EFFICIENT SPECTRUM USE IN COGNITIVE RADIO NETWORKS USING DYNAMIC SPECTRUM MANAGEMENT

by

Tapiwa Moses Chiwewe

Submitted in partial fulfilment of the requirements for the degree
Philosophiae Doctor (Computer Engineering)

in the

Department of Electrical, Electronic and Computer Engineering
Faculty of Engineering, Built Environment and Information Technology

UNIVERSITY OF PRETORIA

November 2016

SUMMARY

EFFICIENT SPECTRUM USE IN COGNITIVE RADIO NETWORKS USING DYNAMIC SPECTRUM MANAGEMENT

by

Tapiwa Moses Chiwewe

Supervisors: Dr G.P. Hancke and Prof. G.P. Hancke

Department: Electrical, Electronic and Computer Engineering

University: University of Pretoria

Degree: Philosophiae Doctor (Computer Engineering)

Keywords: Dynamic spectrum access, cognitive radio networks, industrial wireless sensor networks, Internet of things, spectrum management, spectrum policy, spectrum sensing

Radiofrequency spectrum is a finite resource that consists of the frequencies in the range 3 kHz to 300 GHz. It is used for wireless communication and supports several applications and services. Whether it is at the personal, community or society level, and whether it is for applications in consumer electronics, building management, smart utility networks, intelligent driving systems, the Internet of Things, industrial automation and so on, the demand for wireless communication is increasing continuously. Together with this increase in demand, there is an increase in the quality of service requirements in terms of throughput, and the reliability and availability of wireless services. Industrial wireless sensor networks, for example, operate in environments that are usually harsh and time varying. The frequency spectrum that is utilised by industrial wireless protocols such as WirelessHART and ISA 100.11a, is also used by many other wireless technologies, and with wireless applications growing rapidly, it is possible that multiple heterogeneous wireless systems will need to operate in overlapping spatiotemporal regions in the future. Increased radiofrequency interference affects connectivity and reduces communication link quality. This affects reliability and latency negatively, both of which are core quality service requirements.

Getting multiple heterogeneous radio systems to co-exist harmoniously in shared spectrum is challenging. Traditionally, this has been achieved by granting network operators exclusive rights that allow them to access parts of the spectrum assigned to them and hence the problems of co-existence and limited spectrum could be ignored. Design time multi-access techniques have also been used. At present, however, it has become necessary to use spectrum more efficiently, to facilitate the further growth of wireless communication. This can be achieved in a number of ways. Firstly, the policy that governs the regulation of radiofrequency spectrum must be updated to accommodate flexible, dynamic spectrum access. Secondly, new techniques for multiple-access and spectrum sharing should be devised. A revolutionary new communication paradigm is required, and one such paradigm has recently emerged in the form of Cognitive Radio technology. Traditional methods to sharing spectrum assume that radios in a wireless network work together in an unchanging environment. Cognitive radios, on the other hand, can sense, learn and adapt. In cognitive radio networks, the interactions between users are taken into account, in order for adjustments to be made to suit the prevailing radio environment.

In this thesis, the problem of spectrum scarcity and coexistence is addressed using cognitive radio techniques, to ensure more efficient use of radio-frequency spectrum. An introduction to cognitive radio networks is given, covering cognitive radio fundamentals, spectrum sensing, dynamic spectrum management, game theoretic approaches to spectrum sharing and security in cognitive radio networks. A focus is placed on wireless industrial networks as a challenging test case for cognitive radio. A study on spectrum management policy is conducted, together with an investigation into the current state of radio-frequency spectrum utilisation, to uncover real and artificial cases of spectrum scarcity. A novel cognitive radio protocol is developed together with an open source test bed for it. Finally, a game theoretic dynamic spectrum access algorithm is developed that can provide scalable, fast convergence spectrum sharing in cognitive radio networks. This work is a humble contribution to the advancement of wireless communication.

This thesis is dedicated to my family, including those we've lost.

I dedicate it most especially to my parents.

ACKNOWLEDGEMENTS

I would like to express my deep and sincere gratitude to my supervisor Dr Gerhard P. Hancke who has patiently seen me through my PhD. He has provided me with advice, guidance and a helping hand, all of which have been invaluable.

To Prof. Gerhard P. Hancke who has been a key part of my academic journey, I thank you for your support and the positive role you have played in the lives of many students and the contribution you have made and continue to make as an academic.

To my many advisors and people that have provided me with support that I value greatly including Ms Rochelle Blauw, Ms Mari Ferreira, Ms Heleen Gous, Mr Riaan Coetzee, Mr Peter Bosscha, Mr Paul Olckers, Mr Jacques VanWyk and Dr Solomon Assefa, thank you all very much.

To my friends and colleagues whose camaraderie and words of encouragement have inspired me including Ayanda Tyatyantsi, Bruno Silva, Dithoto Modungwa, Fungai Mandikuwaza, Kibii Komen, Rogerio dos Santos, Tafadzwa Mukwende, Thegaran Naidoo and Zandile Nxumalo, thank you all.

I thank my parents, my sisters and my family at large, whom I love, for their love and support and the positive influence they have on my life, and for helping me to become the man that I am.

I thank God, the Alpha and the Omega, who showers me with grace. My Christian faith has sustained me and provided me with fortitude to keep going through thick and thin; it is an essential part of my life.

LIST OF ABBREVIATIONS

ADC	Analogue-to-Digital Conversion
AP	Access point
ARQ	Automatic repeat request
BS	Base station
CCC	Common control channel
CCI	Co-channel interference
CDMA	Code division multiple access
CR	Cognitive radio
CRN	Cognitive radio network
CSMA	Carrier sense multiple access
CSMA/CA	CSMA with collision avoidance
CSMA/CD	CSMA with collision detection
CSS	Cooperative spectrum Sensing
CTS	Clear-to-send
DAB	Direct access based
DAC	Digital-to-Analog Conversion
DECT	Digital Enhanced Cordless Telecommunication
DFS	Dynamic frequency selection
DN	Decision node
DoS	Denial of service
DSA	Dynamic spectrum Access
DSSS	Direct sequence spread spectrum
ECC	Electronic Communications Committee
EM	Electromagnetic
FC	Fusion center
FCC	Federal Communications Commission
FDD	Frequency division duplex

FDMA	Frequency division multiple access
FHSS	Frequency hopping spread spectrum
GMSK	Gaussian Mean Shift Keying
IA	Information assurance
ICASA	Independent Communications Authority of South Africa
IoT	Internet-of-Things
IPv6	Internet Protocol Version 6
ISM	Industrial, scientific and medical
ITS	Intelligent transport systems
ITU	International Telecommunication Union
ITU RR	ITU radio regulations
IWLAN	Industrial WLAN
IWSN	Industrial wireless sensor network
M2M	Machine-to-machine
MAC	Medium access control
MIMO	Multiple-input multiple-output
MTU	Minimum transmission unit
NE	Nash Equilibrium
NTIA	National Telecommunications and Information Administration
OfCom	Office of Communication
OFDM	Orthogonal frequency-division multiplexing
OFDMA	Orthogonal frequency-division multiple access
O-QPSK	Offset Quadrature Phase Shift Keying
OSA	Opportunistic spectrum access
PCEN	Portable cognitive emergency wireless network
PER	Packet error rate
PoA	Price of anarchy
PSD	Power spectral density

PU	Primary user
PUEA	Primary user emulation attack
QoC	Quality of co-existence
QoS	Quality of service
RF	Radio frequency
RFI	Radio frequency interference
RTS	Ready-to-send
SABRE	South African Band Re-planning Exercises
SATRA	South African Telecommunications Regulatory Authority
SDMA	Spatial division multiple access
SINR	Signal-to-interference-plus-noise Ratio
SKA	Square Kilometre Array
SNR	Signal-to-noise ratio
SoC	System on chip
SR	Software radio
SDR	Software defined radio
SSDF	Spectrum sensing data falsification
SU	Secondary user
SUN	Smart utility network
TCP	Transmission Control Protocol
TDMA	Time division multiple access
TPC	Transmit power control
TVWS	Television White Spaces
UHF	Ultra high frequency
UMTS	Universal Mobile Telecommunication System
U-NII	Unlicensed national information infrastructure
USRP	Universal Software Radio Peripheral
UWB	Ultra wide band

VHF	Very high frequency
WAVE	Wireless access in vehicular environments
WBAN	Wireless body area network
WISA	Wireless Interface for Sensors and Actuators
WLAN	Wireless local area network
WPAN	Wireless personal area network
WRAN	Wireless regional area network
WRC	World radio-communication conference

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 PROBLEM STATEMENT

1.1.1 Context of the problem

At an Apple worldwide developers conference, held in San Francisco in June 2010, the iPhone 4 was being revealed by Steve Jobs. But as he proceeded with the demonstration, disaster struck: he was unable to connect to the Wi-Fi network at the conference center and the demo crashed [1]. The cause of the problem was the 570 Wi-Fi base stations operating in the room, which overloaded the network. In order for him to obtain network access and continue with the demonstration, the airwaves had to be freed up by turning some of the Wi-Fi devices off. An obvious question to ask is if there are other ways to solve such a problem, and, if so, which is the most effective. Answers to these questions can be found in the area of dynamic spectrum management in cognitive radio networks.

Wireless networks today are regulated by a rigid policy for radio frequency spectrum assignment, as government agencies control spectrum utilisation and allocate sections of the spectrum for extended periods of time and over large geographic areas to license holders or service providers. Large portions of the assigned spectrum undergo sporadic use and most spectrum utilisation occurs in certain portions of the frequency spectrum, while a significant portion is under-utilised. Spatio-temporal changes in the use of an allocated spectrum vary from 15% to 85% [2]. In recent years, there has been an upsurge in access to the finite spectrum for mobile services, which has strained traditional spectrum policies. Inefficiencies in the use of spectrum and limited spectrum have necessitated the adoption of a new way of thinking about wireless communication that exploits wireless spectrum in an opportunistic way. This communication system aims to provide communication wherever and whenever required, in a reliable manner and with more efficient use of the radio frequency spectrum [3].

The 1980s saw the development of radio receivers that were reconfigurable for the purpose of radio intelligence in the short-wave range of frequencies. Among the features of these

receivers was bit stream analysis, which involved automatic identification of the modulation scheme of a received signal [4]. With the publication of the IEEE Communications Magazine in April 1995, many radio developers became familiar with reconfigurability. One way to achieve reconfigurability is through the use of a software radio (SR). An SR is a transceiver with communication functions that are realised as programs running on a suitable processor. It comprises all the layers of a communication system, from the physical layer, to the application layer.

A software defined radio (SDR) is a practical implementation of a SR, in which received signals are sampled after a suitable band selection filter, instead of directly sampling antenna output. If an SDR can, in addition, sense its environment, track changes and react upon its findings, then it is referred to as a cognitive radio (CR). CR networks provide mobile users with high bandwidth through a mixed network architecture and techniques for dynamic spectrum access.

