuser detection and smart antennas can be used to increase capacity and coverage.
- Multiple types of handoff (or handover) between different cells including soft handoff, softer handoff and hard handoff

In 3GPP, WCDMA is called Universal Terrestrial Radio Access (UTRA). As mentioned above, WCDMA has two basic modes of operation: FDD and TDD. According to [43], these two modes have the following characteristics, and where some of them are mentioned in Chapter 4 being the ones taken into account for this dissertation:

FDD:

Frequency band: 1920 MHz -1980 MHz and 2110 MHz - 2170 MHz (Frequency Division Duplex) UL and DL

Minimum frequency band required: ~ 2x5MHz

Carrier Spacing: 4.4MHz - 5.2 MHz

Maximum number of (voice) channels on 2x5MHz: ~196 (spreading factor 256 UL, AMR 7.95kbps) / ~98 (spreading factor 128 UL, AMR 12.2kbps)

Channel coding: Convolutional coding, Turbo code for high rate data

Duplexer needed (190MHz separation), Asymmetric connection supported

Receiver: Rake

Receiver sensitivity: Node B: -121dBm, Mobile -117dBm at BER of 10^{-3}

Data type: Packet and circuit switch

Modulation: QPSK

Pulse shaping: Root raised cosine, roll-off = 0.22

Chip rate: 3.84 Mcps

Channel raster: 200 kHz

Maximum user data rate (Physical channel): ~ 2.3Mbps (spreading factor 4, parallel codes (3 DL / 6 UL), 1/2 rate coding), but interference limited.

Maximum user data rate (Offered): 384 kbps (year 2002), higher rates (~ 2 Mbps) in the near future. HSPDA will offer data speeds up to 8-10 Mbps (and 20 Mbps for MIMO systems)

Channel bit rate: 5.76Mbps

Frame length: 10ms (38400 chips)

Number of slots / frame: 15

Number of chips / slot: 2560 chips

Power control period: Time slot = 1500 Hz rate

Power control step size: 0.5, 1, 1.5 and 2 dB (Variable)

Power control range: UL 80dB, DL 30dB

Mobile peak power: Power class 1: +33 dBm (+1dB/-3dB) = 2W; class 2 +27 dBm, class 3 +24 dBm, class 4 +21 dBm

Physical layer spreading factors: 4 ... 256 UL, 4 ... 512 DL

TDD:

Frequency band: 1900 MHz -1920 MHz and 2010 MHz - 2025 MHz (Time Division Duplex) Unpaired, channel spacing is 5 MHz and raster is 200 kHz. Tx and Rx are not separated in frequency, but by guard period.

Minimum frequency band required: ~ 5MHz, ~ 1.6MHz with 1.28 Mcps

Voice coding: AMR (and GSM EFR) codec

Channel coding: Convolutional coding, Turbo code for high rate data

TDMA frame consist of 15 timeslots

Each time slot can be transmit of receive

Duplexer not needed

Asymmetric connection supported

Data by packet and circuit switch

QPSK modulation

Receiver: Joint Detection, (mobile: Rake)

Chip rate: 3.84 Mcps, 1.28 Mcps or 7.68 Mcps

Channel raster: 200 kHz

Maximum RF ch bit rate (kbps): ~ 3.3Mbps (1/2 rate coding, spreading factor 1, 15 timeslots, ex overheads), but interference limited

Frame length: 10ms

Number of slots / frame: 15

Power control period: 100 Hz or 200 Hz UL, ~ 800 Hz DL

Power control step size: 1, 2, 3 dB (Variable)

Power control range: UL 65dB, DL 30dB

Mobile peak power: Power class 1: +33 dBm (+1dB/-3dB) = 2W; class 2 +27 dBm, class 3 +24 dBm, class 4 +21 dBm

Number of unique base station identification codes: 512/frequency

Physical layer spreading factors: for 1.28 Mcps – 1, 2, 4, 8, 16
for 3.84 Mcps – 1, 2, 16
for 7.68 Mcps – 2, 4, 32

WCDMA link-level simulations are over 10 times more compute-intensive than second-generation simulations. In WCDMA interface, different users can simultaneously transmit at different data rates and data rates can even vary in time. UMTS networks supports all current second generation services and numerous new applications and services [43].

2.3.4. UMTS Power Control

According to [46], tight and fast power control is probably the most important aspect in WCDMA, particularly on the uplink. Without it, a single overpowered mobile could block a whole cell.

Sharing the same portion of spectrum during the entire of acceding to the base station comes as one of the problems of CDMA system. If all the users transmit at the same time with the same frequency, each one of them becomes interference for the rest.

Unlike GSM, UMTS has a greater need to combat the near-far problem, since transmitters share transmission frequencies and transmission time (Figure 20). With UE1 and UE2 operating on the same frequency, being only separable at the base station by their respective spreading codes, it may happen that UE1 at the cell edge suffers a path loss, for example 70 dB above UE2 which is near the Base Station (BS). If there was no mechanism for UE1 and UE2 to be power-controlled to the same level at the base station, UE2 could mask UE1 and could block a large part of the cell [47].

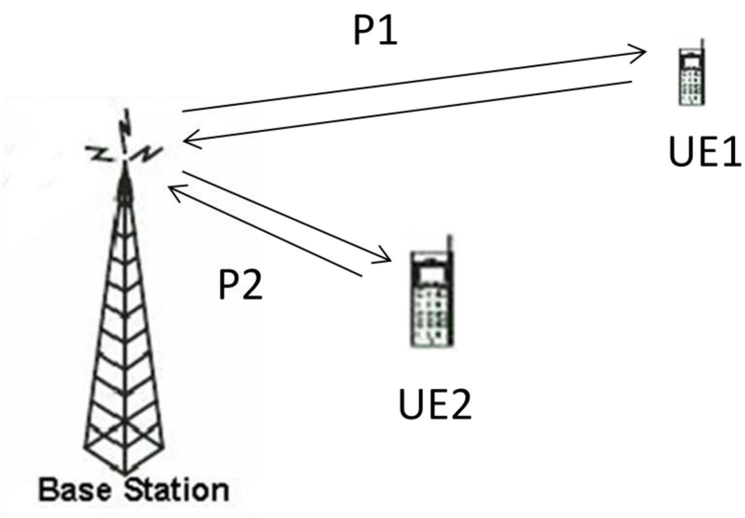


Figure 20 - Near-far problem in CDMA

In a natural environment channel conditions vary in the short and the long term. With this and according to [47], two main power control mechanisms in UMTS are used. The first one is:

- Open loop power control. This is related directly to the path loss. This control has no feedback. It simply sets the initial power at the UE should transmit. This initial setting happens via Radio Resource Control (RRC) signaling. This control finds itself in the UE and the Radio Network Controller (RNC).

Open-loop power control is a mechanism which tries to estimate the transmission path loss by means of the strength of the received signal. Through research this method proved to be inaccurate and the main reason it does not work, is that the fast fading in uplink and downlink is uncorrelated because of the large frequency separation of the respective bands in WCDMA FDD mode. Open-loop power control is used however in UMTS but only to provide a loose initial value for the power settings at the transmitters [47].

And the second, as the solution implemented for UMTS, is a so called closed-loop power control, which is based on a double control loop. This double control loop is divided in Outer Loop Power Control (OLPC) and Inner Loop Power Control (ILPC), described as it follows:

- Outer loop power control. This is related to long term variations of the channel. The base station performs frequent estimations of the received SIR (Signal-to-Interference Ratio) and compares to a target SIR. With a target SIR specified, in order to adjust, if the received SIR is less than this target, transmit power needs to be increased, otherwise it needs to be decreased [48]. OLPC is a mechanism to control the SIR target value the ILPC should be locked on. This mechanism aims to provide the desired Quality of Service (QoS) in terms of Block Error Ratio (BLER). If the received signal is better than required, the SIR target can be lowered so that it meets the error specifications of the service in question. This is also known as slow closed loop power control since it’s processed at the rate of 10-100Hz.

- Inner loop power control. Also known as fast closed loop power control since it operates at a rate of 1500 Hz to combat fast fading. This control is based on the ability of the UE transmitter to adjust its output power in accordance with one or more Transmit Power Control (TPC) commands received in the downlink, in order to keep the received uplink SIR at a given SIR target. The purpose of this control is that even in a fading channel, the received power is maintained constant so as to achieve the BLER target.

The power control is used in uplink and downlink. Fast power control is really important in order to keep interference to a minimum and improving capacity. The problem with fast power control is the spikes in power when deep fades are encountered. Nevertheless, the rate of fast power control can be adjusted in order to adapt to the problem. With this, power control is extremely important in UMTS and its design contains a lot of flexibility that allows power control [47].

2.4. Spectrum Sensing

In order to operate cognitive radios with reliability, the detection of spectrum holes must be precise at link level, which means that certain frequency bands, sometimes, cannot be used for transmission, giving spectrum sensing an important role [49].

Spectrum sensing is one of the essential mechanisms of CR and it implies performing measurements on a part of the spectrum and reaching a decision related to spectrum usage based upon the measured data. Nowadays, the service providers are dealing with a situation in which they need a larger amount of spectrum in order to satisfy the increasing quality of service requirements of users. Such an issue has caused interest in unlicensed spectrum access, and spectrum sensing is regarded as an important enabler for this. If a situation is to be imagined in which there is a licensed user (primary user), any unlicensed (secondary) user it needs to be ensured that the primary user is protected, that is, that no secondary user is causing harm interfering with any of primary user´s operations. Spectrum sensing can be used either to successfully detect the presence (or absence) of a primary user. There are several techniques available for spectrum sensing, each with its own set of advantages and disadvantages that depends on the specific scenario.

2.4.1. Basic Techniques

CR is usually seen as an intelligent wireless communication radio device. One of the main functions is the awareness of the environment and by adapting to it, the transmission and spectral utilization is optimized. This makes spectrum sensing an important function to enable CRs to detect the underutilized spectrum of primary systems and improve the overall spectrum efficiency. According to [49], the conventional spectrum sensing at link level have used to decide between the two following hypotheses:

$$y[n] = \begin{cases} w[n] & H_0 \\ hs[n] + w[n] & H_1 \end{cases} \quad n = 1, \ldots., N$$

Equation 2

where y[n] is the complex signal received by the cognitive radio, s[n] is the transmitted signal of the primary user, w[n] is the Additive White Gaussian Noise (AWGN), h is the complex gain of an ideal channel and N is the number of samples of the observation interval. h and s[n] are going to be convolved instead of multiplied, if the channel is not ideal. The null hypothesis is represented by H_0 where no primary user is present and the alternate hypothesis is represented by H_1 where a primary user signal exists [49].

Even though there are some proposals to describe/characterize spectrum sensing, it is known that cognitive radios have lower priority transmission in relation to a primary user. A fundamental requirement is to avoid interference to potential primary users. On the other hand, primary user networks have no need to change any infrastructure when it comes to spectrum sharing with cognitive networks. Therefore, CR should be able to detect primary user presence through continuous spectrum sensing, independently. Some classes of primary users require different sensitivity and rate of sensing for the detection [50].

According to the knowledge level of the CR equipment on the telecommunication signals transmitted on a free band, several detection techniques may be considered. From several techniques that are available, there are three most known and proposed in the literature [51]: energy or power detection, matched filter and cyclostacionary detection. In this dissertation, energy detection is the technique used as a reference for spectrum sensing. All others all equally important, but this one, presents better characteristics in terms of simplicity.

Energy Detection

It consists in a simple detector that computes the energy of the received signal and compares it to certain threshold level value, deciding whether the signal is present or not. If the primary user signal is unknown, the energy detection technique is an optimum solution when detecting any unknown zero-mean constellation signals. The energy detection is usually realized in time domain or in frequency domain. According to [49] and considering the analyzes in time-domain, the received signal is squared and integrated over the observation interval. The output of the integration is compared to a threshold level to decide if the primary user exists or not. With this, the following binary decision is done:

$$\begin{cases} H_0, \; if \; \sum_{n=1}^{N} |y[n]|^2 \leq \lambda \\ H_1, \quad otherwise \end{cases}$$

Equation 3

where λ is the threshold that depends on the receiver noise.

When it comes to implementation, there are a number of options for energy detection based sensors. When it comes to analogue implementations, an analogue pre-filter is required with fixed bandwidth becoming quite inflexible for simultaneous sensing of narrowband and wideband signals. As for digital implementations, these offer more flexibility by using FFT-based spectral estimates. This architecture supports various bandwidth types and allows sensing of multiple signals at the same time [49]. Figure 21 represents a general architecture for a digital implementation of an energy detector.

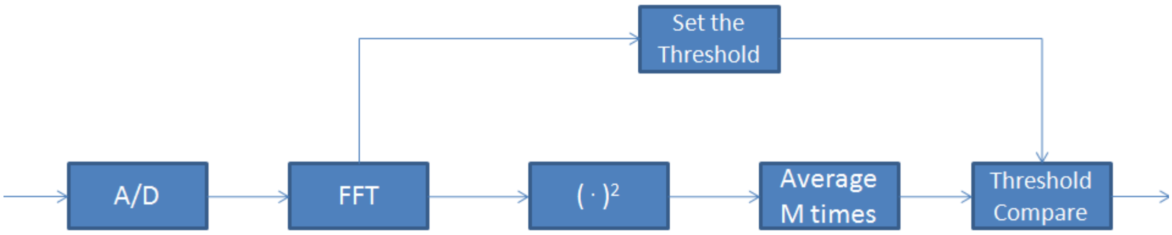


Figure 21 - Digital implementation of an energy detector

Although energy detection method can be implemented without any previous knowledge of the primary user signal, it presents some problems. This method can only detect the signal of the primary user if the detected energy is above the threshold previously defined. Defining the threshold for energy detection can also be a problem since it is highly vulnerable to the changing background noise and especially interference level. Another issue is that this technique cannot distinguish the primary user from the other secondary users sharing the same channel, energy wise [49].

Matched Filter

This technique is based on the fact that using a matched filter is the optimal solution to signal detection in presence of noise since it maximizes the received SNR. This technique requires a previous knowledge of the received signal. With this, it needs to demodulate the signal in terms of, for example, order and modulation type, pulse shaping filter, data packet format, etc. This technique is based on the fact that most telecommunication signals have well-defined characteristics, like presence of a pilot, preamble, synchronization words, etc., allowing the use of this detection technique [51].

Cyclostacionary Detection

When it comes to telecommunication signals fundamentals, these are modulated by sine wave carriers, pulse trains, repeated spreading, hopping sequences, or even present cyclic prefixes, for the purpose use. Hence, an implicit periodicity is present on the signal and they are characterized as cyclostationary, because they exhibit periodicity through their mean, autocorrelation, etc. The fact these characteristic are not present in the noise but only on the signal itself, it enables to differentiate noise from the modulated signal. This is due to the fact that noise is a wide-sense stationary signal with no correlation. With this, the detection technique searches the presence of the cyclostationary characteristic on the tested signal, providing important information to the CR system [51].

3. Measurements Setup and Methodology

In the preceding sections an overview about cognitive radio and the techniques involved is presented. Several researches in the areas [12] [13] [14] have been done to determine the degree to which allocated spectrum bands are occupied in real wireless communication systems. As it has mentioned before, this study complements these works by trying to model the spectrum occupancy.

A measurement setup was assembled for a static spectrum occupancy evaluation. In order to make it suitable for these types of measurements a number of requirements were taken into account. First requirement included the need to evaluate sensing in different frequency bands that are used for different wireless technologies. This narrows the selection of sensing techniques down to energy detection since it is the only method that does not rely on any a priori knowledge of the primary user technology. Second requirement, and also according to [52], other detection techniques usually have a better performance comparing to energy detection technique. Hence, the need for a very sensitive, energy detection setup in order to acquire useful results. Third requirement included a full analysis on the measurements setup in terms of attenuation/gain to every single component and according to these requirements a setup was assembled in terms of measurements quality and measurements management.

