
Germano Gonçalves Capela

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Examination Committee

Chairperson: Prof. Fernando Duarte Nunes (IST)
Supervisor: Prof. António José Castelo Branco Rodrigues (IST)
Member of Committee: Prof. Nuno Miguel Gonçalves Borges de Carvalho (UA)
Member of Committee: Eng. Eduardo José Ludovico Bolas (CINAV – Marinha Portuguesa)

October 2014
Acknowledgements

I would like to thank my supervisors, Professor António Rodrigues and Professor José Sanguino, for providing me the opportunity to work on a very interesting subject and for being always available to answer all my questions.

I would like to thank Eng. Eduardo Bolas for his friendship and for supporting me throughout the course of the master degree.

I would also like to thank my girlfriend, Patrícia, my family and friends and all my colleagues at IST.

Finally I would like to thank the GNU Radio internet community for their support.
Abstract

The VHF band is the first choice for the majority of maritime coastal communications because of its affordability, reliability, ease of use and an adequate effective range (up to 30 nautical miles), but expensive satellite links are typically used for all digital communications. However, future navigation and monitoring technologies, such as e-navigation and shipborne personal communications, require high speed (broadband) communication systems, while maintaining affordability. This thesis describes the implementation of a prototype cognitive radio based on software defined radio technology for opportunistic usage of vacant maritime radio spectrum bands, as an alternative to existing expensive satellite links. After an overview on the most recent advances in cognitive radio technology, the target environment and incumbent user's characteristics is studied and the baseline implementation to address existing issues of maritime communications is presented. The implementation focuses on three essential components: spectrum sensing (a multichannel energy detector), radio transceiver (which uses non contiguous Orthogonal Frequency Division Multiplexing multicarrier modulation) and cognitive medium access control. The implemented cognitive radio uses GNU Radio software for digital signal processing and physical layer design and the Universal Software Radio Peripheral as radio front-end. In order to evaluate the proposed prototype, a set of benchmark simulations based on the expected propagation channel conditions are performed. Then, the prototype is validated in laboratorial tests where it is demonstrated that the system is capable of detecting incumbent user activity and to use vacant spectrum bands without interfering with incumbent users. Finally, some directions towards future work and considerations regarding future implementations are provided.

Keywords

Cognitive Radio, GNU Radio, NC-OFDM, Software Defined Radio, USRP
Resumo

Uma elevada percentagem das comunicações marítimas junto à costa ocorre na banda do VHF, devido à sua fiabilidade, facilidade de utilização, baixo custo e alcance efectivo (até 30 mi). No entanto, existe uma maior procura por sistemas inteligentes e com elevada integração, o que requer sistemas de comunicação de banda larga, mas a um custo suportável. Esta tese descreve a implementação de um sistema rádio cognitivo baseado em tecnologia de rádio definido por software, o qual tem a capacidade de utilizar bandas do VHF de forma oportunista, como sendo uma alternativa aos dispendiosos sistemas satélite. São estudadas as mais recentes tecnologias associadas aos rádios cognitivos, as características da banda de interesse e seus utilizadores primários, sendo com estes elementos proposta uma solução de implementação. Nesta implementação são focados três componentes essenciais: monitorização do espectro (com um detector de energia multi-canal), transreceptor rádio (o qual utiliza a modulação multi-portadora Multiplexagem por Divisão Ortogonal de Frequência) e um gestor cognitivo de acesso ao espectro radioeléctrico. O processamento digital de sinal e implementação da camada física é feito utilizando o software GNU Radio e o periférico rádio Universal Software Radio Peripheral. O protótipo é avaliado através de simulações que reproduzem condições aproximadas de propagação do meio marítimo, mas também é validado em ambiente laboratorial. Neste último, é demonstrada a capacidade do sistema detectar a actividade dos utilizadores primários e de utilizar as bandas livres sem interferir com estes. No final, são feitas considerações sobre eventuais melhorias e trabalho futuro.

Palavras-chave

Software Defined Radio, Cognitive Radio, USRP, GNU Radio, NC-OFDM
# Table of Contents

Acknowledgements ........................................................................................................ iii
Abstract .......................................................................................................................... v
Resumo ........................................................................................................................... vii
Table of Contents ............................................................................................................. ix
List of Figures .................................................................................................................. xi
List of Tables ..................................................................................................................... xv
List of Acronyms .............................................................................................................. xvii
List of Software .............................................................................................................. xxi

1 Introduction .................................................................................................................. 1
  1.1 Motivation and Overview ......................................................................................... 2
  1.2 Contributions and Outline ....................................................................................... 5
    1.2.1 Outline ............................................................................................................... 6

2 Cognitive Radio Technology ......................................................................................... 9
  2.1 Dynamic Spectrum Access ....................................................................................... 10
    2.1.1 Opportunistic Use of Radio-Frequency Spectrum ............................................. 10
    2.1.2 Spectrum Sensing ............................................................................................. 11
    2.1.3 Spectrum Shaping - Transceiver Challenges and Techniques .......................... 17
  2.2 Cognitive Radios ...................................................................................................... 23
  2.3 Software Defined Radios ........................................................................................ 24
  2.4 Related Work .......................................................................................................... 31

3 Proposed Solution ........................................................................................................ 33
  3.1 Introduction ............................................................................................................. 34
  3.2 Scenario Description ............................................................................................... 34
    3.2.1 Opportunistic Usage of the VHF Maritime band .............................................. 36
  3.3 System Architecture ............................................................................................... 40
    3.3.1 Radio Interface ................................................................................................. 40
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.2</td>
<td>Medium Access Control and Duplexing Strategies</td>
<td>41</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Network Synchronization</td>
<td>42</td>
</tr>
<tr>
<td>3.3.4</td>
<td>Coastal / Master Station Design</td>
<td>43</td>
</tr>
<tr>
<td>3.3.5</td>
<td>Vessel / Slave Station Design</td>
<td>45</td>
</tr>
<tr>
<td>3.4</td>
<td>Spectrum Sensing</td>
<td>47</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Frequency Domain Energy Detector Implementation</td>
<td>47</td>
</tr>
<tr>
<td>3.5</td>
<td>NC-OFDM Transceiver Design – The B-VHF Radio</td>
<td>50</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Transmitter Design</td>
<td>50</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Receiver Design</td>
<td>54</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Dynamic Transceiver Reconfiguration</td>
<td>56</td>
</tr>
<tr>
<td>3.6</td>
<td>Cognitive Engine</td>
<td>58</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Cognitive Engine Logical Connections</td>
<td>58</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Network Synchronization</td>
<td>60</td>
</tr>
<tr>
<td>3.6.2</td>
<td>Spectrum Watcher and Spectrum Policy Enforcement</td>
<td>62</td>
</tr>
<tr>
<td>3.6.3</td>
<td>Host Operating System Interface</td>
<td>64</td>
</tr>
<tr>
<td>4</td>
<td>Test and Demonstration</td>
<td>67</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>68</td>
</tr>
<tr>
<td>4.2</td>
<td>Spectrum Sensing Performance Analysis</td>
<td>68</td>
</tr>
<tr>
<td>4.3</td>
<td>Transceiver Performance Analysis</td>
<td>72</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Packet Benchmarking</td>
<td>74</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Spectral Shaping and Radiation Performance Analysis</td>
<td>76</td>
</tr>
<tr>
<td>4.3.3</td>
<td>PU Coexistence Analysis</td>
<td>83</td>
</tr>
<tr>
<td>4.4</td>
<td>Network Synchronization</td>
<td>85</td>
</tr>
<tr>
<td>4.5</td>
<td>Performance Test with IP Data Packets</td>
<td>85</td>
</tr>
<tr>
<td>5</td>
<td>Conclusions</td>
<td>89</td>
</tr>
<tr>
<td>A</td>
<td>Portuguese VHF Spectrum Allocations</td>
<td>95</td>
</tr>
<tr>
<td>B</td>
<td>Channel and Frequency Arrangement</td>
<td>97</td>
</tr>
<tr>
<td>B.1</td>
<td>Radio Regulations Appendix 18</td>
<td>98</td>
</tr>
<tr>
<td>C</td>
<td>GNU Radio OFDM Implementation</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>103</td>
</tr>
</tbody>
</table>
List of Figures

Figure 1.1 – Maritime communications user requirements – integrity vs speed. Source: [2] ...............3
Figure 2.1 - Block diagram of a time domain energy detector. Source: [33]...........................................13
Figure 2.2 - Block diagram of a frequency domain energy detector. .........................................................13
Figure 2.3 – Wavelets-based method detecting sub-band edges (data synthesized with GNU Radio). ..........................................................13
Figure 2.4 – Spectral Autocorrelation Function of a Narrow Band FM (NBFM) signal (data synthesized with GNU Radio and analysed with Python and Scipy) ..........................................................14
Figure 2.5 - Complexity vs Accuracy of spectrum sensing techniques. ......................................................15
Figure 2.6 – Spectrogram (time-frequency) plot of several PU in activity (data synthesized with GNU Radio). .................................................................................................................................16
Figure 2.7 - Spectrum sensing hypothesis decision workflow........................................................................16
Figure 2.8 - Spectrogram (time-frequency) plot of PU activity and spectrum opportunities. .........................17
Figure 2.9 - Example of two different spectrum access schemes: a) Using a single spectrum hole; b) Multiplexing several spectrum holes .............................................................18
Figure 2.10 - Block diagrams of an OFDM transmitter .............................................................................19
Figure 2.11 - Block diagrams of an OFDM receiver .................................................................................19
Figure 2.12 - Basic spectrum shaping using OFDM sub-carrier assignment ..............................................20
Figure 2.13 - PAPR Complementary Cumulative Distribution Function of a DVB-T OFDM signal. Measured with an USRP and GNU Radio and analysed with Python’s Numpy. ........20
Figure 2.14 - Degradation of OOB radiation performance due to signal clipping (data synthesized with GNU Radio). ...................................................................................................................21
Figure 2.15 - Insertion of cancellation sub-carriers to reduce OOB radiation. Source: [63] .................22
Figure 2.16 - Basic cognitive cycle. Source: [3] ....................................................................................23
Figure 2.17 - Basic architecture of a SDR. Source: [66]. .................................................................25
Figure 2.18 – GNU Radio layered Application Programming Interface (API). Source: [67].................26
Figure 2.19 - GNU Radio’s graphical development environment - GNU Radio Companion. ................26
Figure 2.20 - Hardware and software components in a SDR topology ....................................................27
Figure 2.21 - Three different USRP family products from Ettus Research. Source: Ettus Research LLC. .................................................................................................................................28
Figure 2.22 - Internal overview and basic schematic of an USRP1. Source: [69] .................................28
Figure 2.23 – Daughterboard frequency coverage. Source: [68] ...........................................................29
Figure 2.24 - USRP B100 block diagram and USRP B100 + WBX. Source: [68].................................30
Figure 2.25 - HackRF and bladeRF SDR platforms. Source: [70, 71]. ....................................................30
Figure 2.26 - IEEE 802.22 cognitive radio capability overview. Source: [19]. ..........................................31
Figure 3.1 - Overview of Maritime Communications scenarios: a) Long range communications (HF / SATCOM); b) Medium / Short range communications (VHF). .........................35
Figure 3.2 - Hidden node problem illustration. .......................................................................................35
Figure 3.3 - Hidden node problem in cognitive radio scenarios ..............................................................36
Figure 3.4 - VHF telephony signals PSD (soft speech) from three different primary user equipments captured at 156.750 MHz using GNU Radio and USRP (one handheld and two fixed VHF transceivers) ..........................................................37
Figure 3.5 - NBFM PSD of a synthesized signal with GNU Radio ...........................................................38
Figure 3.6 – Digital Selective Call PSD from synthesized signal with GNU Radio. .............................38
Figure 3.7 – AIS channels A and B PSD plot of a recorded signal using GNU Radio and USRP (green plot – maximum envelope, blue plot – detected peak) ........................................... 38
Figure 3.8 - Channel and Frequency allocation chart for VHF MMS. Source: [77] ............................ 39
Figure 3.9 - Typical MMS radio picture - PSD from recorded signal using GNU Radio and USRP. .......................................................... 39
Figure 3.10 - Proposal for B-VHF radio infrastructure architecture .................................................. 41
Figure 3.11 – FDD spectral arrangement proposal for B-VHF application (synthesized data with GNU Radio). .................................................. 41
Figure 3.12 - Proposal for data channels and synchronization channels (synthesized data with GNU Radio). ................................................................ 42
Figure 3.13 - Master station layer stack design for CSMA/CA operation ........................................ 43
Figure 3.14 - Synchronization transceiver bandwidth comparison...................................................... 44
Figure 3.15 - Master station layer stack design for FDD operation .................................................... 45
Figure 3.16 - Slave station layer stack design for CSMA/CA operation ........................................... 46
Figure 3.17 - Slave station layer design for FDD operation .............................................................. 46
Figure 3.18 - Spectrum sensing implementation in GNU Radio .......................................................... 47
Figure 3.19 - Workflow of the spectrum sensing framework ............................................................... 48
Figure 3.20 - FM radio band survey using the proposed energy detector (channel spacing = 100 kHz) .............................................................. 49
Figure 3.21 – NC-OFDM Radio in GNU Radio Companion .................................................................. 50
Figure 3.22 – Inserting a packet into the radio transmitting chain .................................................... 51
Figure 3.23 - Cognitive engine interface with transmitter flowgraph – packet data transmission ....... 51
Figure 3.24 - OFDM modulation section of the transmitter ............................................................... 52
Figure 3.25 - OFDM pre-transmitter section ...................................................................................... 53
Figure 3.26 - Magnitude and phase response for the transmitting filter (normalized frequency) .... 53
Figure 3.27 - B-VHF Radio Output Spectrum Shape ...................................................................... 54
Figure 3.28 - Receiver’s RF front end ............................................................................................... 55
Figure 3.29 - Receiver synchronization and detection ...................................................................... 55
Figure 3.30 - Payload demodulation ............................................................................................... 55
Figure 3.31 - Cognitive engine interface with receiver flowgraph – packet data reception ............ 56
Figure 3.32 - Synthesizing synchronization data - master stations only ....................................... 57
Figure 3.33 - Synchronization data and OFDM radio dependencies ................................................. 58
Figure 3.34 - Cognitive Engine Physical and Logical Channels ....................................................... 59
Figure 3.35 - Synchronization and B-VHF frame structure ............................................................... 59
Figure 3.36 - Switching from B-VHF Mode to SYNC Mode problem. a) slave acknowledge only; b) slave and master acknowledge .................................................. 60
Figure 3.37 - Adopted solution for switching from B-VHF Mode to Sync Mode: a) normal scenario; b) slave loses order packet but switches automatically to sync mode. ........61
Figure 3.38 - Master station state flow ............................................................................................. 61
Figure 3.39 – Slave station state flow ............................................................................................. 62
Figure 3.40 - Spectrum Watcher workflow ...................................................................................... 63
Figure 3.41 - OS interface detail – transmitter side .......................................................................... 64
Figure 3.42 - OS interface detail – receiver side ............................................................................... 65
Figure 4.1 - GNU Radio flowgraph to evaluate the spectrum sensor block ......................................... 69
Figure 4.2 - Spectrum sensing output after PU detection ................................................................. 69
Figure 4.3 - GNU Radio flowgraph that simulates multiple PU NBFM activity ................................ 70
Figure 4.4 - Spectrum Sensing results (Python generated plots) ....................................................... 70
Figure 4.5 - Spectrum sensing output results from multiple PU detection ....................................... 71
Figure 4.6 - Recording signal samples using GNU Radio and USRP .............................................. 71
Figure 4.7 - Using recorded signals to test the spectrum sensing framework. ........................................71
Figure 4.8 - Detection results from recorded signals. ........................................................................72
Figure 4.9 - Data and work flow for simplex tests. ............................................................................72
Figure 4.10 – Graphical representation of the flowgraph for cognitive operation and benchmarking. ................................................................................................................73
Figure 4.11 – Percentage of received and correctly received packets vs SNR for different k factors, SNR [2.0 – 12.0] dB. ......................................................................................74
Figure 4.12 - Percentage of received and correctly received packets vs SNR for different k factors, SNR [5.0 – 8.0] dB. ......................................................................................75
Figure 4.13 - Laboratorial setup for over-the-air analysis. ..................................................................75
Figure 4.14 - Spectrogram (time-frequency) and PSD (averaged over 15 samples) of the transmitted signal. ........................................................................................................76
Figure 4.15 - Spectrogram (time-frequency) and PSD (averaged over 15 samples) of the received signal for SNR=7dB and k=2. .................................................................77
Figure 4.16 - Spectrogram (time-frequency) and PSD of the received signal by the USRP. ............78
Figure 4.17 - OOB and NC radiation details of the transmitted signal. ................................................78
Figure 4.18 - OOB and NC radiation details of the received signal (simulation). .................................79
Figure 4.19 - Transmitted and received signal PSD comparison (simulation). ....................................79
Figure 4.20 - OOB and NC radiation details of the received signal (received by the USRP). ............80
Figure 4.21 - Transmitted and received signal PSD comparison (over-the-air). .................................80
Figure 4.22 - Comparison of results from different clipping levels. ....................................................81
Figure 4.23 – Left band edge comparison between unclipped and clipped signals. .............................81
Figure 4.24 - Filtering effect on PAPR performance. ..........................................................................82
Figure 4.25 - Hardware clipping after the transmit filter. ....................................................................82
Figure 4.26 - Subject test signals. SNR = 7 dB. ....................................................................................83
Figure 4.27 - Interference evaluation at transmitting band. .................................................................83
Figure 4.28 - Interference evaluation at OOB band. ............................................................................84
Figure 4.29 - Interference evaluation at NC band. ..............................................................................84
Figure 4.30 - Synchronization process debugging - spectrogram (time-frequency), PSD plot and console display. .................................................................85
Figure 4.31 - Synchronization message exchange between master and slave. .....................................86
Figure 4.32 - ARP packets captured with Wireshark. .........................................................................87
Figure 4.33 - Packet analysis using station's debugging consoles and Wireshark. ...............................87
Figure A.1 – VHF Radio Services and Applications - Portuguese electronic National Table of Frequency Allocations (eNTFA). Source: [80] .........................................................96
Figure C.2 - GNU Radio ofdm_rx.grc flowgraph. ..........................................................................100
Figure C.3 - GNU Radio ofdm_rx.grc flowgraph. ..........................................................................101
List of Tables