Techniques for dynamic spectrum access enable the best possible channel to be used by the CR. In particular, cognitive radio users will be able to: (1) ascertain the sections of the spectrum that are available and recognise the presence of licensed users whilst operating in a licensed band (*spectrum sensing*); (2) choose the best channel that is available for use (*spectrum management*); (3) collaborate with other users to harmoniously access the channel *(spectrum sharing);* (4) leave the channel on detection of a licensed user *(spectrum mobility)* [2].

1.1.2 Research gap

A large portion of the wireless spectrum assigned to license holders remains under-utilised. The non-efficient utilisation of the finite radio frequency spectrum calls for the development of techniques for dynamic spectrum access, in which users that do not have licenses to use the spectrum are allowed to use licensed spectrum temporarily. This would allow for more comprehensive and flexible use of the available spectrum.

Traditional schemes to allocating spectrum may no longer be applicable as a result of the more flexible and efficient use of spectrum in cognitive radio networks, and more so when licensed users co-exist with unlicensed users. New approaches are required to solve new challenges related to cognitive radio, particularly in spectrum management and dynamic spectrum sharing.

1.2 RESEARCH OBJECTIVE AND QUESTIONS

The research question is, "Is it possible to utilise the limited radio spectrum more efficiently using dynamic spectrum sharing techniques in a way that scales well, is computationally simple, conserves bandwidth and is cost effective?"

The objective of this research is to design a dynamic spectrum management mechanism that will provide:

- highly reliable communication whenever and wherever it is needed
- efficient utilization of the radio frequency spectrum.

In order to answer the over-arching research question, certain supplementary questions had to be answered, i.e.:

- What are the current spectrum access challenges?
- What is the current state of cognitive radio networks?
- What efforts have been made to create standards for cognitive radio protocols?
- What are the current policies that regulate spectrum access?
- How congested is the radio frequency spectrum?
- Which environments are more negatively affected by spectrum congestion?
- What options are there to achieving multiple access to shared spectrum?
- What platforms can be used to perform experimental studies on dynamic spectrum access?
- What dynamic spectrum access methods will yield benefits over the traditional spectrum access methods?

1.3 APPROACH

The research methodology was to carry out the following.

1. A literature study:
    a. Relevant literature on cognitive radio networks was identified.
    b. Relevant literature on dynamic spectrum management in cognitive radio networks was identified.
    c. The identified literature was studied.
    d. Various approaches to dynamic spectrum management were identified.
    e. The different approaches to dynamic spectrum management were investigated and compared.
2. Design of a dynamic spectrum management mechanism:
    a. A novel cognitive radio protocol was designed.
    b. A spectrum access model was created.
    c. A novel dynamic spectrum sharing algorithm that seeks to maximise spectral efficiency and communication reliability was designed.
3. Implementation:
    a. The cognitive radio protocol was implemented using a software radio framework.
    b. Different networks that use the designed dynamic spectrum sharing algorithm were simulated to evaluate how the new algorithm performs.
    c. Data was identified and collected that could give statistically significant results and could be used for evaluation and comparison to results from past studies.
4. Assessment:
    a. The real world performance of the developed cognitive radio protocol was profiled.
    b. The new dynamic spectrum sharing algorithm was benchmarked against a previously developed algorithm including variations of the algorithms that use different decision rules.
    c. The results were analysed and discussed.

1.4 RESEARCH GOALS

The goals of this research were as follows:

- To investigate approaches to dynamic spectrum management and the policies used to manage radio frequency spectrum.
- To develop a novel cognitive radio protocol that can be used to achieve efficient spectrum use and mitigate against interference in harsh or congested radio environments.
- To implement and demonstrate the performance of the novel cognitive radio protocol.
- To develop an algorithm for dynamic spectrum sharing that can alleviate spectrum access challenges and benchmark its performance.

1.5 RESEARCH CONTRIBUTION

There are a number of contributions that have arisen out of this research study that are summarised below:

- The development of the first and only spectrum allocation chart that shows how the entire radiofrequency spectrum is allocated to different applications and services in South Africa [5].
- A magazine article on spectrum management policy in South Africa and the rest of the world that highlights the problems of real and artificial spectrum scarcity, and contrasts traditional fixed spectrum assignment schemes with new and emerging dynamic spectrum access schemes [5].
- A journal article on the use of cognitive radio networks in industrial wireless networks that are usually harsh, have stringent quality of service requirements, and involve co-existence of different radio technologies [6].
- A conference paper on the design and development of a novel Cognitive radio protocol that enables opportunistic multi-band operation between UHF television bands and the shared Industrial, Scientific and Medical band [7].
- A journal article on a new game theoretic algorithm for multi-channel dynamic spectrum sensing and access that builds on a previously developed algorithm through performance improvements for faster convergence and greater scalability.

1.6 OVERVIEW OF STUDY

This study will give a detailed account of cognitive radio networks and dynamic spectrum management; it covers topics such as spectrum sensing, spectrum management, spectrum sharing and spectrum mobility. An analysis of policy issues governing the management of radio frequency spectrum will be presented. Work that was done to develop the first radio frequency spectrum allocation chart for the Republic of South Africa will be presented, as well as the chart itself. Details on the design and implementation of a novel dynamic spectrum access algorithm and the accompanying cognitive radio protocol that was implemented using software radio will be provided and the performance will be characterised. Finally, a reflection and assessment of the work done will be presented.

CHAPTER 2 LITERATURE STUDY

2.1 CHAPTER OBJECTIVES

The objectives of this chapter are to detail the literature relevant to the research topic of efficient spectrum use in cognitive radio networks, present the current situation in the field of cognitive radio networks and give a critical analysis of the different techniques that are used in this field. Special focus is placed on industrial wireless networks that have to contend with environments that are usually harsh and time varying, which sets them apart from other types of wireless networks, such as wireless home and office networks.

2.2 INTRODUCTION

Wireless technologies have been considered an appealing alternative for distributed control systems, automotive systems, industrial and factory automation, and other interconnected embedded systems [8], [9], [10]. They offer several advantages over traditional wired communication systems, such as enhanced physical mobility, fewer infrastructure requirements, less risk of cable damage, reduced connector trouble and simplicity with upgrading [11], [12]. Industrial and factory environments pose significant challenges for wireless communications. Industrial applications set high requirements for reliability, while these applications also operate in environments that are arguably more prone to interference [8], [13]. Coexistence is also an increasingly important aspect when implementing industrial wireless sensor networks (IWSNs). With industrial applications no longer confined to controlled factory environments, and now extending to applications such as building automation, smart grids and consumer utility use monitoring and control, these networks must be tolerant of and able to co-exist with other industrial and consumer wireless systems. Any candidate radio system must maintain the required quality-of-service (QoS) in a co-existing environment and favourable transmission quality when functioning as a stand-alone system [14]. As the use of wireless networks continues to increase with growing consumer interests and with initiatives like the Internet-of-Things, radio spectrum is becoming a scarce commodity and practitioners will need to consider new approaches to co-existence and the utilisation of temporarily free bands.

The regulation of radio spectrum today is based on a fixed spectrum assignment policy, where government agencies regulate spectrum usage and assign portions of the spectrum over extended periods of time and large geographic areas to license holders or services such as mobile cellular communication or terrestrial television. Large portions of the allocated spectrum are utilised intermittently and the spectrum is congested at particular regions of the spectrum space, while a considerable part of it is left under-utilised. Use of assigned spectrum in time and space varies from 15% to 85% [2]. The inefficient use and scarcity of spectrum has demanded a new paradigm in wireless communication, to ensure that the available wireless spectrum is exploited opportunistically. In such a paradigm, reliable communication is provided wherever and whenever needed, and radio spectrum is used more efficiently [3].

Cognitive radio technology is a communication paradigm that has emerged in recent years that can mitigate interference and enhance reliability in a heavily congested wireless industrial network. A formal definition of a cognitive radio is: *"Cognitive radio: A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets."* [15]. Long-established methods of sharing spectrum assume that network nodes collaborate categorically in an unchanging environment [16]. However, with cognitive radio networks (CRNs), interactions with other users and the dynamic environment must be taken into account, in order to adapt the operational configuration.

CRs are not limited to a set of channels as in frequency-agile approaches; they are more general and can operate in different frequency bands. Through an intelligent decision making process, which considers sensed spectrum variations and the actions of other users in the network, the tight requirements for reliable and real-time communication in industrial networks can be met. This would help to avoid loss of time and money or physical damage. There are several existing approaches to avoiding interference in these networks, with some following an approach similar to CR with support for spectrum sensing and dynamic frequency selection. CR still offers the opportunity to ensure media

access in heavily congested areas, as well as to extend the lower layers of existing IWSN protocol stacks to find additional bandwidth for additional channels or high-bandwidth communication [6].

In this chapter, a discussion of the benefits and challenges of using CR in industrial environments is initiated, with the focus being on different interference sources, co-existence and existing multi-access techniques. Next, an overview of spectrum sensing techniques is given. This is followed by a presentation of dynamic spectrum management and a discussion on the use of game theory in terms of sharing spectrum. Finally, security issues in CRNs, as an aspect that directly affects the reliability of IWSNs is covered.

2.3 WIRELESS INDUSTRIAL NETWORKS

2.3.1 Interference in wireless industrial networks

Industrial environments often have a higher QoS requirement than that typically found in homes and offices. More communication devices are involved and the number is more variable. It is necessary to meet specific safety and security requirements, and performance must be deterministic with certain degradation. Coupled with the harsh environment, this means that spectrum resources vary over time and space. This situation may be exacerbated by device mobility and traffic fluctuations.

Multipath fading, radio interference and noise are the root causes of problems affecting the reliability of data and effective operating range in wireless communication systems. The interference affects the successful delivery of packets and the controller then has to operate with an incoherent view of a physical process [17]. Interference due to multipath fading occurs when several versions of a transmitted signal arrive at a receiver due to reflection off obstacles such as factory floors and walls. This causes a phase variance between different copies of the signal, resulting in destructive interference, and ultimately reduced signal strength, lower network throughput and reduced communication range.

When different radio signals exist in the same place, at the same time, and in a common frequency range, then radio frequency interference (RFI) occurs. This is particularly a problem when using devices that operate in the industrial, scientific and medical (ISM) band and the unlicensed national information infrastructure (U-NII) band, which are both unlicensed and used for different networks, including wireless personal area networks (WPANs) and wireless local area networks (WLANs). This situation can be exacerbated by poor frequency planning and a crowded frequency spectrum. WirelessHART, ISA 100.11a, WISA (Wireless Interface for Sensors and Actuators), ZigBee, Wi-Fi and Bluetooth devices operate in the 2.4 GHz ISM band, as do other devices such as welding equipment, radio frequency lighting, microwave ovens and cordless phones. Industrial WLAN (IWLAN) expands the function of IEEE 802.11 based consumer Wi-Fi to achieve performance improvements such as greater reliability, enhanced roaming, a greater communication range and deterministic operation. Table 2.1 gives a comparison of different industrial wireless platforms that need to co-exist [18], [19] and [20].

Table 2.1 Wireless Industrial Standards.