This chapter presents the main aspects in terms of hardware and software used in/with the measurements setup, and it is organized as follows: section 4.1 gives a brief description of the measurements setup location; section 4.2 presents the measurements setup itself and a description of it; section 4.3 gives a characterization on every single component of the measurements setup, followed by section 4.4 which presents a full analysis of the measurements setup taking into account all of the loss/gain elements of the system. Finally, section 4.5 presents the all the software used and created in order to enhance the statistics of the analysis presented in Chapter 4.

3.1. Measurement Site Location

All the measurements were performed in a scenario that showed characteristics of having some spectrum occupancy. The measurement equipment was placed on the rooftop of the Electronics, Telecommunications and Informatics Department (DETI) at the University of Aveiro marked with a yellow circle (latitude: 40º 38’ 00” north; longitude: 8º 39’ 35” west) and its location is presented by Figure 22. All the measurements were performed outdoors and during classes’ period, in order to guarantee the most realistic scenario in an urban environment. The setup was placed there since the conditions for this kind of setup were ideal. The room on top of the department, with appropriate conditions, provided a secure place to have all the instrumentation needed and it allowed the antenna to be positioned and connected with a low attenuation cable, not having many curves on it.

Figure 22 - Setup's Location and 2 Base Stations Locations in the city of Aveiro

3.2. Setup's Components

An appropriate measurement setup for CR spectrum survey should be able to detect, covering a wide range of frequencies, a large number of transmitters of the most diverse nature, from narrow to wide-band systems and from weak signals received near the noise floor to strong signals that may overload the receiving system. According to the purpose of the measurement intended, the settings differ and different configurations need to be assembled depending on filters, amplifiers among other settings.

A general schematic of the measurements setup is given by Figure 23, representing all the elements that form the assembled setup for this work.

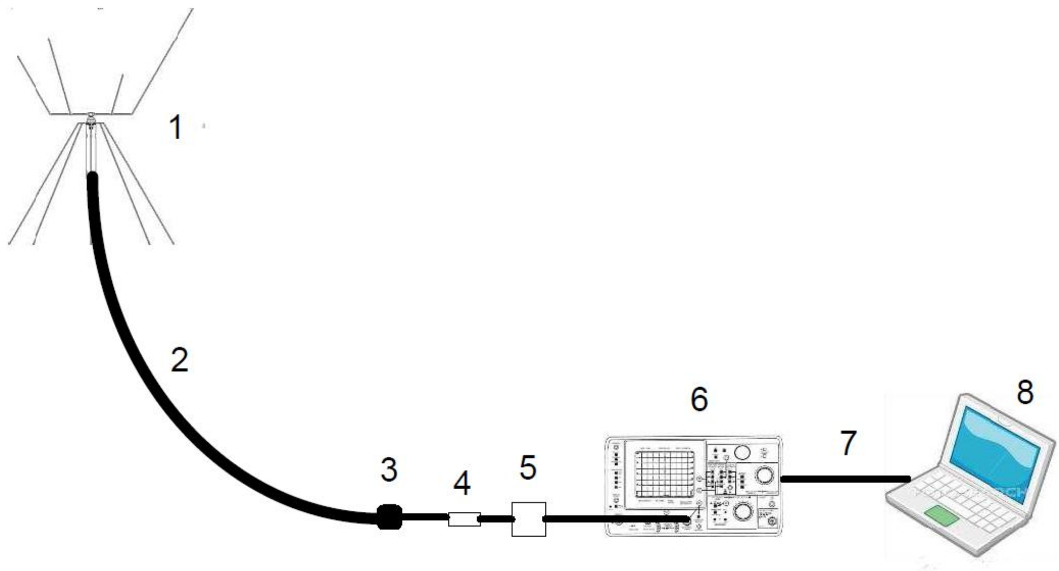


Figure 23 – Measurements Setup (1 – M-POL Antenna 2 – Low Attenuation Cable 3 – N-SMA Adapter 4 – Filter 5 – Pre-Amplifier 6 – Spectrum Analyzer 7 – Ethernet LAN Cable 8 – Portable Computer)

The following sub chapters give a full description of the considered setup, and a description of every single component presented in the measurements setup. Figure 24 presents the inside of the room where the measurements were done. The antenna was located outside the room and it will be presented later in sub-chapter 3.3.2.

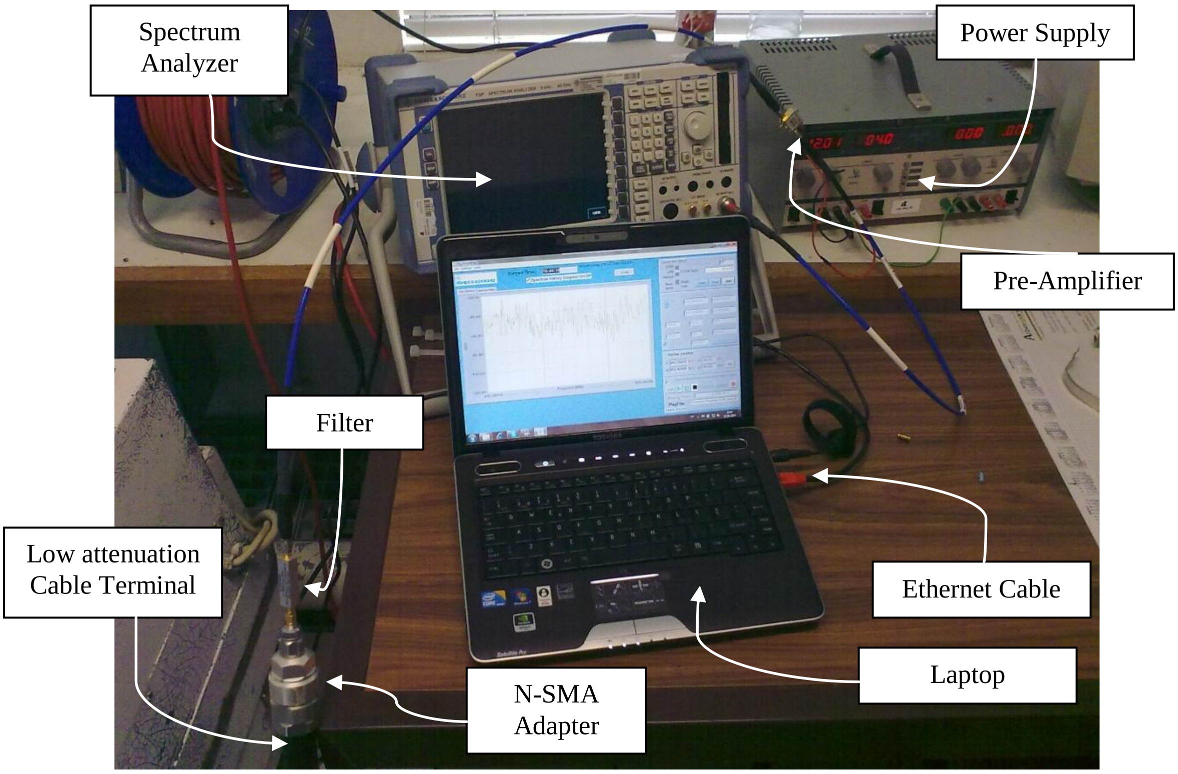


Figure 24 - Measurements Setup (Inside's build)

3.2.1. Setup Description

Figure 23 represents the measurement setup composed of a high bandwidth omnidirectional (Multi-Polarized) antenna (25MHz − 6GHz) from MP Antenna company, with typical 3dBi gain. A semi-rigid low attenuation cable (typical < 0.12 dB/meter at 5GHz) with about 8 meters, a high steeply passband filter (500MHz − 1GHz for GSM900, 1GHz − 2GHz for DCS1800), a high bandwidth preamplifier (15dB gain at 950MHz), a Spectrum Analyzer (SA) and a portable computer with an acquisition program. From the low attenuation cable, to the SA, the components are connected with thin cable with SMA connectors. The preamplifier gain is such that the GSM signal (−102dBm in 200 KHz, sensitivity level) is brought above the noise level of the SA, but not enough to generate visible intermodulation products due to non linearity of the input mixer of the SA. The SA is set in the highest sensitivity *i.e.* with 0dB attenuation of the input attenuator. The total signal in 500MHz − 1GHz band (pass band of the filter) at the input of the SA was about −17dBm. The secure signal level in terms of intermodulation is below −10dBm. Another criterion in choosing the filter is that the higher passband frequency is not more than one octave from the lower passband frequency. This avoids the second order intermodulation products to be inside the passband. The characteristics above mentioned represent the main ones we worked with. In the next chapters each component is described so that a full overview of the band, from 25MHz to 6GHz, is acquired.

3.3. Components' analyzes

All components chosen for this research have been carefully selected in accordance to our analysis needs. Each of them was previously analyzed for suitability with the bandwidth that covered the frequencies we intended to measure.

3.3.1. Spectrum Analyzer

The use of a SA for the measures brought some concerns when it comes to setup. The Rohde & Schwarz (R&S) FSP-40 spectrum analyzer was chosen one for measurements setup. This spectrum analyzer has some basic characteristics like the following ones [53]:

- Frequency range: 9 kHz to 40 GHz
- Resolution Bandwidth: 1 Hz to 10 MHz
- Displayed average noise level: -155 dBm (1 Hz)
- Phase noise: -113 dB (1 Hz) at 10 kHz
- Adicional filters:
    - Channel filters from 100 Hz to 5 MHz and RRC filters
    - Fast Fourier Transform (FFT) filters from 1Hz to 30 kHz
    - Electromagnetic Interference (EMI) bandwidths and quasi-peak detector
- Measurement applications for cellular standards and general purpose, e.g. phase noise, noise figure, etc.

All of these characteristics are considered in the setup analysis presented in 3.4. Some parameters were chosen in order to improve the quality of the measurements done. The most important settings considered were the following ones, always depending on the chosen band.

- Measurement mode (single/continuous)
- Frequency mode (Start frequency/Stop frequency or Center frequency)
- Resolution Bandwidth (RBW)
- Video Bandwidth (VBW)
- Reference Level
- Detector type
- Level Offset
- Sweep Time
- Sweep Points
- Attenuation Level

All of these settings are defined on Chapter 4 according to the selected band. Another characteristic was considered a bit more careful (T_{sweep}) according to the consideration taken by R&S itself, described as it follows. According to [54], through the use of analog or digital Intermediate Frequency (IF) filters the maximum allowed sweep speed is limited by the transient time of the IF filter and video filter. The transient time has no effect if the video bandwidth is larger than the resolution bandwidth. In this case, the required transient time increases inversely with the square of the resolution bandwidth, so with a decrease of the resolution bandwidth by the factor n the required minimum sweep time becomes n^2 longer. The following applies:

$$T_{Sweep} = k \cdot \frac{\Delta f}{B_{IF}^2}$$

Equation 4

,where $\mathbf{T_{Sweep}}$ = minimum sweep time required (with given span and resolution bandwidth), in seconds,

$\mathbf{B_{IF}}$ = Resolution bandwidth, in Hz

$\mathbf{\Delta f}$ = span to be displayed, in Hz

k = proportionality factor

The proportionality factor k depends on the type of filter and the permissible transient response error. For analog filters made up of four or five individual circuits, the proportionality factor k is 2.5.

3.3.2. Antenna

The antenna (Figure 25) was deployed on top of the DETI at the University of Aveiro in line of sight with the Telecommunications antenna's operators.

Figure 25 - Antenna deployment

Through the graphic in Figure 26 the values that are crucial for the measurements statistics are 900MHz and 1800MHz. The values considered were 3.1dBi and 2.8dBi for GSM900 and GSM 1800 respectively.

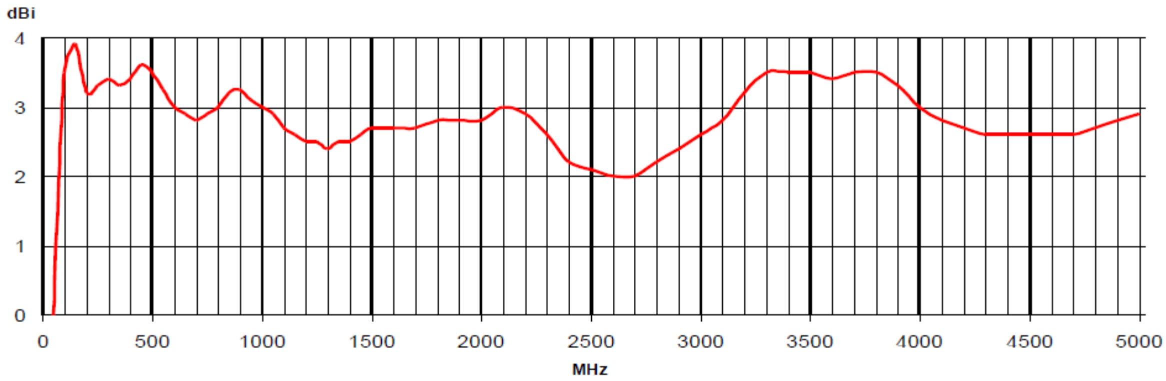


Figure 26 - Gain vs. Frequency of the antenna

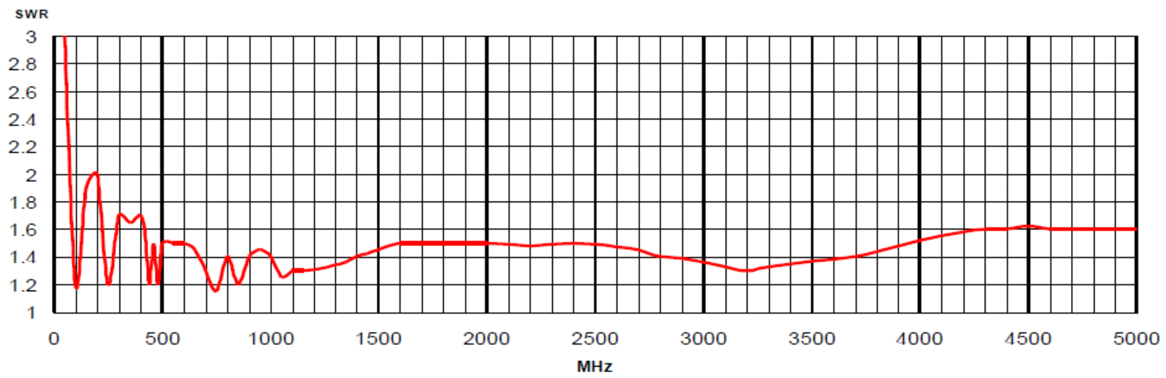


Figure 27 - VSWR

The influence of VSWR in the transmitted power is also a data considered in the measurements setup. According to the two following equations:

$$\text{Return loss} = 10\log(\text{Pr} / \text{Pi}) = 20\log(\text{Er} / \text{Ei})$$

Equation 5

$$\text{Mismatch Loss} = 10\log(1 - \rho^2)$$

Equation 6

Where Pr is the Power of the reflected wave, Pi is the Power of the incident wave, Er is the Energy of the reflected wave, Ei is the Energy of the incident wave and ρ is the reflection coefficient of the antenna.

We can conclude that the VSWR values of the used antenna do not have a great influence in terms of mismatch loss, which is a measure of how much the transmitted power is attenuated due to reflection. The values of VSWR between 1.2 and 1.5 (Figure

27) results in a mismatch loss of a maximum of 0.177 dB, which represents a small influence in the measurement values.

Super-M Ultra Base Station antenna seamlessly covers the frequency range from 25 MHz to 6 GHz (120 MHz - 6 GHz transmit) and provides wireless communication in “Real World” obstructed Non-Line-Of-Sight (NLOS) environments. In non-line-of-site obstructed environments the M-POL Super-M Ultra Base Station can outperform non-multipolarized 8dBi gain antennas [55].

3.3.3. Low Attenuation Cable

The cable selected to connect the antenna with the rest of the components till the SA is characterized by having low attenuation. With this, the need of a big gain from its end onwards is avoided and allows the possibility for the setup to detect lower signals.

Figure 28 represents the S_{21} parameter data measured for the cable used on the measurements setup. The data was analyzed from 100MHz till 5GHz. For the frequencies considered (900MHz and 1800MHz) the attenuation is 0.5243dB and 0.6549dB respectively.