Table 1.1 – Available Digital Maritime Communication Systems..........................................................2
Table 2.1 - Test outcome vs occurrence for spectrum sensing hypothesis test. .....................................17
Table 2.2 - USRP motherboard characteristics per USRP Series. Source: [68]........................................29
Table 3.1 – Transmitting filter settings ..................................................................................................53
Table 4.1 - Spectrum sensing initial setup. ............................................................................................68
Table 4.2 - Transceiver setup for transceiver performance analysis. .......................................................73
Table A.1 - Portuguese frequency allocation table that includes MMS channels. Source: [80].............96
Table B.2 - RR - Appendix 18 - based on WRC-12 (Final Acts) .............................................................98
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC</td>
<td>Analogue-to-Digital Converter</td>
</tr>
<tr>
<td>AIS</td>
<td>Automatic Identification System</td>
</tr>
<tr>
<td>ANACOM</td>
<td>Autoridade Nacional de Comunicações</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>ARPA</td>
<td>Automatic Radar Plotting Aid</td>
</tr>
<tr>
<td>ARQ</td>
<td>Automatic Repeat reQuest</td>
</tr>
<tr>
<td>AWGN</td>
<td>Additive White Gaussian Noise</td>
</tr>
<tr>
<td>BER</td>
<td>Bit Error Rate</td>
</tr>
<tr>
<td>B-VHF</td>
<td>Broadband Very High Frequency Communications</td>
</tr>
<tr>
<td>CC</td>
<td>Cancellation sub-Carriers</td>
</tr>
<tr>
<td>CCDF</td>
<td>Complementary Cumulative Distribution Function</td>
</tr>
<tr>
<td>CDF</td>
<td>Cumulative Distribution Function</td>
</tr>
<tr>
<td>CEPT</td>
<td>Conference of European Postal and Telecommunications</td>
</tr>
<tr>
<td>CFD</td>
<td>Cyclostationary Feature Detection</td>
</tr>
<tr>
<td>CINAV</td>
<td>Centro de Investigação Naval</td>
</tr>
<tr>
<td>COGEU</td>
<td>COGnitive radio systems for efficient sharing of TV white spaces in EUropean context</td>
</tr>
<tr>
<td>CR</td>
<td>Cognitive Radio</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundant Check</td>
</tr>
<tr>
<td>CSMA</td>
<td>Carrier Sense Multiple Access</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
</tr>
<tr>
<td>DAC</td>
<td>Digital-to-Analogue Converter</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DECT</td>
<td>Digital Enhanced Cordless Telecommunications</td>
</tr>
<tr>
<td>DFT</td>
<td>Discrete Fourier Transform</td>
</tr>
<tr>
<td>DSA</td>
<td>Dynamic Spectrum Access</td>
</tr>
<tr>
<td>DSC</td>
<td>Digital Selective Calling</td>
</tr>
<tr>
<td>DSP</td>
<td>Digital Signal Processing</td>
</tr>
<tr>
<td>DVB-T</td>
<td>Digital Video Broadcasting — Terrestrial</td>
</tr>
<tr>
<td>DySPAN</td>
<td>Dynamic Spectrum Access Networks</td>
</tr>
<tr>
<td>ED</td>
<td>Energy Detector</td>
</tr>
<tr>
<td>EPIRB</td>
<td>Emergency Position-Indicating Radio Beacons</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FDD</td>
<td>Frequency Division Duplexing</td>
</tr>
<tr>
<td>FDM</td>
<td>Frequency Division Multiplexing</td>
</tr>
<tr>
<td>FEC</td>
<td>Forward Error Correction</td>
</tr>
<tr>
<td>FFT</td>
<td>Fast Fourier Transform</td>
</tr>
<tr>
<td>FM</td>
<td>Frequency Modulation</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
</tr>
<tr>
<td>FSK</td>
<td>Frequency Shift Keying</td>
</tr>
<tr>
<td>GMDSS</td>
<td>Global Maritime Distress and Safety System</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>GMSK</td>
<td>Gaussian Minimum Shift Keying</td>
</tr>
<tr>
<td>GRC</td>
<td>GNU Radio Companion</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>HF</td>
<td>High Frequency</td>
</tr>
<tr>
<td>IALA</td>
<td>International Association of Lighthouse Authorities</td>
</tr>
<tr>
<td>ICE</td>
<td>International Cometary Explorer</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IDFT</td>
<td>Inverse Discrete Fourier Transform</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IHO</td>
<td>International Hydrographic Organization</td>
</tr>
<tr>
<td>IIR</td>
<td>Infinite Impulse Response</td>
</tr>
<tr>
<td>IMO</td>
<td>International Maritime Organization</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISEE</td>
<td>International Solar-Environment Explorer</td>
</tr>
<tr>
<td>ISM</td>
<td>Industrial, Scientific and Medical</td>
</tr>
<tr>
<td>IST</td>
<td>Instituto Superior Técnico</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Networks</td>
</tr>
<tr>
<td>LLC</td>
<td>Limited Liability Company</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MF</td>
<td>Matched Filter</td>
</tr>
<tr>
<td>MF</td>
<td>Medium Frequency</td>
</tr>
<tr>
<td>MIT</td>
<td>Massachusetts Institute of Technology</td>
</tr>
<tr>
<td>MMS</td>
<td>Maritime Mobile Service</td>
</tr>
<tr>
<td>MSS</td>
<td>Mobile Satellite Spectrum</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>NAVTEX</td>
<td>Navigational Telex</td>
</tr>
<tr>
<td>NBFM</td>
<td>Narrow Band Frequency Modulation</td>
</tr>
<tr>
<td>NC</td>
<td>Non Contiguous</td>
</tr>
<tr>
<td>NC-OFDM</td>
<td>Non Contiguous OFDM</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NTFA</td>
<td>National Table of Frequency Allocation</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OFDMA</td>
<td>Orthogonal Frequency Division Multiple Access</td>
</tr>
<tr>
<td>OOB</td>
<td>Out-Of-Band</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>P25</td>
<td>Project 25</td>
</tr>
<tr>
<td>PAPR</td>
<td>Peak-to-Average Power Ratio</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PDU</td>
<td>Packet Data Unit</td>
</tr>
<tr>
<td>PER</td>
<td>Packet Error Ratio</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>PMR</td>
<td>Private Mobile Radio</td>
</tr>
<tr>
<td>PSD</td>
<td>Power Spectral Density</td>
</tr>
<tr>
<td>PSK</td>
<td>Phase Shift Keying</td>
</tr>
<tr>
<td>PTS</td>
<td>Partial Transmission Sequence</td>
</tr>
<tr>
<td>ACronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>PU</td>
<td>Primary User</td>
</tr>
<tr>
<td>QAM</td>
<td>Quadrature Amplitude Modulation</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>ROC</td>
<td>Receiver Operating Characteristic</td>
</tr>
<tr>
<td>SATCOM</td>
<td>Satellite Communications</td>
</tr>
<tr>
<td>SDR</td>
<td>Software Defined Radio</td>
</tr>
<tr>
<td>SHF</td>
<td>Super High Frequency</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-Noise Ratio</td>
</tr>
<tr>
<td>SU</td>
<td>Secondary User</td>
</tr>
<tr>
<td>SYNC</td>
<td>Synchronization</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>TETRA</td>
<td>Terrestrial Trunked Radio</td>
</tr>
<tr>
<td>TR</td>
<td>Tone Reservation</td>
</tr>
<tr>
<td>TV</td>
<td>Television</td>
</tr>
<tr>
<td>TVWS</td>
<td>Television White Spaces</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UHD</td>
<td>Universal Hardware Driver</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra High Frequency</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>USRP</td>
<td>Universal Software Radio Peripheral</td>
</tr>
<tr>
<td>VHF</td>
<td>Very High Frequency</td>
</tr>
<tr>
<td>WGN</td>
<td>White Gaussian Noise</td>
</tr>
<tr>
<td>WRC</td>
<td>World Radio Conference</td>
</tr>
<tr>
<td>WT</td>
<td>Wavelets Transform</td>
</tr>
</tbody>
</table>
## List of Software

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baudline</td>
<td>Time-frequency browser designed for scientific visualization of the spectral domain</td>
</tr>
<tr>
<td>GNU Radio</td>
<td>Development toolkit to implement software-defined radios and signal processing systems</td>
</tr>
<tr>
<td>Matlab</td>
<td>High-level language and interactive environment for numerical computation, visualization, and programming.</td>
</tr>
<tr>
<td>Microsoft Excel</td>
<td>Spreadsheet software</td>
</tr>
<tr>
<td>Microsoft PowerPoint</td>
<td>Slide show presentation and schematic design software</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td>Text editor software</td>
</tr>
<tr>
<td>Microsoft Visio</td>
<td>Schematic design software</td>
</tr>
<tr>
<td>Python Interpreter</td>
<td>Language interpreter for Python language</td>
</tr>
<tr>
<td>Wireshark</td>
<td>Packet analyser, network troubleshooting, and communications protocol analyser</td>
</tr>
</tbody>
</table>
This chapter provides a brief overview of the maritime communication systems, recent regulatory developments and opportunistic usage of radio spectrum. It is also discussed the paradigm change brought by cognitive radios and their role in the design of future communication systems. The contributions and merits of the thesis and the structure of this document are also presented.
1.1 Motivation and Overview

The importance of maritime economical activities is unquestionable: oceans cover about 70% of the earth’s surface and over 90% of the world’s goods are transported by merchant fleets.

Existing maritime data communication systems are reduced to a small group of options. On the low HF and MF bands, there are some military and amateur digital modes, as well as the well know Navigation Telex (NAVTEX). However, these are mostly dedicated narrowband systems that are not suitable for general purpose communication links. On the VHF band, which is typically the first choice for most line of sight and coastal communications, we have the Automatic Identification System (AIS) and the Digital Selective Calling (DSC). Again, these are application-specific systems (the firsts is for automatic positioning and the second is a paging system for distress alerts and short messaging), that cannot be used for generic data communications. Legacy analogue VHF radios\(^1\) are still extensively used by mariners for ship-to-ship and ship-to-shore communications near coastline waters.

The International Maritime Organization (IMO), an agency under the aegis of the United Nations (UN), has being promoting a new concept termed e-navigation (electronic navigation). According to a report by the Working Group on Maritime Security [1], e-navigation techniques will harmonize, integrate and enhance information from legacy and modern navigation systems, improving safety and security in commercial shipping through better organization and exchange of data between ships and shore. However, such complex information systems require a network infrastructure, which is not currently available, at least for an acceptable cost.

Existing electronic navigation services (not yet e-navigation services) are supported by a very narrow group of shipborne digital communication systems (Table 1.1). Most of these systems are application-specific, non interoperable and can’t / shouldn’t be used for other purposes (most of them support safety and distress applications).

Table 1.1 – Available Digital Maritime Communication Systems.

<table>
<thead>
<tr>
<th>System</th>
<th>Band</th>
<th>Throughput</th>
<th>Bandwidth</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAVTEX</td>
<td>HF, MF</td>
<td>100 b/s</td>
<td>500 Hz</td>
<td>Information / Distress</td>
</tr>
<tr>
<td>DSC</td>
<td>VHF MF/HF</td>
<td>1.2 kb/s 100 b/s</td>
<td>3.5 kHz 800 Hz</td>
<td>Short messaging / Distress</td>
</tr>
<tr>
<td>AIS</td>
<td>VHF</td>
<td>9.6 kb/s - 2 ch.</td>
<td>12.5 kHz</td>
<td>Automatic vessel tracking</td>
</tr>
<tr>
<td>SATCOM</td>
<td>SHF</td>
<td>&lt; 4 Mb/s</td>
<td></td>
<td>IP data / Telephony</td>
</tr>
</tbody>
</table>

As for terrestrial based communication systems (GSM, UMTS and LTE), since their networks typically don’t consider maritime coverage, cannot be considered an option for maritime data communications.

With the exception of SATCOM, existing maritime digital data can’t serve multipurpose communication applications. SATCOM is the only true broadband, multipurpose data service. Despite its installation and operating costs, it offers an almost global coverage (getting coverage at the earth poles can be

\(^1\)Existing VHF analogue communications date from the early 70’s.
difficult) and it is very reliable.

Figure 1.1 – Maritime communications user requirements – integrity vs speed. Source: [2]

Considering the current maritime communications panorama, as the research in [2] shows, only low bit-rate services are implemented (lower level of Figure 1.1).

This survey also shows that most of the focus in maritime communication systems will also be in non-maritime purposes, such as personal communications and entertainment (Figure 1.1). One can imagine how difficult it would be to offer personal communications to every cruiser passenger, at an affordable price, since typical SATCOM operation costs may range from 1 to 30 US$ per Mbyte of consumed data.

Furthermore, it is a well known fact that in the future, the overall cost per megabyte of data for SATCOM systems is not expected to decrease, due to the cost of launching and operating satellites and ground control stations. This proves that besides e-navigation purposes, the maritime telecommunications marketplace calls for new connectivity services, with open opportunities for high speed at affordable prices.

Regarding the VHF maritime spectrum panorama, in similar spectrum scarcity or underutilization scenarios, cognitive radios have been proposed as a possible solution to improve spectrum efficiency [3-5]. One of the most prominent cases is related to analogue TV switch-off and spectrum reframing [6-10] – these spectrum opportunities are often called TV white spaces (TVWS).

In fact, regulatory authorities, such as the Federal Communications Commission (FCC), have been developing regulatory efforts to promote and facilitate spectrum usage [11]. In addition, for the specific case of TVWS, the FCC proposed allowing operation in the broadcast television spectrum at locations where that spectrum is not being used [12, 13].

Most spectrum sharing initiatives emerged as a consequence of some recent technological evolutions. One of the most remarkable publications that reports how these technological evolutions could play an important role changing the paradigm of spectrum utilization is a thesis by Mitola [4]. Mitola formulated the now well known concept of cognitive radio, bearing in mind that a special type of radio would be up
to that task: the software defined radio (SDR). A cognitive radio is, in fact, a dynamic spectrum access capable device. Due to its perception, self awareness and learning capabilities, a cognitive radio is able to determine in what conditions it can use the radio spectrum at a specific instant and location – dynamic - and then access that radio spectrum without interfering with the rightful users – spectrum access [3].

The concept of cognitive radio clashes with most typical methods of spectrum allocation. The radio spectrum is an intangible resource and most common spectrum allocations are little more than a set of rules that primary user systems must observe when using their assigned spectrum. This kind of spectrum allocation method usually leads to spectrum underuse (in certain geographic areas), which is the case of TVWS.

The design of the physical aspects of a communication system turned out to be easier and more achievable with few hardware resources using SDR’s. Software radios currently have enough resources to implement and replicate most existing (hardware implemented) telecommunication systems. One of the most prominent and promising SDR tool is GNU Radio [14, 15]. The GNU Radio project is a community open-source project that was created in 1998 in MIT and it is an official GNU project (free software foundation) since 2004. It consists of software platform that provides a wide range of DSP tools, so general purpose PC’s can implement signal processing functions rather than relying on the dedicated DSP or FPGA based hardware.

SDR applications rely on advanced hardware peripherals (end point of the actual SDR), such as the Universal Software Radio Peripheral (USRP), which is designed and produced by Ettus Research™. An USRP is a scientific grade and affordable equipment, which became a standard in software defined radios, addressing a broad range of research, academic, industrial and defense applications.

A very good and unusual example of how software radios may empower and revolutionize the telecommunications universe is the ongoing project to recapture an old, but active, NASA (National Aeronautics and Space Administration) spacecraft probe named International Solar-Environment Explorer (ISEE-3) (renamed in the 80’s to International Cometary Explorer (ICE)) [16]. NASA launched this spacecraft in the early 70’s, but eventually the mission was discontinued (which includes all ground equipment at the Deep Space Network²). In order to recapture the spacecraft, project crew members replicated ground station control transceivers using GNU Radio and USRP’s. The team successfully established contact and communicated with the spacecraft, which is at a distance of 1.79 Mkm from the earth (consulted at 29/07/2014), equipped with late 70’s telecommunication equipment. This project demonstrates the flexibility of software defined radios and its applicability to ground commercial or deep space telecommunication systems.

Recent developments in spectrum policy and regulatory domains, notably those issued by the FCC, will allow more flexibility and efficiency in the use of the radio spectrum. These developments are

---

² A world-wide network telecommunication sites, located in America, Spain, and Australia, that supports interplanetary spacecraft missions.
highly encouraging for those seeking to investigate in the domain of new (opportunistic) cognitive communication systems. As stated in previous paragraphs, TVWS related projects are the best examples. According to Jianfeng et al. [17], since the FCC initiated “The National Broadband Plan” [18] and approved the final rules for unlicensed devices in the TV bands in 2010 [12], a lot of academic and industrial initiatives started to explore this opportunity. As a matter of fact, there is a set of existing and ongoing standard developments that intend to take advantage of the opportunistic usage of radio spectrum. The Institute of Electrical and Electronics Engineers (IEEE) Wireless Regional Area Networks standard (IEEE 802.22) [19], is an example of a cognitive radio standard for TV band opportunistic operation.

Another initiative regarding TVWS named COGEU (Cognitive radio systems for efficient sharing of TV white spaces in European context) [20] comprises multiple achievements concerning cognitive radio system implementation. This project addresses all the dynamic spectrum access system components and evaluates the coexistence of secondary services in already allocated spectrum bands (TVWS). It comprises a very complete spectrum sensing framework that addresses cutting edge spectrum sensing techniques [21], as well as transceiver techniques that assure PU compliancy [20]. COGEU is also a good example of a new business opportunity empowered by spectrum opportunities [22].

All these initiatives intend to facilitate broadband usage, which is exactly what digital maritime communications need. Maritime communications represent a huge business opportunity, competing with SATCOM for coastal coverage.

1.2 Contributions and Outline

The main contribution of this thesis is the study and implementation of complete cognitive radio system, using software defined radio technology, for opportunistic usage of the radio spectrum.

This project aims to develop a cognitive communication system, integrating the essential processing components to achieve dynamic spectrum access, as well as the necessary network integration, over-the-air network synchronization. It is out of the scope of this project investigating and implementing cutting edge techniques, such as spectrum sensing algorithms or spectrum shaping techniques. The merits of this project are the integration of several cognitive radio components, the usage of software defined radio technology for physical and MAC layer design, leading to a fully functional prototype cognitive radio.

Maritime networks and telecommunication systems are probably the least studied communication infrastructures [23]. For decades, mariners have been using the same telecommunication infrastructure, based on expensive satellite links and low throughput ground based services. There are few works addressing complete cognitive radio implementations. There are various efforts and frameworks working on cognitive radio technology, but most of them are focused in particular sub areas of knowledge, such as, spectrum sensing techniques [24] or radio transceiver techniques [25,
The IEEE 802.22 standard is probably the most complete cognitive radio standardization effort, but it was designed to operate in the TVWS [19] only. In [27], a prototype cognitive radio implementation uses IEEE 802.11 wireless LAN technology, which limits its utilization to the 2.4GHz ISM band. Moreover, the primary user – secondary user scenario is not applicable for the maritime environment.

The final implementation should result in an end-to-end wireless communication system, with cognitive features and dynamic spectrum access capabilities. This project should contribute to solving some of the maritime communications limitations that were previously discussed.

This implementation may be used to deploy a shore based, coastal network, supporting broadband connections using the VHF MMS band. This network can support e-navigation services, as well as, standard data services, such as internet access. A coastal VHF network may be used by the military, merchant and passenger vessels, increasing their number of options in terms of data services. However, this system does not replace existing SATCOM services, and can only be an effective competitor or a complement to SATCOM for coastal ranges.

Specific contributions of this thesis are:

- Development of a new digital communication system, in the VHF band, for maritime applications;
- Implementation of a complete telecommunication system using software defined radio technologies;
- Development of a spectrum sensing framework for the detection of multiple narrowband signals in the VHF band;
- Implementation of reconfigurable and flexible radio transceivers;
- Development of a cognitive framework with dynamic spectrum access features;

This thesis was done with the collaboration of the Portuguese Navy – Centro de Investigação Naval and Instituto Superior Técnico – Instituto de telecomunicações, from the University of Lisbon. Some of the conclusions, as a result of the developed work, intend to give some guidelines to future directions in maritime telecommunication systems, as well as directions to future research projects involving software defined radios for digital communication systems.

### 1.2.1 Outline

This thesis is organized in five chapters that provide an overview and understanding of the problem, related work and technologic reviews, implementation and design details, testbeds and benchmarks, results and conclusions. The present chapter provides an overview of the available maritime communication systems and their limitations, as well as general understanding of possible solutions and improvements, describing related work and cutting edge telecommunication technologies.

Chapter 2 provides an overview of the most important concepts about dynamic spectrum access and cognitive radio systems. Some regulatory frameworks are reviewed and important definitions and
statements regarding spectrum sharing are extrapolated to this work.

System design and implementation details are described on the third chapter. The chapter starts with an overview on maritime communications scenario. Primary user equipment (VHF radio transceivers) specifications and MMS spectrum allocations are analysed and a strategy to deploy the cognitive radio system is proposed. Implementation description comprises radio transceiver planning and design, including reconfigurable features, spectrum sensing framework and cognitive medium access layer design. All decisions and implementation details are explained and demonstrated conveniently with software simulations or real measurements.