	IWLAN	**ZigBee**	**WirelessHART**	**ISA 100.11a**	**WISA**
Bandwidth	22 MHz	2 MHz	2 MHz	2 MHz	1 MHz
Channels, Selection	14, static	16, static	15, dynamic	15, dynamic	77, dynamic
Data Rate	11-54 Mbps	250 kbps	250 kbps	250 kbps	1 Mbps
Frequency Band(s)	2.4 GHz, 5 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz
MAC Layer	IEEE 802.11	IEEE 802.15.4	Proprietary	Proprietary	Proprietary
Radio	IEEE 802.11b/g/a	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.1
Topology	Star	Star, Full-Mesh	Full-Mesh	Star, Star-Mesh, Full Mesh	Cellular, Star

While one cause of RFI is co-channel interference (CCI), where two or more radio transmitters use the same frequency, another cause is electromagnetic radiation from other unforeseen sources. Whatever the cause, the operation of sensitive communication equipment is disturbed [21]. Interference signals can be classified as broadband or narrowband. Narrowband interference is predominantly caused by intentional transmissions, whereas broadband interference is usually caused by incidental radio frequency emitters [22]. Broadband sources have a relatively flat power spectral density across a wide range of frequencies, whereas narrowband signals are modelled as a continuous wave at a specific frequency. Broadband interference can come from arc/vapor lamps, computers, electrostatic discharge, electric switch contacts, ignition systems, inverters, motors, pulse generators, thermostats and voltage regulators. Narrowband interference can be caused by cellular telephones, electronic ballasts, local oscillators, microwave and ultrasonic equipment, pager transmitters, power-line hum, radio and television transmitters [23], and so on. Figure 2.1 indicates some of the interference sources found in industrial environments.

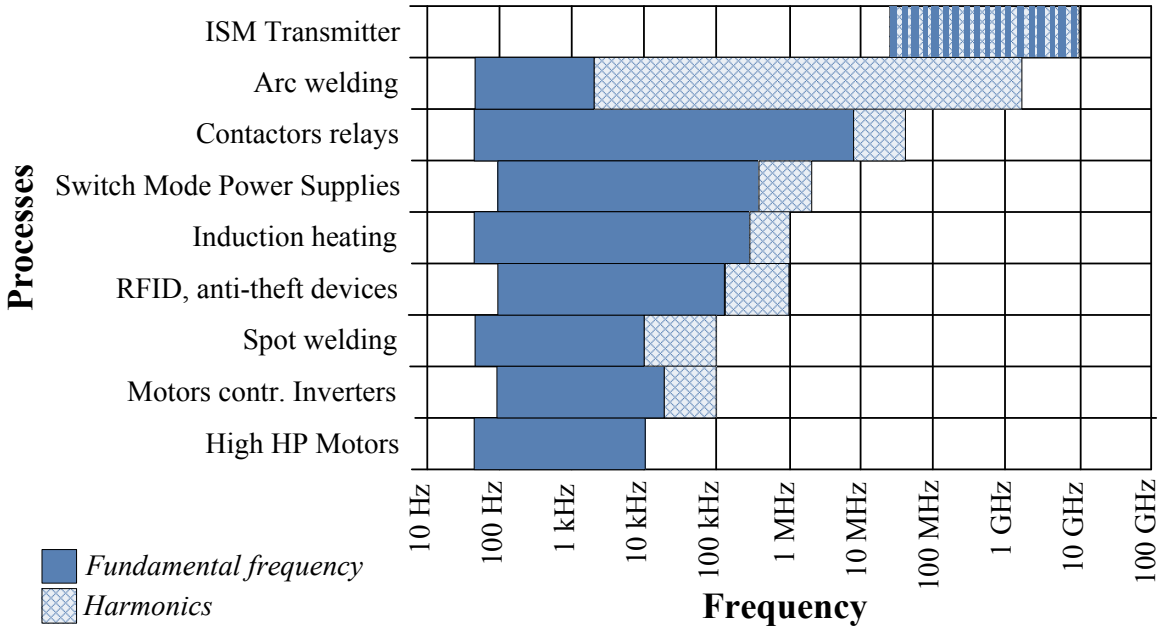


Figure 2.1. Frequency of different processes and devices in industry. Adapted from [24], with permission.

2.3.2 Interference management using traditional techniques

Most traditional schemes used to manage interference make use of multiple access techniques that are classified as being either deterministic or random. Multiple access techniques isolate stacks of radio resources allocated to multiple users within radio range of each other, such that each user communicates using an exclusive set of radio resources at any time. Other interference management techniques include spread spectrum, diversity, power control and MIMO.

2.3.2.1 Deterministic assignment multiple access

Deterministic multiple access schemes are contention-free and seek to avoid collisions, by allotting radio resources (including code, channel and time-slot) to several radios from a central entity [25]. It is possible to use contention free schemes in time, frequency, code and space division multiple access networks.

- In *time division multiple access* (TDMA), access to a frequency band is scheduled in time. When the time comes for a user to send or receive data, all other users are kept inactive during the allotted timeslot. With TDMA, it is necessary for all nodes to be synchronised to avoid interference [26].
- Another multiple-access scheme for wireless systems is *frequency division multiple access* (FDMA). With this technique, a frequency band is split into several channels and each channel is allocated to a single user. Any communication signals sent or received by the user do not cause interference to other users' transmissions. Orthogonal frequency-division multiple access (OFDMA) is a multi-user adaptation of the widely used orthogonal frequency-division multiplexing (OFDM) digital modulation scheme. OFDMA achieves multiple access by dynamically assigning a sub-set of sub-carriers to single users.
- A more advanced digital technique is *code division multiple access* (CDMA). This is a common part of third and fourth generation wireless communication systems. CDMA enables several users to be multiplexed over a common physical channel, by using a unique coding scheme in which each transmitter is assigned a code and spread-spectrum technology [27], [28].

- *Spatial division multiple access* (SDMA) makes use of information gathered in the spatial dimension and the temporal dimension to attain meaningful advancement transmitting wireless information. Significant increases in capacity, coverage and quality of wireless systems are attainable through spatially selective transmission and reception of RF energy. Spatial multiplexing and diversity is achieved by using technologies such as antenna arrays and multi-dimensional non-linear signal processing.

2.3.2.2 Random multiple access

In contention-based random channel access schemes, nodes contest one another to send data using the shared wireless channel. If no collision arises, a sent packet is then received successfully. A collision occurs when several nodes send data at the same time and the signal-to-interference-plus-noise ratio (SINR) at the receiver is then below the SINR floor necessary to decode the sent packet without error. In the event of a collision, it is possible for a node to try to resend the packet. The particular method chosen to retransmit the packet is decided by the protocol in use. Some popular contention-based channel access schemes are [29]:

- ALOHA: In this scheme, nodes transmit packets immediately when they have a packet to send. In the event of a collision, the packet is retransmitted later. ALOHA functions by dividing time into slots, and packets are aligned to the time-slots being sent.
- Carrier sense multiple access (CSMA): This is a probabilistic channel access scheme in which a node senses the state of the channel prior to attempting transmission. The node initiates a transmission attempt if the channel is idle. Should a collision occur, the node waits for a packet transmission interval before transmitting the packet again. Two enhanced variations of CSMA are CSMA with collision detection (CSMA/CD) and CSMA with collision avoidance (CSMA/CA). CSMA/CD is not workable in wireless networks. In CSMA/CA, should the channel be sensed as being busy before transmission, transmission is delayed for a random amount of time, in order to decrease the probability of collision occurring.

2.3.2.3 Spread spectrum techniques

Two used spread spectrum techniques are *direct sequence spread spectrum* (DSSS) and *frequency hopping spread spectrum* (FHSS). DSSS can address a crowded spectrum, but is far from sufficient [30]. Should the power of the interfering signal fall within the jamming margin, then DSSS can remove all interference. FHSS provides a reduced likelihood of collision with other transmissions. DSSS is preferred for low to medium narrowband interference, whereas FHSS is preferred for heavy interference environments and applications with elevated bandwidth requirements involving a great deal of data. Similar to spread spectrum, *Ultra wide band* (UWB) communications transmit in such a way so as not to interfere with using traditional narrowband and carrier waves in the same frequency band.

2.3.2.4 Diversity schemes, power control and MIMO

Besides the techniques detailed above, different diversity schemes may also manage interference and consequently improve link quality and reliability, e.g. path diversity, channel diversity, temporal diversity and transmit power control (TPC). Likewise, multiple-input multiple-output (MIMO) approaches, where multiple antennas are used at the transmitter and receiver, may be adopted. For multi-user MIMO approaches, SDMA techniques can be employed.

2.3.2.5 Multiple access techniques with wireless industrial platforms

The multiple access techniques of typical wireless industrial platforms are constructed by combining the previously discussed techniques. Some of these are discussed below.

- WISA utilises TDMA and frequency division duplex (FDD), where the uplink channel used is different to the downlink channel. The TDMA scheme is managed by the base station of each cell. Additionally, a frequency-hopping scheme is used to further assist in avoiding interference.
- WirelessHART uses a TDMA scheme with time-slots of 10 ms. A time-slot can be allocated to an individual device or multiple devices where a CSMA/CA mechanism is used. Frequency hopping is also applied and the channel to be used is indicated by a network manager, which also allocates time-slots to devices.

- ISA 100.11a also uses a TDMA scheme where time-slots are configured according to a slotted channel-hopping pattern or a slow channel-hopping pattern. The network manager manages the TDMA scheme.
- ZigBee has two communication modes, namely beaconed and non-beaconed mode. In beaconed mode, a super-frame slotted structure (comprising two parts) is used. The first part of the frame is for general use, with CSMA/CA being used for access. The second part of the frame comprises slots dedicated to specific nodes in the network. In non-beaconed mode, an unslotted CSMA/CA based multiple access scheme is used.

2.4 COGNITIVE RADIO

In section 2.3.1 different sources of interference in wireless industrial networks were identified. As was highlighted, many industrial wireless platforms (such as IWLAN, WirelessHART, ISA 100.11a and WISA) operate in the unlicensed ISM bands. However, using unlicensed bands results in challenges such as mutual interference between dissimilar co-existing radio systems and spectrum scarcity. This interference can cause the SINR at receivers to fall below the required threshold required to communicate successfully. Traditional interference mitigation schemes highlighted in section 2.3.2 do not address these challenges of mutual interference and spectrum scarcity.

One solution is to use licensed spectrum regulated by bodies, such as the Federal Communications Commission (FCC), which is a long and costly process. Another option is to use the unlicensed 5 GHz band, which has the advantage of being less crowded, although it is susceptible to the same problems as the 2.4 GHz band [8].

Using CRs is another solution that does not suffer from the shortcomings indicated above. CRs have features such as spectrum sensing and reconfigurability that can adequately solve the challenges identified. The co-existence of co-located dissimilar wireless networks that must provide QoS guarantees can benefit from using CRs.

2.4.1 Cognitive radio fundamentals

CRs are borne out of a software radio, which is a transceiver that provides communication functions that are realised as programs running on a suitable processor. CRs comprise all the layers of a communication system, from the physical layer to the application layer [4]. A SDR is a practical implementation of a software radio in which received signals are sampled after a suitable band selection filter instead of directly sampling antenna output. In addition, if a SDR can sense its environment, track changes and react upon its findings, then it is referred to as a CR. CRNs can provide high bandwidth wireless communication to users through dynamic spectrum access (DSA) techniques and heterogeneous architecture approaches.