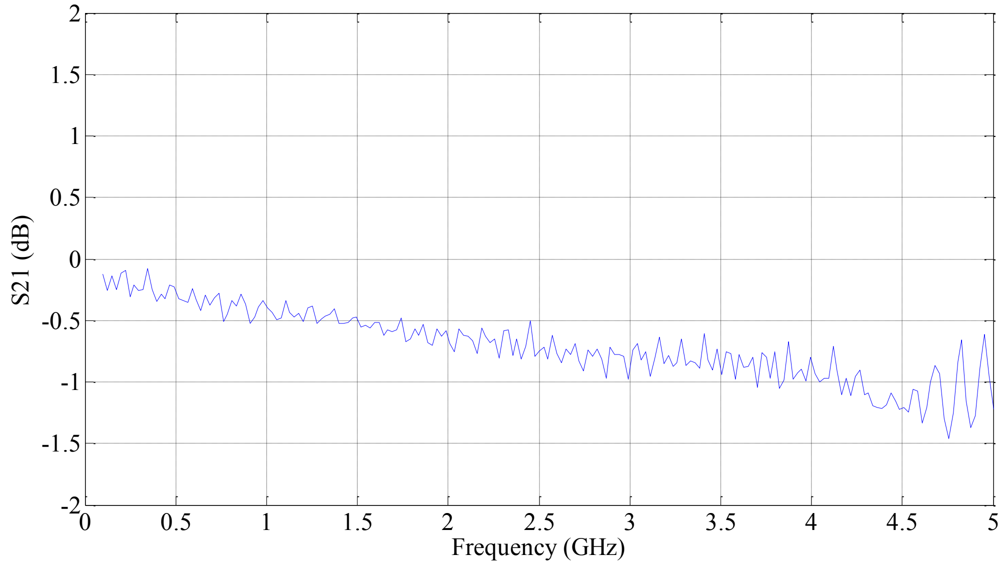


Figure 28 - Cable's S parameter data

3.3.4. Filter

The total power in the spectrum bandwidth considered was one of the main concerns for the measurements setup. The use of a filter was needed to prevent an overload in the SA. The overload in the SA would not allow the acquisition properly. For that reason personalized filters were acquired to prevent this situation. One with a range from 500MHz to 1GHz and another one with a range from 1GHz to 2GHz (Figure 29).

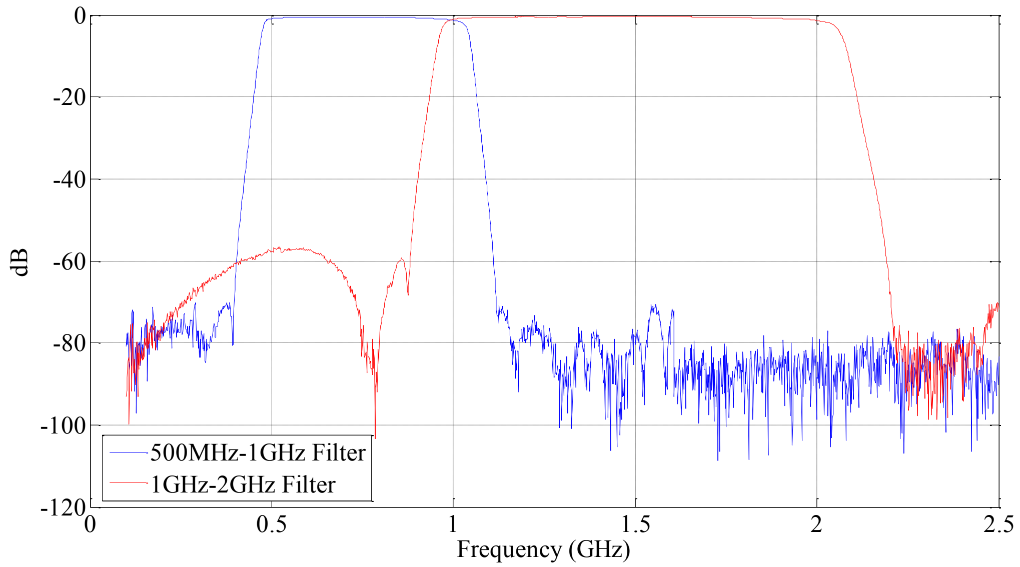


Figure 29 - Setup's Filters

Each filter was used for the specific bandwidth, the 500MHz-1GHz for GSM900 and the 1GHz-2GHz one for GSM1800. It also allows limiting the received power so that measurements are allowed to be taken without having an overload in the SA. The non use of the filter would cause an overload in the SA and no measurements would be allowed in some cases, to be taken hence allowing to amplify the signal received and placing it above the noise level.

Table 2 – Filter's Specifications

Item	Technical Specification (Filter 1)	Technical Specification (Filter 2)
Center Frequency (f0) (MHZ)	750	1500
Frequency Range (MHz)	500-1000	1000-2000
Insertion Loss @f0 (dB)	1.0 max	1.5 max
VSWR	1.5 Typ.	1.5 max
Rejection (dB)	60 min @ 300MHz	60 min @ 800MHz
	60 min @ 1200 MHz	60 min @ 2200MHz
Connectors	SMA-Female	SMA-Female

3.3.5. Pre-Amplifier

The amplifier chosen for the measurements was an amplifier from Mini-Circuits with a wide bandwidth from 20MHz to 6GHz, with a noise figure of 3.3dB typical. Two Pre-Amplifiers were available during the frequency analyzing and during the measurements tests. According to the data given in the datasheet (Figure 30), the two amplifiers were analyzed in a Vector Analyzer to determine the gain values for each one of them.

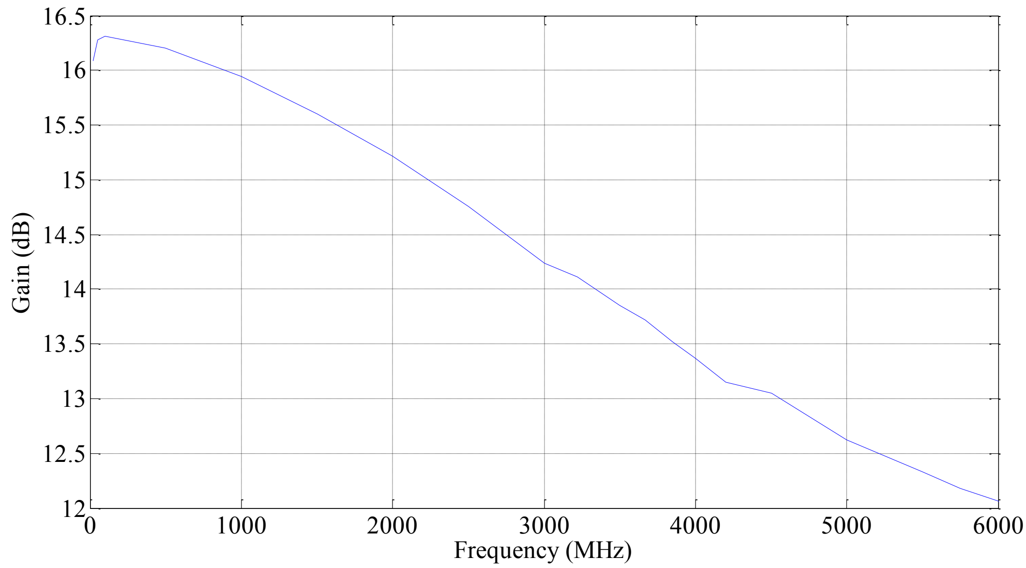


Figure 30 - Typical Performance Curve for the Amplifier ZX60-6013E-S+ @ 25ºC

The two amplifiers were characterized for the parameter S_{21} so that the correct gain values could be taken into account. Figure 31 shows the Gain Curves for the two amplifiers from 500MHz to 2.5GHz (device limits) and the Datasheet Gain Curve so we can compare the three of them. The one used on the setup was the Amplifier 2, and the Amplifier 1 was used as a reserve in case the other one failed.

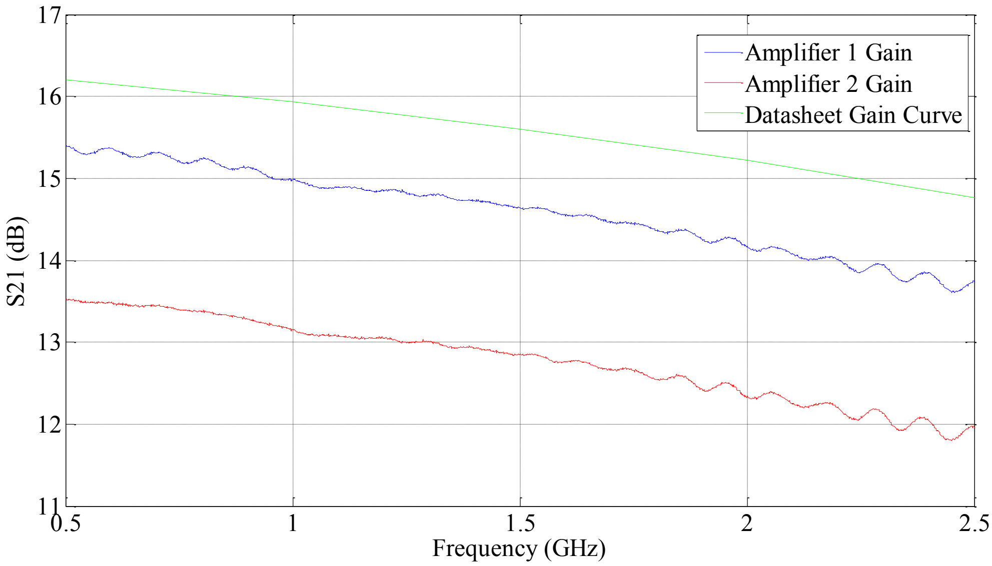


Figure 31 - Gain curves

3.4. Setup analysis

Figure 32 shows the equivalent circuit of the measurement setup from the preamplifier to inside the SA including the sum of the internal noise. S_i is the input signal and N_i is the noise signal at the input. These two signals are already combined before the preamplifier, despite showing the combination at the input. G_1 is the Power Gain of the preamplifier, N_{SA} is the internal noise signal of the SA, S_0 is the output signal resulting from S_i, and N_0 is the output noise signal. Also, there is one variable, the noise figure of the preamplifier NF, which is not shown.

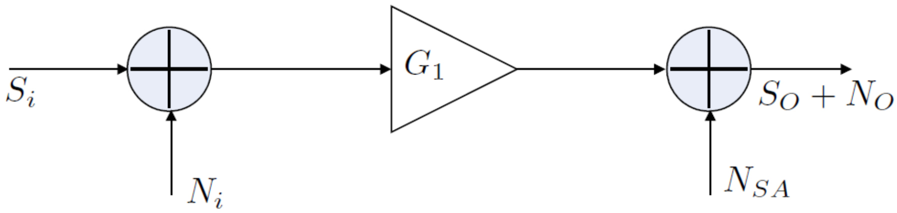


Figure 32 - Equivalent Circuit of the measurement setup from the preamplifier to the inside of the Spectrum Analyser

The power of these signals is measured in logarithmic form (dBm/Hz), and the noise figure (NF), as well as the gain G_1 in dB. N_i depends on the environment noise caught by the antenna and the noise added by the lossy elements before the preamplifier. S_i is the power of the signal caught by the antenna at the measured frequency, attenuated by the lossy elements before the preamplifier. How much S_i must be above N_i in dB (or the signal to noise relation in linear) in function of the gain G_1, considering the limit case of $S_0 = N_0$ is then calculated. This last condition limits the point which can separate signal from noise. The minimum of that function could be described by Equation 7.

$$\begin{cases} \{\widehat{G_1}\} & = \arg min_{\{G_1\}}[S_i - N_i] \\ S_0 & = N_0 \\ S_0 & = S_i + G_1 \\ N_0 & = 10\log\left(10^{\frac{N_i+NF+G_1}{10}} + 10^{\frac{N_{SA}}{10}}\right) \end{cases}$$

Equation 7

S_i is given by

$$S_i = -G_1 + 10\log\left(10^{\frac{N_i+NF+G_1}{10}} + 10^{\frac{N_{SA}}{10}}\right)$$

Equation 8

Considering $N_i = -174dBm/Hz$ (best case), NF = 3.5dB and constant with the preamplifier gain, $N_{SA} = -155dBm/Hz$, then the Figure 33 presents $S_i - N_i = f(G_1)$. Looking at Figure 33, it is concluded that the solution of Equation 7 for G_1 is infinity. And the value reached at infinity for $S_i - N_i$ is NF (by the limit of Equation 8 minus N_i in both sides with G_1 to infinity).

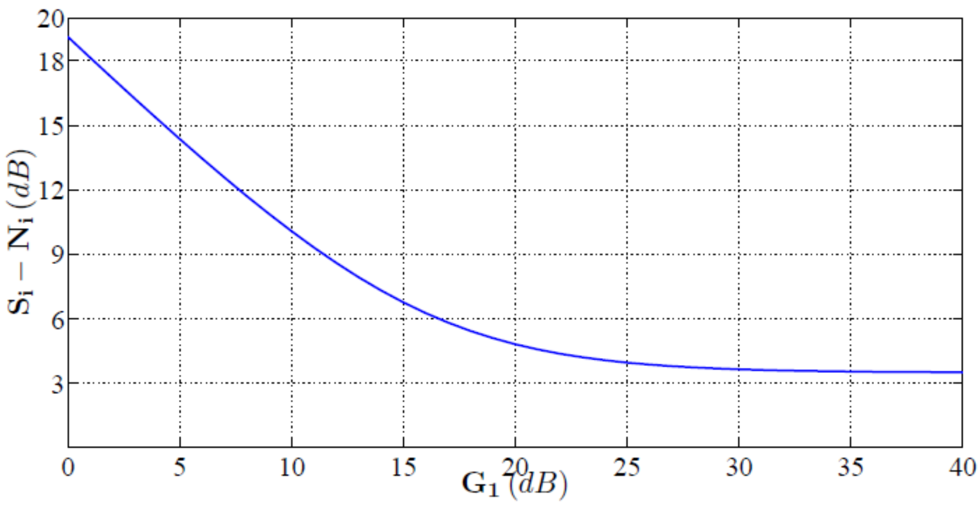


Figure 33 - Si –Ni in function of G1

The lossy elements before the amplifier are taken into account in order to calculate the minimum GSM signal that can be detected with this setup. Furthermore, the antenna gain is also taken into account. The lossy elements mentioned above will amplify (or add in dB) the noise induced by the antenna. This amplification is equal to the attenuation induced to the signal (Cable attenuation times Filter Attenuation - plus if in dB). This attenuation amount is represented by α_{dB}. Figure 34 represents the operations made to the signal and to the noise from the antenna to the preamplifier input. In an ideal scenario the noise at the antenna output will be the thermal noise (N_{th}) and equal to −174dBm/Hz ($10^{N_{env}/10} = 0$, environmental noise power equal zero). Considering a gain G_1 equal to infinity and that the antenna catches the lowest detectable power. Then,

$$\begin{cases} S_i - N_i & = NF \\ N_i & = -174dBm/Hz + \alpha_{dB} \\ S_i & = S_{A_{in}} + G_A - \alpha_{dB} \end{cases}$$

Equation 9

which is equivalent to

$$S_{A_{in}} = -G_A + 2\alpha_{dB} - 174dBm/Hz + NF$$

Equation 10

The attenuation of the cable connecting the antenna, plus the pass band filter attenuation was considered to be $\alpha_{dB} = 1.5dB$. The antenna gain is 3dBi and considering the noise figure 3.5dB, then $S_{A_{in}} = -170.5dBm/Hz$ or $S_{A_{in}} = -117.5dBm/(200KHz)$. This is the lowest GSM signal detectable with this setup.