A description of the testing methodology for proposed system is provided in chapter 4. Analysis and tests include software simulations of the real scenario, as well as several benchmarks with radio hardware in controlled environments. A final test demonstrates the coexistence between PU MMS radios and the proposed system.

Chapter 5 provides general overview over the obtained results and achievements. Learned lessons and suggestions for future work are taken from these results, in addition to final conclusions. A general overview of the project and comments about its utility is provided, giving a general understanding about the main constraints and achievements.
Chapter 2

Cognitive Radio Technology

This chapter provides an overview about Cognitive Radio (CR) concepts, followed by an overview on related work and similar implementations. CR concepts and techniques analysis includes a state-of-the-art review. Regarding the implementation of a CR, software defined radio concepts and implementation techniques are also provided. In the end, a review on state-of-the-art and related work highlights the merits and the innovative aspects of this project.
2.1 Dynamic Spectrum Access

Dynamic Spectrum Access (DSA) is the generic designation created to address a set of techniques that compose agile and spectrum aware radios. DSA radios utilize the radio spectrum in a dynamic manner, rather than in a fixed approach. In most cases, this approach improves the spectrum utilization. DSA is a fundamental for opportunist use of the radio spectrum using cognitive radios.

Min, S., et al [28] define DSA as “a new spectrum sharing paradigm that allows secondary users to access the abundant spectrum holes or white spaces in the licensed spectrum bands (...) alleviating the spectrum scarcity problem (...).” The IEEE has a dedicated framework for dynamic spectrum access network technologies and associated regulatory policies, named Dynamic Spectrum Access Networks (DySPAN) framework. It also defines DSA as the ability to dynamically access alternative locally/temporally unused spectrum bands [29].

However these definitions seem generic enough to accommodate all sorts of radio-related techniques, the involved complexity is not implicit to the definition of DSA. As a matter of fact, according to Mitola’s work [4], a CR is much more than a DSA device, since it can learn from the environment and adapt behaviors based on observations and previous knowledge. Nevertheless, CR’s may use DSA as the means access radio spectrum, solving the problem of spectrum scarcity [5].

A simple example of a DSA capable system, without cognitive capabilities, is the Digital Enhanced Cordless Telecommunications (DECT™). DECT cordless phones dynamically select vacant channels based on a spectrum measurement [30], which is the simplest form of DSA. Terrestrial based networks, such as GSM, UMTS or LTE also follow some of the DSA philosophy regarding the allocation of radio, time or code resources.

DSA covers several knowledge areas, including spectrum sensing, spectrum shaping, network architecture and behavior and so on. Since this project intends to implement a CR system, most of these knowledge areas will be addressed and put into practice in the final model. However, the amount of work effort was not evenly distributed with radio related aspects getting the biggest share of interest.

2.1.1 Opportunistic Use of Radio-Frequency Spectrum

Most of previous discussions are made around a very important concept: opportunistic use of radio spectrum. In fact, if there wasn’t an “opportunity”, most discussions about solutions to spectrum scarcity wouldn’t make any sense.

Opportunistic spectrum usage is the act of accessing locally / temporally unused spectrum bands that are legally assigned to rightful users – primary users (PU) – by users that do not own the conventional rights to that spectrum - secondary users (SU) [29]. In fact, spectrum assignments can be issued to a
service provider or to service. GSM systems, for instance, not only have an assigned radio band, but also specific portions of that radio band are assigned to private companies who commercialize GSM (service providers). On the other hand, cordless phone systems, for instance, have an assigned radio band, but users don’t need to get a license in order to deploy and operate such systems.

In order to access these spectrum bands, SU’s should take the necessary precautions to avoid interfering with PU’s, which otherwise could cause service disruptions. Some important aspects of this coexistence must be considered, such as, what can be considered unoccupied spectrum or what can be considered an interfering signal. These two aspects depend on the type of PU service and also on SU perception capabilities. When the FCC issued the authorization for TVWS operation by unlicensed users [12], some basic rules were set:

- TV channel occupancy decision criteria must be defined – regulatory authorities should define in what conditions a spectrum band can be considered available for unlicensed users;
- SU’s must be able to detect unused TV channels (by means of geo-location techniques and/or spectrum sensing techniques) – SU’s must be able to detect PU activity using geo-referenced information (i.e.: consulting some spectrum database) or conducting spectrum sensing surveys. However, FCC leaves spectrum sensing as an optional feature in some situations;
- SU’s must comply with significant restrictions and technical protections – not only SU’s must be able to identify available bands, they must fulfill technical aspects that assure they won’t interfere with PU (i.e.: adequate spectrum shaping techniques);

The TVWS scenario is a good example of what regulatory authorities may need to consider before authorizing secondary operation of already assigned radio spectrum.

However, there are significant differences between TV broadcast and VHF MMS (regarding PU operating modes and mobility). For the TVWS case, PU’s are fixed broadcasting stations, located in well known positions (facilitating geo-location and coverage prediction). Moreover, TV broadcasting equipment is remotely monitored by TV broadcasters, which may also contribute to improve the accuracy of geo-location databases. On the other hand, VHF MMS PU’s can be fixed coastal stations or moving vessels, with various power settings and installation configurations.

Despite some scientific efforts to demonstrate and express the importance of new strategies and future directions for maritime communications [2, 31, 32], none of the existing regulatory frameworks or authorities is addressing spectrum opportunities regarding the VHF MMS band.

### 2.1.2 Spectrum Sensing

Being aware of the surrounding environment is the first task performed by any cognitive system. For this reason, spectrum sensing is by far the most important component of a cognitive radio system. Spectrum sensing is the process of detecting primary users and determining if the licensed spectrum is accessible [33].

Spectrum knowledge can be reached through geo-location databases or by local spectrum sensing,
and for some implementations, obtaining information directly from the radio spectrum can be an optional feature [21]. For this implementation, sensing is a mandatory feature for any SU, reducing the chances of interfering with incumbent PU’s, and also simplifying the final architecture.

Spectrum sensing frameworks can have different computational and implementation complexities, depending on the amount and type of features to be detected, and its accuracy is usually expressed in probability of detection and probability of false alarm. The effectiveness of a spectrum sensing framework depends on a number of aspects, such as sensing duration, PU signal strength (signal to noise ratio), previous knowledge about PU features or channel propagation effects. Depending on the application, there is a typical trade-off between speed and accuracy, both critical aspects of spectrum sensing [24]. Some techniques perform slower and are more computationally demanding, but lead to more accurate results.

A very common classification for spectrum sensing algorithms is based on the amount or type of information used to perform the detection, as indicated by COGEU [34]. These categories are: noise dependent detection – spectrum sensor uses information on noise power only; feature detection – requires previous knowledge about PU signal and noise power; blind detection – requires no information about PU or noise power. However, some of these techniques may require filter banks or even a channelizer to perform multiple signal detection, increasing the overall complexity of the sensing framework.

Spectrum sensing can also be classified in terms of network infrastructure. Network nodes may contribute to a bigger data collection database, with a sensing authority that audits all sensing operations. This type of centralized sensing can also be considered as cooperative sensing, since all network nodes contribute to an enhanced radio picture.

Since we have previous knowledge about PU attributes, feature detection based methods may be adequate for this implementation. Nevertheless, since multiple channel detection is required, one must evaluate if these techniques have reasonable processing / speed performances for this application. Multiple signal detection requires previous knowledge about channel spacing and bandwidth.

### 2.1.2.1 Noise Dependent Detection

Noise dependent techniques do not require little knowledge about PU’s characteristics (channel bandwidth and spacing), but require good knowledge on noise power level and statistics. The two most common techniques are the energy detector and the wavelet based detector.

- **Energy Detector (ED)**

The energy detector (also known as radiometer) compares the channel energy with a metric that depends on the noise level (decision threshold) to decide if the channel is occupied or not. This technique is a common approach to spectrum sensing since it has low computational complexity (compared to other techniques) [34] and can be implemented in both time and frequency domain. To adjust the detection threshold, the ED requires knowledge on noise level in the band of interest. If the band of interest is wider than the channel bandwidth, or multiple channels are present in the band of
interest, the time domain energy detector requires channelization (filtering and analysing channels individually).

\[ x(t) \rightarrow \text{BPF} \rightarrow \text{ADC} \rightarrow \frac{1}{T} \sum_{n=-\infty}^{\infty} |x_n|^2 \rightarrow > \lambda \]

Figure 2.1 - Block diagram of a time domain energy detector. Source: [33].

The signal can be filtered in the analogue domain (Figure 2.1) or in the digital domain using a digital filter. The estimated energy is then compared with a threshold (which depends on the noise level) to decide whether a PU is present or not.

\[ x(t) \rightarrow \text{ADC} \rightarrow \text{PSD Estimate} \rightarrow \sum X_n \rightarrow > \lambda \]

Figure 2.2 - Block diagram of a frequency domain energy detector.

Both time and frequency ED implementations are simple and generic (they can detect unknown signals with no previous information). However, ED’s cannot differentiate interference or noise from the signals of interest. The frequency domain implementation can easily perform multiple signal detection, without filter banks, using a single power spectral density (PSD) estimate. For this reason, the frequency domain implementation of the ED is a good candidate for this project’s spectrum sensing framework. The main drawback of the ED is its susceptibility to noise uncertainty. The ED is also frequently used as a benchmark (reference) for other spectrum sensing techniques.

- Wavelets Transforms (WT)

Wavelet Transforms are a general purpose technique for detecting irregularities, such as in image processing or in other time series. According to [35], the same approach can be used to detect spectrum irregularities produced by source signals within the band of interest. WT-based technique for spectrum sensing operates in the frequency domain, detecting irregular edges in the signal PSD (as opposed to irregularities in time series) [35].

![Wavelets-based method detecting sub-band edges (data synthesized with GNU Radio)](image)

Figure 2.3 – Wavelets-based method detecting sub-band edges (data synthesized with GNU Radio).

In [35], a wavelet-based method is able to scan multiple signals within the same band, simultaneously identify all sub-bands, without previous knowledge about the number of sub-bands.
Nevertheless, experimental work on wavelet-based spectrum sensing [35, 36] shows that however this technique is able to detect multiple unknown signals, it requires high sampling rate, high spectral resolution and computationally complex calculations, which is a drawback for real time applications, such as cognitive radios.

### 2.1.2.2 Feature Detection

Feature detection techniques require previous knowledge about PU signals and noise. Incoming signals can be demodulated and known features or signatures (i.e.: repeating patterns) can be identified.

These techniques have the ability to distinguish between different types of signals and high resilience to noise uncertainty [34]. Nevertheless, signals must be individually demodulated and analysed which is a main drawback for multiple signal detection.

- **Matched-Filter (MF)**

MF detection is referred as the optimum detection technique in very low signal-to-noise ratio (SNR) scenarios, when the received signal is known [37]. MF also requires a small amount of samples for a certain target probability of false alarm and missed detection when compared with other techniques. However, MF-based detectors must demodulate source signals individually, which can lead to very complex and computationally demanding implementations. In order to detect a digital signal, for instance, a MF-based detector must have previous knowledge about source signal bandwidth, carrier frequency, modulation scheme, frame format, etc.

- **Cyclostationary Feature Detection (CFD)**

However communication systems are usually modeled as if they were stationary random processes, transmitted radio signals are in general coupled with carriers, preambles, pilot carriers or even cyclic prefixes, which may result in periodic patterns named cyclostationary features [38]. In Figure 2.4 spectral shapes in different time instants indicate the presence of cyclostationary features, as a result of the frequency modulation (FM).

![Spectral Autocorrelation Function of a Narrow Band FM (NBFM) signal (data synthesized with GNU Radio and analysed with Python and Scipy).](image)

Figure 2.4 – Spectral Autocorrelation Function of a Narrow Band FM (NBFM) signal (data synthesized with GNU Radio and analysed with Python and Scipy).
Some TVWS projects extensively explore these properties to detect digital TV signals periodic features, such as the cyclic prefix [21, 24, 38, 39]. As a result of the fact that noise is wide-sense stationary – two noise samples at different instants are uncorrelated – it doesn’t present any cyclostationary features and CF detectors use this property to distinguish noise from known PU signals. Moreover, since different PU signals have different cyclostationary features, CF detectors may be able to distinguish and classify different PU’s signals. TVWS frameworks frequently take advantage of this property to distinguish digital TV signals from wireless microphones that operate in the same band [21].

Although CF detectors require large number of samples (slower analysis) and significant processing effort (due to spectral correlation computation), they are very robust to noise uncertainty, thus suitable for low SNR scenarios. For this implementation, this technique is too complex for multiple user detection.

### 2.1.2.3 Blind Detection

As the name suggests, blind detection based techniques do not require any knowledge on source signals or noise statistics. In [40], covariance statistical property is used to distinguish source signals from noise. Covariance-based detection is a feasible technique because the statistical covariance matrices or auto-correlation of signal and noise are usually different. Moreover, the statistical covariance matrix of noise is determined by the receiving filter [40].

According to COGEU’s research [34], these techniques have an interesting set of positive aspects, such as the immunity to noise uncertainty. However, blind detection techniques turn to be quite complex to implement and again require single channel analysis.

![Complexity vs Accuracy of spectrum sensing techniques.](image)

Since spectrum sensing is not the only piece of this project, a trade-off between implementation complexity and requirement fulfillment must be achieved. Moreover, in order to reduce the overall complexity of the cognitive radio, every separate component must be as simple as possible, so the radio can still perform several tasks in parallel with no performance penalty to any of the components.

Sensing techniques that require single channel analysis cannot be considered for implementation,
since this project is about detecting multiple PU.

![Spectrogram](image)

Figure 2.6 – Spectrogram (time-frequency) plot of several PU in activity (data synthesized with GNU Radio).

Frequency domain ED and WT methods are the only studied techniques that can detect multiple PU's in a single spectrum scan. WT is more computationally demanding than the ED (ED requires only one spectral estimation) and it is as susceptible to noise uncertainty as the ED (both noise dependent techniques). Considering implementation and computational complexity, as well as flexibility, frequency domain ED was chosen for this project’s implementation.

### 2.1.2.4 Hypothesis Test and Decision Threshold

Any sensing problem can be generally formulated as a binary decision where the hypothesis test decides whether there is signal present or there in no signal present:

Hypothesis 0: There is only noise present; Hypothesis 1: There is signal present

After collecting and processing a specific number of samples, the spectrum sensing algorithm computes its decision metric, which is then compared to a decision threshold (which is specific of each sensing technique).

![Hypothesis decision workflow](image)

Figure 2.7 - Spectrum sensing hypothesis decision workflow.

Where $m$ is the metric given by the sensing algorithm and $\lambda$ is the decision threshold.

To evaluate the performance of a sensing technique, the final decision is classified as a correct detection – statistically described by the probability of detection ($P_d$) or an incorrect detection – statistically described by the probability of false alarm ($P_{fa}$):

\[
P_d = \text{Prob} \ (m > \lambda \ | \ H_1) \quad \text{if } m > \lambda \text{ and a PU is effectively present, that is a correct detection;}
\]
\[
P_{fa} = \text{Prob} \ (m > \lambda \ | \ H_0) \quad \text{if } m > \lambda \text{ but a PU is not present, that is an incorrect detection.}
\]
Table 2.1 - Test outcome vs occurrence for spectrum sensing hypothesis test.

<table>
<thead>
<tr>
<th>Occurrence</th>
<th>PU present</th>
<th>PU not present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Outcome</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( m &gt; \lambda )</td>
<td>True Positive</td>
<td>False Positive</td>
</tr>
<tr>
<td>( m &lt; \lambda )</td>
<td>False Negative</td>
<td>True Negative</td>
</tr>
</tbody>
</table>

Since \( P_d \) and \( P_{fa} \) are two degrees of freedom of the binary test, in order to compare performance in different threshold values and conditions, receiver operating characteristic (ROC) curves can be used to illustrate the performance of a spectrum sensing classifier. ROC curves visually translate the sensitivity (correct detection and false alarm rate) of a sensing algorithm for different decision thresholds, variable settings or channel conditions [21]. Nevertheless, classifier comparison and evaluation is out of the scope of this project and will not be addressed.

### 2.1.3 Spectrum Shaping - Transceiver Challenges and Techniques

A major aspect of cognitive radio implementation is the way the radio accesses available radio spectrum (spectrum opportunities, or spectrum holes). The simplest form of spectrum access consists of utilizing a secondary service that uses the same bandwidth of PU services, which is a simple approach for wide band incumbent services, such as the digital TV (in Europe a digital TV channel occupies 8 MHz of bandwidth). However, in most cognitive radio scenarios, SU intend to utilize as much available bandwidth as possible, aggregating the largest amount of available spectrum holes (previously PU channels). With narrowband incumbent services, in order to obtain a decent bandwidth, sub channel aggregation is almost mandatory (which is the case of MMS).

![Spectrogram (time-frequency) plot of PU activity and spectrum opportunities.](image)

Because PU channels are very unlikely to be contiguous (Figure 2.8), transceiver techniques that can still take advantage of the available spectrum holes should be used.

In Figure 2.8, five spectrum holes are available, but the largest one is only 120 kHz wide, which is not much bandwidth for a digital communication system. However, if the opportunistic cognitive radio is able to aggregate all five spectrum holes, the resulting bandwidth is about 310 kHz.

Considering the scenario above, and assuming that SU’s must not interfere with PU’s, two approaches can be adopted.
Figure 2.9 - Example of two different spectrum access schemes: a) Using a single spectrum hole; b) Multiplexing several spectrum holes.

The first approach is to simply choose the widest spectrum hole available. For this approach, the transceiver should only adapt its transceiver bandwidth and tune frequency to the selected spectrum hole (Figure 2.9 a)).

In a more complex approach, a SU may aggregate the available spectrum holes, synthesizing and transmitting multiple sub signals or using a multicarrier modulation, such as Frequency Division Multiplexing (FDM) (Figure 2.9 b)).

However, the spectrum pooling scheme illustrated in Figure 2.9 b) can be quite complex to implement and spectrally inefficient, if a conventional FDM implementation is used – each sub-channel must be individually modulated and then synthesize them in a single signal, which is then transmitted.

Since dynamic spectrum access and cognitive radios have been proposed to solve spectrum scarcity problems, transmission across non-contiguous portions of spectrum attracted numerous research efforts [25, 26, 41-49]. Aggregate and utilize multiple spectrum holes without interfering with incumbent users is a major challenge for the transceiver design, when developing a cognitive radio with DSA capabilities.

As opposed to conventional FDM, Orthogonal FDM (OFDM) is utilized by several communication systems because of its considerable high spectral efficiency, multipath delay spread tolerance,
immunity to the frequency selective fading channels [50]. OFDM is a particular form of multicarrier modulation, where a single data stream is transmitted over a number of overlapping (but still orthogonal) lower rate subcarriers. As a matter of fact, OFDM can be utilized as modulation technique only, which is the case of IEEE 802.11 based local area networks (LAN) [51], or as modulation and multiple access technique (in this case is named OFDMA), which is the case of the fourth generation terrestrial networks (LTE) [52].

![Block diagram of an OFDM transmitter](image)

**Figure 2.10 - Block diagrams of an OFDM transmitter.**

OFDM is also very popular due to its straightforward implementation (Figure 2.10), since the equipment complexity can be greatly reduced by eliminating any pulse shaping, and by using the Discrete Fourier Transform (DFT) to implement the modulation / demodulation process [53] (Figure 2.10 and Figure 2.11).

![Block diagram of an OFDM receiver](image)

**Figure 2.11 - Block diagrams of an OFDM receiver.**

Inverse DFT (IDFT) and DFT are typically implemented using Fast Fourier Transforms (IFFT and FFT respectively), which are easily implemented by any DSP circuit or software.