In CR terminology, *primary users* (PUs) - also known as *incumbent users* - are licensed users with legacy rights or a higher priority to utilise a particular part of the spectrum. *Secondary users* (SUs) - also referred to as *cognitive users* - are unlicensed users with a lower priority, who exploit the spectrum opportunistically such that PUs do not suffer harmful interference from them. As a result, SUs must possess CR capacity, such as dynamic spectrum access techniques, that will allow them to function in the most favourable channel. Only users with a tangible legal or regulatory right to the spectrum are considered PUs. With unlicensed bands there are no PUs, e.g. in ISM frequency bands, where most of the industrial wireless network technology operates. Despite the perceived importance of some applications, SUs compete equally for the same resource.

A CRN can be multi-band, multi-channel, multi-service and multi-standard [4]. CRs give SUs the ability to: (1) detect licensed PUs and evaluate which parts of the wireless spectrum are available for use (spectrum sensing); (2) select the best available spectrum channel (spectrum decision); (3) coordinate access to this channel with other SUs (spectrum sharing), and; (4) vacate the channel when a licensed user is detected (spectrum mobility) [31]. The dynamic spectrum access operation, where CRs use temporarily unused spectrum (also known as white space or a spectrum hole), is illustrated in Figure 2.2.

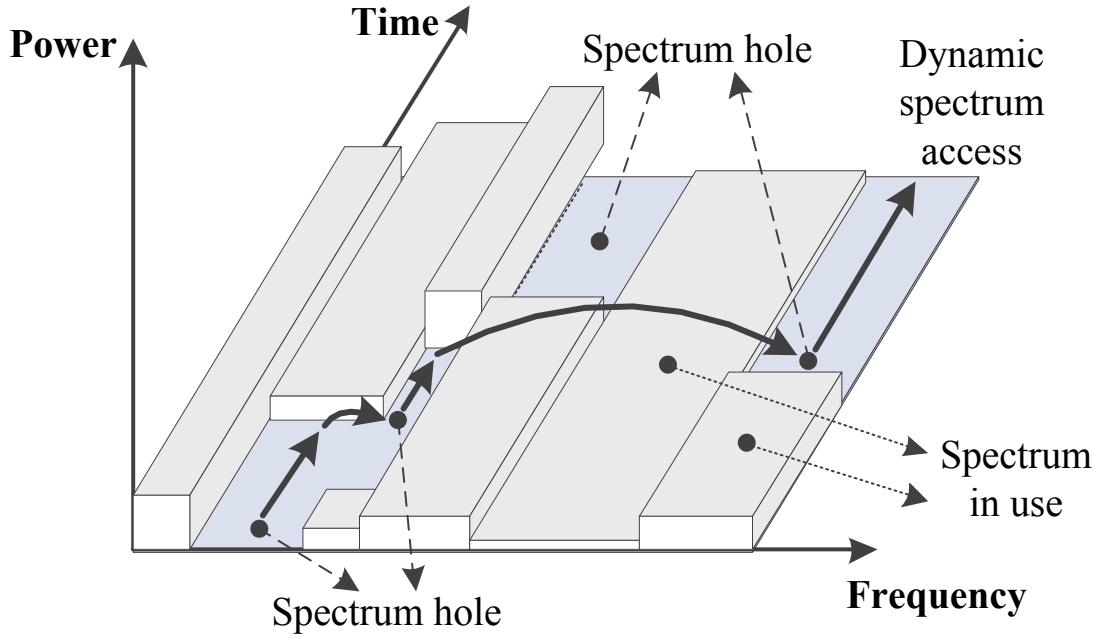


Figure 2.2. Spectrum hole concept. Adapted from [31], with permission.

The two main characteristics of a CR are its *cognitive capability* and *reconfigurability* [32].

- Cognitive capability: This enables the platform to determine the current occupancy of the spectrum. Information on spectrum utilisation should be available on an ongoing basis and updated on the platform's spectrum allocation module, in order for the transmission parameters to be set. Spectrum sensing approaches can be of two types: wideband and narrowband. The accuracy of spectrum access decisions, when using wideband sensing, is negatively affected by delays in getting spectrum utilisation information. Narrowband sensing, however, investigates a small portion of the spectrum and, as a result, spectrum access opportunities can be missed. Nonetheless, the fast response time of narrowband sensing can more accurately track the dynamic nature of spectrum utilisation.
- Reconfigurability: This enables the configuration of the transceiver's operating parameters to be changed in real time, without modifying the hardware components that affect radio transmission. Configured transceiver parameters include the operating frequency, modulation type, error control scheme and transmission power. Using

MIMO antennas can produce significant increases in spectral efficiently and give rise to a cognitive MIMO radio that offers ultimate flexibility with four degrees of freedom, i.e.: carrier frequency, channel bandwidth, transmit power and multiplexing gain [3].

To provide the above capabilities, a new structure for the radio frequency (RF) transceiver is required. The most important parts are shown in Figure 2.3. These include the baseband processing unit and the radio front-end, that were initially proposed for SDRs [2]. The RF front-end amplifies, mixes and performs analogue-to-digital conversion (A/D) of the received signal, while the baseband processing unit modulates and demodulates the signal. To accommodate the dynamic RF environment, a control bus can be used to re-configure each constituent part. A unique feature of the CR transceiver is that it has a wideband RF front-end that can sense simultaneously over a wide range of frequencies [33]. The RF hardware should be adjusted to operate anywhere in a large spectrum range; this is leveraged by hardware technologies that include an adaptive filter, a power amplifier and a wideband antenna.

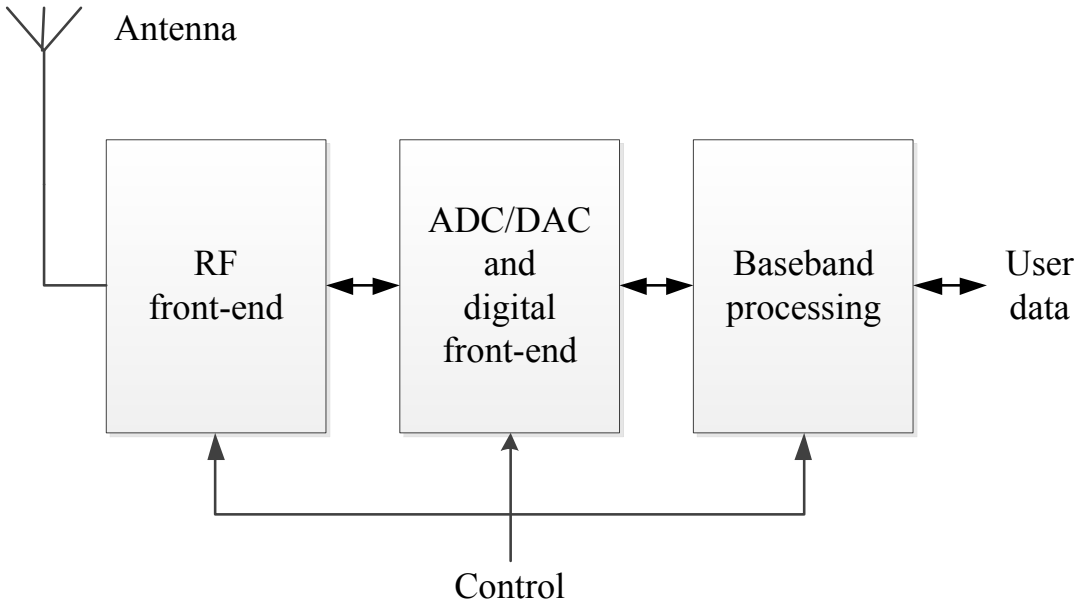


Figure 2.3. Cognitive radio transceiver architecture. Republished with permission of IEEE, from [2]; permission conveyed through Copyright Clearance Center, Inc.

There are several advantages of using CR solutions. CRs can prolong the useful service life of communication systems by allowing the possibility to change radio configurations on

CR equipment that has already been placed into service. CR applications that have already been invested in can be ported to new SDR platforms that are more capable. It becomes easier to keep up with the rapid evolution of communications standards [34], as base stations and other radios can have their software upgraded.

Some challenges exist, however, concerning the CR transceiver. Receiving transmissions from several radios that operate using different bandwidths, at different power levels and in different locations means that the CR transceiver needs to sense weak signals in a large dynamic range, which is a major design problem [2].

2.4.2 Interference management and QoS

With CRNs, interference can be avoided by taking advantage of the secondary system, i.e. a new system deployed within a service area of a *legacy* primary system, which can interpret signals sent in the primary system [35]. SUs are continuously exposed to signals from the PUs and techniques to avoid this interference should be employed. SUs can sense the channel just prior to transmission and periodically during transmission and so maintain awareness of spectrum opportunities. It is possible for a channel that has been identified by a SU as being available to suddenly become occupied by a PU during transmission, which can result in harmful collisions and interruptions. Predictive modelling can avoid such scenarios [36]. Through careful design of CRNs, significant gains in terms of interference are attainable [37].

Each industrial application has its own set of QoS requirements. Safety data has high fail-safety and reliability demands, while closed-loop controls and machine control have high response-time demands. Data transmitted for visualisation and recording purposes requires a high data rate. Wireless networks are prone to failure, but the reliability of IWSNs can be improved by using CRNs and taking advantage of their ability to provide efficient mechanisms for failure prevention and recovery and provide dependable communication and uniform QoS in varying circumstances. A study into dynamic spectrum sharing in the TV band demonstrated a system with low noise, high receiving sensitivity and anti-interference competence [38].

CRs have been used in Television White Spaces (TVWS) to solve the problem of interference between portable cognitive emergency wireless networks (PCENs) [39]. IEEE 802.22, a wireless regional area network (WRAN) based on CR has been analysed to determine its Transmission Control Protocol (TCP) performance, and cross-layer solutions were suggested to boost its throughput [40]. A new metric called quality of co-existence (QoC) [41] was proposed to indicate how well SU networks and mixed PU and SU networks co-exist. Interference in multi-hop CRNs can also be controlled using routing solutions [42] and topology control [43]. A cross-layer CRN framework was proposed for smart grids, which mitigates the adverse effect of noisy and congested spectrum bands [44]. In [45], a practical model for cumulative interference in CRNs was developed and then used to develop a power control scheme for low interference and good secondary network QoS. Throughput aware routing has been used to address the QoS requirements in CRNs [46]. Queuing theory can be used to analyse the impact of PUs' maximum tolerable delay on SUs performance [47]. An area that has yet to be explored is that of developing a low-power industrial sensor node in the CR paradigm, together with the controlling mechanisms for channel hand-off, in order to contend with RF interference in a dynamic wireless channel [11].