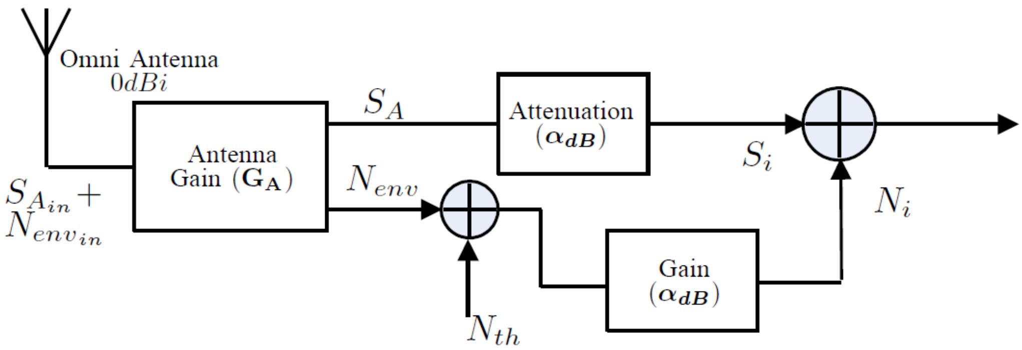


Figure 34 - Equivalent circuit of the measurement setup from antenna to

3.5. Software used

To be able to record the measures, appropriate software was tested/used on the measurements setup. The software is compatible with the SA used, from Rohde & Schwarz. The program is called FSx_RecordPlay, it is freeware, and it is available from R&S [53]. Figure 35 represents the main window used to configure the type of measurements to be taken, and record it on the hard drive.

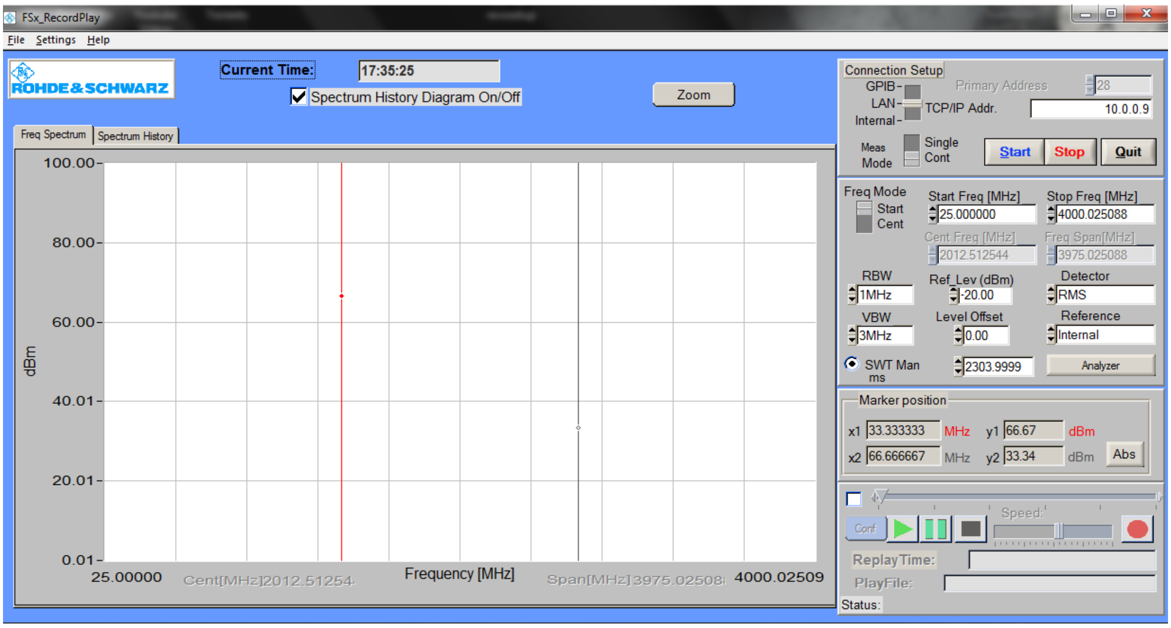


Figure 35 - FSx_RecordPlay main window

Figure 36 represents part of the file stored from the program FSx_RecordPlay. The file is composed by an initial header, which contains all of the information used to configure the program settings, and a part of the power values measured (represented in 32 bits), represented in symbols. In order to provide data representation and a statistical treatment of the measurements, a Matlab program was created to read and treat the data stored.

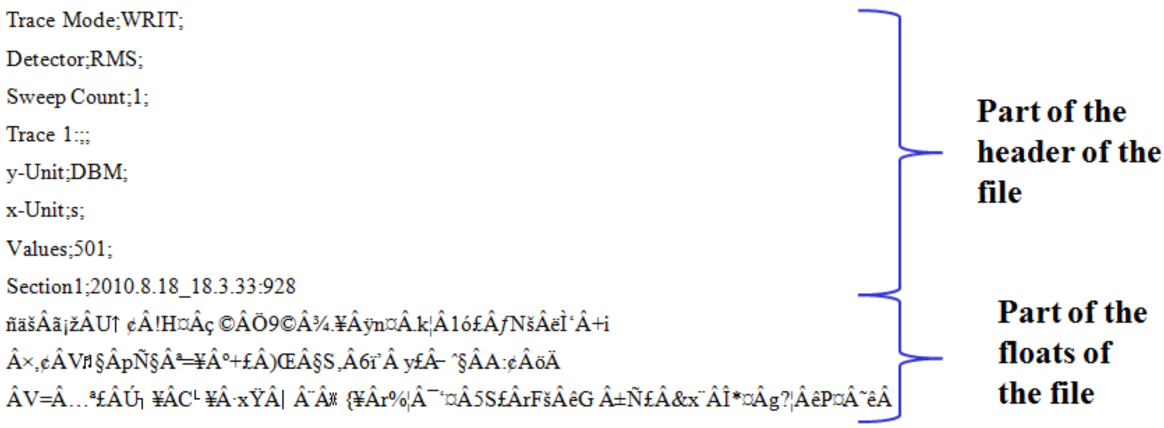


Figure 36 - Representation of the stored files from the program FSx_RecordPlay

After reading the header, some considerations are taken into account like data size, processing speed, among others, a basic menu is presented to the user in order to choose a data representation or statistic treatment. Figure 37 represents the main menu with the basic options for the main tests.

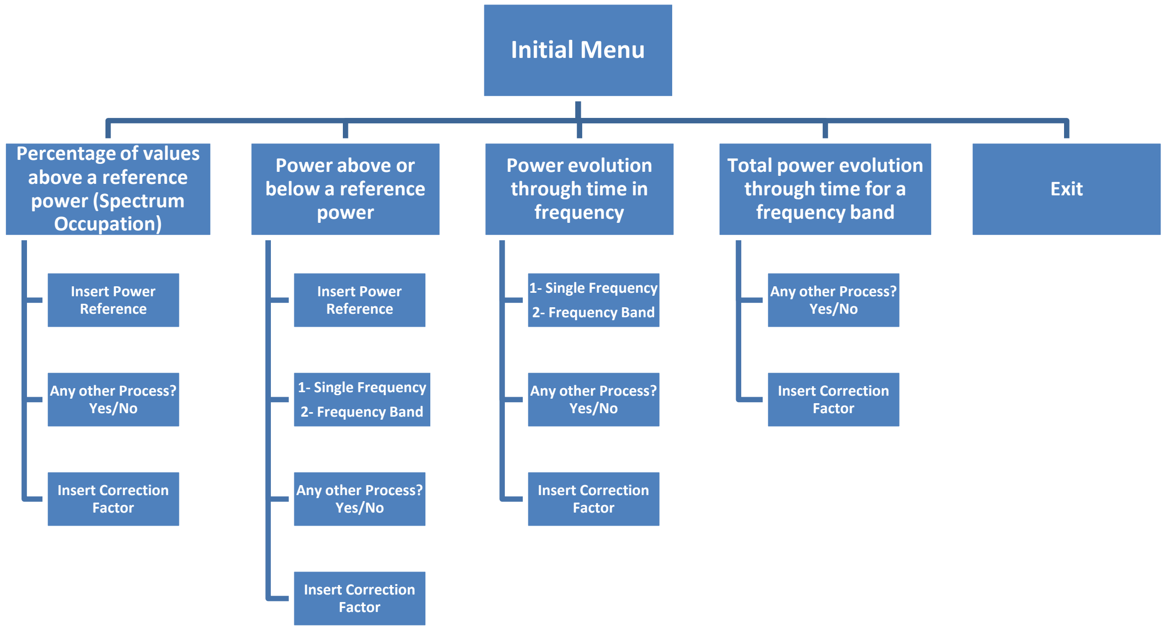


Figure 37 - Main menu of the created program

The program created allows the possibility for the user to represent the data collected, to do statistical tests and to observe them in plot/bars graphics. Appendix A presents in detail the program created in Matlab with all of these options described and examples of graphic representation done by these options.

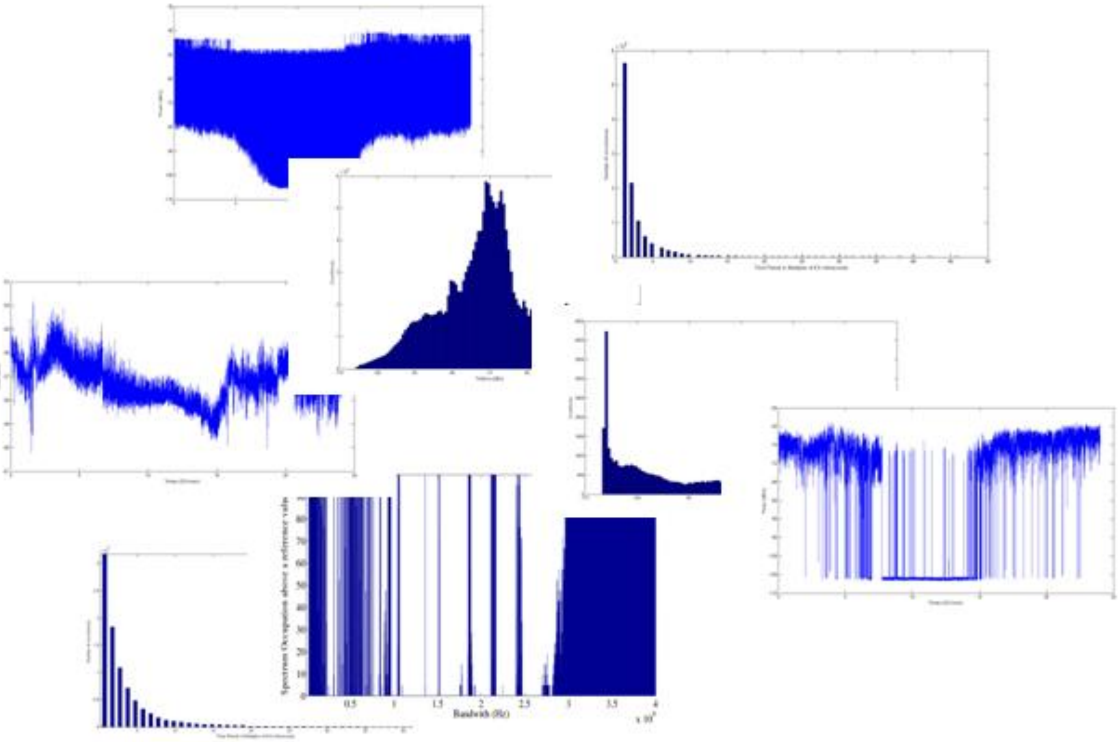


Figure 38 - Different types of tests done

After running several tests (Figure 38) on the collected data, some considerations were concluded and proper measurements were taken to obtain the best possible results in terms of statistics. All of the considerations were taken into account upon the setup's configuration and measurements type/frequency. In the following chapter, all the measurements/statistics are presented.

4. Measurements and Statistics

This chapter presents all the analysis done on the data recorded and obtained through the measurements setup as described in the previous chapter. The analysis of the collected data enabled modelization of spectrum's behavior. Before taking specific measurements in the GSM band an overview of the spectrum occupancy was measured to see which bands would be propitious to take measures from, and to better understand a simple occupation of the spectrum from 25MHz to 6 GHz. With this, specifications are presented for the selected frequencies. Following, the results of the statistical measurements and occupancy results are presented to provide with sufficient information that will be applied in creating models of spectrum behavior.

4.1. Spectrum Occupancy

To be aware of the spectrum occupancy some measurements were taken with the program FSx_RecordPlay, on the full bandwidth. Figure 39 presents the measurement taken and an overview of the full bandwidth can be observed in terms of power. Some of the most important frequencies used nowadays are easy to identify in the measured band.

The total power measured is one of the main factors taken into account, hence the use of filters in our setup. Frequencies like radio, television, UMTS (FDD, downlink) are a few examples of total power to be avoided in the measurements taken, since the total power received on the SA would provoke an overload, like it was mentioned on the previous chapter.

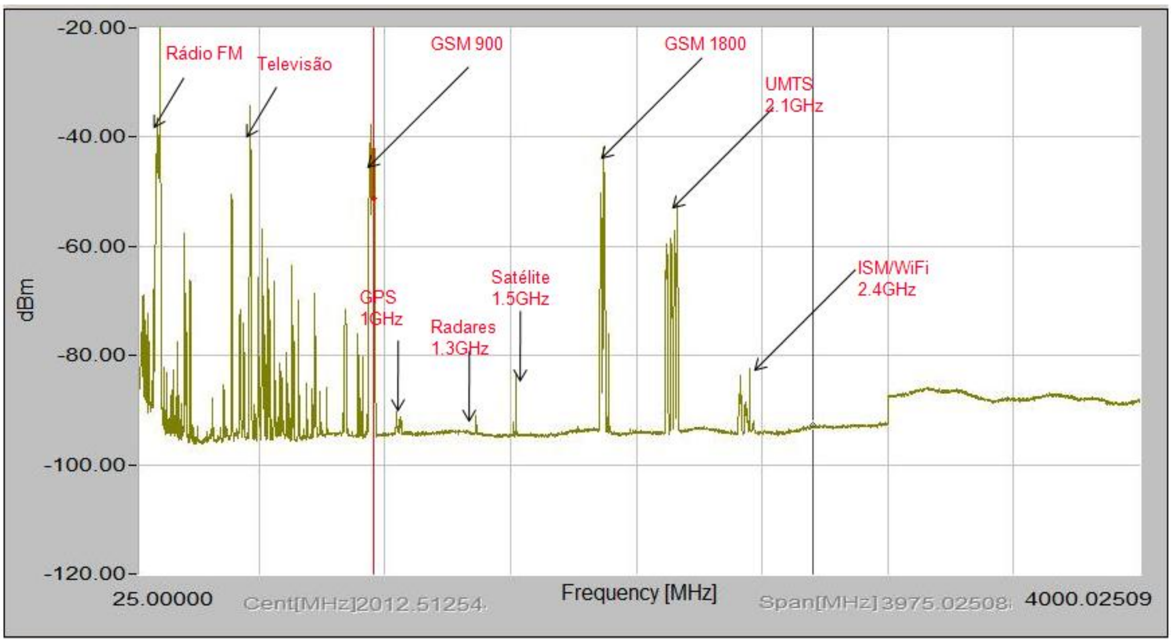


Figure 39 - Spectrum Occupancy from 25MHz to 4GHz

In order to evaluate the spectrum occupancy more specifically, the first algorithm test is used to observe the % of spectrum occupancy above a reference value. Figure 40, Figure 41 and Figure 42 represent the spectrum occupancy in % with different values of power reference. The occupation percentage obtained is 5.2%, 34% and 64.9% respectively.