Since OFDM sub-carriers are individually assigned and modulated, considering the scenario illustrated in Figure 2.8, sub-carriers that superpose PU signals can be turned off, thus achieving some sort of spectrum shaping, as illustrated in Figure 2.12. This spectrum shaping concept, which can be used as a spectrum pooling scheme, is often named non-contiguous OFDM (NC-OFDM) [25, 54].
Nevertheless, OFDM systems have some limitations and drawbacks. OFDM suffers from relatively high peak-to-average power ratio (PAPR) and, if not properly contained, high out-of-band (OOB) radiation [55, 56]. NC-OFDM will also suffer from relatively high non-contiguous radiation (for the same reason that has high OOB radiation) [42, 55]. Since conventional OFDM does not employ any pulse shaping, sinc-type pulses are produced (in the frequency domain) and both OOB and NC bands will suffer from spurious unwanted radiation left from the modulated sub-carriers [42].

OFDM modulation suffers from high PAPR because sub-carrier signals add constructively in phase very often, producing large peaks in the transmitted signal [53] (PAPR typically increases with the number of sub-carriers). High amplitude peaks can, in fact, be clipped by the hardware and / or saturate the amplifier, causing signal distortions. To avoid signal distortion, power amplifiers are typically set to operate in a region where signal clipping is very unlikely to occur, which also results in inefficient operation [53, 56]. Due to its stochastic characteristics in OFDM systems, PAPR is often expressed in terms of Cumulative Distribution Function (CDF) or Complementary Cumulative Distribution Function (CCDF).

Figure 2.13 - PAPR Complementary Cumulative Distribution Function of a DVB-T³ OFDM signal. Measured with an USRP and GNU Radio and analysed with Python’s Numpy.

Figure 2.13 plots the CCDF characteristic of DVB-T OFDM signal, with PAPR values between 6.67 dB

³ Digital Video Broadcasting — Terrestrial; it is the digital TV broadcasting European-based consortium standard that uses OFDM as modulation technique.
and 11.85 dB, which are typical PAPR values for OFDM modulated signals.

According to [56], PAPR reduction techniques can be categorized as distorting techniques, such as signal clipping (clipping forced before the analogue circuits) or signal scrambling techniques, such as tone reservation (TR) or partial transmission sequence (PTS).

Signal clipping is by far the most widely used technique of PAPR reduction due to its simplicity, but often results in low bit error rate (BER) performance or spectrum distortions, for instance, increasing OOB radiation (Figure 2.14). Therefore, signal clipping must be correctly performed, usually before filtering, and a trade-off between BER and PAPR performance must be found.

![Figure 2.14 - Degradation of OOB radiation performance due to signal clipping (data synthesized with GNU Radio).](image)

From a DSA point of view, spectrum agility, reconfigurability and radiation isolation from PU’s are the major challenges of the transceiver design when using a NC-OFDM modulation scheme. However, side effects originated by high PAPR, for instance, must be analysed and its impact on the overall system performance mitigated.

### 2.1.3.1 Spectrum Shaping with Non-Contiguous Orthogonal Frequency Division Multiplexing

Due to its spectrum shaping and reconfigurability capabilities, NC-OFDM is a good candidate for CR’s with DSA capabilities. Moreover, NC-OFDM can also be used to support radio resource sharing among SU’s, in an OFDMA fashion (NC-OFDMA?) [57].

The goal of NC-OFDM modulation is to access PU radio spectrum by deactivating sub-carriers that could potentially interfere with PU signals, thus transmitting only over the remaining active sub-carriers. Concerning PU compliancy, as referenced in the previous section, OFDM systems suffer from high OOB / NC radiation, therefore conditioning its effectiveness as spectrum shaping technique.

As a matter of fact, OFDM is being used for many years as modulation technique in various commercial systems, so OOB radiation has always been an issue. Well known OOB radiation reduction techniques typically operate by softening time-domain pulse shapes (time-domain symbol shaping), which is the case of time-domain windowing [58, 59], or by manipulating the outputted spectrum in the frequency-domain, which is the case of guard bands insertion [50], constellation
expansion and manipulation [55], digital filtering [48] or cancellation sub-carriers (CC) [42, 60-63].

Among all these techniques, the concept of CC attracted a lot of attention because it can be used to mitigate both OOB and NC radiation [55]. This promising technique operates by inserting some “special” sub-carriers in the edges of the OFDM band, thus cancelling some of the spurious unwanted radiation that flows to the NC band [63].

![Diagram](image)

**Figure 2.15** - Insertion of cancellation sub-carriers to reduce OOB radiation. Source: [63].

In order to implement this technique, some of the previously useful carriers are sacrificed to become CC’s (green sub-carriers in Figure 2.15). These CC’s do not carry useful data and their weights and modulation is precisely controlled to cancel unwanted radiation (red waves in Figure 2.15). Just by visual analysis of Figure 2.15, some immediate drawbacks of CC’s are observed: since some of the data sub-carriers are made useless, the overall throughput is reduced; there is a trade-off between the number of CC’s and the width of the cancellation area (optimization range [42]); CC’s will affect both NC and data carrier bands, thus distorting the useful signal and affecting BER performance.

Because the computation of CC’s is an optimization problem, its real-time implementation is computational complexity. Also, there is a negative impact in BER and PAPR performance [42, 63].

Before deciding to implement any extra spectrum shaping techniques (in addition to simple sub-carrier selection), the coexistence limits between PU and SU must be evaluated in both NC and OOB band areas. It may happen that simple sub-carrier selection is enough to assure no interference to PU’s. Moreover, the level of transmitter-receiver coordination must also be assessed, since spectrum shaping has critical importance concerning receiver synchronization aspects, i.e. the transmitter should keep the receiver informed about OFDM symbol structure and embedded aids for synchronization. When using CC’s technique, for instance, both transmitter and receiver should be aware of which of the sub-carriers are data carriers, which are cancellation carriers and which are unused carriers.
For the case of OOB radiation reduction, a transmitting filter may be enough to achieve reasonable spectrum cancellation. A digital transmitting filter can be easily implemented through an infinite impulse response (IIR) digital filter (typically low number of coefficients).

To sum up, recent work on NC-OFDM proves that this technique meets the essential requirements to give CR spectrum shaping capabilities. However, when designing a NC-OFDM transceiver, some key aspects, such as PAPR and OOB / NC radiation require further analysis and investigation, thus assuring both system efficiency and coexistence between opportunistic users and incumbent users.

Moreover, the coexistence problem involves multiple aspects beyond spectrum shaping, such as distances and path loss between PU and SU, SU receiver sensitivity and modulation resilience to interference, Human perception of interference, etc.

2.2 Cognitive Radios

As stated above, in order to improve radio spectrum utilization (while accommodating new communication services and applications), CR’s need more than just DSA capabilities.

Cognitive radio was originally proposed by Mitola [4], and since then has been suggested as a possible solution to improve spectrum efficiency [3-5]. Mitola coined the concept of cognitive radio, bearing in mind that a special type of radio would be up to that task: the software defined radio (SDR). In a dynamic spectrum access (DSA) context, a cognitive radio uses its self awareness and learning capabilities to determine in what conditions the radio spectrum can be accessed [3].

The cognition cycle typically starts with a sensing activity, where spectrum holes are detected. Then, radio scene analysis enables transceiver reconfiguration and continuous learning (Figure 2.16).

![Figure 2.16 - Basic cognitive cycle. Source: [3]](image-url)
After gathering knowledge on radio spectrum activity, the CR produces configuration settings, considering spectrum policies and other sources of information in the decision process. Since the transceiver settings may dynamically change over time, in a network context, all cognitive nodes must be aware of the current settings (the process described by network synchronization). This series of dependent events is typically coordinated by a management authority, the cognitive engine.

During its operation, CR’s cyclically interact with the surrounding environment, thus deciding on the suitable spectrum access for a specific moment and location.

There is no standard architecture or strict design for a CR. As Haykin mentions [3], the development of cognitive radio is still at a conceptual stage. A CR can only be effective (and disruptive) if it is still able to coexist with incumbent services (not being intrusive). Therefore, CR design must consider specific aspects of the target radio band, PU operation profiles, availability of complementary sources of awareness, etc.

CR opportunistic personality raises other issues in some environments, such as multiuser cognitive radio networks, where secondary opportunistic users might be forced to compete or cooperate, in order to utilize available radio spectrum.

Like any other concept, CR is subject to various interpretations. As mentioned above, from the spectrum occupancy point of view, a CR can be a simple device that uses the radio spectrum based on its spectrum sensing capabilities, which is the case of some existing communication systems (for instance: DECT, Wireless LAN’s, etc.). On the other hand, from an opportunistic use point of view, a CR can be described as a complex device that takes decisions based on spectrum measurements and previous knowledge, has the ability to learn and to coordinate with other peers strategies to access, share and take advantages of radio spectrum opportunities.

This project implements the CR concept, where the cognitive device gathers the essential features (sensing, shaping, coordination, learning, etc.) enabling opportunistic usage of vacant bands within the maritime radio spectrum. Cognitive radios can be a solution for opportunistic usage of VHF maritime bands. The VHF maritime spectrum is not heavily used by incumbent users, which frequently leads to the existence of spectrum holes, which can be detected and used by secondary cognitive users in an opportunistic basis.

2.3 Software Defined Radios

The concept of CR was made possible not only because of new regulatory developments, but also due to amazing technological evolutions, such as software defined radios. Moreover, one of the most remarkable features of CR’s is reconfigurability, which is currently achievable using software defined radios.

Its first reference goes back to the early 80’s, when Raytheon, formerly E-Systems, coined the term
"software radio" in a company newsletter [64]. However, the first scientific publication on SDR dates from 1992 by Mitola [65] — curiously, the same investigator that a few years later proposed the concept of cognitive radio. Also, before SDR’s were made possible, designing and prototyping with the physical layer of a radio system was typically only for those who mastered hardware tinkering and had access industrial grade technology.

![Software Defined Radio Diagram](image)

**Figure 2.17 - Basic architecture of a SDR. Source: [66].**

SDR is the ultimate radio technology, converging two key technologies: digital radio, and computer software. With digital radios, most of the signal processing is made in the digital domain, keeping it as close as possible to RF front-end, and the analogue portion of the radio to the essential (upconversion and amplification). Components that have been typically implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are implemented by means of software or programmable hardware instead.

In terms of software frameworks for SDR application development, there are a few important players among the software community, but GNU Radio [15] is by far the most popular SDR development toolset. GNU Radio is a free and open-source software development toolkit that provides signal processing blocks to implement software radios.

What makes GNU Radio different from other digital signal processing tools is the way samples flow along the processing chain. GNU Radio’s core is based on a scheduler, which is responsible for “moving” samples between processing blocks. The scheduler moves large amounts of samples stored in memory between blocks, instead of sample by sample, which is a very efficient manner of moving memory (memory copies). The way scheduler works is what makes GNU Radio very efficient, thus suitable for real time signal processing.
GNU Radio essentially uses two programming languages: Python and C++. Python provides a higher level of abstraction than C++, as well as quicker prototyping and testing. The top-level specification of a flow graph can be written in Python, but in order to achieve DSP grade speeds, all signal processing should performed in C++ code. As a matter of fact, the whole application can be written in C++, since Python acts like a higher level gluing mechanism. GNU Radio Companion (GRC) is a graphical tool that is very useful for quick flowgraph deployment – in fact, GRC just generates a Python script containing the designed flowgraph.

GNU Radio Companion (GRC) is a graphical tool that is very useful for quick flowgraph deployment – in fact, GRC just generates a Python script containing the designed flowgraph.

GNU Radio can be used with low-cost external RF hardware (radio peripherals) to create software-defined radios, or without any hardware for simulation purposes. GNU Radio is widely used in hobbyist, academic and commercial environments to support both wireless communications research and real-world radio systems. Since it is digital signal processing toolkit, GNU Radio can also be used for other non radio purposes, such as audio processing.

GNU Radio is being used for all sorts of signal processing for communication systems and has been
used in a variety of public demonstrations, including commercial communication systems, such as P25\(^4\), IEEE 802.11, ZigBee\(^5\), Bluetooth\(^6\), RFID\(^7\), DECT, GSM, and even LTE. Moreover, GNU Radio has a vigorous community of users, reporters and developers, with permanent support for new developers.

In order to set up a complete radio system, GNU Radio needs to interface with a hardware radio peripheral (which actually sends the signals over the air). The hardware interface typically deals with raw IQ samples and performs digital upsampling, digital-to-analogue conversion and RF upconversion (Figure 2.20). Hardware peripherals with enough resources to perform some digital signal processing may alleviate software effort on the computer host side.

![Figure 2.20 - Hardware and software components in a SDR topology.](image)

The hardware peripheral core is often based in Field Programmable Gate Arrays (FPGA) or high processing power microcontrollers, which perform fundamental interfacing between host DSP software application, digital-to-analogue converters (DAC) and analogue-to-digital converters (ADC). Then, ADC’s and DAC’s also interface with the analogue upconverter and power amplifier.

This project uses USRP’s as hardware peripherals. The USRP’s are FPGA based peripherals, and by default they interface with host computers, through GNU Radio for instance, sending and receiving IQ raw samples of the digitized signals.

---

\(^4\) Project 25 (P25 or APCO-25) is a suite of standards for digital radio communications for use by federal, state/province and local public safety agencies in North America (equivalent to TETRA system in Europe).

\(^5\) ZigBee is a specification for a communication protocol stack used to create personal area networks built from small, low-power digital radios.

\(^6\) Bluetooth is a wireless technology standard for exchanging data over short distances (using ISM bands) for fixed and mobile devices.

\(^7\) Radio-frequency identification (RFID) is a wireless non-contact technology that uses electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags.
The USRP hardware is produced and sold by Ettus Research, which is a National Instruments company since 2010. One of the core objectives for the design of the USRP peripheral, was that it would be cheap enough to be affordable for radio community developers and academics, but still with instrumentation grade quality. It was initially developed to address the hardware requirements of the GNU Radio project, so there's a strong bond between GNU Radio and USRP [15, 68].

The USRP is described by two basic components, the motherboard – which holds the FPGA, DAC’s and ADC’s – and one or more daughterboards – which performs RF front-end tasks, such as up/down conversion and amplification.

An Universal Hardware Driver (UHD), encapsulates everything needed to control all of the USRP hardware in a single driver, thus enabling software developers to use USRP hardware transparently without worrying about low level details of daughterboard control, for instance.

Ettus Research offers four USRP product lines: X Series – high-end and high-performance, scalable SDR platform for designing and deploying next generation wireless communications, Network Series - high-bandwidth, high-dynamic range processing capability and with network connection (Ethernet), Bus Series – low-cost Universal Serial Bus (USB) connection devices and Embedded Series – USRP
with embedded operating system (OS) capabilities to operate as a standalone device.

Table 2.2 - USRP motherboard characteristics per USRP Series. Source: [68].

<table>
<thead>
<tr>
<th>USRP Model</th>
<th>Interface</th>
<th>Total Host BW (MSPS)</th>
<th>Daughterboard Slots</th>
<th>ADC Resolution (bits)</th>
<th>ADC Rate (MSPS)</th>
<th>DAC Resolution (bits)</th>
<th>DAC Rate (MSPS)</th>
<th>MIMO Capable</th>
<th>Internal GPS Disciplined Oscillator (Optional)</th>
<th>1 PPS/Ref Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>N210</td>
<td>Gig. Eth.</td>
<td>50/100</td>
<td>1</td>
<td>14</td>
<td>100</td>
<td>16</td>
<td>400</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>N200</td>
<td>Gig. Eth.</td>
<td>50/100</td>
<td>1</td>
<td>14</td>
<td>100</td>
<td>16</td>
<td>400</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>B100</td>
<td>USB 2.0</td>
<td>8/16</td>
<td>1</td>
<td>12</td>
<td>64</td>
<td>14</td>
<td>128</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>USRP1</td>
<td>USB 2.0</td>
<td>8/*</td>
<td>2</td>
<td>12</td>
<td>64</td>
<td>14</td>
<td>128</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>E100</td>
<td>Embedded</td>
<td>8/16</td>
<td>1</td>
<td>12</td>
<td>64</td>
<td>14</td>
<td>128</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>E110</td>
<td>Embedded</td>
<td>8/16</td>
<td>1</td>
<td>12</td>
<td>64</td>
<td>14</td>
<td>128</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The B100 USRP was the ideal model for an entry level, with 8 MHz of bandwidth (with 12 bit ADC precision). The motherboard-daughterboard configuration also offers an important degree of flexibility, since the user may choose the most suitable daughterboard according to the target application.

The WBX daughterboard (50 MHz – 2.2 GHz) is the only daughterboard that has both transmit and receive capabilities for the VHF band (30-300 MHz).

The B100 USRP + WBX Daughterboard bundle (also known as the SDR starter kit by Ettus) was a cost effective choice and will be used for this project’s implementation.
On the software side, GNU Radio is the right tool to use, since it has an extensive library of processing tools, including several hardware peripheral interfaces, as well as an active and supportive community. Moreover, there a lot of knowledge sources and projects that utilized both GNU Radio and USRP hardware to develop SDR applications.

The growing popularity of SDR technology among the hacker, security and open-source communities is empowering a set of ongoing hardware peripheral projects, such as Great Scott Gadgets’ HackRF project [70] and Nuand’s bladeRF project [71]. These two projects extend SDR peripheral affordability, offering interesting alternatives to Ettus’ products. However, for scientific grade platforms, Ettus’ products are still recommended.

These two boards have all the components integrated in the same board (unlike the motherboard-daughterboard paradigm), which puts them in a better position in terms of production costs, but with less flexibility in terms of frequency coverage.
2.4 Related Work

The IEEE 802.22 standard is probably the most complete example of a cognitive radio system implementation, designed to operate in the TVWS [19]. This system features a network stack where the cognitive components are separated from the data, control and management planes.

The IEEE 802.22 cognitive plane consists of a form of spectrum policy enforcement (security sublayer 2). In the case of a base station, cognitive security means that the local spectrum sensing together with database information is used to determine spectrum availability, define spectrum authorization and allocation for cognitive subscribers.

IEEE 802.22 also defines self coexistence mechanisms for cognitive cells. This means that base stations must permanently coordinate with each other which channels are available and which are in use for that cell. This enables dynamic channel balancing and allocation among cognitive cells. An overview on the structure of the IEEE 802.22 cognitive structure is illustrated in Figure 2.26.

![Figure 2.26 - IEEE 802.22 cognitive radio capability overview. Source: [19].](image)

Nevertheless, most of the investigation efforts focus in demonstrating solutions for the individual components and capabilities, such as spectrum sensing implementations [38, 39, 72] or allocation and management schemes [73, 74], rather than demonstrating the feasibility of the complete cognitive radio, which is the main goal of this implementation.

In [27], a prototype cognitive radio implementation based in the IEEE 802.11 MAC + PHY (WLAN) implementation is presented. This implementation considers the existing WLAN implementation as a starting point for the implementation, and on top of this, a management overlay takes care of network synchronization. The authors refer that synchronization (i.e. exchange of list of current available channels) is a major challenge for their implementation, which is also an important concern for this project. However, in [27] the synchronization procedure is performed in the same physical channel as data communication, which can be a major drawback in case no physical channel is available. Moreover, there is a lot of abstraction from the physical aspects of the radio system, which reduces flexibility in many aspects, such as frequency and bandwidth selection or spectrum shaping (for channel aggregation). In this thesis, however, there is a big focus in low level aspects, such as radio transceiver reconfigurability, and it is also assumed that the cognitive engine and data interfaces
should use independent data channels for higher flexibility.