2.4.3 Benefits and limitations of cognitive radio approaches in industrial wireless sensor networks

Current IWSNs typically operate in the congested unlicensed ISM frequency bands. CR could allow these networks the flexibility to operate in licensed bands as SUs. For critical communication, some co-operation with PUs will be required to ensure availability of spectrum over extended periods. This co-operation entails negotiation and spectrum management and enforcement, and is best guaranteed with standardisation, which is a core requirement of IWSNs [19].

Current CR standardisation efforts are focused on exploiting TVWSs [48]. This is in response to new regulations by regulators worldwide, which allow the use of unused TV bands in the ultra high frequency (UHF) and very high frequency (VHF) bands. These

activities cover the IEEE 802.22 WRAN, the IEEE 802.11 WLAN and the IEEE 802.15 WPAN. IEEE 802.22 [49] is a CR standard for WRANs and is arguably not yet suitable for small IWSNs, such as building automation, although applications covering large geographic areas could be catered for by this standard, e.g. those involving smart utility networks (SUNs) and infrastructure monitoring. Standardisation efforts more attractive to industrial users are IEEE 802.11af [48] and IEEE 802.15.4m [50]. IEEE 802.11af can be of benefit to industry if, for instance, an IWLAN is adapted to support this standard. IEEE 802.15.4m seeks to enable IEEE 802.15.4 wireless networks to take advantage of TVWS spectrum and this can be of great advantage to industrial standards such as WirelessHART and ISA 100.11a. Once these standardisation activities are complete, it will be possible to estimate the implementation cost and complexity, and commercial devices will then become available. Ettus Research and National Instruments already offer Universal Software Radio Peripheral (USRP^{TM}) platforms that can be used for research, experimentation and prototyping of CRs.

Given ongoing regulatory and standardisation efforts to cater for legal licensed band operation of CRs, the more immediate impact of CRs might be to allow more efficient operation of IWSNs in congested unlicensed space. With the increased use of wireless consumer devices and the boundaries between consumer and industrial wireless networks becoming blurred, improved co-existence is required. This can be seen, for instance, when operating building automation networks in residential buildings and with the monitoring of critical infrastructure in cities. CR technology is designed for a competitive environment, and it is therefore well suited to providing co-existence and resistance to different RFIs. Inherently, networks using CR technology are resistant to interference, which results in fewer communication errors. There is a lower channel access delay and a decreased number of retransmissions, leading to less jitter and lower latency. There is no need to manually configure channel access for the network, as through self-organisation, network nodes decide which channels to use as their environment changes.

The exact requirements for industrial wireless communication vary across applications and from one engineer's opinion to another. These properties of CR appear to match up well

with the basic IWSN requirements, i.e.: redundancy, tolerance to interference [11], [12], [30], [18] timely transmission, reduced latency, reduced retransmissions, lower frame loss [12], [30], [18], and increased robustness in communication links due to changing environment, network topology or node location [11], [12], [30], [18].

CRs have higher complexity compared to traditional wireless systems and the benefits of adopting them must be weighed against economic and technical consequences. IWSNs often comprise resource-constrained devices [11], [12]. Reduced computational resources limit the choice of CR features that can be implemented; for example, wideband spectrum sensing may not be well suited to resource-limited devices. This does not mean that CRs are not feasible for IWSNs, as the remaining options can still work well. For example, narrowband sensing with cooperation among nodes can be used, instead of wideband sensing. Another alternative is to have an infrastructure-based network with a node hierarchy, so that devices with more resources at their disposal perform tasks that are more computationally intensive or that require special hardware capabilities. The results are then shared with less powerful devices in the network that can then, for example, change their operational characteristics based on this, such as PHY parameters. One area of interest is whether devices could do spectrum sensing and channel selection in a timely manner, so as to not introduce significant time delays when setting up new channels, which would negatively affect real-time communication.

CRNs are not at a stage where they offer a complete alternative to existing industrial wireless networking technology. Aspects of CR technology could be integrated into the lower layers of existing industrial wireless protocol stacks, in order to: provide improved resistance to interference; increase the number of channels; set up ad-hoc high-bandwidth channels, which provide for non-traditional industrial uses, such as multi-media applications that may involve video monitoring or transmitting visual data for cyber-physical systems [18]. Simple cognitive aspects, such as dynamic channel selection, carrier sensing and multiple access are already used by existing industrial protocols, so looking at the more advanced concepts in this area is the logical next step to improve these network stacks.

Advanced CR features allow for real-time adaptation of resource utilisation where the characteristics, needs and demands of different applications are automatically taken into consideration. This can include traffic patterns and bandwidth requirements. Unlike traditional wireless networks, such continuous adaptive behaviour is an advancement that could cater for a dynamic environment and circumstances. A CR could, for example, exploit the cyclic nature of most real-time traffic in industrial networks, so as to create adaptive medium access control (MAC) scheduling schemes that enhance the efficiency of spectrum occupation and network throughput.

2.5 SPECTRUM SENSING

CR introduces opportunistic use of spectrum white spaces not utilised by licensed users [51]. To do this, the ability of CRs to sense, measure, learn and be aware of channel features, spectrum availability, signal power, the working environment, user applications and their requirements, existing nodes and networks, local policies and other regulations on their operation, is used [52]. In CRNs, SUs need a cognitive capability such as reliable spectrum sensing, in order to evaluate if a channel is in use by an incumbent user, and to then change the radio parameters in order utilise an unused region of the spectrum. Spectrum sensing is therefore a critical component for establishing a CRN. Detection reliability can be improved by employing cooperative spectrum sensing (CSS). The various aspects of spectrum sensing are shown in Figure 2.4 [52].

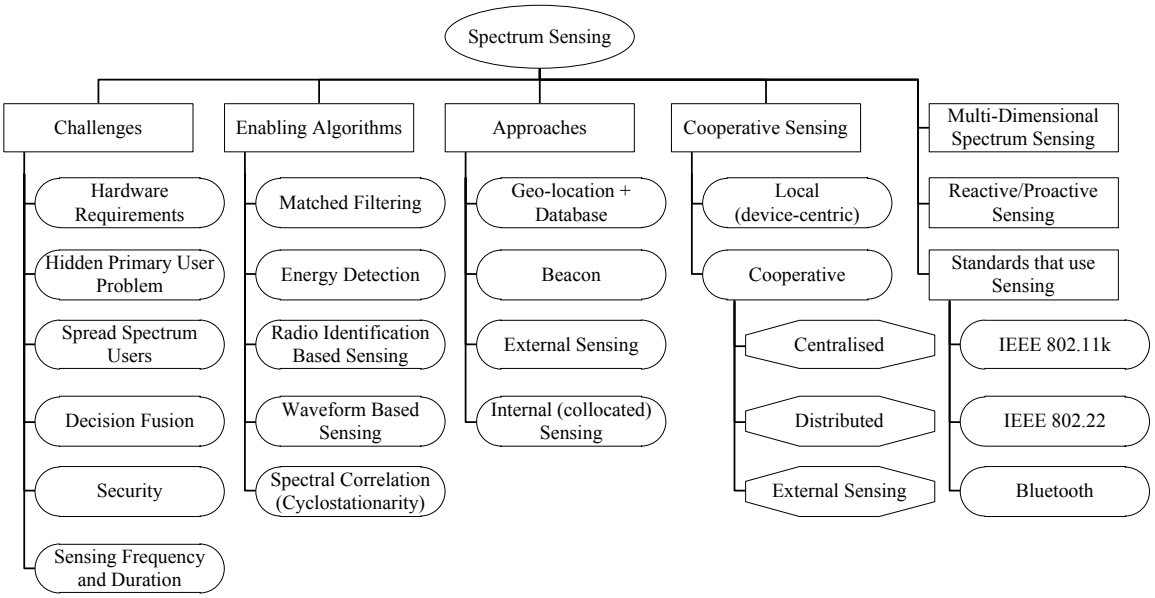


Figure 2.4. Different aspects of spectrum sensing for cognitive radio. Republished with permission of IEEE, from [52]; permission conveyed through Copyright Clearance Center, Inc.

2.5.1 Multiple hyperspace dimensions

The definition of a spectrum opportunity determines how spectrum space is measured and exploited. The conventional spectrum opportunity definition is "*a band of frequencies that are not being used by the primary user of that band at a particular time in a particular geographic area*" [53] and only the three dimensions of frequency, time and space are exploited. Traditional sensing methods consider these three dimensions, but other dimensions can be considered to discover spectrum opportunities. It is possible to tackle the co-existence problem using the concept of multi-dimensional electromagnetic (EM) space utilisation, where the dimensions of frequency, time, space, code, power and polarisation can distinguish different wireless signals [14]. Cognitive radio uses these dimensions as shown in Table 2.2.

Table 2.2 Main Dimensions of Hyperspace [14] used by Cognitive Radio.

Dimension	**Opportunity**
Frequency	Make use of frequency multiplexing.
Time	Make use of time multiplexing.
Space	Location dependent communication or exploiting spatial transmission features through techniques such as directional antennas.

Transmissions that use spread spectrum, frequency or time-hopping codes are unfamiliar to traditional spectrum sensing algorithms and pose a major problem for spectrum sensing. The dimensions introduced produce a radio space that can be defined as "*a theoretical hyperspace occupied by radio signals, which has dimensions of location, angle of arrival, frequency, time, and possibly others*" [54]. This hyperspace may be referred to as electrospace, radio spectrum space, transmission hyperspace or merely spectrum space, and it can illustrate how the radio environment can be shared among multiple (licensed and/or unlicensed) systems.

2.5.2 Spectrum sensing for cognitive radio

2.5.2.1 Energy detection

Energy detection is a semi-blind spectrum sensing method that estimates the energy of a received PU signal and compares it to a threshold value, in order to decide on the presence of a PU. The optimal threshold value depends on the estimated noise power. Also known as radiometry, it has low implementation and computational cost and does not require a priori information of the PU signal, unlike other detection methods. Its main drawback is its reliance on accurate noise estimation, which is typically very difficult to achieve, especially in environments with low signal-to-noise ratio (SNR) [55], [56]. It is also very difficult to detect PUs that use spread spectrum signals, using energy detection [57].

2.5.2.2 Feature based detection

Feature based detectors exploit known properties of a PU signal for detection. The exact implementation of a feature based detector depends on the property of the PU signal being exploited. In systems where the PU signal contains periodicity, usually because of signal modulation, detection can be performed using the cyclic auto-correlation function [58], [59]. This is due to the redundancy in signal periodicity, which results in modulated signals being cyclostationary with autocorrelation. Known as cyclostationary-based detection, this form of spectrum sensing usually only requires knowledge of one or two periodic features in the PU signal to achieve good detection results [60]. It has the added advantage of being able to distinguish PUs from each other, the background noise and other transmissions [61].

PU signal features can also be exploited to identify the communication technology employed by PUs in radio identification based sensing. Detectors extract signal features such as channel bandwidth and cycle frequencies, and use machine learning techniques to classify the technology being used [57], [62], [63].