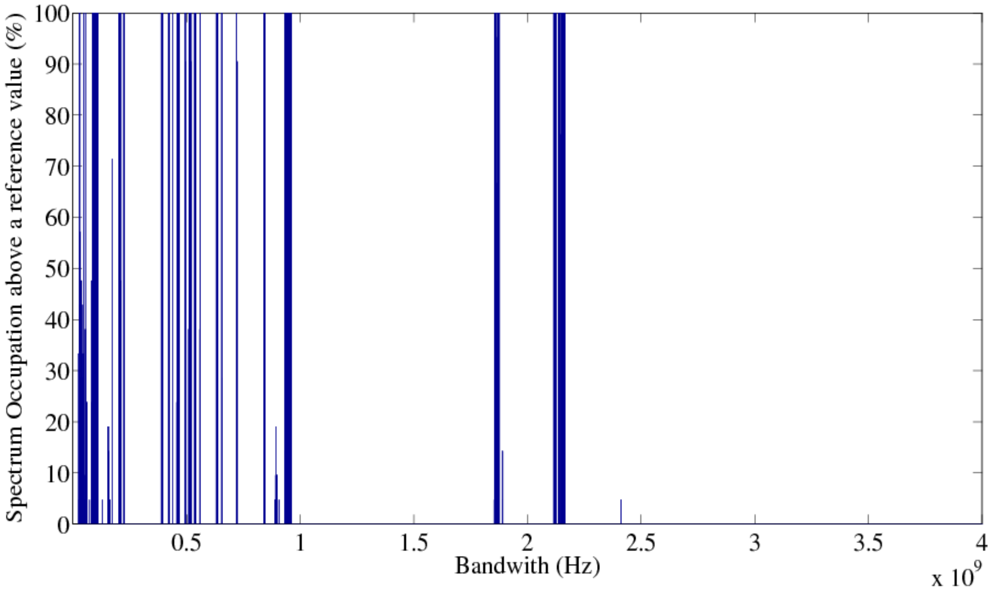


Figure 40 - Spectrum Occupancy with -80dBm of reference value

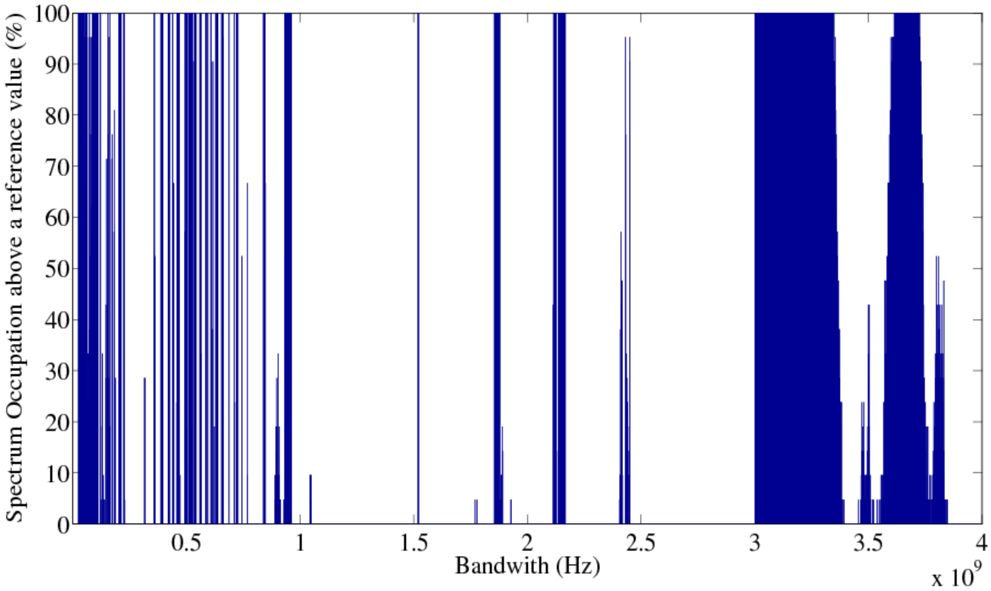


Figure 41 - Spectrum Occupancy with -90dBm of reference value

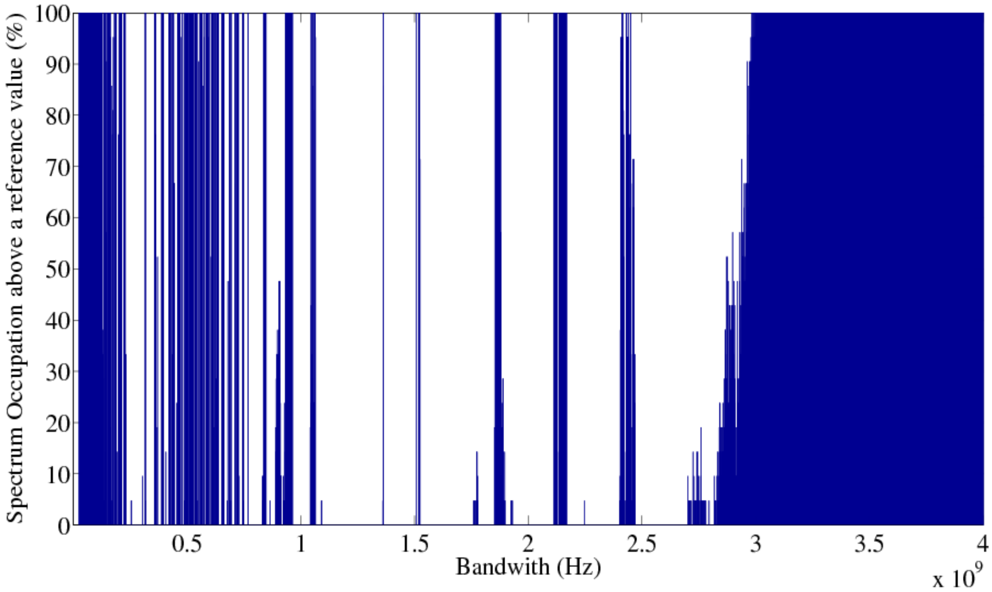


Figure 42 - Spectrum Occupancy with -95dBm of reference value

4.2. Measurements Specifications

In order to enhance the measurements' specificity in GSM, ANACOM (Portuguese Communications Regulator) was asked for the frequency bands attributed to the mobile operators. ANACOM also mentions that the operators have a network license for these frequencies, which are managed according to their needs and based on an efficient use of spectrum. A location of the base stations in the region of Aveiro was also supplied (with GPS coordinates), but for reasons of confidentiality these are not identified in terms of which operator holds them (Figure 43).

Figure 43 – GSM base station's location in the region of Aveiro

The following table represents the frequency bands, in terms of GSM, for the current mobile operators in Portugal.

Table 3 - GSM frequency bands attributed to mobile operators

Operador	Faixa de Frequências		Quantidade	Tecnologia
	Downlink	*Uplink*		
Vodafone	935.1-943.1 MHz	890.1 - 898.1 MHz	2 x 8 MHz	GSM 900
Optimus	943.1-950.9 MHz	898.1 - 905.9 MHz	2 x 7.8 MHz	
TMN	950.9-958.9 MHz	905.9 - 913.9 MHz	2 x 8 MHz	
Vodafone	1854.9 - 1858.1 MHz e 1867.9 - 1870.7 MHz	1759.9 - 1762.9 MHz e 1772.9 - 1775.7 MHz	2 x 6 MHz	GSM 1800
Optimus	1870.7 - 1876.7 MHz	1775.7 - 1781.7 MHz	2 x 6 MHz	
TMN	1858.5 - 1861.7 MHz e 1865.1 - 1867.9 MHz	1763.5 - 1766.7 MHz e 1770.1 - 1772.9 MHz	2 x 6 MHz	

When it comes to the measurements itself, these were taken at a distance of 250 meters (measured with GPS) from the nearest GSM base station during school period. This base station covers, the University Campus with a population of approximately 15000 students, using GSM900 and DCS1800 bands. Two GSM operators are co-located at this base station belonging to the studied GSM900 band to one operator and the studied DCS1800 band to the other. The measurements were done with a resolution bandwidth of 100 KHz at 501 points covering in excess all GSM900 downlink band (Figure 44) and the allocated part of the DCS1800 band (Figure 46).

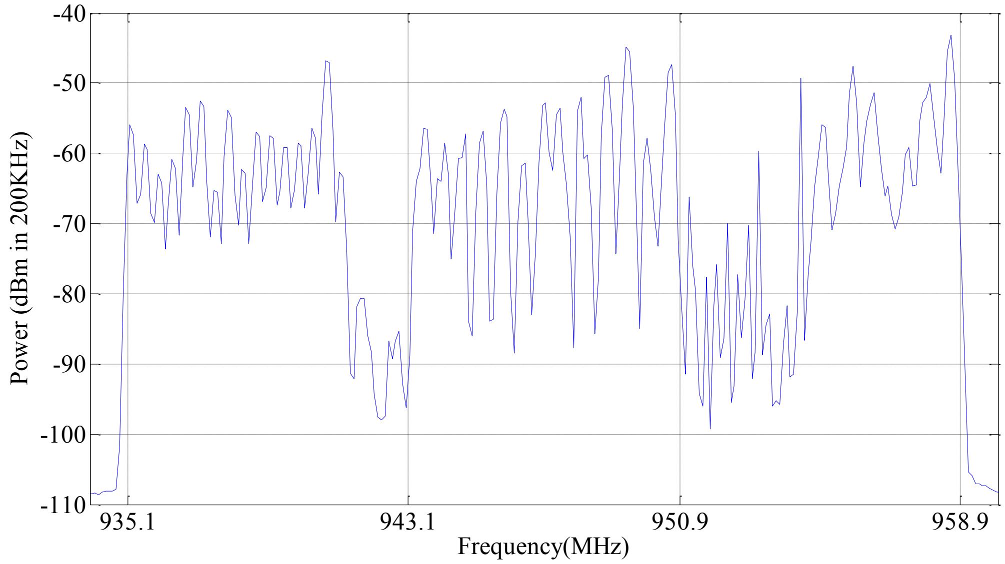


Figure 44 - Typical Power Spectrum Density at 5H19 for GSM900

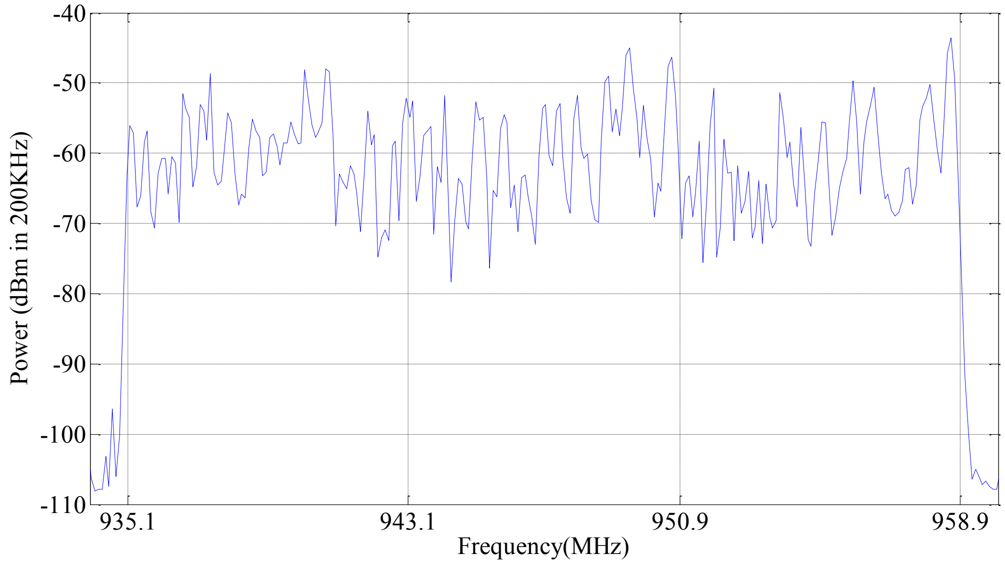


Figure 45 - Typical Power Spectrum Density at 13H for GSM900

Each measured 100 KHz covers one side of the 200 KHz GSM band. In the case of single frequency, the 501 points were measured in a specific frequency with a span equal to zero. The measured power was adjusted to reflect the power received at the output of the equivalent unit gain antenna (see Figure 34, at output of the Omni-Antenna) and for the bandwidth of 200 KHz it was added 3dB. The time at each measurement point was set to the frame period (about 4.62ms) giving a sweep time about 2.4 seconds. There is practically no delay between consecutive measurements. Figure 44 shows the spectrum occupancy of GSM900 band at 5H19 of a working day. The frequency axe's ticks are the limits of the bands of the three Portuguese GSM operators. Figure 45 shows the spectrum occupancy of GSM900 band at 13H in the same 24 hours.

Aveiro City is a plane region and because of that the antenna is at line of sight of several base stations, hence the high occupancy. In that situation two base stations with a decade of distance (in relation to the setup antenna) one from another could originate a difference (in dB) on the received power as low as 20dB (assuming that the same power is being transmitted). The power measurements done for this sectorized base station shows that the power received from the other sectors, is not more than 20dB below (measured in the Broadcast Control Channels (BCCH) which has no frequency hopping). Figure 46 shows the spectrum occupancy of the DCS1800 band at 5H19 of a working day. ANACOM allocates spectrum according to the operator's needs and requirements. For this reason, there are two bands for each of two operators and a larger band for one operator only. Figure 47 shows the spectrum occupancy of the DCS1800 band at 13H in the same 24 hours.

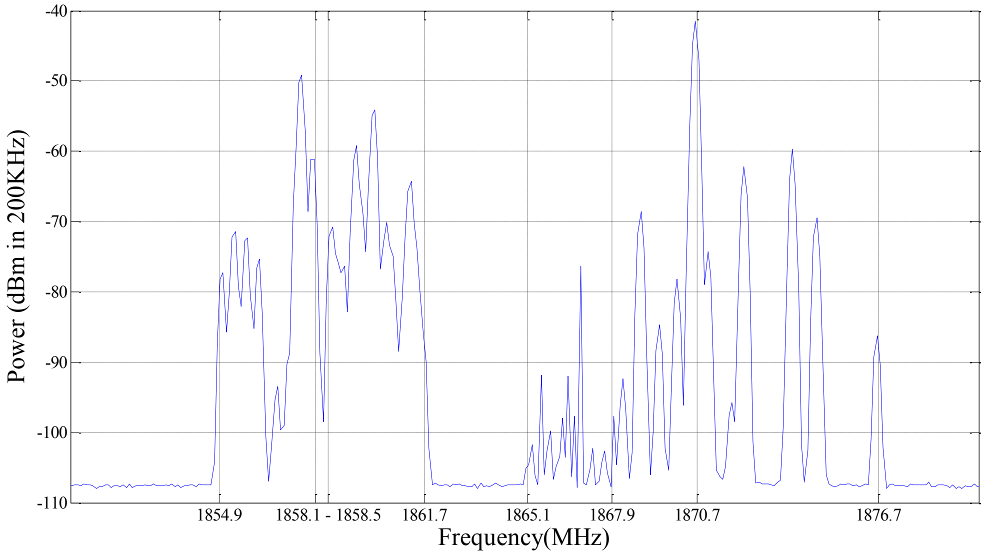


Figure 46 - Typical Power Spectrum Density at 5H19 for DCS1800

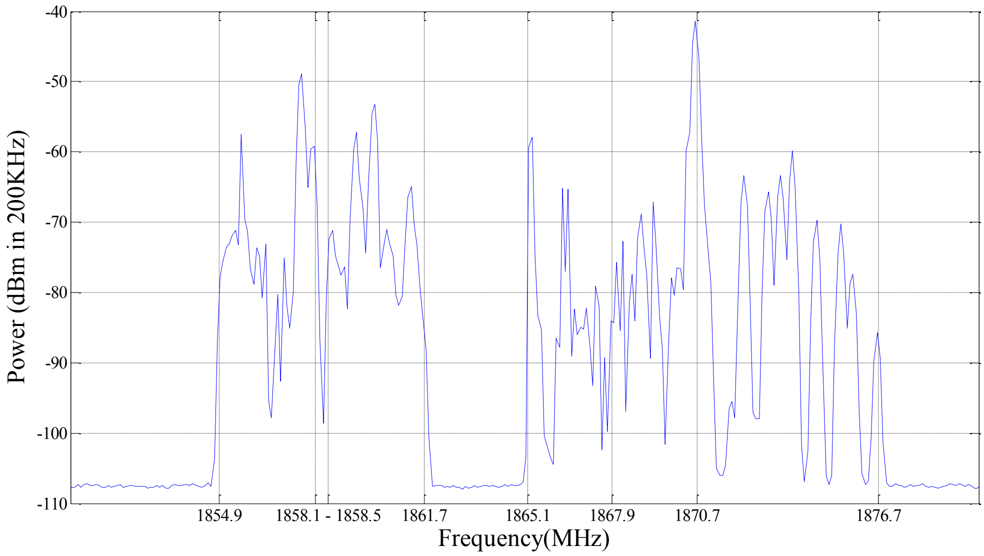


Figure 47 - Typical Power Spectrum Density at 13H for DCS1800

4.3. Statistic Measurements

Measurements were made during four consecutive working days and the power profile was similar between days. Figure 48 presents the power variation at the 953.9 − 954.1MHz band in one of the four days measured. The correspondent power occurrence is presented in Figure 49.