An interesting approach for cognitive radio using SDR technology (GNU Radio and USRP) is described in [75, 76]. This implementation stresses the adaptability features of an OFDM based physical layer together with a sensing component, but the networking and cognitive aspects have reduced importance. In this thesis, cognitive processing (cognitive engine) and thus network synchronization is considered as important as spectrum sensing and shaping in cognitive radio design. As a matter of fact, in a complete cognitive radio design, most of the sensing and transceiver techniques do not make sense in a network environment if the synchronization capability is not present. This kind of integration is the main goal of this thesis, rather than developing advanced, but sectoral contributions for cognitive radio implementation.
Chapter 3

Proposed Solution

The adopted architecture for the proposed CR system is described in this chapter, as well as an overview about planning and requirements. Implementation details, design decisions and adopted concepts are also provided in this chapter.
3.1 Introduction

In this chapter the proposed solution for opportunist usage of the maritime VHF band is described. The broadband VHF communication system will be based on cognitive radio technology, which can be used to detect and take advantage of vacant spectrum bands. The reconfigurability characteristics of cognitive radios are easily achieved with software defined radios. GNU Radio is a digital signal processing software toolkit suitable for very fast, real time signal processing. Together with the USRP peripheral, which is a radio frequency digitizer and transceiver, flexible and customizable radio systems can be easily prototyped and tested.

The Maritime Mobile Service (MMS) is a licensed service for the 156 MHz to 174 MHz band, where radio channels are statically allocated and equitably used by PU’s. This static spectrum allocation leads to spectrum underutilization, so frequent spectrum holes are available for secondary usage. By detecting these opportunities, a cognitive radio can adjust its transceiver settings and use these vacant bands for its own benefit (the B-VHF system).

Since VHF communications are used mostly in near shore communications, the B-VHF system can be based on a cellular architecture, where coastal fixed stations can be gateways to the fixed networks, as well as base stations (managing sensing activities, network resources and synchronization). This architecture simplifies network management, as well as resource management and network synchronization. Implementing cutting edge sensing or transceiver techniques or developing new cognitive learning mechanisms is out of the scope of this implementation. Regulatory issues regarding secondary usage of allocated radio spectrum will not be addressed as well.

This implementation uses the GNU Radio software toolkit for the majority of the physical layer processing. GNU Radio works in a streaming fashion, and is capable of performing very fast operations, so it is suitable for real time digital signal processing. On the other hand, most of the control operations, post signal processing and inter-layer logics were implemented using Python scripting language and some with its language packages. An USRP B100 peripheral with a WBX daughterboard handles analogue domain interfacing and RF frontend operations.

3.2 Scenario Description

The first task of the cognitive radio is detecting the presence of multiple primary users (PU) within the target VHF spectrum. The final goal is to identify spectrum opportunities (holes), that cognitive, secondary users, may access and use.

Mariners typically use analogue VHF communications to coordinate maneuvers and safety procedures
with other ships and to coordinate harbor movements with port controls (Figure 3.1).

![Figure 3.1 - Overview of Maritime Communications scenarios: a) Long range communications (HF / SATCOM); b) Medium / Short range communications (VHF).](image)

The goal of this implementation is to exploit spectrum opportunities that arise from VHF maritime spectrum under usage, specifically between 156 MHz and 174 MHz. Spectrum holes will be used to establish broadband VHF communications (B-VHF), creating an important alternative to current available data systems (SATCOM only).

Like other wireless mobile communication systems with share spectrum resources, such as IEEE 802.11 LAN standards, there is always the hidden node problem. Wireless LAN standards typically use Carrier Sense Multiple Access (CSMA), so network nodes can access the spectrum without interfering with each other (collisions). CSMA measures the current energy present on the channel using an energy probe, which means that network nodes can only detect other nodes that are within their radio range.

In Figure 3.2, although the Access Point is in the range of both Clients A and B (meaning both clients can communicate with the access point), they aren’t in the range of each other, which if they transmit simultaneously, may cause collisions at the access point.

![Figure 3.2 - Hidden node problem illustration.](image)

In a cognitive radio network scenario, the hidden node problem exists if the network uses a CSMA method to share radio resources, but also exists between cognitive nodes (SU) and incumbent
primary users (PU) upon spectrum sensing. For the latter, the hidden PU problem is similar to the hidden node problem in CSMA.

In Figure 3.3, Vessel B is in the range of Coast Station A (yellow ring) and they communicate using MMS, for instance, Station A is sending a DSC message to Vessel B. Cognitive Vessels C and D are using a cognitive link to communicate, assuming that PU Vessel B, which is in their range (red ring), is not using MMS spectrum.

![Figure 3.3 - Hidden node problem in cognitive radio scenarios.](image)

In this case, two problems occur: since Station A is not in the range of Vessels C and D, these vessels will not detect its transmissions, resulting in an incorrect spectrum picture; since Vessel B is in the range of both transmitting stations, SU signal will collide and interfere with PU signal and Vessel B will not be able to receive Station A transmissions.

This problem requires additional PU precaution when taking a decision on spectrum usage. Complementary information sources, such as databases or cooperative sensing should be used to avoid PU service disruption.

### 3.2.1 Opportunistic Usage of the VHF Maritime band

The Maritime Mobile Service is a telecommunication licensed service, meaning that, the assigned radio spectrum is available for the users that utilize the service, and no license, purchase or utilization costs are associated to its utilization. Anyone who possesses MMS compliant equipment is a valid user of the MMS.

Most of the standardization efforts concerning the MMS spectrum are discussed in the World Radio Conferences (WRC), and consequently International Telecommunication Union (ITU) recommendations have been updated accordingly. A brief, but complete, history about the MMS can be found in [77].

The MMS uses the band between 156 MHz and 174 MHz, and primary user’s telephony equipments
must be compliant with the ITU's R M.489-2 recommendation [78]. The main transceiver specifications are:

- Channel spacing: 25 kHz;
- Maximum frequency deviation (corresponding to 100% modulation): +/- 5 kHz;
- Maximum transmitter bandwidth: 16 kHz;
- Frequency modulation with a pre-emphasis characteristic of 6 dB/octave.

In order to utilize available spectrum holes at the VHF MMS band, the cognitive system must detect accurately the presence of NBFM signals such as those illustrated in Figure 3.4. As mentioned before, the MMS VHF band ranges between 156 MHz and 174 MHz and Appendix S18 [77] defines channels and frequencies for MMS services (telephony, data, emergency and distress).

According to the measurements conducted onboard navy's vessels (Figure 3.4), the effective bandwidth of the NBFM voice signals is about 10 kHz (considering that the noise floor was about -100 dB). Using specifications information and real measurements, PU can be synthesized using GNU Radio for simulation and testing purposes.

![Figure 3.4 - VHF telephony signals PSD (soft speech) from three different primary user equipments captured at 156.750 MHz using GNU Radio and USRP (one hand-held and two fixed VHF transceivers).](image)

GNU Radio has already the necessary processing blocks to synthesize FM signals (filters and modulators), which can be extensively used for simulation purposes. Figure 3.5 shows the PSD plot of
a synthesized NBFM signal, resulting in a 10 kHz signal for the average soft speaking telephony voice quality.

![Figure 3.5 - NBFM PSD of a synthesized signal with GNU Radio.](image1)

The DSC service, which operates in 156.525 MHz (Channel 70), is specified by ITU Recommendation M.493-13 [79]. DSC uses a two level frequency shift keying (FSK) modulated signal that fits the same bandwidth of telephony channel (Figure 3.6).

![Figure 3.6 – Digital Selective Call PSD from synthesized signal with GNU Radio.](image2)

AIS system signals also indicate PU activity. Unlike the telephony service, AIS transponders use two fixed frequencies (channel A and B), and transmit digital modulated - Gaussian Minimum Shift Keying (GMSK) - data packets in a bursty mode. The two AIS channels are 50 kHz separated from each other (carrier frequencies are 161.975 MHz and 162.025 MHz), and each channel has a bandwidth of about 12 kHz (Figure 3.7).

![Figure 3.7 – AIS channels A and B PSD plot of a recorded signal using GNU Radio and USRP (green plot – maximum envelope, blue plot– detected peak).](image3)
Since mariner’s safety is the most important role of the MMS, channels 70 (DSC) and 16 (channels 75 and 76 are guard bands to channel 16), should have additional protection against any eventual SU interference. Moreover, these channels are recognized as Global Maritime Distress and Safety System (GMDSS) channels (Figure 3.8). For the purpose of this implementation, the use of these channels is avoided.

The most recent updates related to the MMS discussed at WRC’s intend to improve spectrum utilization efficiency (interleaving narrower spacing), but keeping the static allocation paradigm. Even with these improvements, exploiting spectrum holes is still a possibility. Figure 3.9 illustrates a typical VHF radio picture with several PU’s in activity.

In terms of national regulations, Autoridade Nacional de Comunicações (ANACOM) assures the planning, management and control of the radio spectrum. Because Portugal is a member of the European Community, ANACOM “adopts harmonized channels at European level, in the scope of the spectrum planning works in the Conference of European Postal and Telecommunications (CEPT), or at world level, resulting from the harmonization within the International Telecommunication Union,
Radiocommunications Sector (ITU-R)” [80]. Regarding the MMS frequency bands, the National Table of Frequency Allocation (NTFA), which is elaborated by ANACOM, defines the national application of spectrum allocations (Annex B).

3.3 System Architecture

The architecture of the broadband VHF communication system (B-VHF) was kept as general as possible, but some of the implemented features address specific issues of the target application. Spectrum sensing and spectrum policy enforcement, resource management and medium access control have particular importance to assure reasonable quality of service for SU’s and low interference to PU’s services. Some components may contribute to the same goal, and there are also some dependencies between.

The majority of the specifications are centered on the network’s radio interface, since most of the challenges arise from spectrum usage and sharing. However, future work must address some critical network aspects that are not focused in this implementation, such as sensing database management or routing protocols.

3.3.1 Radio Interface

A simple base station (coastal stations) - mobile station (vessels) approach, inspired by commercial mobile systems, is a simple approach for a coastal based network implementation. Most commercial systems, terrestrial (GSM, UMTS or LTE) and local area (Wireless LAN’s or DECT) use this architecture because it is a simple and efficient form of network management. Other architecture paradigms may be studied in the future, such as ad-hoc networking, which may improve the efficiency of the cognitive network.

Base stations are the gateways of land based network and they will be responsible for spectrum sensing management and radio picture compilation (Figure 3.10). Base stations (or master station, since they act as authorities in the network) will also coordinate network synchronization and signaling – the simplest way to manage network information is by centralizing information. Mobile users (or slave stations) must synchronize with base stations (and share spectrum sensing information), acquiring information about available radio resources and synchronization elements.
Besides spectrum sensing, radio interface design must consider PU compatible transmissions, medium sharing and access among SU’s and duplexing strategies.

### 3.3.2 Medium Access Control and Duplexing Strategies

The first explored option was a CSMA-style approach for medium access control (MAC). For simplicity, radios use the same band for uplink (vessel – coastal station) and downlink (coastal station – vessel), similarly to WLAN’s. Network nodes should access the physical medium in a non aggressive mode, using collision avoidance techniques (CSMA/CA). Carrier sense with collision avoidance is a very simple technique and doesn’t require any signaling. However, communications are half-duplex only, with a performance penalty due to inevitable collisions.

On the other hand, non-contiguous VHF bands may be used as an advantage, and a frequency division duplexing (FDD) technique can be implemented. Given that the available radio spectrum might be non-contiguous, uplink and downlink streams may use different bands, as illustrated in Figure 3.11.

![Figure 3.10 - Proposal for B-VHF radio infrastructure architecture.](image)

This technique enables full-duplex communication, but CSMA/CA can no longer be applied for uplink.
(because slave stations’ receivers are tuned to the downlink band) thus other medium access techniques, such as, time division multiple access (TDMA), must be used for uplink medium access. TDMA techniques are theoretically simple, but turn to be hard to implement, since all network nodes must be timely synchronized with the network.

3.3.3 Network Synchronization

It is important to clarify that network synchronization it’s not the same as transmitter-receiver synchronization (carrier synchronization, symbol timing synchronization, etc.). Network synchronization refers specifically to network and cognitive aspects of the system.

In order to access PU’s radio spectrum, all network users (master and slave stations) must be aware of the most updated version of spectrum picture and policy, and use the same transceiver settings.

During the synchronization process, master stations broadcast the necessary data to configure transceiver’s accordingly (information regarding available bands, receiver synchronization specifications, etc.). The harmonization of transceiver configuration assures PU compliancy, as well as network interoperability.

A simple solution to provide network synchronization consists of using a dedicated low bit-rate / narrowband channel to broadcast synchronization data and other network signaling (beacon style), as suggested in Figure 3.12. Similar approaches have been used in the past by well proven communication systems, such as GSM [81].

![Synchronization Channel](image)

**Figure 3.12 - Proposal for data channels and synchronization channels (synthesized data with GNU Radio).**

The synchronization channel is broadcasted by master stations and slave stations obtain the necessary network synchronization elements by periodically tuning to this channel. Ultimately, as spectrum management authorities, master stations should inform slave stations when to switch to the synchronization channel, in order to update network and spectrum usage settings.
Other network-related advanced operations, such as handover between coastal stations, may also be implemented using this topology.

3.3.4 Coastal / Master Station Design

Previous paragraphs provided some guidelines for master and slave station design. Master and slave will have slightly different designs since they play different roles in the cognitive network, mainly in terms of management and coordination capabilities. Also, CSMA operation and FDD operation require slightly different designs.

Master station mandatory tasks:

- Spectrum sensing (not exclusive for master stations);
- Manage the recognized spectrum picture and feed a spectrum database;
- Enforce spectrum policy generating and broadcasting network settings;
- Coordinate medium access (frequency duplexing mode);

Despite the unusual software defined radio implementation, this implementation also provides an interface with upper network stack layers (operation system), enabling generic traffic to flow on the cognitive network.

The basic layer stack structure for a master station is illustrated in Figure 3.13, following the seven layer nomenclature of Open Systems Interconnection (OSI) model used for the internet.

Figure 3.13 - Master station layer stack design for CSMA/CA operation.

Because this project is a software defined radio implementation, physical processing layer (PHY layer) is performed by software and by the hardware peripheral, the USRP device. In software all DSP operations occur in GNU Radio and Python. With this design, the USRP hardware peripheral is
responsible for digital – analogue interfacing only, and GNU Radio performs all DSP operations (modulation, filtering, etc.).

At the physical-software layer, there are two different hardware transceivers, one dedicated to synchronization and another transceiver for NC-OFDM dynamic spectrum access (or B-VHF transceiver). The synchronization transceiver is simpler than the B-VHF transceiver, but both share the same base OFDM implementation.

In order to “shrink” as much as possible the synchronization bandwidth, since the USRP lowest sample rate that is 125 kS/s (the DAC works at 64 MS/s and the maximum interpolation factor is 512), an appropriate carrier allocation (with extra disabled side lobe carriers) and a sharp transmitting filter reduces the transmitted bandwidth (Figure 3.14).

![Figure 3.14 - Synchronization transceiver bandwidth comparison.](image)

Although the radio outputs a 125 kHz signal, the occupied bandwidth is about 70 kHz. With this simple modification, the synchronization channel uses a fairly small bandwidth, which is desirable for bandwidth economization.

The other two software implemented physical components are the CSMA/CA probe, which measures the power level at the channel and the spectrum probe, which collects samples for spectrum analysis (for further spectrum sensing).

Above the physical layer, a MAC layer (which is also software implemented) holds the cognitive engine and its sub components. The synchronization manager coordinates the synchronization process between master stations and slave stations. The CSMA/CA engine manages the medium access and frame flow between physical layer and upper network layers. The spectrum watcher is a surveillance mechanism that keeps network synchronization data up-to-date (performing spectrum sensing and consulting spectrum databases), and feeds the synchronization manager and the B-VHF transceiver with this data. Further details concerning the cognitive engine are addressed in section 3.6.

For FDD operation, the cognitive engine works in a similar to CSMA/CA operation (Figure 3.15). Spectrum sensing should cover uplink and downlink bands, thus synchronization data can be synthesized for both links. For this reason, larger amounts of synchronization data might be generated.
Some of the implementation aspects, such as uplink medium access in FDD operation – which requires extra signaling protocols, are beyond what is feasible for this project’s schedule and will not be addressed. The final implementation considers only CSMA operation due to its simplicity and effectiveness.

### 3.3.5 Vessel / Slave Station Design

Slave stations are simplified versions of master stations, since they don’t require management features. Although slave stations perform spectrum sensing, they can’t take decisions on spectrum usage, so information regarding spectrum sensing should be forwarded to a master station, as a contribution for the recognized radio picture. This technique is often referenced as cooperative sensing [82-84]. Cooperative sensing can improve the range of PU detection, as well as the accuracy of detections. However, cooperative sensing bears an inherent delay penalty, due to network delays, as investigated in [84].

Although the cognitive engine coordinates MAC layer operations and its sub-components, for slave stations, the B-VHF transceiver is commanded remotely by a master’s cognitive engine (through the synchronization process – red dotted line in Figure 3.16). Remote configuration is a critical aspect for the presented architecture. Every time a master station wants to reconfigure the radio transceivers because a new spectrum constraint was detected, for instance, its cognitive engine sends control messages with configuration settings (synchronization data) that are then used by slave stations to reconfigure their radio transceivers. Moreover, every time a new slave wants to join the network or when an existing slave loses connectivity, slave stations should switch to the synchronization channel to obtain the correct radio settings.
Figure 3.16 - Slave station layer stack design for CSMA/CA operation.

For FDD operation (Figure 3.17), slave stations also have a duplexing engine, which is also commanded by a master station, through a synchronization logical channel.

Figure 3.17 - Slave station layer design for FDD operation.

Since CSMA/CA requires less signaling operations and less synchronization data, it will be implemented as duplexing and medium access and sharing technique. Moreover, CSMA/CA does not require any precise time synchronism between network nodes, which simplifies its implementation.
3.4 Spectrum Sensing

The main challenge for the spectrum sensing framework is the ability to detect multiple narrowband signals from a single spectrum survey, in the shortest possible period of time. Most of the previously referenced techniques, such as, feature detection or covariance detection, require an isolated channel analysis (channel by channel analysis), which is not suitable for this application. Moreover, spectrum sensing is one of several parallel tasks that the cognitive radio continuously performs, as described in previous sections.

3.4.1 Frequency Domain Energy Detector Implementation

Frequency domain energy detectors essentially depend on a spectral estimation, which can be obtained using several different techniques. Noise dependent techniques, such as the energy detector, also require accurate noise power estimates to define decision thresholds.

In order to perform spectrum analysis, the spectrum sensor obtains samples from the desired spectrum when network nodes are in an idle state (not transmitting). Then, a Python based processing script computes the spectral estimation, noise level estimate and channel detection.

Although not present in Figure 3.18, the USRP source block is simultaneously connected to the receiver radio block (described in section 3.5).

Figure 3.18 - Spectrum sensing implementation in GNU Radio.

The USRP source is tuned to the target frequency (this is actually applicable for CSMA/CA and FDD operation) and set to the operating bandwidth (restrained by the sample rate). Because the spectrum sensor block operates with vectors of samples, the outputted samples from the USRP source are fed to a stream to vector probe block (converting the stream of samples into a stream of vectors of samples). The length of the observation vector is determined by the observation time and sample rate, but due to memory allocation alignment issues, the actual length is set to a power of two (example: sample rate = 1 MS/s, observation time = 2 ms, number of samples / observation = 2000 samples, actual number of samples = 2048).
The spectrum sensor block is a custom designed block for this project that performs spectral estimations, power and PAPR measurements and channel detection.

Because spectrum sensing is an asynchronous task, the spectrum sensor block only performs spectrum-related measurements on request. Besides its streaming features, GNU Radio also enables asynchronous communication between processing blocks (grey lines in Figure 3.18) and these messages are exchanged with control blocks, such as the cognitive engine (cognitive engine MAC in Figure 3.18). Every time a block makes a request, the spectrum sensor block receives a message at message port “PDU from_cogeng”. Then, the block processes the request (a spectrum survey or a PAPR measurement) and replies with a message (sent from message port “PDU spec_msg”): a list of the occupied channels or a PAPR measurement.