2.5.2.3 Coherent detection

Coherent detection is used when PUs transmit signals with patterns known to the detector. These patterns are usually used by the PU for channel estimation and frequency synchronisation. Examples of such patterns include pilot signals, preambles, midambles and spread sequences. Detection could be performed by correlating the PU signal received with a known copy of the signal [55], [64]. The result of the correlation is then compared with a threshold value to determine the presence or absence of a PU. This form of detection, known as waveform or correlation-based detection is more reliable and has a shorter convergence time compared to energy detectors.

Alternatively, a matched filter could also be used for detection of PUs when the known patterns are transmitted. Matched filter detectors reach a probability of misdetection very quickly, but at the cost of large implementation complexity and power consumption [65],

[66]. Another drawback of matched filter detectors is that they require almost perfect knowledge of the characteristics of the PU signal to demodulate the received signals.

2.5.2.4 Other sensing methods

Multitaper spectrum estimation, random Hough transform and wavelet transform estimation [52] are other methods for sensing spectrum. Multitaper spectrum estimation has been demonstrated to approximate a maximum likelihood power spectral density (PSD) estimator and is nearly optimal for wideband signals in a proposed algorithm [3]. The algorithm is computationally intensive, but is less complex than the maximum likelihood estimator. The random Hough transform has been used to detect radar pulses in IEEE 802.11 communication system channels [67]. It is possible to use it to discover any signal that has a periodic pattern. Wavelets have been used to detect a wideband signal's PSD edges [68], which are found at the boundaries between occupied and empty bands. After finding the edges, the power within each frequency band is estimated. It is then possible to make a binary classification of the frequency spectrum bands as being empty or occupied. Multi-resolution spectrum sensing can be accomplished while leaving the sensing circuitry unaltered through altering the carrier frequency and pulse width of the wavelet basis functions [69].

2.5.3 Feasibility of sensing methods in industrial environments

The performance of an energy detector mostly depends on the accuracy of noise power estimation. It has been shown that a deviation of 1 dB in the estimation of noise variance results in energy detection performing worse than other feature based detection methods. The varying nature of background noise, due to factors such as temperature fluctuation [70] in an industrial environment, make it difficult to implement an accurate energy detector. The inability of energy detectors to detect spread spectrum signals means they would be unsuitable for industrial applications that use DSSS and FHSS [57].

Feature based detectors are more robust to changing background noise, while also providing higher detection accuracy than energy detectors. Waveform based detectors have better convergence time than energy detectors at low SNR, making them suitable for

industrial applications [55]. Waveform based detectors require PUs to transmit known pilot symbols or patterns [52] that may not be possible with some industrial applications. Cyclostationary based detectors are more complicated and have a higher observation time than waveform based detectors. Matched filter detectors are the optimal detectors, if perfect knowledge of the PU signal is available. The high cost in terms of implementation complexity and energy make this method unsuitable for most industrial applications [52].

With industrial applications that use spread spectrum techniques, spectrum sensing becomes difficult using the methods discussed. Some suggest that this problem could be mitigated if the detectors [52] are provided with information about the hopping patterns and signal synchronisation. This problem can also be avoided if new spectrum sensing methods are developed that exploit spectral opportunities in the code dimension. The different spectrum sensing algorithms are compared in Figure 2.5 according to complexity and accuracy.

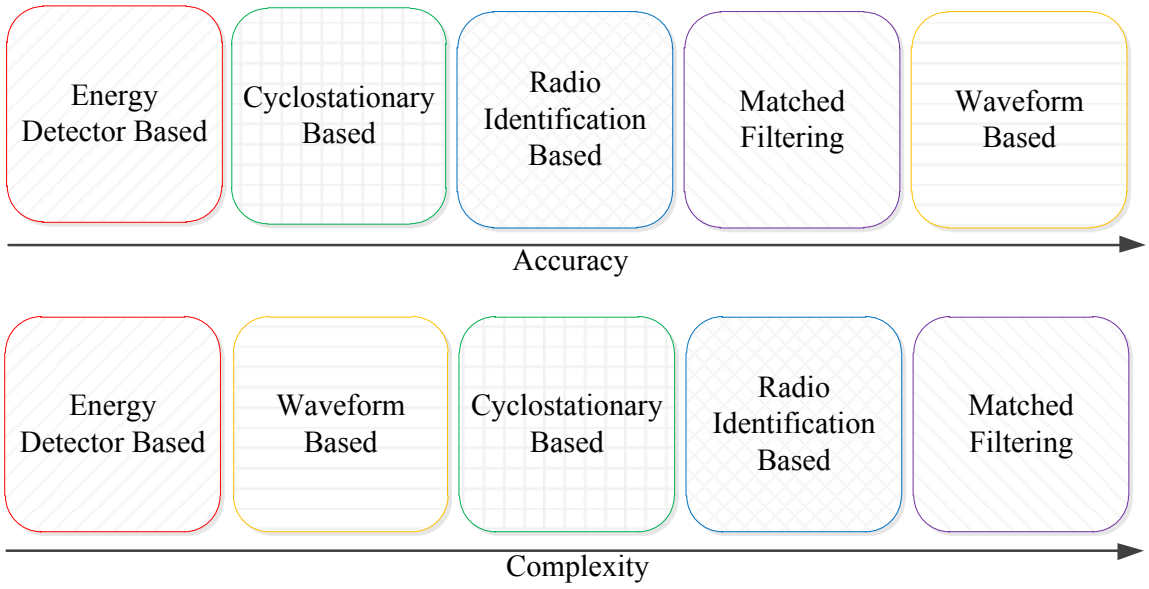


Figure 2.5. Main sensing methods ranked according to sensing accuracy and complexity. Republished with permission of IEEE, from [52]; permission conveyed through Copyright Clearance Center, Inc.

2.6 DYNAMIC SPECTRUM MANAGEMENT

Fluctuations in the spectrum available and the various requirements for QoS of different applications impose challenges in wireless networks, which can be addressed by dynamic spectrum management with CRs [2]. In spectrum management, the best available spectrum band to meet a user's communication requirements is selected, while not creating undue interference for other users.

Dynamic spectrum management stands in contrast to conventional co-existence management, which seeks to achieve co-existence through careful network planning, restrictions on the use of radio systems, and network organization by a human expert or a specialized tool. Procedures, guidelines and standards have been drafted for co-existence management such as is in the VDI/VDE 2185 guideline part 2 and the technical specification IEC/TS 62657-2. Such co-existence management can be complex and costly, but it has shown that co-existence in wireless automation systems is possible given the small data payloads and typical communication intervals. Dynamic spectrum management is self-organising and can achieve automated co-existence management, so as to maintain a high level of reliability with each process and high global system availability.

2.6.1 Spectrum decision

Deciding on the best spectrum band from among the available bands under the QoS requirements of the applications is referred to as spectrum decision [2], [71]. In the first step of spectrum decision, statistical PU information and local readings from CRs are used to characterise each band (spectrum characterisation). The next step is to select the most suitable spectrum band, based on the earlier characterisation (spectrum selection). Finally, there may be a need for a SU to reconfigure the communication protocol, hardware and the RF front-end under the QoS requirements and the prevailing radio environment. This is the reconfiguration step.

Some challenges in spectrum decision include supporting spectrum decision over heterogeneous spectrum bands, using a cooperative framework with reconfiguration, and

designing adaptive spectrum decision models that consider application needs and spectrum capacity [2].

2.6.1.1 Spectrum characterisation

The available spectrum holes show different time varying characteristics. They should be characterised in a way that considers temporal variations in the radio environment and factors such as signal bandwidth and frequency. Parameters that represent a particular spectrum band must therefore be defined as follows [31]:

- *Interference temperature:* The allowable power of a SU can be determined using the interference level at the receiver of a PU. This is then used to estimate the capacity of the channel.
- *Path loss:* This is tightly coupled to the frequency and range, as path loss increases with operating frequency, culminating in a loss in transmission range. Increasing transmission power can compensate for the loss in range, but other users may experience an increase in interference.
- *Wireless link errors:* The error rate of the channel changes according to the choice of modulation scheme and the in-band interference level.
- *Link layer delay:* Each spectrum band will require a different link layer protocol to address the differences in wireless link error, interference and path loss. The result will be different link layer delays.
- A metric that captures the statistical characteristics of licensed networks to depict the inherent fluctuations of secondary networks has been proposed. This metric is called the *primary user activity* [2]. Given that there is uncertainty regarding the availability of a spectrum band for the entire duration of a SUs communication, approximation of the PU activity is essential in spectrum decision.

2.6.1.2 Spectrum selection

Once the available spectrum bands are characterised, the most suitable band must be chosen. This choice is made using a spectrum selection rule based on QoS requirements, data rate, spectrum characteristics, delay bound, transmission mode and the acceptable error rate. SUs cannot gain exclusive access to a reliable wireless channel for extended

periods because of the operation of primary networks. In addition, CRs may not identify any individual spectrum band that meets user requirements. As a result, CRs can use transmissions using multi-radio in which each transceiver is tuned to different bands of non-continuous spectrum for various users, and transmit data concurrently, as shown in Figure 2.6.

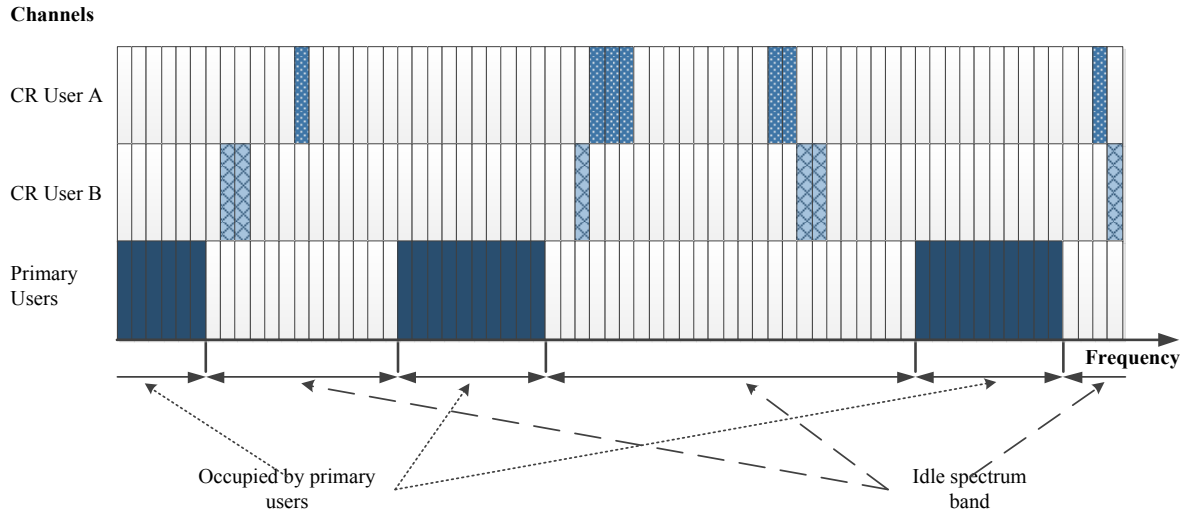


Figure 2.6. Channel structure of the multi-spectrum decision. Republished with permission of IEEE, from [2]; permission conveyed through Copyright Clearance Center, Inc.