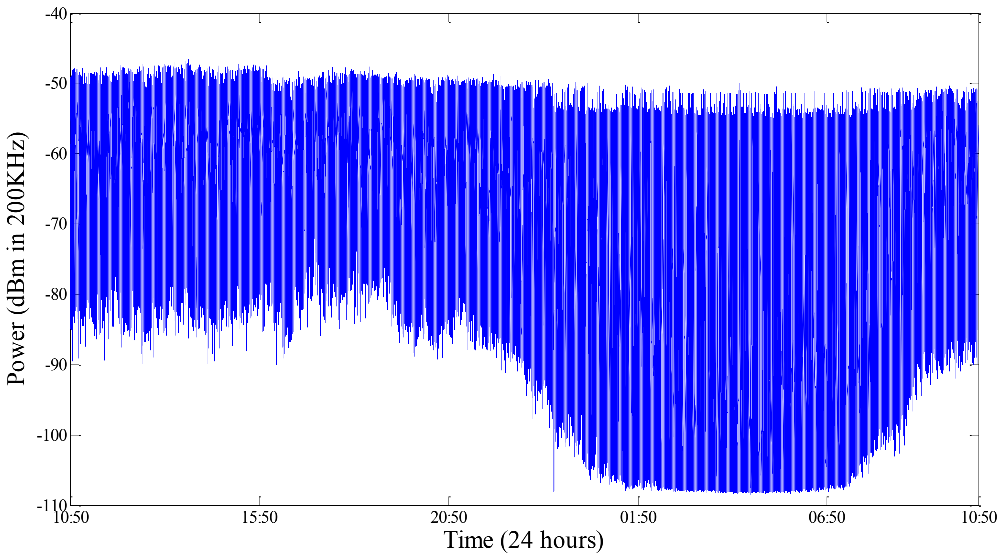


Figure 48 - Power in the 953.9 – 954.1MHz band during one day

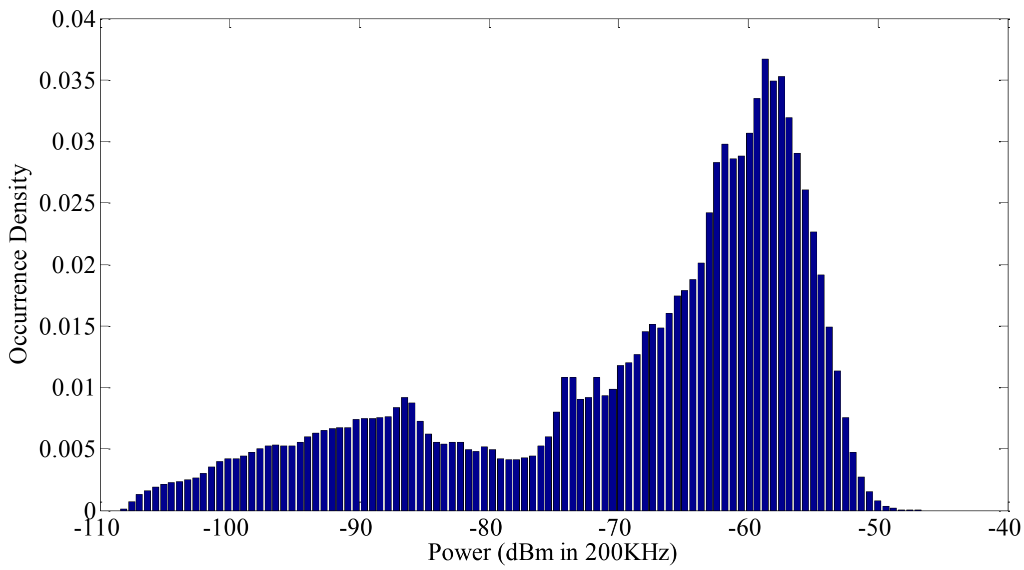


Figure 49 - Power Occurrence Density in the 953.9 – 954.1MHz band

Figure 50 presents the power variation during a working day in the band of 1856.9 − 1857.1MHz with the correspondent power occurrence presented in Figure 51. For the time statistics a threshold must be defined. The threshold was set approximately 10dB above the noise level, just a few dBs below the minimum level needed to detect the signal with an adequate error probability. The decision level for GSM900 was −98dBm/200KHz and −90dBm/200KHz for DCS1800.

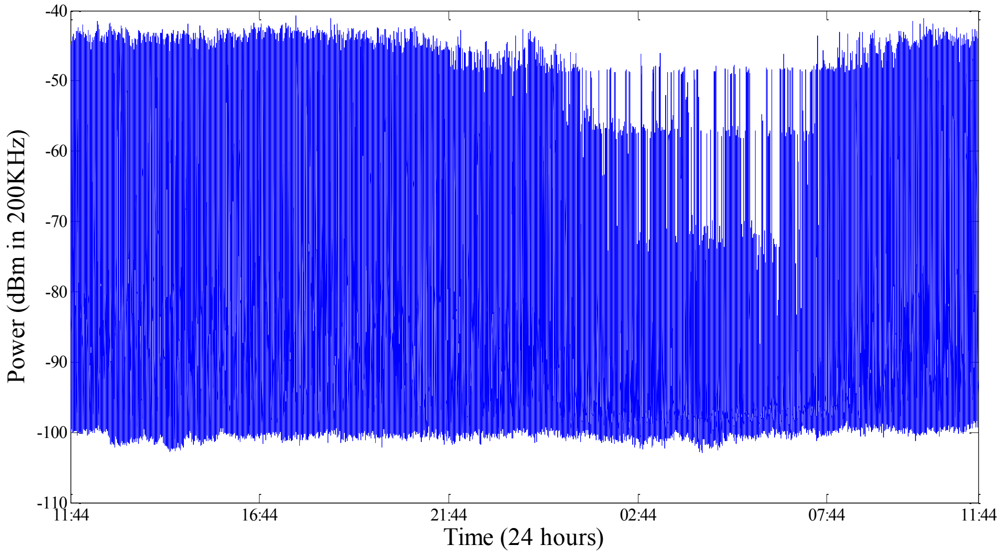


Figure 50 - Power in the 1856.9 – 1857.1MHz band during one day

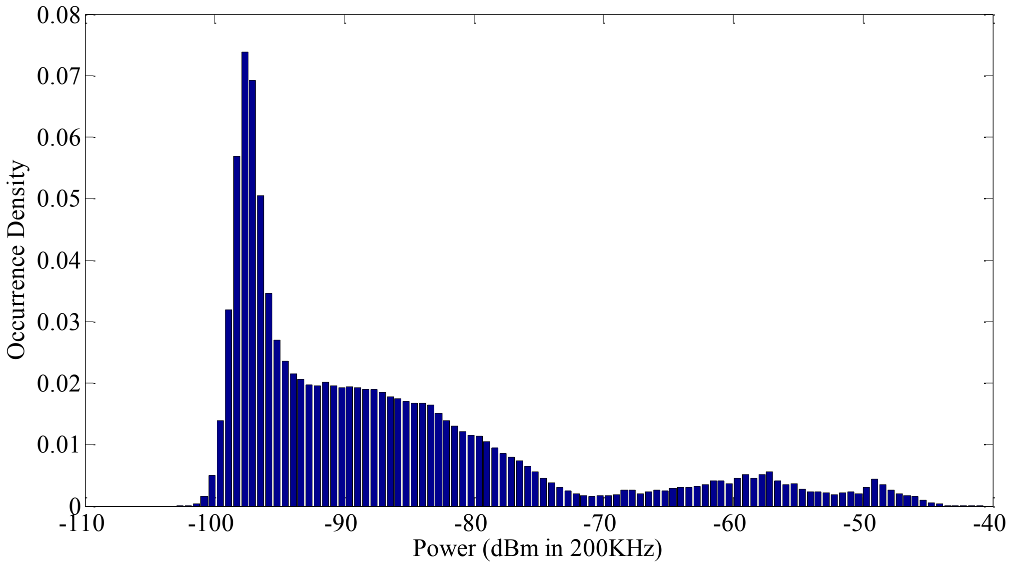


Figure 51 - Power Occurrence Density in the 1856.9 – 1857.1MHz band

4.4. Occupancy Results

With the measurements done, a characterization of the spectrum in terms of occupancy was required. Figure 52 shows the time period of opportunities distribution for the measured GSM900 band. By doing the logarithmic of the vertical axes (turns an exponential in a straight line) it can be concluded that this distribution has an exponential behavior with the first bin ill-conditioned. The total time of the opportunities is about 50 minutes in 24 hours which indicates high occupancy. About 39 minutes (of 50) is one frame opportunities. Figure 53 represents the correspondent time between opportunities distribution. This distribution has an exponential behavior with the first bin ill-conditioned.

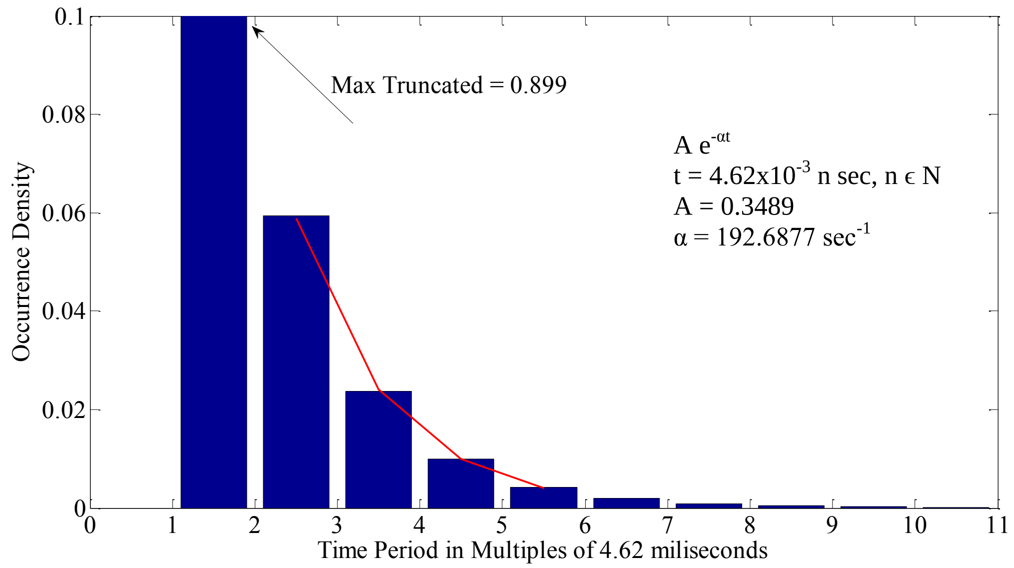


Figure 52 - Time period of opportunities distribution of the measured GSM900 band with -100 of reference value

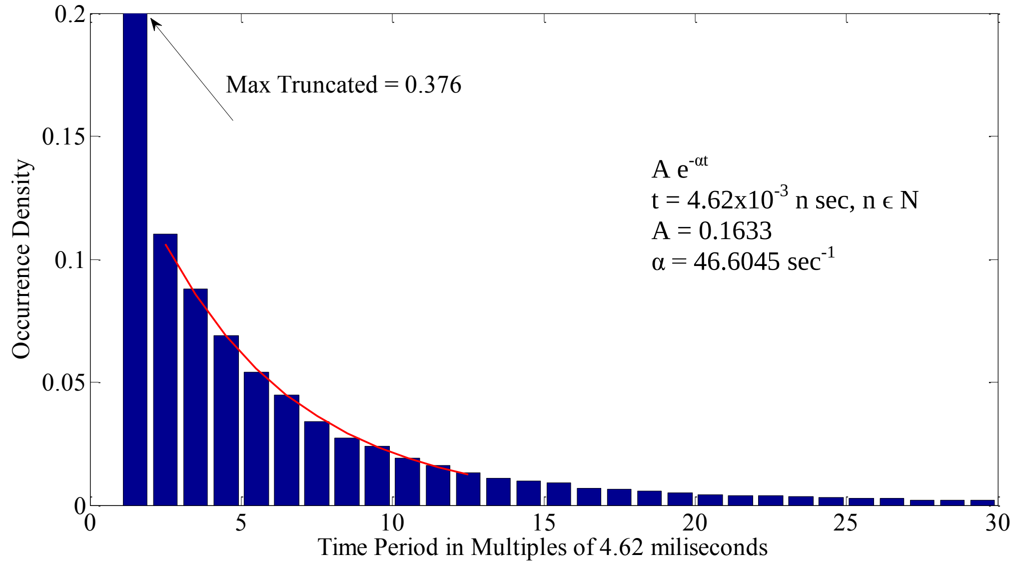


Figure 53 - Time between opportunities distribution of the measured GSM900 band with -100 of reference value

Figure 54 shows the time period of opportunities distribution for the measured DCS1800 band. This distribution presents a deviation from an exponential behavior. The total time of the opportunities is about 10 hours in 24 hours, which indicates relative low occupancy. About 2.4 hours (of 10) is one frame opportunities. It is found opportunities as long as 28 seconds (outside the horizontal axes represented in Figure 54). Figure 55 represents the correspondent time between opportunities distribution. This distribution has an exponential behavior with the first bin ill-conditioned.

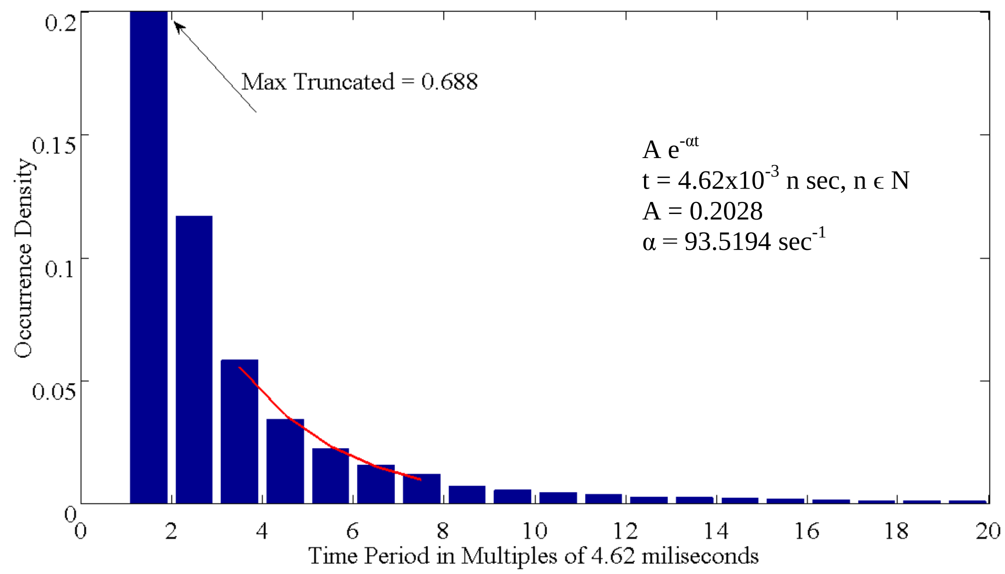


Figure 54 - Time period of opportunities distribution of the measured DCS1800 band with -90 of reference value

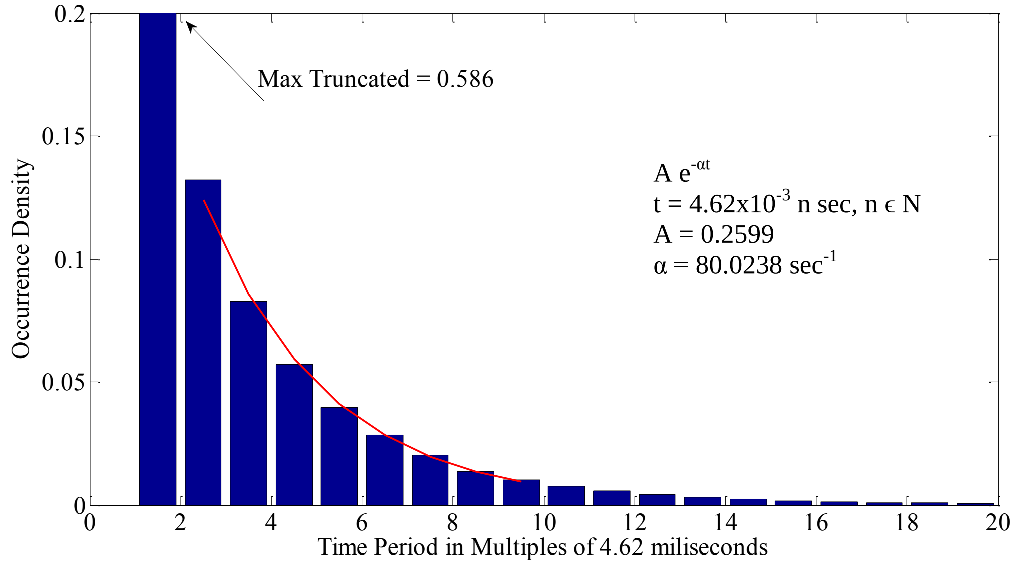


Figure 55 - Time between opportunities distribution of the measured DCS1800 band with -90 of reference value

4.5. UMTS Measurements Results

UMTS was also considered in this work as a possible band for the use of CR systems. Even though some restraints mentioned on the previous chapters, for spreading and despreading, the measurements were done in order to characterize and analyze the possibility of secondary users use some holes on the allocated spectrum.