The spectrum scanner implementation has two spectral estimators implemented, enabling comparison between estimators and debugging. The first method is based on Welch’s method for spectral estimation [85], and the other is based on simple FFT computation.

After performing the spectral estimation, the scanner takes the scanning settings, such as sample rate (total bandwidth), primary user’s channel rate (channel spacing) and frequency resolution (FFT length) and performs channel by channel, energy detection (Figure 3.19).

![Figure 3.19 - Workflow of the spectrum sensing framework.](image)

The spectral resolution (signal bandwidth per FFT bin) depends on the sample rate and FFT length. For 1 MS/s sample rate and spectral estimations with FFT length between 1024 and 4096, spectral resolutions range between 976.6 Hz and 244 Hz per FFT bin. These spectral resolutions are much smaller than PU channel rates and spacing and should provide enough precision.

Spectral resolution also defines the relation between FFT bin and correspondent channel frequency, as well as the ratio between bandwidth (Hz) and binwidth (FFT bins). The integration interval (energy detection) is determined by both spectral resolution and channel bandwidth (channel bandwidth is usually less than channel spacing).

The FM radio spectrum enables a good proof of concept survey (Figure 3.20).

---

8 Packet Data Unit
The power per channel is obtained by integrating the PSD for each channel within the expected channel bandwidth. To detect MMS telephony PU’s in a 1 MHz (1 MS/s) band, each channel is 25 kHz distant from the next channel (51 FFT bins @ 2048 FFT length). Each telephony channel occupies less than 10 kHz which corresponds to an integration interval of 20 FFT bins (less than channel spacing).

3.4.1.1 Noise Power Estimation and Decision Threshold

The relation between decision threshold and noise power level for a certain target probability of false alarm for an energy detector is given by the expression:

\[ T_{hr} = \sigma^2 + \frac{\sqrt{2} Q^{-1}(P_{fa})}{\sqrt{N_s}} \]

Where \( \sigma^2 \) is the variance of Additive White Gaussian Noise (AWGN) \( N_s \) is the number of samples and \( Q^{-1} \) is the inverse of the tail probability of the standard normal distribution (Q function) given by:

\[ Q(x) = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{x} \exp \left( -\frac{y^2}{2} \right) \, dy \]

Therefore, a precise noise power estimate is critical to achieve the desired detection / false alarm rate. However, since there is a fair amount of uncertainty estimating noise power level (depends on the current location, interference, etc.), estimating noise levels should be constantly updated during the communication process.

Since the spectrum sensor computes the power of each channel, the noise floor level can be defined as the lowest power level detected (weakest channel detected). Then, the decision threshold can be computed based on this value.
3.5 NC-OFDM Transceiver Design – The B-VHF Radio

GNU Radio has its own OFDM implementation, providing some dedicated processing blocks for OFDM modulation. Extensive documentation about this framework describes how it can be explored and developed to construct OFDM based applications [86]. There are demonstrations of its usage in all-software DVB-T transmitter and receiver or IEEE 802.11 LAN’s.

The implementation of the NC-OFDM transceiver is based on GNU Radio’s OFDM framework, and most of the usable components were reused. There are two essential models within GNU Radio’s repository of examples, ofdm_tx.grc and ofdm_rx.grc, which provide the basic structure of an OFDM transmitter and receiver.

Concerning this project, the main changes and improvements to GNU Radio’s OFDM existing implementation regard packet data transmission, spectrum shaping, PAPR contention and medium sharing and access techniques.

The NC-OFDM radio (or B-VHF radio) accepts data packets from the IP layer (Figure 3.21 - payload_source), and sends them the over-the-air through the USRP peripheral.

On the opposite path, the NC-OFDM radio decodes frames received from the USRP peripheral and delivers them to the IP layer (Figure 3.21 - payload_sink). The cognitive engine also uses the NC-OFDM radio to send control data and signaling over the cognitive network.

The following paragraphs give further detail about the implementation of the radio transceiver.

3.5.1 Transmitter Design

As stated above, the main challenges for the transmitter design are the development of non-contiguous spectrum shaping techniques and to enable all necessary features for packet transmission. However, this implementation was not made from scratch, since all basic features of an OFDM transmitter are already implemented by GNU Radio’s OFDM framework. A complete description about GNU Radio’s OFDM implementation can be consulted in [86] (Annex C).
3.5.1.1 Packet Data Transmission

Although GNU Radio was originally designed for synchronous data streams, most recent versions support asynchronous data streams as well - message passing and tagged streams [86]. This project uses this feature to pass packetized data through the OFDM radio, enabling external applications to send packet data (in this case, from the IP layer through the CSMA/FDD engine).

Figure 3.22 illustrates the few changes that were made to the original ofdm_tx.grc flowgraph, enabling packet data transmission (message source and message queue).

![Figure 3.22 - Inserting a packet into the radio transmitting chain.](image)

The control of the cyclic redundancy check (CRC) is made from outside of the transmitter flowgraph (from the control Python script) simplifying packet loss control. Both header and payload bits are also scrambled before the modulation process. Bit scrambling is an optional feature that can be disabled.

The packet flow through the transmitter flowgraph is managed by the CSMA/FDD engine, which is part of the cognitive engine (Figure 3.23). The interface between GNU Radio blocks and external features is easily done with Python. The cognitive engine also controls a cognitive logical channel implemented in a header that is added to the data packet (Figure 3.23 – cognitive engine header).

![Figure 3.23 - Cognitive engine interface with transmitter flowgraph – packet data transmission.](image)
### 3.5.1.2 OFDM Modulator

After the symbol stream is formed, the flowgraph performs OFDM modulation by data symbols to available subcarriers and then an IFFT is applied. Also, a cyclic prefix is added for symbol spacing (acts as a time guard), which also generates a periodic feature that can be used by the receiver for frame detection and limiting (Figure 3.24).

![OFDM Modulator Flowgraph](image)

**Figure 3.24 - OFDM modulation section of the transmitter.**

OFDM sub-carriers are classified in occupied sub-carriers, or data symbols, and pilot sub-carriers. Pilot sub-carriers are fixed-symbol sub-carriers used for channel estimation, since they are known signals for the receiver [87]. The carrier allocator block sorts the incoming symbols onto the remaining OFDM sub-carriers.

Simple spectrum shaping is achieved by setting up the carrier allocator with the information generated by the cognitive engine (through the spectrum watcher). This means that the cognitive engine can match the transmitted B-VHF spectrum to the available VHF spectrum (through the spectrum sensing process) manipulating the occupied carriers, as well as pilot carriers. The NC-OFDM transceiver also uses synchronization words, which are known OFDM symbols preceding OFDM frames. GNU Radio’s OFDM implementation uses these preambles to mark the beginning of a frame and to perform Schmidl & Cox synchronization method [88] at the receiver side.

After carrier allocation and pilot symbol insertion, parallel aligned symbols are fed into the IFFT. Then, the OFDM cyclic prefixer adds a cyclic prefix and performs parallel to serial conversion.

### 3.5.1.3 RF Front End

In order to control the radiated spectrum, level control and filter configuration are also controlled by the spectrum watcher (Figure 3.25).
The level control block clips the sample stream above the configured threshold (forces signal clipping). The transmitting filter is an IIR filter designed with a GNU Radio tool named GNU Radio filter design. For lower complexity (low number of coefficients, thus lower number of operations), IIR filters are the adequate choice compared with finite impulse response (FIR) filters.

Considering an ODFM signal with 128 sub-carriers of which 20 are side-lobe subcarriers (10 for each side-lobe) a transmitting IIR filter for OOB reduction can be designed with the following settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Type</td>
<td>Low pass IIR</td>
</tr>
<tr>
<td>IIR Design</td>
<td>Elliptic</td>
</tr>
<tr>
<td>End of Pass Band</td>
<td>0.9 (normalized)</td>
</tr>
<tr>
<td>End of Stop Band</td>
<td>0.93 (normalized)</td>
</tr>
<tr>
<td>Mass Loss Pass Band</td>
<td>0.1 dB</td>
</tr>
<tr>
<td>Attenuation in Stop Band</td>
<td>80 dB</td>
</tr>
<tr>
<td>Number of Coefficients</td>
<td>9 Forward / 9 Feedback</td>
</tr>
</tbody>
</table>

However, phase response distortion might be an issue when multiple filters are combined to reduce NC and OOB radiation simultaneously, and so should be avoided (Figure 3.26). As described in section 2.1.3, the use of IIR filters for this type of application has been proposed, theoretically, in [48].

![Figure 3.26 - Magnitude and phase response for the transmitting filter (normalized frequency).](image)

As analysis and training tools (training GNU Radio block development), some GNU Radio processing
blocks were implemented in C++ and Python languages. The clipper block is a GNU Radio C++ implemented block, performs signal clipping given a threshold level.

The PAPR measurement block is Python implemented block, which takes advantage from Numpy’s signal processing libraries. Moreover, developing blocks in Python is typically faster and simpler that in C++.

The spectrum of the signal produced by the B-VHF transmitter is illustrated in Figure 3.27. Some features can be easily observed: the four pilot carriers (slightly shifted to the left of the spectrum due to the spectrum hole on the right side); sharp spectrum edges due to the transmitting filter.

![Figure 3.27 - B-VHF Radio Output Spectrum Shape.](image)

It will be also important to evaluate the effect of dc offset produced by the USRP (it is only visible after the signal is transmitted to the air). A possible solution to get around the dc offset is telling the USRP to deviate the dc offset to a specific spectrum position where it will not interfere with the received signal or with PU’s.

### 3.5.2 Receiver Design

GNU Radio’s OFDM receiver performs the essential receiver operations, such as, frequency, timing and frame synchronization, as well as channel estimation and equalization. As a matter of fact, most of the receiver structure was kept without any further change. A complete description about GNU Radio’s OFDM implementation can be consulted in [86] (Annex C).

The USRP peripheral performs RF down-conversion and A/D conversion. Then, the output baseband signal is fed to an automatic gain control circuit (software implemented). The cognitive engine (through the synchronization data) assures that the USRP is set to the correct tune frequency and sample rate (Figure 3.28).
3.5.2.1 **Frame Synchronization and Detection**

To decode the incoming sample stream, the receiver is also configured by the cognitive engine.

The original OFDM implementation uses data aided synchronization. For simplicity, the original synchronization implementation was kept since blind frame detection and synchronization would be quite difficult to implement. Network synchronization assures that both transmitters and receivers share the same OFDM symbol structure and synchronization aids – this is the reason why the network synchronization process is so crucial for this implementation.

As illustrated in Figure 3.29, the receiver uses information about cyclic prefix and sync words to decode OFDM frames. OFDM header information is also used to equalize frames and to estimate channel behavior.

Once a frame is detected, the receiver reverses the remaining modulation process on the payload (FFT, equalization, serialization and demodulation) (Figure 3.30).
In order to perform correct payload demodulation, the receiver must have information about sub-carrier arrangement and symbol modulation (BPSK, PSK or M-QAM). These parameters are also set by the cognitive engine (through the spectrum watcher for master stations and sync manager for slave stations).

As expected, there's no specific component at the receiver side that compensates for spectrum shaping applied by the transmitter (apart from sub-carrier arrangement).

### 3.5.2.2 Packet Data Reception

After successful frame detection and demodulation, data packets are sent to a message sink and queued. The integrity of the received data is then checked by the cognitive engine using a cyclic redundant check (CRC) and forwarded according to the information retrieved from the cognitive engine header (IP packet or synchronization packet). The cognitive engine also checks the origin of the packet, discarding own packets that might feedback through the transceiver chain (Figure 3.31).

![Figure 3.31 - Cognitive engine interface with receiver flowgraph – packet data reception.](image)

The receiver does not inform the cognitive engine of receiving difficulties (i.e.: not being able to decode packets even in the presence of signal), which might be useful to detect incorrect synchronization between master and slave, unexpected presence of PU’s, etc. However, the cognitive engine checks for unusual bursts of bad CRC’s, and switches the radio to synchronization mode, in order to reacquire synchronization data.

### 3.5.3 Dynamic Transceiver Reconfiguration

In the previous section, the software implemented physical transceiver was described as dynamically reconfigurable by the cognitive engine. These reconfigurable settings are shared among all network nodes through the synchronization process.

Reconfigurable settings (synchronization data):

- FFT length – number of total OFDM sub-carriers;
- Occupied carriers – OFDM data sub-carriers (for FDD operation: uplink occupied carriers + downlink occupied carriers);
- Pilot carriers – OFDM pilot symbol sub-carriers (for FDD operation: uplink pilot carriers + downlink pilot carriers);
- OFDM frame length – total length (in bytes) of an OFDM frame;
- Tune frequency – Hardware transmitter / receiver center frequency (for FDD operation: uplink center frequency + downlink center frequency);
- Payload modulation – Modulation scheme for OFDM payload (BPSK, QPSK or M-QAM);
- Sample rate – sample stream rate ⊗ occupied bandwidth by the system;
- Synchronization words – fixed OFDM symbols used for receiver synchronization.

The cognitive engine generates the synchronization data based on a spectrum constraint (list of unavailable frequencies provided by the spectrum scanner). The spectrum constraint is converted in OFDM sub-carrier constraint (through a spectrum translator function) and then the synchronization data is produced basin on this information (Figure 3.32).

![Figure 3.32 - Synthesizing synchronization data - master stations only.](image)

Master stations run the procedure described above every spectrum survey. However, if the spectrum constraint remains unchanged, the synchronization process is skipped, saving time.

The reason why synchronization words must also be updated is because they depend on the available sub-carriers and also because they are randomly generated (thus cannot be generated by each of the network stations).

Figure 3.33 sums up all transceiver dependencies from synchronization data. This methodology allows some degree of freedom in terms of transceiver setup. However, it also results in a slight complex and time consuming synchronization process.
3.6 Cognitive Engine

The cognitive engine is the true brain of the cognitive radio transceiver. It coordinates all transceiver activities from spectrum sensing, through network synchronization to medium access control. In fact, classic MAC tasks are performed within the cognitive engine.

The cognitive engine implements something that can be considered as an approximation to Mitola’s proposal for a cognitive radio [4], acting as the brain of the system. In fact, the brain is spread along the whole radio network, since every network node is a branch of this brain as sensors of the communication environment. Master station’s cognitive engine is the center of the brain and slave stations are its extensions.

GNU Radio’s existing OFDM implementation is a fundamental aspect of this design. In order to build a complete infrastructure (with a sensing mechanism, cognitive processing, transceiver, etc), most of the infrastructure design derives from the initial OFDM implementation. Nevertheless, the OFDM suffered the necessary adaptations and improvements in order to match the initial requirements.

3.6.1 Cognitive Engine Logical Connections

However the cognitive engine operates at the typical MAC layer level, it not only performs typical MAC layer functions, but it also performs cognitive radio functions. To perform both operations, the cognitive engine needs two logical connections, one for cognitive radio control and signalling and another for
general data. The proposed architecture considers two different radio transceivers (which operate in different bands), a synchronization transceiver (SYNC transceiver) and the NC-OFDM data transceiver (B-VHF transceiver).

However synchronization data and packet data flow through different physical channels (SYNC and B-VHF), the cognitive engine must be able to reach all network stations despite the current physical channel is use.

For this reason, the cognitive engine may implement its logical connection with other stations using any of the physical channels. This way, master's cognitive engine can reach and fully control any slave cognitive engine in both SYNC and B-VHF modes (Figure 3.34).

![Cognitive Engine Physical and Logical Channels](image)

Figure 3.34 - Cognitive Engine Physical and Logical Channels.

This feature is critical to coordinate the synchronization procedure while B-VHF communications are in progress. The cognitive engine adds its header to B-VHF frames, implementing a logic connection between cognitive engines across the B-VHF network (Figure 3.35).

![Sync Frame and B-VHF Frame](image)

Figure 3.35 - Synchronization and B-VHF frame structure.

For instance, switching from B-VHF mode to SYNC mode can be remotely commanded by a master's cognitive engine using the logical channel implemented on the B-VHF physical channel (Figure 3.35).
3.6.1 Network Synchronization

Concerning the network synchronization process, the presented logical channel architecture has some limitations when switching between physical channels. When a master station sends the switching command using the B-VHF physical channel, slaves switch to SYNC mode, but then they can no longer acknowledge each other because they are in different physical channels. If a master switches to SYNC first, the same occurs.

Taking the GSM network example, there is a set of logical and physical channels that are used to perform operations similar to those described in this implementation [81]. Some of the physical channels are continuously broadcasting network information, such as, frequency correction information or synchronization information [81]. But unlike GSM, due to hardware and processing capacity limitations, this implementation is not able to support simultaneously more than one physical channel. This of course reduces network efficiency, but it is also an elegant technique that combines all cognitive radio tasks in a simple structure.

In order to coordinate all the synchronization process using the cognitive engine logical channel, a very simple protocol was implemented. Switching between physical channels with a typical acknowledge mechanism can lead to some problems, as illustrated in Figure 3.36.

![Figure 3.36 - Switching from B-VHF Mode to SYNC Mode problem. a) slave acknowledge only; b) slave and master acknowledge.](image)

Since there is always a chance one of the stations doesn’t receive the last acknowledge, this implementation adopts neither of those options. Instead, for this implementation, no acknowledge mechanism is adopted.

With no acknowledge mechanism, master stations have no confirmation that all slave stations received the order to switch from B-VHF mode to SYNC Mode. However this technique has a clear drawback (slaves can miss the synchronization process), it reduces dramatically signaling traffic (N slaves would send N acknowledges).
In the worst case scenario (Figure 3.37 b)), a slave station looses the signaling packet, but after a certain period of time switches automatically to SYNC mode.

![Diagram](Figure 3.37 - Adopted solution for switching from B-VHF Mode to Sync Mode: a) normal scenario; b) slave looses order packet but switches automatically to sync mode.)

In this case, an out-of-synchronization situation, slave stations have a trigger mechanisms (slave unlock thread) that prevents slave stations from being in B-VHF mode more than a certain period of time (much larger than the synchronization cycle periodicity). SYNC mode acts as a rendezvous state for synchronization.

The synchronization cycle can be represented as state machine (Figure 3.38). Once a master station switches to B-VHF mode, the spectrum watcher triggers a timer, which is set to the minimum sensing periodicity.

![Diagram](Figure 3.38 - Master station state flow.)

Every time the watcher wants to update the spectrum picture (periodical update or triggered by other

---

9 Out-of-synchronism means that a slave station exceeded a certain period of time without going through the synchronization process.
events such as excessive packet loss), it triggers all stations to switch to SYNC mode (muting any existing transmissions on PU bands. Before spectrum analysis all stations must be in idle or muted state so spectrum sensing can be performed without SU interference. Once in SYNC mode, the master station broadcasts updated sync data, or, in case there is no update, the synchronization is skipped (skip command is sent). Each slave station then acknowledges whether the synchronization was successful or not, so masters can stop broadcasting sync data, and then switch to B-VHF mode. Slave stations also switch automatically to SYNC mode when the unlocking mechanism detects the station lost synchronism or missed a synchronization trigger sent by the master station (Figure 3.39).

![SLAVE COGNITIVE ENGINE Diagram](image)

Figure 3.39 – Slave station state flow.

### 3.6.2 Spectrum Watcher and Spectrum Policy Enforcement

In previous sections, the spectrum watcher was introduced and its role within the cognitive engine structure explained. In fact, the spectrum watcher is responsible for all spectrum management related tasks, from spectrum sensing to synchronization data generation.