Spectrum selection is influenced by the underlying CRN topology [71]. In centralised infrastructure-based CRNs with a point-to-multipoint topology, the spectrum selection is normally performed at the base station (BS) or access point (AP). In distributed multi-hop CRNs, spectrum selection can be done either: locally in a non-cooperative fashion that does not involve the exchange of information; or cooperatively where SUs exchange information, thus allowing the global channel state to be discovered quickly and accurately, albeit with greater communication overhead. Multiple hops and variable spectrum opportunities make up the communication session, hence there is a close link between the rule to select spectrum and routing protocols in distributed CRNs, and hence a dynamic decision framework is needed that can accommodate the changing channel conditions and user requirements for QoS.

2.6.1.3 Reconfiguration

Aside from the selection of routes and spectrum bands, another aspect of spectrum decision is reconfiguration in CRNs. Protocols for separate layers of the protocol stack need to accommodate the channel parameters of the spectrum in use. An example of this is in ad-hoc CRNs where, as a result of multi-hop communication, the spectrum decision function must look at the end-to-end route [31]. The available spectrum bands will differ from hop to hop, resulting in spectrum dependent connectivity, which makes it difficult to calculate the optimal pairing of spectrum bands and the routing path to be used. Selection of spectrum band and the routing path must therefore be done simultaneously.

The proper communication modules need to be selected once the spectrum has been decided; this includes the physical layer technology. Adaptive protocols have been developed that can ascertain the best combination of modulation, coding scheme and the transmission power for a new spectrum band, which is done by taking into account changes in signal attenuation [72].

2.6.2 Spectrum sharing

The wireless channel is a shared medium and, as a result, it is necessary to coordinate the transmission attempts between different SUs. In order for this to work effectively, several MAC protocol functions should be included in spectrum sharing. The co-existence of SUs and licensed PUs in CRNs, and the large number of spectrum opportunities, introduce some spectrum sharing challenges in CR networks. Theoretically, the amount of RF spectrum available covers the entire RF range (3 kHz to 300 GHz), although, in practice, it is more limited than this, due to propagation concerns and other technical constraints, including hardware limitations that make some portions more preferable. Sharing spectrum with licensed users is known as *vertical spectrum sharing* and this produces licensed band operation of the CRN. Sharing spectrum with unlicensed radio systems is known as *horizontal spectrum sharing* and gives rise to unlicensed band operation of the CRN. An example of a CRN network architecture is shown in Figure 2.7.

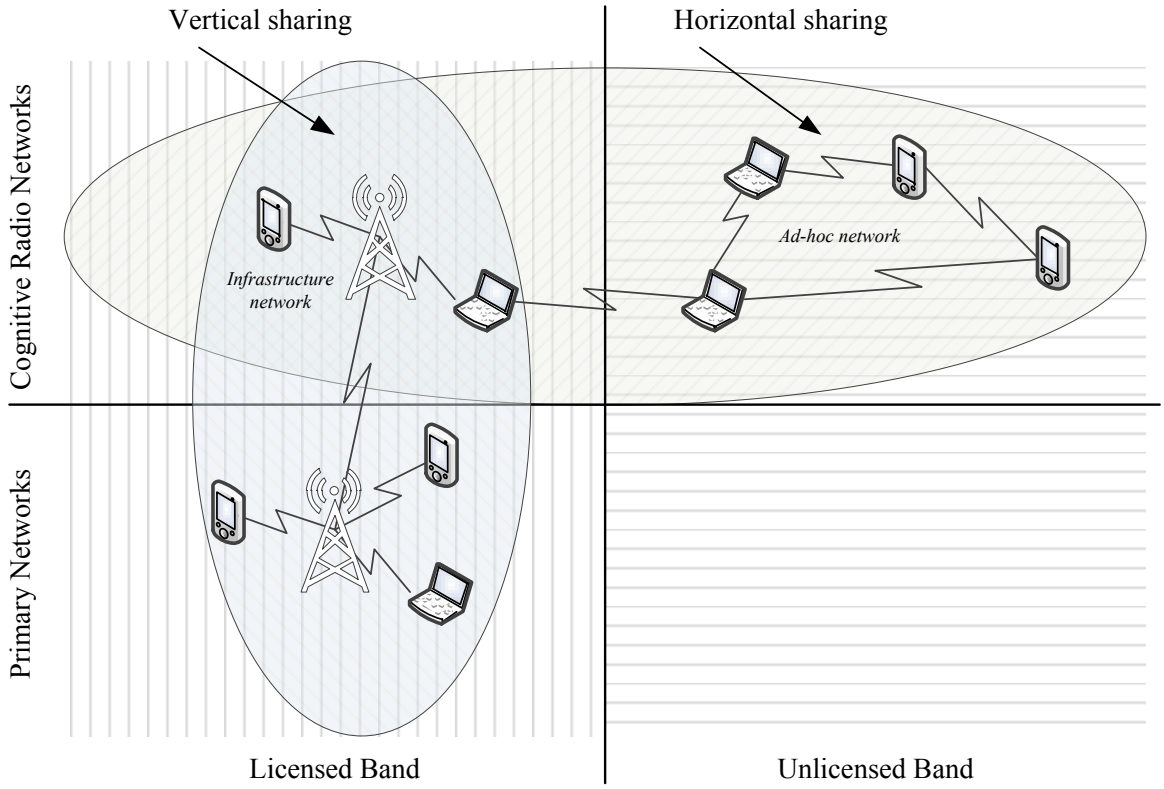


Figure 2.7. Example CRN architecture. Adapted from [31], with permission.

2.6.2.1 Classification of approaches

Four attributes can be used to classify approaches for solving spectrum sharing challenges, namely the *architecture, spectrum allocation behaviour, spectrum access technique* and *scope*. The architecture can be: *centralised*, where there is control by a central entity; or *distributed*, where individual nodes carry out local policies collaboratively to share spectrum. In terms of allocation behaviour, this can be *cooperative* or *non-cooperative*. Cooperative spectrum sharing exploits the interference measurements of all nodes in such a way that the effect of transmission by one node on other nodes is taken into consideration [73]. In non-cooperative sharing, solutions are determined using local information considering a single node only. Cooperative approaches perform better than non-cooperative ones, and provide a closer approximation of the global optimum.

The access technology used in spectrum sharing can be overlay spectrum sharing or underlay spectrum sharing [74]. In underlay spectrum sharing, the techniques used spread the transmitted signal over a large band of spectrum, so that PUs regard transmissions by CR nodes as noise, and simultaneous uncoordinated spectrum usage is achieved. These techniques include OFDM, UWB and spread spectrum. Transmission power can be strictly limited in underlay sharing to reduce potential interference. In overlay sharing there is opportunistic access to spectrum white spaces, while avoiding harmful interference to other radios using the same spectrum, whether or not the frequency is assigned to licensed users. This approach requires new protocols and algorithms. Dynamic frequency selection (DFS) is a simple example of overlay sharing. In terms of scope, spectrum sharing techniques can be inside a CR network (intra-network spectrum sharing) or between multiple co-existing CR networks (inter-network spectrum sharing), as shown in Figure 2.8.

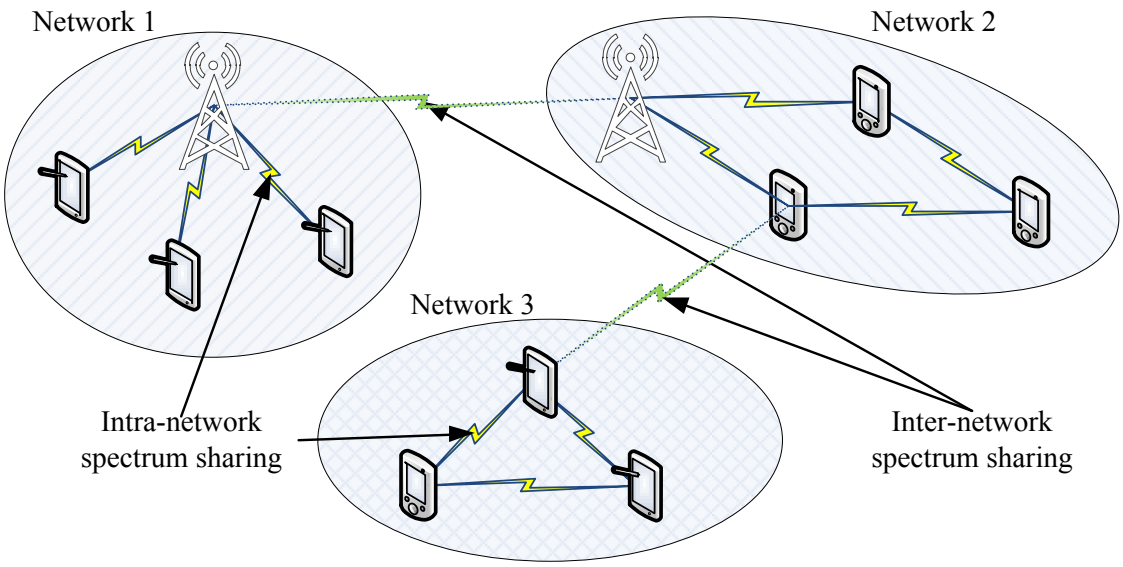


Figure 2.8. Inter-network and intra-network spectrum sharing in CRNs. Republished with permission of IEEE, from [2]; permission conveyed through Copyright Clearance Center, Inc.

2.6.2.2 Resource allocation

Resource allocation in spectrum sharing can be based on: *power control,* where SUs adjust their transmission power to attain resource equity and meet QoS requirements; or *channel allocation,* where SUs select the proper channels to use. Traditional approaches to spectrum sharing are based on fully cooperative, static, centralised models that are not applicable to dynamic environments and where SUs must adjust their operating parameters based on interaction with the environment and other users [16].

Spectrum sharing using power control in a multi-user CR environment involving competition and cooperation is a multi-user communication theoretic problem. A full appreciation of multi-user communication theory has yet to be established, although there are two diverse disciplines of information theory and game theory that can help solve this challenging problem. Iterative water filling is one particular information theory-based technique that can be used for power control [3].

Graph theory has been investigated for solving the channel allocation problem, where the problem is reduced to a variant of the graph colouring problem; however, the global optimisation problem has been shown to be NP-hard and is typically not practical. Some heuristic-based approaches have been suggested, which produce good solutions [59], [75], [76]. Game theory, local bargaining and rule-based techniques can also be used for channel allocation.

From the above, it can be seen that game theory can be used for both power control and channel allocation. In addition, it can provide an efficient distributed scheme for sharing spectrum that describes the conflict and cooperation between SUs. It allows interaction between SUs to be modelled and formulated and, as a result, enables each SU to reasonably determine its best course of action [31], [77]. Better flexibility of radio resource usage can be achieved to improve system performance, while complexity and signalling overhead is reduced. Game theory is therefore well suited to spectrum sharing and is described in more detail in section 2.7.