As for measurements in GSM, ANACOM was asked to provide us with the frequency bands attributed to the mobile operators for UMTS. The management of these frequencies is done the same way for GSM and each mobile operator is responsible for their usage. The location of the base stations for FDD was also supplied (with GPS coordinates, and the same terms of confidentiality are applied, hence they are not identified in terms of which operator holds them (Figure 56).

Figure 56 - UMTS FDD base station's location in the region of Aveiro

According to ANACOM, the following table represents the allocated frequency bands in UMTS, for the current mobile operators in Portugal.

Table 4 – UMTS frequency bands attributed to mobile operators

Operator	Frequency Bands		Amount	Technology
	Downlink	Uplink		
Vodafone	1915,1-1920,1 MHz		5 MHz	UMTS TDD
Optimus	-		-	
TMN	1910,1-1915,1 MHz		5 MHz	
Not Attributed	1900,1 – 1910,1 MHz		10 MHz	
Vodafone	2110,3-2130,1 MHz	1920,3 – 1940,1 MHz	2 x 20 MHz	UMTS FDD
Optimus	2130,1-2149,9 MHz	1940,1 – 1959,9 MHz	2 x 20 MHz	
TMN	2149,9-2169,7 MHz	1959,9 – 1979,7 MHz	2 x 20 MHz	

With this, measurements were done in order to verify the considerations above mentioned. The measurements were done mainly for FDD downlink because of the characteristics of this band. TDD and FDD uplink present levels of transmission below the noise level, therefore they cannot be measured without any type of demodulation or any previous knowledge of the band.

The fact that there was no filter for UMTS band, our measurements setup was suppressed in some components. The main structure stayed the same but some elements like the filter and the amplifier weren't used and other considerations in terms of settings were taken. When it comes to the considered values for the antenna and the low attenuation cable are the following ones, 3dBi and 0.6306dB respectively. These values are for a 100 kHz band but since UMTS is organized differently than GSM, there's the need of considering a factor of $-10 * log_{10}(100kHz)$ and adding to the previous values in order to obtain the real attenuation in Hz. For FDD downlink, the measurements were divided in 2 parts because of its frequency distribution.

The first measurements part (2110.305MHz to 2160.305MHz) was done with a resolution bandwidth of 100 KHz and a video bandwidth of 300KHZ at 501 points. The sweep time was 5.0225 seconds, considering already the T_{Sweep} from the SA.

The second measurements part (2149.905MHZ to 2174.905MHz) was done with a resolution bandwidth of 100 KHz and a video bandwidth of 300KHZ at 251 points. The sweep time was 2.51625 seconds, considering already the T_{Sweep} from the SA.

In the end, the last part of the first measurements was not considered since only part of the TMN frequency band was measured. These few measures were suppressed and the second measurements part was added to the first. With this, an overview of the FDD downlink is presented on Figure 57.

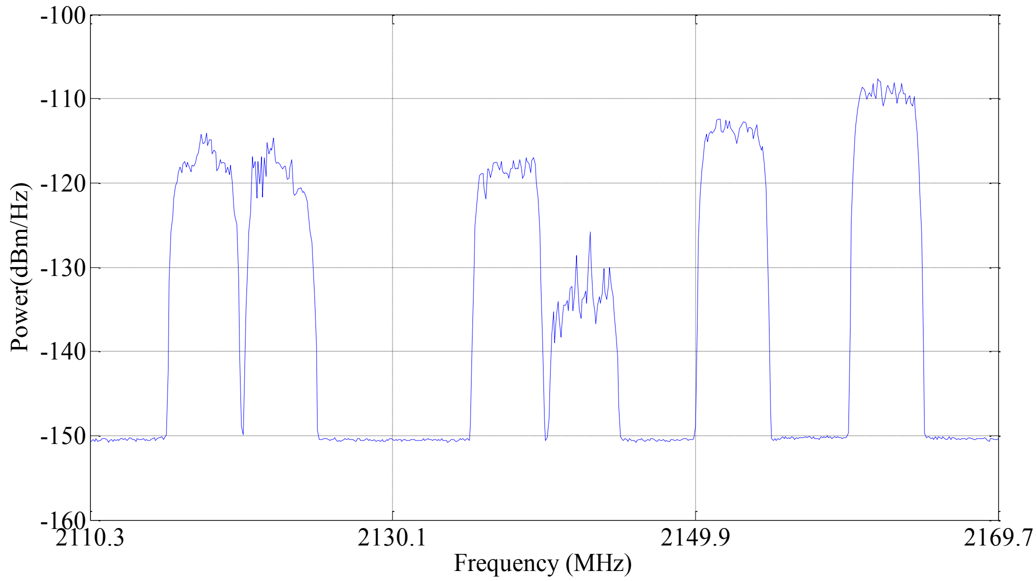


Figure 57 - FDD downlink frequency bands overview

Figure 57 show that some of the frequencies are not in use by the operators being a possible choice for secondary users through CR systems to enhance the use of spectrum. In addition, the top parts of the used frequencies show irregularities. This is due to the fact that the measurements were not done instantaneously and, when one point at one frequency was measured, the next point had a different power since it was measured in a different time instant.

5. Conclusions

The main goal stated at the beginning of this dissertation was to study and model occupancy, so it can be defined how secondary users would opportunistically share spectrum with primary systems.

Considering the main focus of this dissertation, the non occupancy total time of spectrum was examined to evaluate the potential of one determined band opportunistic use.

For the purpose of this study, a measurement setup was assembled to obtain power profiles during a working day. Through a revision of the state of the art concerning occupancy modeling and technical properties considerations of the primary systems, measurements were taken and recorded. A Matlab program was created for the purpose of obtaining statistical analysis of the spectral power data collected.

By doing the logarithm on the vertical axe of an exponential function graphic the result is a straight line. This method verifies if a determined curve is exponential. Through the points obtained by that linearization it can be obtained the least square straight line parameters. By doing the logarithm inverse operation it can be obtained the exponential parameters like amplitude and decay from the least square straight line parameters. This was the way to model and parameterize the exponentials distributions obtained from the measured data

The obtained statistical results allowed the creation of a model of occupancy and non occupancy for a GSM 900 band and a DCS1800 band. Regarding the statistical analysis of the time period of opportunities for the measured GSM900 band, it showed that the distribution has an exponential behavior with the first bin ill-conditioned. An exponential behavior is also attributed to the correspondent time period between opportunities distribution (estimation) with first bin ill-conditioned. The total time of the opportunities is about 50 minutes in 24 hours which indicates high occupancy. About 39 minutes (of 50) is one frame opportunities. This particular band was one with lowest traffic of the entire GSM900 spectrum. It can be concluded that the entire GSM900 spectrum is not suitable for opportunistic usage due to its high occupancy.

Concerning the time period of opportunities distribution for the measured DCS1800 band, the exponential behavior is present with the first and second bin ill-conditioned. Also, for the correspondent time period between opportunities distribution an exponential behavior is present, with the first bin ill-conditioned. The total time of the opportunities is about 10 hours in 24 hours, which indicates relative low occupancy. About 2.4 hours (of 10) is one frame opportunities. Opportunities as long as 28 seconds are found in the recorded data for this band. It can be concluded that this DCS1800 frequency has low occupancy, enough to enable opportunistic use.

Regarding the UMTS spectrum, a measurement in all bandwidth was done in order to verify the spectrum occupancy, for opportunistic use by CR systems. In this case the detection of the band is easier since UMTS usage is always done with BCCH channels on. For the UMTS spectrum, some of the frequencies previously allocated for mobile operators are not in use, being a possible choice of spectrum usage for secondary users.

5.1. Continuing work

While some key results for cooperative communication have already been obtained, there are many more issues that remain to be addressed. Results indicate that spectrum utilization of GSM900 is very high with the band being available for 1 frame transmission only about 39 minutes in 24 hours. Measurements in bands more suitable might be of more use for the CR systems, therefore the continuation of measurements analyzes, is somehow important for future CR systems considerations. Furthermore, whereas, highly populated GSM bands can be modeled by a distribution, a probabilistic model matching the less crowded (more useful for CR systems) bands can be obtained with the already implemented setup.

Different measurements can be done in the DCS1800 spectrum, in order to obtain more models for opportunistic use.

At the moment is also being developed a double setup based in the single measurements setup, with similar characteristics. These measurements will provide different types of information (e.g. power correlation between two spatial separated points) important in fusion analysis. A program in Labview is underdevelopment to collect the synchronous power measurements of the 2 setups.

Contributions to conferences

The main results obtained from this work were resumed into a paper which is entitled: "*GSM Downlink Spectrum Occupancy Modeling*", Luís Mendes, Luís Gonçalves and Atílio Gameiro. It was submitted and accepted for the **22nd IEEE Personal Indoor Mobile Radio Communications** - *PIMRC'11 - Cognitive Radio and Spectrum Management*, which will take place in Toronto, Canada from 11 of September to 14 of September 2011.

Appendix A

Matlab program used to represent and analyze the recorded data obtained from the Rohde & Schwarz program (FxRecord_Play)

The program created simultaneously with the measurements setup, gives the support needed to provide data representation and data analyzes, fundamental for this dissertation. The program can be executed by the filename *"Program_reading.m"*, that initially presents the user the first request to insert the name of the file considered together with its extension (Figure 58).

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Programa de testes de acordo com o programa FSxRecordPlay
Luis Miguel Vinhas Mendes
Instituto de Telecomunicações
Universidade de Aveiro
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Insira o nome do ficheiro: |
```

Figure 58 - First request

After entering the name of the file, the main menu shows and presents the user the main options (Figure 59). The user needs to choose an option number from 1 to 4 according to the user's needs, or use the number 5 to exit the program.

```
Opções de Processamento disponiveis
1 - Percentagem de valores acima de uma potência de referência
2 - Potência do sinal acima ou abaixo da potência de referência
3 - Evolução da potência ao longo do tempo para uma dada frequência
4 - Evolução da potência total ao longo do tempo para uma gama de frequências

5 - Sair do programa

Insira a opção pretendida:
```

Figure 59 - Main options

Option 1: Presents the percentage of values above a reference power

This option internally accesses a different file called *"processamento_1.m"* to do all of its processing, and on Matlab's command window it requires the user to provide a reference power of its choice, after this, the program asks if there's any other main option to run, and in the end it asks the user if there's a "correction factor" (in dBs) in case the measurements were done with gains or attenuations that need to be considered (Figure 60).

```
Insira a opção pretendida: 1
Insira uma Potência de Referência: 90
Deseja fazer mais algum processamento? (1-Sim 2-Não): 2
Introduza factor de correcção (0 - se não quiser um factor):
```

Figure 60 – Series of settings required to the user for option 1 chosen

This "correction factor" is the sum of all gains and attenuations used on the measurements, that it will be discounted on every single data value recorded by the program FsRecord_Play. The Matlab program will then analyze the collected and corrected data, and provide a graphic with the information needed. One example of the final representation for this option is presented by Figure 61.

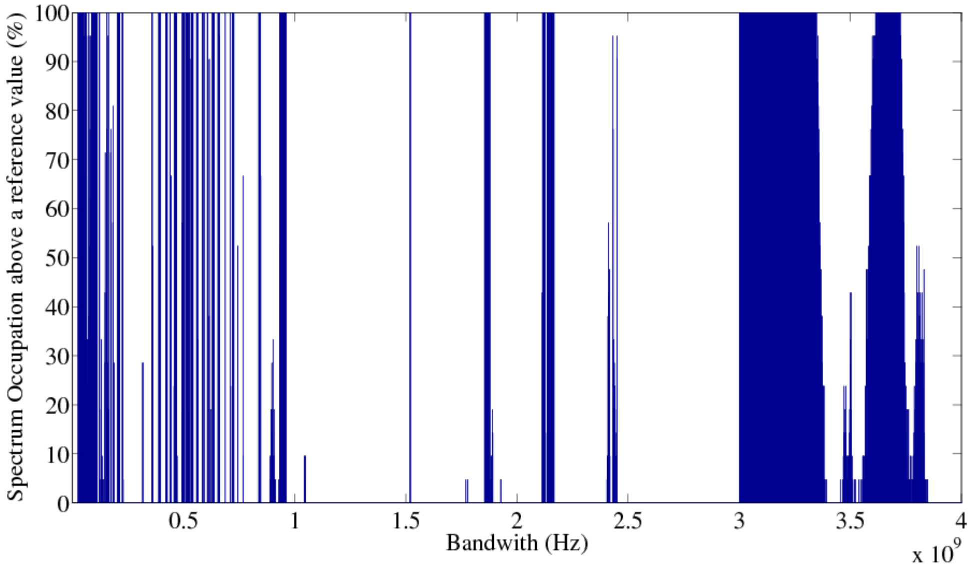


Figure 61 - Example of a resulting data analyzes for option 1

This option provides also additional information, such as the frequency/band analyzing and the time that took for processing all the data.

```
Gama de frequências considerada: 25000000 Hz - 4.000025e+009 Hz
Elapsed time is 0.341739 seconds.
```

Figure 62 - Additional information for option 1

Option 2: Signal power above or below a reference power

This option it requires the user to provide a reference power of its choice, if the data recorded is for single frequency or a range of frequencies, if there's any other main option to run, and in the end it asks the user if there's a "correction factor" (in dBs) in case the measurements were done with gains or attenuations that need to be considered. There are 2 options when Option 2 is selected. The first requires a data file with single frequency recorded, and the other one requires a data file with a range of frequencies recorded. The single frequency option selected gives a warning mentioning that the frequency used is going to be the one recorded on the header part of the file selected (Figure 63). The range of frequencies option selected, asks the user for a frequency select, in this case a number from 0 to *"valores_lidos"* (maximum value of values read), in order to proceed with the data analyzes on that frequency (Figure 64). The frequency chosen for this last option is selected this way in order to avoid problems in selected frequencies with decimal values.