The spectrum policy is defined based on previous knowledge about channel activity and statistics, as well as PU radio characteristics (section 3.2.1). One of the most relevant spectrum policy elements is the minimum periodicity in which stations must update the radio picture. However, cognitive engines may change this periodicity and update the spectrum picture whenever convenient, since channel conditions can change over time – this is why these are cognitive radios: they have the ability to learn from the environment. This means that the base time reference for the spectrum watcher is the periodicity of spectrum sensing periodicity.

As discussed previously, the spectrum watcher timer is triggered at the same time the B-VHF mode is started (Figure 3.40). After this waiting period, the watcher tells the cognitive engine to trigger both master and slave stations to stop B-VHF activity (muting all ongoing transmissions) and to switch to SYNC mode (master station stays in an idle transient mode until the sync data is ready).
If the watcher detects some change in the spectrum picture, the spectrum policy enforcer (following the spectrum policy) translates the spectrum constraint into OFDM sub-carrier constraint and then in sync data.

This implementation enables spectrum policy definition with the following elements:

- **Concerning spectrum sensing:**
  - Minimum periodicity;
  - Sensing duration;
  - Search bandwidth;
  - Channel spacing and channel bandwidth;
  - Probability of detection / false alarm;
  - PSD spectral resolution;

- **Concerning transceiver specification:**
  - Minimum cancellation bandwidth (per detected PU channel);
  - Maximum power level at NC and OOB band zones;

As a first approach, one may define some spectrum policy based only on existing knowledge about PU’s and channel activity. However, spectrum policy must be fine tuned and constantly updated because it also depends on host behavior (due to hardware and software performance). Performance issues are addressed in chapter 4.

Synchronization data is generated according to the current spectrum policy. In fact, the spectrum restraint translation in transceiver settings is the actual policy enforcement. In this implementation, the policy enforcer generates synchronization data in three steps. It starts with OFDM sub-carrier arrangement where the usable sub-carriers = total sub-carriers – constrained sub-carriers – side band sub-carriers. Then, from the usable sub-carriers it chooses four equally spaced sub-carriers to become pilot carriers. Finally, for the remaining data sub-carries, two synchronization words are generated (based in an existing GNU Radio implementation – “_make_sync_word1” and “_make_sync_word2”). The other synchronization elements (number of OFDM sub-carriers,
modulation, etc.) may also be updated, or not, depending on the spectrum constraint and spectrum policy (example: the carrier frequency might change due to excess of spectrum constraints).

In a complete spectrum unavailability scenario, the system may hop to another band by changing the carrier frequency. Different bands may also have different spectrum policies.

### 3.6.3 Host Operating System Interface

Although not strictly necessary for a proof of concept, this implementation enables host machines to use the designed MAC + PHY layers as network interface device through which IP traffic can be sent. This functionality is achieved by using an interface between the OS and MAC layer called Linux TUN/TAP\(^{10}\) driver [89]. There is an example of its usage in some GNU Radio’s examples (tunnel.py).

According to [89], the TUN/TAP interface was intended to imitate network interface cards (NIC), but without the actual physical connection, so user applications could interface with NIC’s without using the physical layer (only at a software level). TUN works with IP frames and TAP works with Ethernet frames. With access to IP packets (using the TUN interface), a SDR can use this feature to transmit packets over the air through any radio hardware peripheral.

The second half of the interface is within the medium access agent (CSMA/FDD) and receiver queue watcher (receiver callback function). In order to prevent the medium access agent from stalling, waiting for new IP packets, the agent periodically checks for a trigger coming from the spectrum watcher.

The CSMA/FDD engine checks for new IP packets to be sent, cycling through the operations illustrated in Figure 3.41. If no packet is detected within a small period of time, an exception is raised, and the engine quickly checks for triggers (i.e.: switch to SYNC mode). Figure 3.41 also describes in detail the process of sending a packet through the B-VHF physical channel.

![Figure 3.41 - OS interface detail – transmitter side.](image)

\(^{10}\) TUN/TAP provides packet reception and transmission for user space programs, emulating network devices supported entirely in software.
On the receiver side, a complementary mechanism processes the incoming packets. A watcher mechanism sets off a callback function that deals with existing messages in the message queue.

The present implementation does not have a retransmission mechanism, an automatic repeat request (ARQ), since this mechanism is already implemented by the upper layer stack. CRC integrity check is intentionally out of the transmit/receive flow-graphs, to facilitates debugging and statistical analysis. To ignore frames that can feedback through the receive chain, source/destination tag from cognitive engine’s header is checked and own frames are discarded (Figure 3.42).

At this point, a lot of design decisions might be questionable. The presented implementation is a trade-off between objectives, time schedule, development complexity and know-how. In fact, most MAC layer functionalities could have been implemented in custom made GNU Radio processing blocks.

Without a fragmentation mechanism, the radio only accepts fixed-length packets from the IP layer – this means that the maximum transmission unit (MTU) must be set to that value at setup. Also, forward error correction can also be implemented in future developments to improve performance.
Chapter 4

Test and Demonstration

This chapter starts by providing a description of the test scenarios for the simulations and real communication links. Some initial benchmark tests are provided in controlled conditions, using synthesized and real PU signals. Then, a PU radio is used to generate spectrum activity and the whole system capabilities are evaluated.
4.1 Introduction

This chapter demonstrates and evaluates individually cognitive radio system components, such as the spectrum sensing block, transceiver blocks and cognitive engine block. First, these components were tested and evaluated to establish baselines. Finally, the cognitive radio was tested as complete system, were each block performs its specific function.

The coexistence between NC-OFDM transceivers and PU is also demonstrated and assessed. The interference perception induced by the NC-OFDM transceivers on VHF voice calls was subjectively evaluated by Human subjects.

Additive WGN and line of sight fading (Rice fading) channels were implemented to approximate the expected maritime propagation channel.

4.2 Spectrum Sensing Performance Analysis

In order to establish a baseline for the spectrum sensing framework, two benchmark tests were performed, one with real captured signals and another with synthesized signals. Synthesized signals are useful for debugging and experimenting specific scenarios while real data validates the performance of the detector in the presence of incumbent user signals.

The overall performance of the spectrum sensor processing block, as a multichannel detector, is highly dependent on the performance of single channel detection. For the implemented energy detector, the accuracy of the detector essentially depends on the actual SNR at the detection instant.

Table 4.1 - Spectrum sensing initial setup.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensing time</td>
<td>2048 samples = 2,048 ms @ 1MS/s</td>
</tr>
<tr>
<td>FFT size</td>
<td>4096 bins</td>
</tr>
<tr>
<td>Channel spacing</td>
<td>25 kHz</td>
</tr>
<tr>
<td>Search bandwidth</td>
<td>12.5 kHz</td>
</tr>
<tr>
<td>PSD technique</td>
<td>FFT based method</td>
</tr>
</tbody>
</table>
The AWGN + Fading block (Figure 4.1) emulates a simple Rician fading channel and an Additive WGN. The flowgraph in Figure 4.1 also has a SNR leveler so AWGN amplitude can be adjusted.

Figure 4.1 - GNU Radio flowgraph to evaluate the spectrum sensor block.

Figure 4.2 illustrates the resulting detection with a single PU present.

Figure 4.2 - Spectrum sensing output after PU detection.

Using the same approach illustrated in Figure 4.1, GNU Radio can be used to simulate several PU’s (Figure 4.3).
Figure 4.3 - GNU Radio flowgraph that simulates multiple PU NBFM activity.

The output sample stream can be saved to a file to feed another flowgraph to simulate a communication channel with PU activity included. Also, saving the output data to a file enables post processing with other analysis tools such as Matlab® or Python with Numpy and Scipy.

Figure 4.4 shows the results from a spectrum scan using the implemented energy detector, allowing a graphical visualization of how the detector measures channel power and performs detection.

Figure 4.4 - Spectrum Sensing results (Python generated plots).

In order to continuously evaluate the spectrum sensor block, the simulation setup was connected to the spectrum sensor processing block. The GNU Radio block continuously outputs a spectrum constraint (list of occupied channels), and in this case the result is printed for further analysis (Figure 4.5).
An alternative method to test the spectrum sensing framework consists in using previously recorded real signals. Using a simple GNU Radio flowgraph and a USRP (Figure 4.6), spectrum samples can be recorded to a file and then used as test signals (Figure 4.7). Figure 4.6 - Recording signal samples using GNU Radio and USRP. Figure 4.7 - Using recorded signals to test the spectrum sensing framework. In Figure 4.8 the PSD of the recorded test signal confirms the output message from the spectrum sensor block containing the occupied channels (spectrum constraint). This framework revealed to be very useful to quickly test new conditions and scenarios, as well as quick iteration through the sensing algorithms, which validates the spectrum sensing framework as capable of detecting multiple PU.
Results confirm and demonstrate that the designed energy detector is able to detect multiple narrowband signals in a single spectrum scan, which fulfils the needs of this implementation.

### 4.3 Transceiver Performance Analysis

The objective of this test is to establish a baseline for packet burst transmission using the NC-OFDM transceiver (B-VHF transceiver). Every test starts with the spectrum sensing process (master station) and then the synchronization procedure between sender and receiver takes place. After the synchronization process is completed, the sender (master station) transmits several bursts of data packets (Figure 4.9). This test enables various RF performance and packet related measurements, including: spectrum shaping, PAPR, coexistence between PU and SU, error rates (packet drops vs total number of packets).

![Figure 4.8 - Detection results from recorded signals.](image)

Figure 4.8 - Detection results from recorded signals.

This test has multiple features and settings that can be tuned to recreate multiple test conditions. In a
pure simulation scenario (hardware-free), a channel model can be implemented with the previously referenced blocks. Table 4.2 summarizes the settings for the transceiver tests.

Table 4.2 - Transceiver setup for transceiver performance analysis.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System bandwidth</td>
<td>1MS/s</td>
</tr>
<tr>
<td>OFDM FFT size</td>
<td>128 bins</td>
</tr>
<tr>
<td>OFDM Cyclic Prefix size</td>
<td>32 bins (1/4)</td>
</tr>
<tr>
<td>Symbol modulation</td>
<td>QPSK</td>
</tr>
<tr>
<td>OFDM Frame size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Cancelation band (per PU detected)</td>
<td>50 kHz → 7 OFDM bins</td>
</tr>
</tbody>
</table>

For this test, instead of transmitting and receiving IP packets (“from app” and “to app” in Figure 4.10), the cognitive engine is configured to synchronize and then send bursts of packets continuously from the sender to the receiver. The spectrum sensor block is used to define an initial spectrum constraint, enabling predefined simulated PU conditions.

The setup for both simulation and over-the-air is based on the same flowgraph (Figure 4.10). For hardware-free simulation purposes, instead of the USRP’s, hardware interfaces can be emulated by UDP sockets (UDP sources and sinks). Channel models can be added to the simulation frameworks, like the previous spectrum sensing simulations.

Transceiver analysis will focus on half-duplex, CSMA operation. This operation mode is simpler to analyse and provides the fundamental aspects of transceiver operation.

Figure 4.10 gives a graphical idea of testing framework. Some of the represented processing blocks are actually controlled by an external script that manages most of the asynchronous operations regarding sender-receiver synchronization and flowgraph reconfiguration.

Figure 4.10 – Graphical representation of the flowgraph for cognitive operation and benchmarking.
The number of correctly received and total received packets is controlled monitoring the CRC32 check. Spectrum shaping analysis and other post-processing measurements are performed using recordings from the outputted signals to files at the receiver and transmitter sides.

### 4.3.1 Packet Benchmarking

The simulated scenario includes an AWGN channel model combined with a line of sight fading model (Rician fading, which is typical for above water communications). Packets are sent from the sender to the receiver each 10 ms and the receiver counts the received and correctly received packets for each channel condition. All simulations also consider the presence of a PU (randomly assigned within the operation band, forcing the B-VHF transceiver to operate with a NC spectrum.

As a coarse observation, SNR ranged from 2 dB to 12 dB and Rician k factor from 10 to 1. The results are illustrated in the following figures. Above 90% of correctly received packets is considered to be an acceptable performance for the B-VHF transceiver, which is equivalent to a packet error rate (PER) of less than 10%.

Results illustrated in Figure 4.11 show that the system has a turning point in performance between 5 and 8 dB, where the receiver is able to start decoding packets and obtain some of them correctly. It is good to recall that the transceiver has no error correction capability – the CRC32 only checks for frame integrity.

![Figure 4.11](image)

Figure 4.11 – Percentage of received and correctly received packets vs SNR for different k factors, SNR [2.0 – 12.0] dB.

Results also show that the applied fading has little impact in the overall system performance. Some of
the fading effects and fluctuations of the received signal are eventually accommodated by the receiver through the automatic gain controller and channel equalizer. For a 7 dB SNR, the percentage of correctly received packets is above 90%, for all fading levels, which is an acceptable loss ratio.

Further results confirm that the fading has little effect on the receiver performance and that the 90% regime is achieved above 7 dB SNR – for 7 dB SNR, PER = 6.6%. Figure 4.12 also reveals that above 6.6 dB the receiver is able to decode more than 90% of the transmitted packets, but less than 80% are decoded correctly.

Figure 4.12 - Percentage of received and correctly received packets vs SNR for different k factors, SNR [5.0 – 8.0] dB.

For over-the-air testing, two computers, each connected to an USRP, were used as transmitting and receiving stations in a laboratory setup. The USRP’s were 4 m apart from each other, and standard monopole antennas were used, as illustrated in Figure 4.13.

Figure 4.13 - Laboratorial setup for over-the-air analysis.
Both transmit and receive gains were adjusted to avoid any signal saturation or distortion and providing enough signal strength at the receiver side.

For the benchmark test, the receiver got 100% of the transmitted packets, of which 99% were received correctly. This simple test proves that the developed framework is fully functional with hardware peripherals for over-the-air communications.

### 4.3.2 Spectral Shaping and Radiation Performance Analysis

Using the same setup from the previous section, transmitted and received signal samples were recorded for further analysis, including spectrum shaping metrics such as NC radiation, OOB radiation and PAPR.

For the simulation test, the model channel was configured with the settings for which the system achieved an acceptable performance in the previous tests (SNR = 7 dB, \( k = 2 \)). Over-the-air measurements were also made under the same previous settings.

![Figure 4.14 - Spectrogram (time-frequency) and PSD (averaged over 15 samples) of the transmitted signal.](image)

The transmitted and received signals (Figure 4.14 and Figure 4.15) reveal the 4 pilot tones as well as the absence of the center tone (for the cases in which the hardware DC has to be accommodated within the useful band). Also, the spectrum decays at the edges (suppressing OOB radiation) and at 0.1 MHz from the carrier frequency are also noticeable. For the transmitted signal, the obtained OOB
cancelation is much prominent than NC cancelation, as a result of the effect of the IIR transmitting filter.

However, in the presence of noise, received signal inspection reveals that the power level within the OOB and NC zones is about the same magnitude (about -80 dB), which might confirm that the obtained NC band cancellation might be enough to enable coexistence with PU’s.

![Spectrogram](image)

**Figure 4.15** - Spectrogram (time-frequency) and PSD (averaged over 15 samples) of the received signal for SNR=7dB and k=2.

Also, the spectrum decays at the edges (suppressing OOB radiation) and at 0.1 MHz from the carrier frequency (NC hole) are also noticeable. Moreover, the spectrogram plot also confirms the presence of the three suppressed spectrum areas (two sidebands and spectrum hole) of about the same magnitude, as well as some visible signal fluctuations (different signal intensities are observed over time), as a result of Rice fading.

Simulations offer an interesting preview of the expected results, but hardware peripherals can also induce other (not yet accounted) artifacts to the transmitted signal, such as clipping or quadrature imbalancements.

As for over-the-air signal analysis, transmitted signals have the same characteristics as the previous simulations (since they are recorded before the hardware peripheral). On the receiver side, the log file records all incoming signals, even when no transmission is taking place, so the 10 ms interval between packets can be perceived (Figure 4.16).
For over-the-air transmission, the NC band cancellation about the same level of OOB cancellation, which confirms preliminary simulated results. This result is highly dependent on power control (transmitting gain) since for higher gain levels NC cancellation band will not be as strong as OOB cancellation.

### 4.3.2.1 Out-of-band and Non-contiguous Radiation Analysis

OOB radiation cancellation is achieved combining of 8 OFDM cancelled sub-carriers and an IIR transmitting filter. The result of this combination is a power level of about -155 dB in the OOB zone of the spectrum (before the hardware peripheral). NC radiation cancellation is achieved only by disabling 50 kHz worth of OFDM subcarriers (7 OFDM sub-carriers @ 1MS/s), which results in -80 dB of radiated power level (Figure 4.17).
Results from Figure 4.17 also show that with no additional radiation cancelation technique, NC level is about 15 dB below the average OFDM signal level, which demands for further investigation in terms of PU coexistence.

In Figure 4.18, investigation on OOB and NC radiation of the received signals reveals that, in the presence of noise, the signal level is about the same for both cases. These results suggest that, as long as the transmitted power is kept to the minimum – SNR = 7 dB was the lowest SNR level for which the system achieved a satisfactory performance – the NC radiated power is about the same level of background noise.

![Figure 4.18 - OOB and NC radiation details of the received signal (simulation).](image)

In Figure 4.19, a comparison between transmitted and received signals PSD’s enables visual confirmation of the effect of background noise in OOB and NC bands.

![Figure 4.19 - Transmitted and received signal PSD comparison (simulation).](image)

Figure 4.20 shows that for the case of over-the-air transmission, NC radiation level is about 5 dB above the OOB radiation level, which confirms the results from the simulated scenario. Experimental results are quite identical to the simulation results, which can be helpful in developing new techniques and proving new concepts.
However, these over-the-air results do not replicate accurately the expected conditions for maritime communications, where other sources of noise and interference may change current results.

In terms of hardware-induced signal artifacts, some local oscillator leakage (direct current (DC) offset) is periodically observable (blue spike in Figure 4.21). Although the DC offset cannot be eliminated, the transmitter can shift it to a desirable spectrum zone where it won’t corrupt either transmitted signals or PU signals. In this case, since the carrier OFDM bin is disabled, the DC offset shows up in the carrier frequency but does not affect the receiver.

In Figure 4.21 the effect of background noise is again visible in the side bands. These results also enhance the importance of power control to prevent high NC radiation levels in order to avoid interference to PU’s.

However, the effect of NC radiation on PU quality of service involves other variables, such as ambient noise level, loss path, SU power control, etc. Additional investigation about coexistence between SU and PU is described in section 4.3.3.

### 4.3.2.2 Peak-to-average Power Ratio Analysis

PAPR is an important performance metric for any communication system where the analogue end of
the transmitter (D/A converter and power amplifier) may reduce the effect of previously applied signal transformation, such as filtering. As referenced in section 2.1.3.1, OFDM (and NC-OFDM) suffers from relatively high PAPR, typically between 10 dB and 12 dB maximum.

PAPR measurements were taken considering the previous baseline of SNR=7 dB, k=2 and no clipping, which resulted in a PER of 6.7%. In order to measure PAPR, the received samples file was analysed with a Python processing script that computes PAPR and generates the characteristic CCD function.

The NC-OFDM transmitter (Figure 3.25) implements a simple clipping mechanism. The amplitude of the OFDM signal is scaled by a factor of 0.01, thus the clipper threshold level must be about the same order of magnitude. To simplify, clipping factor is expressed relatively to 0.01, the reference signal amplitude – Clp[\%] = 0.01/clip_threshold*100, where 0% clipping corresponds to no signal clipping.

Since the implemented PAPR reduction technique is based in signal clipping, the signal is clipped before the transmit filter is applied (Figure 3.25), contradicting the OOB radiation increase effect.

In Figure 4.22, results show that there is a significant reduction in PAPR for a 50% clipping, but not for higher clipping ratios. With 50% of clipping ratio, there is a 1 dB reduction in the maximum PAPR and an increase of 3.7% in PER, which is still below the 10% reference level. As expected, PER increases as the clipping ratio increases.