```
Insira a opção pretendida: 2
Insira uma Potência: -100
Modo de processamento: 1 - Frequência única 0 - Gama de Frequências: 1
WARNING - Frequência considerada na leitura dos dados
Deseja fazer mais algum processamento? (1-Sim 2-Não): 2
Introduza factor de correcção (0 - se não quiser um factor):
```

Figure 63 – Example of series of settings required to the user for option 2 chosen (Single frequency option)

```
Insira a opção pretendida: 2
Insira uma Potência: -100
Modo de processamento: 1 - Frequência única 0 - Gama de Frequências: 0
Insira a Frequência de referência: 150
Deseja fazer mais algum processamento? (1-Sim 2-Não): 2
Introduza factor de correcção (0 - se não quiser um factor):
```

Figure 64 – Example of series of settings required to the user for option 2 chosen (Range of frequencies option)

The Matlab program will then analyze the collected and corrected data, providing 2 bars graphics with the information for time period of opportunities, and another one for time between opportunities. One example of the final representation for this option is presented by Figure 65. The same additional information as in Option 1 is provided.

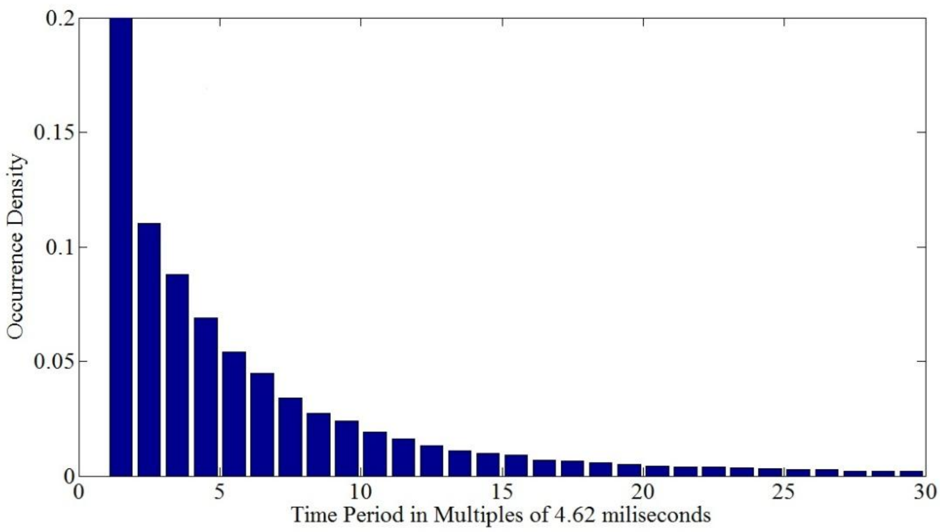


Figure 65 - Example of one bar graphic provided by the matlab program for option 2

Option 3: Power vs. time for a given frequency/band of frequencies

This option it requires the user to provide a reference power of its choice, if the data recorded is for single frequency or a range of frequencies, if there's any other main option to run, and in the end it asks the "correction factor" (in dBs). Likewise Option 2, there are 2 options when Option 2 is selected. The first requires a data file with single frequency recorded (Figure 66), and the other one requires a data file with a range of frequencies recorded (Figure 67). The option for the range of frequencies presents another request for the selected frequency. The analysis for the range of frequencies is done only for the selected frequency, requested by the program.

```
Insira a opção pretendida: 3
Modo de processamento: 1 - Frequência única 0 - Gama de Frequências: 1
Deseja fazer mais algum processamento? (1-Sim 2-Não): 2
Introduza factor de correcção (0 - se não quiser um factor):
```

Figure 66 – Example of series of settings required to the user for option 3 chosen (Single frequency option)

```
Insira a opção pretendida: 3
Modo de processamento: 1 - Frequência única 0 - Gama de Frequências: 0
Insira uma Frequência: 150
Deseja fazer mais algum processamento? (1-Sim 2-Não): 2
Introduza factor de correcção (0 - se não quiser um factor):
```

Figure 67 - Example of series of settings required to the user for option 3 chosen (Range of frequencies option)

The Matlab program will then analyze the collected and corrected data, providing 3 graphics. One of them is a plot with the information for Power vs. Time, another one is a bar graphic with Number of Occurrences vs. Power, and the last one is a bar graphic with Occurrence Density vs. Power. One example of the final representation for this option is presented by Figure 68. The same additional information as in Option 1 is provided.

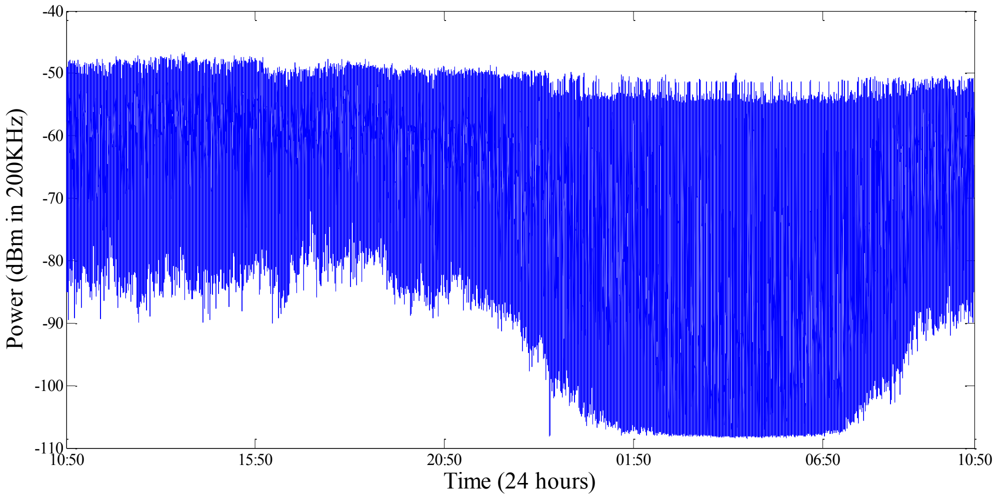


Figure 68 - Example of one graphic provided by the matlab program for option 3

Option 4: Total Power vs. Time for a frequency band

This option it only asks the user if there's any other main option to run, and in the end it requires the "correction factor" (in dBs) for the data analyzes.

```
Insira a opção pretendida: 4
Deseja fazer mais algum processamento? (1-Sim 2-Não): 2
Introduza factor de correcção (0 - se não quiser um factor):
```

Figure 69 - Example of series of settings required to the user for option 4 chosen

The Matlab program will then analyze the collected and corrected data, and provide a graphic with the information needed. One example of the final representation for this option is presented by Figure 70. The same additional information as in Option 1 is provided. This option allowed in this work, to calculate the power at the mixer's entrance of the SA.

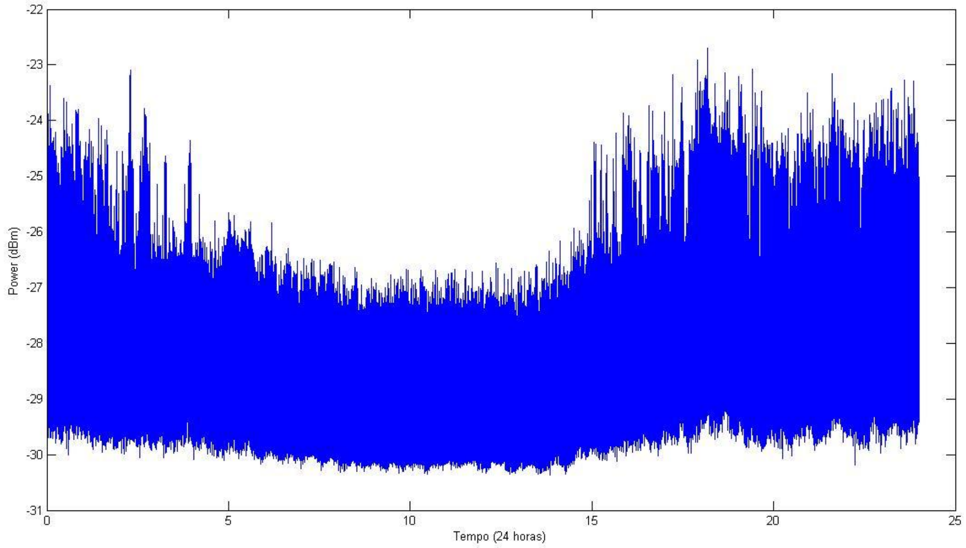


Figure 70 - Example of one graphic provided by the matlab program for option 4

Option 5: Exits the program

This option exits the program.

6. References

[1] J. R. Timo Halonen, Juan Melero, *GSM, GPRS and edge performance: evolution towards 3G/UMTS*: John Wiley and Sons, 2003.

[2] E. TC-SMG, "Multiplexing and Multiple Access on the Radio Path" in *GSM 05.02: European digital cellular telecommunications system (Phase 2)*, ed, September, 1994.

[3] A. W. R. W. Broderson, D. Cabric, S. M. Mishra and D. Willkomm, "CORVUS: A Cognitive Radio Approach for Usage of Virtual Unlicensed Spectrum" Tech. Rep.2004.

[4] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Phd Thesis, Royal Institute of Technology (KTH), Kista, Sweden, 2000.

[5] R. Akalu, "Spectrum Management and Cognitive Radio in Ireland," presented at the Competition and Regulation in Network Industries (CRNI), Brussels, Belgium, 2008.

[6] D. S. Peter Steenkiste, Gary Minden, Dipankar Raychaudhuri, "Future Directions in Cognitive Radio Network Research," NSF Workshop Report2009.

[7] J. Mitola, "Cognitive Radio for Flexible Mobile Multimedia Communications," presented at the 6th International Workshop on Mobile Multimedia Communications (MoMuC), San Diego, CA , USA, 1999.

[8] J. Mitola. Cognitive Radio Architecture: The Engineering Foundations of Radio XML [Online].

[9] B. Fette, Ed., *Cognitive radio technology*. Amsterdam: Elsevier, 2006, p.^pp. Pages.

[10] QOSMOS. (2010). *http://www.ict-qosmos.eu/home.html*.

[11] Mobnet. (2011). *http://www.av.it.pt/mobnet/*.

[12] P. Marques, H. Marques, J. Ribeiro, A. Gameiro, "Coexistence Analysis and Cognitive Opportunities Selection in GSM Bands," presented at the IEEE 69th Vehicular Technology Conference. VTC Spring, Barcelona, Spain, 2009.

[13] a. F. C. M. López-Benítez, "Spectrum Occupancy in Realistic Scenarios and Duty Cycle Model for Cognitive Radio," *Advances in Electronics and Telecommunications*, vol. 1, pp. 26–34, April 2010.

[14] H. J. V. Blaschke, T. Renk, C. Kloeck, and F. K. Jondral, "Occupation Measurements Supporting Dynamic Spectrum Allocation for Cognitive Radio Design" presented at the 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), Orlando, Florida, USA, 2007.

[15] T. W. Hazlett, "Optimal Abolition of FCC Spectrum Allocation" *Journal of Economic Perspectives*, vol. 22, 2008.

[16] J. R. A. Matthias Wellens, Martin Gordziel and Petri Mahonen, "Evaluation of Cooperative Spectrum Sensing based on Large Scale Measurements" presented at the New Frontiers in Dynamic Spectrum Access Networks DySPAN, Chicago, IL, Oct. 2008

[17] F. C. C. (FCC), "Report of the Unlicensed Devices and Experimental Licenses Working Group" November, 2002.

[18] B. L. David Maldonado, Akilah Hugine, Thomas W. Rondeau, Charles W. Bostian, "Cognitive radio applications to dynamic spectrum allocation: A discussion and an illustrative example" presented at the Proc. Dynamic Spectrum Access Nets, Baltimore, MD, 2005.

[19] W. B. C. S. Laboratory. (2008). *http://santos.ee.ntu.edu.tw/research.html*.

[20] M. K. W. Siegmund H. Redl, Malcolm W. Oliphant, *GSM and Personal Communications Handbook*. Boston, London: Artech House, 1998.

[21] Ericsson, "EN/LTZ 123 5374 R1B GPRS System Survey" Ericsson1999.

[22] F. Hillebrand, *GSM & UMTS: The Creation of Global Mobile Communications*: Wiley, 2001.

[23] H.-J. V. Jörg Eberspächer, *GSM - Switching Services and Protocols*: John Wiley & Sons, 1999.

[24] Ericsson, "The evolution of EDGE" Ericsson2009.

[25] R. R. a. G. Americas. (2007, EDGE, HSPA and LTE: The Mobile Broadband Advantage.

[26] M.-B. P. Michel Mouly, *The GSM System for Mobile Communications*: Telecom Publishing, 1992.

[27] L. Harte, *Introduction to GSM - Physical Channels, Logical Channels, Network Functions, and Operation*, 2nd ed.: Althos, 2009.

[28] Agilent. (2008). *About GSM Design Library*. Available: http://edocs.soco.agilent.com/display/ads2008U1/About+GSM+Design+Library

[29] COST231, *Digital Mobile Radio towards Future Generation Systems*: COST 231 Final Report, 1999.

[30] W.-S. H. Yu-Huei Tseng, Ce-Kuen Shieh, "The Influence of Propagation Environment in a Live GSM Network" presented at the International Computer Symposim (ICS 2002), Hualien, Taiwan, 2002.

[31] F. Hägglund, "Improved Power Control for GSM/EDGE" MSc, Luleå University of Technology, Luleå, Sweden, 2005.

[32] M. Kabir, "TCOM1010 Cellular Mobile Systems and Services - GSM Radio (Part 2)" CSU Fullerton, Fullerton2009.

[33] H. A. a. K. W. Magnus Almgren, "Power control in a cellular system" presented at the IEEE 44th Vehicular Technology Conference (VTC), Stockholm, Sweden, 1994.

[34] F. G. F. Gunnarsson, J. Blom, "Estimation and Outer Loop Power Control in Cellular Radio Systems" Linköping University, Linköping, Sweden2001.

[35] ETSI. (2011). *http://www.etsi.org/*.

[36] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed.: Prentice Hall, 2001.

[37] P. Prabakaran. 2003, Tutorial on Spread Spectrum Technology.

[38] L. M. R. Pickholtz, and D. Schilling, "Spread spectrum for mobile communications," *IEEE Transactions on Vehicular Technology*, vol. 40, 1991.

[39] L. H. J. S. Blogh, Ed., *Third Generation Systems and Intelligent Wireless Networking: Smart Antennas and Adaptive Modulation* Wiley-IEEE Press, 2002.

[40] Maxim, "An Introduction to Spread-Spectrum Communications" Maxim Integrated Products, Sunnyvale, CA, U.S.2003.

[41] C. Andren. 1997, A Comparison of Frequency Hopping and Direct Sequence Spread Spectrum Modulation.

[42] S. Natarajan, "CDMA versus TDMA" *infosecwriters*, 2006.

[43] UMTSworld. (2003). *www.umtsworld.com*.

[44] L. C. C. Gonçalves, "Detecção Multiutilizador no Domínio da Frequência para Sistemas DS-CDMA" PhD, Electronic, Telecommunications and Informatics Department, University of Aveiro, Aveiro, Portugal, 2009.

[45] A. T. Harri Holma, *WCDMA for UMTS: Radio Access for Third Generation Mobile Communications*, 3rd ed.: John Wiley & Sons, 2004.

[46] D. A. T. Dr Harri Holma, *WCDMA for UMTS: HSPA Evolution and LTE*, 5th ed.: Wiley, 2010.

[47] M. Laner, "Evaluation and Modeling of Power Control Information in a 3G Cellular Mobile Network" Wien Technical University, Wien, 2009.

[48] F. G. Fredrik Gunnarsson, "Control theory aspects of power control in UMTS," *Elsevier,* 2003.

[49] K.-C. C. a. R. Prasad, *Cognitive Radio Networks*: John Wiley & Sons Ltd, 2009.

[50] S. M. M. Danijela Cabric, Robert W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios" presented at the Conference Record Thirty-Eighth Asilomar Conference on Signals, Systems and Computers 2004.

[51] D. N. J. Pérez-Romero, M.López-Benítez, F. Casadevall, "Towards More-Efficient Spectrum Usage: Spectrum Sensing and Cognitive-Radio Techniques" Technical University of Catalonia, Barcelona, Spain, 2011.

[52] A. T. a. R. W. B. Danijela Cabric, "Spectrum Sensing Measurements of Pilot, Energy, and Collaborative Detection" presented at the Military Communications Conference, MILCOM, Washington, DC, Oct. 2006

[53] R. Schwarz. (2011). *http://www.rohde-schwarz.pt/*.

[54] C. Rauscher, *Fundamentals of Spectrum Analysis*. München, Germany: Rohde & Schwarz, 2001.

[55] MPAntenna, "Super-M Ultra Base" United States Patent, 2009.