![Figure 4.22 - Comparison of results from different clipping levels.](image)

There is a reduced impact on OOB radiation, since the clipping is before the IIR filtering (Figure 4.23).

![Figure 4.23 – Left band edge comparison between unclipped and clipped signals.](image)
On the other hand, clipping and filtering produce opposite effects on signal frequency response [56]. As Figure 4.24 illustrates, this effect confirms a clipping – filtering duality.

![Figure 4.24 - Filtering effect on PAPR performance.](image)

Results confirm the expected effect of filtering in terms of PAPR. A measurement before the IIR filter confirms that the clipping technique can achieve more than 1 dB of PAPR reduction if the signal is not filtered after clipping. However, as seen in previous results, combining clipping and filtering slightly reduces PAPR (1 dB).

The above results also point to another interesting observation: clipping may occur at the hardware peripheral (analogue components) which may result in frequency response performance degradation. For instance, if the signal is clipped (by hardware components), the effect of filtering (for OOB radiation reduction) is reduced (Figure 4.25).

![Figure 4.25 - Hardware clipping after the transmit filter.](image)

Hardware clipping can be a bottleneck for OOB radiation performance if filtering is the radiation reduction countermeasure. In [90], a joint OOB and PAPR reduction technique is studied. In this paper, it is simulated that combining partial transmit sequences and optimized phase rotations can improve simultaneously OOB radiation and PAPR performances. This technique might be address as future work in case PAPR becomes a performance bottleneck, but currently is out of the scope of this thesis.
Although 1 dB might not be much in terms of PAPR reduction, it’s a fair gain for a simple implementation and low computational complexity technique. Moreover, whenever need, this technique can be used without significant PER or performance penalties.

4.3.3 PU Coexistence Analysis

The coexistence limits between NBFM signals and NC-OFDM signals are evaluated in this section. This test is based on a subjective evaluation of the voice quality over a NBFM transmission in the presence of the previous WGN + Fading model channel and a NC-OFDM signal. The subject NC-OFDM signal is generated using the implemented infrastructure, considering the presence of one PU (Figure 4.26).

The NC-OFDM and PU signals can be shifted across each other using a frequency translating filter, so interference can be measured at transmitting, NC and OOB bands.

Case 1: Transmitting band

In this scenario the PU signal is totally indistinguishable from noise and interference (Figure 4.27). This is a total interference situation that will cause total loss of service to incumbent users.

Figure 4.26 - Subject test signals. SNR = 7 dB.

Case 2: OOB band

In terms of voice perception, there is no perceptible speech within the received signal.
The OOB radiation is dramatically reduced by the transmitting filter and it is not expected any perceptible interference (Figure 4.28).

For this scenario, the voice communication is totally perceptible and the combined effect of background noise and OOB interference has little impact on voice quality.

**Case 3: NC band**

For this scenario (Figure 4.29), since the NC radiation level is somewhat above the background noise, it is expected some impact on the communication experience, but not a disruptive impact.

Subjective results reveal a minor impact in voice perception and some background interference is noticeable. Even in this condition, the PU service might not be disrupted since it still possible to establish a voice call with acceptable audio quality. Further analysis revealed that for higher NC-OFDM signal levels (relative to the PU level), the background interference increases, but the voice call is still perceptible.
4.4 Network Synchronization

As stated in section 3.3.3 (implementation aspects of the synchronization channel, a dedicated radio channel (and thus a radio transceiver) is utilized by master stations to broadcast network synchronization data among network slaves.

The synchronization protocol is very simple, since there is previous knowledge of the number of expected packets on each synchronization process. After receiving all the SYNC packets, slaves send and acknowledge, instead of acknowledging all received packets, and then the master station stops broadcasting SYNC packets once all slaves acknowledge.

As Figure 4.30 shows, there is a 1 s gap between packets bursts, so slaves have enough time to check for the integrity of the received data and report synchronization success to master station.

Figure 4.30 - Synchronization process debugging - spectrogram (time-frequency), PSD plot and console display.

For the above settings, synchronization data usually occupies less than 10 packets (several tests revealed that 10 packets is enough to accommodate most of the synchronization data configurations), the reason why the spectrogram in Figure 4.30 exhibits straight lines at the end of each packet burst (the last 2 or 3 packets are empty).

The details of the synchronization procedure in the communication process context are described in the next section.

4.5 Performance Test with IP Data Packets

The objective of this test is to assess the OS interface and how transparent the MAC + PHY layers are. This implementation works like a tunneling mechanism, since IP packets are transferred across the cognitive network transparently for the upper layers.
This test consists in a series of ping requests / responses (ICMP protocol) between two stations (PC + USRP). For simulation purposes, the hardware peripherals (USRP’s) can be emulated using UDP sockets (simulator to previous sections). During the communication process, the network communication is periodically interrupted for cognitive network synchronization as referred previously in Chapter 3. When a new slave station joins the network, new IP and MAC addresses are assigned by the configuration script (TUN/TAP interface) and also a new cognitive engine address is assigned (this address is used for cognitive engine tasks only).

There is a small delay penalty resulting from the physical layer processing implemented in software. Moreover, the implemented MAC layer produces fixed length frames despite the size of the IP packets, which also reduces the efficiency of the protocol, particularly for small IP packets. In simulation environment, there is also an additional delay from the encapsulation of the sample stream in the socket interfaces.

For simulation cases, the socket IP addresses from the current machine and destination machine must be specified. The NIC card IP address, which is the IP address of the machine for the cognitive network, is also specified and a new network interface is created.

After the initial setup, all stations go to synchronization mode: slaves wait for SYNC messages; master station performs an initial spectrum sensing and starts the synchronization process with slave stations (Figure 4.31).

![Figure 4.31 - Synchronization message exchange between master and slave.](image)

The current implementation supports multiple slave synchronization (master confirms all slaves got synchronization correctly), but only when USRP peripherals are used, because in simulation setups UDP sockets are point to point connections.

After the synchronization procedure, all stations switch to B-VHF mode and the cognitive network is established. Then, the Address Resolution Protocol (ARP) starts the standard procedure for address
resolution so other communication services, such as the Internet Control Message Protocol (ICMP) can be started (Figure 4.32).

![Figure 4.32 - ARP packets captured with Wireshark.](image)

In Figure 4.32, ICMP packets (ping requests) are captured after the ARP protocol discovers the requested users. It should be recalled, however, that these are upper layer procedures, and the cognitive layer does not interfere in this process. The IP and MAC addresses only have meaning to the NIC and IP layer, since the cognitive layer has its own address and resolution mechanisms. This way, the cognitive layer keeps its transparency towards the upper layers.

Using the debugging consoles, packets can be monitored and compared with Wireshark captures (Figure 4.33)

![Figure 4.33 - Packet analysis using station's debugging consoles and Wireshark.](image)

In this test, the master station performed 644 ping requests and received 533 ping responses, which yields 17% packet loss. However, it should be recalled that some packets were lost due to periodic interruptions for network synchronization. The round trip times range between 662 ms and 4200 ms for simulation setups and between 10 ms and 50 ms for over the air setups.
In this chapter, a summary of all the implementation process is provided. Then, considering the most relevant results, the final conclusions are highlighted. A general overview of the implementation is given, referring the most significant achievements, as well as key limitations. Future work topics are also given.
This thesis describes the implementation of a software defined and cognitive radio system, using GNU Radio digital signal processing toolkit and USRP radio peripherals. The main goal was to implement a radio communication system with cognitive personality, which uses vacant VHF maritime bands in an opportunistic fashion. The utilization of GNU Radio and USRP as SDR tools was emphasized, and used for simulation, demonstration and measurement wherever possible.

An initial survey on state-of-the-art dynamic spectrum access techniques exposed the potential progress of cognitive radio communication systems. Recent developments in various areas, such as spectrum sensing and shaping techniques or software defined radios also demonstrate the importance of cognitive radios in next generation digital communication systems. Then an overview on related work was provided, where the main differences and innovative aspects of this project can be noticed. After reviewing the essentials of dynamic spectrum access and cognitive radios, the necessary techniques and methods were selected for further implementation.

Chapter 3 (design and implementation), begins with an overview on VHF maritime communications infrastructure, including typical primary user equipments and communication scenarios, which provided the essential requirements for the final implementation. The implemented communication system follows a master-slave topology, where VHF coastal stations (masters) act as deciders in terms of spectrum usage and spectrum policy enforcement towards vessels (slave stations). A complete description of the cognitive stations is also provided, pointing the differences between master and slave stations and defining strategies for coordination, medium access and sharing. Then, the cognitive radio implementation is described in functional blocks: spectrum sensor block, which implements a frequency-domain multiuser energy detector; radio transceiver block, which implements a NC-OFDM reconfigurable transceiver; cognitive engine block, which implements a middle layer between IP and physical layers (cognitive + MAC layer) and enables cognitive processing, network synchronization and coordination.

During the implementation process, some specific DSA aspects were stressed, such as spectrum sensing, spectrum shaping, dynamic reconfiguration and network synchronization. The spectrum sensing block has the ability to detect multiple primary users in a single spectrum survey, enabling fast and reliable detection of several narrow band signals (using spectral estimations and scanning mechanisms). The radio transceiver is based on GNU Radio’s base OFDM implementation, which provided the base transceiver implementation. In order to obtain a reconfigurable non-contiguous OFDM transceiver, spectrum shaping techniques and reconfigurability support features were added. Spectrum policy enforcement is implemented using a synchronization procedure (network synchronization), which uses a dedicated radio channel, so master stations can broadcast policy enforced radio transceiver settings among network users. A two mode communication system was implemented: B-VHF mode, which uses the NC-OFDM transceiver over vacant spectrum bands, and SYNC mode, which uses a fixed allocated band for network synchronization.

The development of an effective and efficient network synchronization turned out to be a very challenging task. As a coordinator node, master station’s cognitive engine uses a logical channel for cognitive data and signaling, implemented in both B-VHF and SYNC physical channels. This approach
proved to be effective, but lacks of efficiency, since it uses a fixed allocated channel and requires interruption of B-VHF communications.

The interface of the middle layer with upper layers was smartly implemented using the TUN/TAP Linux mechanism. Using the TUN feature, the cognitive + MAC layer interacts directly with a virtual NIC that receives and delivers IP packets to the operating system.

In order to establish a baseline for each of the implemented blocks and for the whole system, evaluation tests and measurements were performed. All the simulation tests were performed under an AWGN + Fading (Rice – with line of sight) simulated channel, which emulates the expected conditions of maritime communications scenario. Over-the-air tests were performed under a laboratorial setup.

The spectrum sensor block was evaluated in single user detection and multiple user detection, as well as integrated in the cognitive decision mechanism.

Another benchmark test defined the conditions under which the NC-OFDM transceiver achieves acceptable performance (below 10% of packet loss) under controlled SNR and fading conditions. This test demonstrated that for high fading environments (k=2) the system achieves acceptable performance above 7 dB SNR, which shows how resilient the equalization mechanisms of the OFDM receiver are. Then the spectrum signatures of the radio transmitter were evaluated. Spectral measurements show that digital filtering before the hardware peripheral achieves deep OOB radiation cancelation, which is a typical drawback of OFDM systems. Spectral measurements also show that, although not as effective as filtering, NC spectrum cancelation obtained by OFDM sub-carrier disabling, achieves a reasonable cancellation level in low SNR environments (relative to the transceiver benchmark) when the NC level is compared with noise floor.

Further investigation on the radiated signals also showed that, like other OFDM-based systems, this implementation also suffers from high PAPR (about 11 dB max.). However, there are no evident signs of distortion due to hardware clipping. Results also show that a small PAPR reduction (about 1dB) can be achieved using simple signal clipping before IIR filtering, without relevant signal distortions (increasing of OOB radiation).

In order to verify the effectiveness of the implemented spectrum shaping techniques, a simple and quick coexistence test with PU was performed. Coexistence limits evaluation, namely in terms of tolerance to interference, turns out to be very subjective when analyzing analogue signals (PU telephony service), since it is difficult to define the point where the service is disrupted (it's a subjective evaluation, subject to Human perception of interference and noise). Coexistence tests show that the transceiver induces a very small amount of interference in the OOB band (impossible to differentiate from background noise), and an acceptable level of interference in the NC band (noticeable and distinguishable from background noise, but not enough to break up a voice communication).

Finally, a demonstration shows the integration of all processing components into the cognitive radio. Two cognitive radios were used (2 PC's + 2 USRP's), one as master station and the other as slave station. This test demonstrates how PU's are detected and the spectrum constraint is formulated for later network synchronization. Then, as a proof of concept, ARP and ICMP internet protocols were
analysed using Wireshark tool, where packets could be picked in several communication moments.

ICMP ping tests show that the system offers a round trip time of the order of magnitude as other wireless communication protocols (tens of ms), although there is a delay penalty introduced by the software processing of the physical layer. On the other hand, communication interruptions for network synchronization revealed to have little interference on the communication process (only a few packets were lost or delayed during synchronization processes). The implemented operating system – cognitive middle layer is totally transparent for end to end communications, since operating systems use the cognitive radio as a regular NIC. Laboratorial tests and measurements also show stable performance, with minor bugs or exceptions.

It was proved that it is possible to implement a cognitive radio system using software defined radios and radio peripherals for opportunistic usage of vacant spectrum bands in the VHF maritime spectrum. Despite being a prototype, the implemented radio system is able to detect and adjust its transceiver settings for dynamic spectrum access. Moreover, the designed system is able to establish a cognitive protocol that broadcasts network synchronization data, so it can be used in point-to-multipoint communication systems.

Finally, it important to recall that this thesis covered most of the important topics on cognitive radio design and implementation using software defined radios, but also exposed a lot of digital signal processing aspects and techniques, as well as its applicability in radio design. Interacting and interfacing with radio hardware peripherals also offered an important experience in terms of real world communication system implementation. Using GNU Radio and USRP enabled a lot of new discovers from the radio world, as well as fast prototyping, experiencing and simulation.

Future Work:
Various improvements can be addressed in future projects, concerning the network topology, medium access strategies, node design, signal processing and evaluation tests. It is suggested to improve the individual functionalities of each component organized in the following areas:

- Spectrum Sensing:
  o Implement other multiuser detectors, such as wavelets based method;
  o Integrate external sources of information in the sensing process, such AIS and ARPA data;
- B-VHF transmitter:
  o Implement more effective NC radiation reduction techniques such as cancellation carriers, improving NC radiation cancellation;
  o Implement non distortive PAPR reduction techniques.
- B-VHF receiver:
  o Implement blind synchronization techniques (avoiding the necessity of knowing sub-carrier allocation, sync words, etc.);
  o Feedback decoder information to upper layers for reception conditions monitoring;
• Radio Peripheral:
  o Implement an optimization algorithm that automatically sets the DC offset to a band zone where it will not harmfully interfere with receivers or PU’s;
  o Implement some of the DSP algorithms over the available FPGA resources, increasing performance and reducing load from the host PC.

• Network synchronization:
  o Implement other synchronization typologies, possibly without using a dedicated physical channel;
  o Improve protocols with more effective acknowledge mechanisms;
  o Implement alternative synchronous protocols with less signaling;
  o Implement the integration of the synchronization protocols in upper layers (IP or application);

• Spectrum policy enforcement:
  o Implement a spectrum sensing database with management;
  o Improve learning mechanisms based on diverse sources of information;
  o Improve and take advantage of cooperative sensing.

• Cognitive + MAC layer design:
  o Enable variable IP packet size;
  o Implement forward error correction (FEC) schemes;
  o Use NIC specific elements, such as MAC addresses for cognitive management;
  o Study the implementation of a security mechanisms based on the MAC/PHY layer;

• Testing and Evaluation:
  o Expose and test the prototype in a multiple PU scenario;
  o Test the prototype in a real maritime environment;
  o Evaluate more extensively PU coexistence and the introduced interference by SU for various spectrum bands;
Annex A

Annex A. Portuguese VHF Spectrum Allocations

This annex provides the current Portuguese VHF spectrum allocation
Figure A.1 – VHF Radio Services and Applications - Portuguese electronic National Table of Frequency Allocations (eNTFA). Source: [80]

Table A.1 - Portuguese frequency allocation table that includes MMS channels. Source: [80].

<table>
<thead>
<tr>
<th>Frequency bands [MHz]</th>
<th>Radio services</th>
<th>Applications</th>
<th>Channeling</th>
</tr>
</thead>
<tbody>
<tr>
<td>156.0125 - 157.4375</td>
<td>Maritime Mobile</td>
<td>Maritime communications</td>
<td>25 kHz</td>
</tr>
<tr>
<td>156.525 - 156.525</td>
<td>Maritime Mobile</td>
<td>DSC</td>
<td></td>
</tr>
<tr>
<td>157.4325 - 158.0125</td>
<td>Maritime Mobile</td>
<td>Maritime communications</td>
<td>25 kHz</td>
</tr>
<tr>
<td>158.050 - 160.600</td>
<td>Land Mobile</td>
<td>PMR&lt;sup&gt;11&lt;/sup&gt;</td>
<td>12.5 kHz</td>
</tr>
<tr>
<td>160.6125 - 162.3375</td>
<td>Maritime Mobile</td>
<td>Maritime communications</td>
<td>25 kHz</td>
</tr>
<tr>
<td>161.975 - 161.975</td>
<td>Maritime Radionavigation</td>
<td>AIS</td>
<td>25 kHz</td>
</tr>
<tr>
<td>162.025 - 162.025</td>
<td>Maritime Radionavigation</td>
<td>AIS</td>
<td>25 kHz</td>
</tr>
<tr>
<td>162.650 - 169.400</td>
<td>Land Mobile</td>
<td>PMR</td>
<td>12.5 kHz</td>
</tr>
<tr>
<td>169.175 - 169.175</td>
<td>Land Mobile</td>
<td>On-site paging</td>
<td>25 kHz</td>
</tr>
<tr>
<td>169.400 - 169.475</td>
<td>Land Mobile</td>
<td></td>
<td>50 kHz</td>
</tr>
<tr>
<td>169.4125 - 169.4625</td>
<td>Aids for hearing impaired</td>
<td></td>
<td>50 kHz</td>
</tr>
<tr>
<td>169.475 - 169.4875</td>
<td>Social alarms</td>
<td></td>
<td>12.5 kHz</td>
</tr>
<tr>
<td>169.4875 - 169.5875</td>
<td>Aids for hearing impaired</td>
<td></td>
<td>50 kHz</td>
</tr>
<tr>
<td>169.5875 - 169.600</td>
<td>Social alarms</td>
<td></td>
<td>12.5 kHz</td>
</tr>
<tr>
<td>169.800 - 173.9875</td>
<td>Land Mobile Service</td>
<td>PMR</td>
<td>12.5 kHz</td>
</tr>
<tr>
<td>173.965 - 174.015</td>
<td>Aids for hearing impaired</td>
<td></td>
<td>50 kHz</td>
</tr>
</tbody>
</table>

<sup>11</sup> Private Mobile Radios such as TETRA or P25.
Annex B

Annex B. Channel and Frequency Arrangement for VHF MMS

This annex provides some of the regulatory data concerning the VHF maritime bands.
B.1 Radio Regulations Appendix 18

Table B.2 - RR - Appendix 18 - based on WRC-12 (Final Acts)
Annex C

Annex C. GNU Radio OFDM Implementation

This annex exposes the original GNU Radio OFDM implementation examples ofdm_tx.grc and ofdm_rx.grc.
Figure C.2 - GNU Radio ofdm_rx.grc flowgraph.
Figure C.3 - GNU Radio ofdm_rx.grc flowgraph.
References


European Telecommunications Standards Institute (ETSI), "Digital cellular telecommunications system (Phase 2+): Multiplexing and multiple access on the radio path (3GPP TS 45.002 version 11.3.0 Release 11)," ed, France, 2013.