2.6.3 Spectrum mobility

Spectrum mobility occurs when a SU needs to change its operating spectrum band. This is largely due to PU activity on a spectrum that the CR would have previously selected as the best available spectrum. Adaptive protocols that adhere to channel conditions at the operating frequency are required for different layers of the network stack. These protocols must be resilient to spectrum hand-off and the delays that come with it. Spectrum mobility management in CRNs ensures seamless and speedy changeover, resulting in minimal performance loss when performing spectrum hand-off. Protocols for mobility management require details on the time taken for spectrum hand-off, which can be obtained from a sensing algorithm. After obtaining this information, ongoing communications can proceed with minimal loss in performance.

2.7 GAME THEORY FOR SPECTRUM SHARING

Game theory is a mathematical tool that analyses strategic interactions between multiple decision makers [16]. Using a game theoretic model to study CRNs has several advantages, the first of which is that it enables the action and behaviour of network users to be analysed using an established structure. Secondly, game theory provides measures to determine the most favourable solution to the problem of spectrum sharing. Game theory offers well-defined equilibrium criteria and can be used under diverse game conditions in order to measure the optimality of a game. This is useful, as spectrum sharing is a challenging multiple objective optimisation problem. Thirdly, distributed methods to share spectrum dynamically, using local information alone, can be developed when using non-cooperative game theory.

Four categories can be used to classify game theoretic spectrum sharing schemes, namely: (1) non-cooperative games and Nash equilibrium; (2) economic games, auction games and mechanism design; (3) cooperative games, and; (4) stochastic games.

A strategic form game theory model has three main components:

- a finite set of players, denoted by N;

- a set of actions, denoted by A_i for each player i; and
- a payoff/utility function, denoted by $u_i: A \rightarrow \mathbb{R}$ which measures the outcome of player i and which is determined by the actions of all players, $A = \times_{i \in N} A_i$.

2.7.1 Non-cooperative games and Nash equilibrium

Non-cooperative games are those in which interactive players make decisions independently. When each player plays its best strategy, while considering the action of other players, the equilibrium attained is known as Nash equilibrium (NE). NE does not provide details on how to arrive at the equilibrium, but gives information on the eventual equilibrium outcome. The equilibrium exists, but is not always unique and has to be determined for each case. When SUs do not have global knowledge, they can begin by using their discretion and use a rule-based update strategy giving a prediction that converges with the equilibrium. A shortcoming of NE is that in adversarial games involving selfish players, it is prone to over competition.

Formally, the NE of a strategic game $\langle N, (A_i), (u_i) \rangle$ is a profile $a^* \in A$ of actions, so that for every player $i \in N$

$$u_i(a_i^*, a_{-i}^*) \geq u_i(a_i, a_{-i}^*) \tag{2.1}$$

for all $a_i \in A_i$ where a_i denotes the strategy of player i and a_{-i} denotes the strategies of all players other than player i. The most beneficial strategy of response for each player is defined in NE as follows:

$$a_i^* \in B_i(a_{-i}^*) \text{ for all } i \in N. \tag{2.2}$$

The **best response function** of player i is known as the set valued function, formally

$$B_i(a_{-i}) = \{a_i \in A_i: u_i(a_{-i}, a_i) \geq u_i(a_{-i}, a_i')\} \text{for all } a_i' \in A_i. \tag{2.3}$$

It is possible for a game to have multiple equilibrium points, in which case it is desirable to evaluate the performance of each and find the optimal one, if it exists. However, defining optimality in such scenarios, which involve multi-objective optimisation, is not simple. A

popular way to do so is to use Pareto optimality, i.e. a payoff profile where no one strategy can improve a player's performance without degrading that of another.

Formally, let $U \in R^N$ be a set. Then $\mathbf{u} \in U$ is Pareto efficient if there is no $\mathbf{u}' \in U$ for which $u_i' > u_i$ for all $i \in N$; $\mathbf{u} \in U$ is **strongly Pareto efficient** if there is no $\mathbf{u}' \in U$ for which $u_i' \geq u_i$ for all $i \in N$ and $u_i' > u_i$ for some $i \in N$. The *Pareto frontier* is defined as the set of all $\mathbf{u} \in U$ that are Pareto efficient.

In [78] a non-cooperative spectrum, access game is considered where SUs access several spectrum holes in licensed bands simultaneously. The existence of a NE is demonstrated and settings for equilibrium spectrum access are derived. A comprehensive analysis of the competitive spectrum access game is presented under different system settings and it is shown that an increase in the number of SUs increases the price of anarchy (PoA). The PoA also increases as the number of wireless channels increase.

2.7.2 Economic games, auction games and mechanism design

How people interact with one another in markets can be dealt with by applying game theory to economics. Useful theoretical results and games of interest are produced covering auction theory and micro-economics. There are several reasons why economic games can be applied in CRNs. First, economic models are suitable in scenarios in which PUs can sell rights to unutilised spectrum in the secondary spectrum market. The exchange can be carried out through pricing, auctions or similar means. Second, economic games are not confined to scenarios with explicit buyers and sellers, but can extend to include spectrum sharing situations that do not involve secondary spectrum markets. Third, it is important to appreciate CRNs from an economic point of view and formulate efficient processes to control the spectrum market, as the success will depend greatly on the combination of policy, markets and technology.

2.7.2.1 Oligopolistic competition

In a completely competitive market, the point where the demand and supply curves meet is the market equilibrium denoted by (p^*, q^*).

$$q^* = \mathcal{D}(p^*) \text{ and } q^* = \mathcal{S}(p^*). \tag{2.4}$$

At the opposite extreme is a monopoly, where one firm controls the market of one product. Supposing that the price linked to the price of quantity q is $\mathcal{C}(q)$, the profit,

$$u(q) = q\mathcal{D}^{-1}(q) - \mathcal{C}(q), \tag{2.5}$$

is maximized through application of the first order condition

$$\frac{\partial u(q)}{\partial q} = \mathcal{D}^{-1}(q) + \frac{\partial \mathcal{D}^{-1}(q)}{\partial q} - \frac{\partial \mathcal{C}(q)}{\partial q} = 0. \tag{2.6}$$

An oligopoly is a more complicated market that lies between a monopoly and full competition: due to large obstacles to participate in economics, there are few firms. Due to the low number of firms, each can affect the price, and, subsequently, other firms (e.g. influence their price selection strategy and the quantity of goods they supply to the market). This relationship can be modelled through several game theory constructs, such as the *Cournot game,* the *Bertrand game,* the *Stackelberg game* and the *Cartel maintenance game*. These methods can be used in different spectrum markets.

2.7.2.2 Auction games

Auction theory is an applied form of game theory that investigates attributes and relationships in auction markets. An auctioneer conducts an auction by sourcing bids from prospective purchasers, and the result of the auction is determined by the rules of the auction. Four simple ways to classify an auction are:

- English (open ascending price) auction: an auction in which participants bid openly against each other, with each subsequent bid being higher than the previous bid, until a bid remains, which wins the product (as there is no higher bid).
- Dutch (open descending price) auction: an auction in which the auctioneer begins with a high asking price, which is lowered until a bidder accepts the price asked.

- Second price (sealed bid) auction: in this type of auction, all bidders submit a sealed bid at the same time and the highest bidder wins the product at the price of the second highest bid.
- First price (sealed bid) auction: in this type of auction, all bidders submit a sealed bid and the product goes to the highest bidder at that bid price.

In [79] an auction based mechanism between primary and SUs is proposed for spectrum leasing. The scheme is cooperative and numerical results show that the primary network could achieve a higher throughput with cooperation, as opposed to when there is no cooperation between users. SUs are shown to increase their quality of service and PUs enjoy other benefits such as increased link reliability.

2.7.2.3 Mechanism design

Mechanism design seeks to answer the question of which is the most favourable product assignment. A "principal" designs the game structure and chooses a mechanism that serves the interest of players. Players known as "agents" have privileged information known only to themselves, as in auction games. The principal asks the agents for some "messages", in order to elicit their private information regarding the game. Incentives are given to players in the form of monetary gains known as "transfers", as the agents are not necessarily honest. In mechanism design, incentives and resource constraints are equally taken into account when allocating spectrum using privileged information.

2.7.3 Cooperative games

Cooperative games arise when there is a common understanding among network users on the way to share available spectrum opportunities fairly. Cooperative games can be put into two main categories, namely bargaining games and coalition games.

2.7.3.1 Bargaining games

In bargaining games, individuals negotiate an agreement that benefits all parties. Decisions cannot be imposed on any player without that player's consent, as players have conflicting interests. In a bargaining game with two players - $N = \{1,2\}$ - (extendable to accommodate

additional players) by agreement, player 1 has utility u_1 and player 2 has utility u_2. In an instance in which they do not agree, then they have utilities u_1^0 and u_2^0 respectively. All potential utility pairs are in the set U.

A two-player **bargaining problem** is defined as the pair $\langle U, (u_1^0, u_2^0) \rangle$, where U $\subset \mathbb{R}^2$ is a compact and convex set, and there exists at least one utility pair $(u_1, u_2) \in \mathbb{R}^2$ such that $u_1 > u_1^0$ and $u_2 > u_2^0$. A **bargaining solution** is a function $(u_1^*, u_2^*) = f(U, u_1^0, u_2^0)$ that assigns a bargaining problem $\langle U, (u_1^0, u_2^0) \rangle$ to a unique element of U.

Several bargaining games have been proposed in literature. In [80] a two-tier spectrum access market was proposed. In the first tier, PUs trade spectrum to a set of SUs for a long period using a Nash bargain game model. The SUs then use the second tier to redistribute the spectrum amongst each other on a smaller time-scale, using a strategic bargaining game. A new Nash bargaining game was proposed for OFDMA CRs in [81]. On average, the proposed game is shown to achieve close to optimal capacity.

2.7.3.2 Coalition games

Coalition games describe how a group of players can collaborate through cooperative associations that will advance their payoff in a game. In [82], a partitioned coalition game was proposed that encompasses spectrum sharing and spectrum sensing. The game allows SUs to freely switch between coalitions, depending on the time spent on spectrum sensing and spectrum access. A hedonic coalition game was proposed in [83], for both spectrum sensing and sharing, with a coalition representing SUs that can sense and use a specific channel. Results show that SUs achieve better utility with iteration and converge to a partition that is stable both individually and in terms of Nash-stability.

2.7.4 Stochastic games

A stochastic game involves a dynamic environment with constant game state transitions that are based on action taken by the players. CRNs are dynamic in a time-varying radio environment and are influenced by player action, e.g. occupying a spectrum segment, and, as a result, change spectrum opportunities. As stochastic games are designed for dynamic

environments, this approach is potentially more suited to CRNs, compared to the other game options. Stochastic games can be used for *spectrum auction, transmission control* or *anti-jamming defence* in CRNs [16].

2.8 SECURITY

To deploy industrial CRNs successfully, it is necessary to develop and put in place security procedures that will guarantee the resilience of the network and individual CR nodes against security attacks. Many industrial applications may be mission critical and may have certification or standardisation requirements that make security crucial. The peculiarities of industrial networks restrict the use of classical approaches to security [84]. The cognition and re-configurability of CRs, which are central to their functioning, introduce a new class of security concerns distinct from those evident in conventional wireless networks [85]. Vulnerabilities present in this new CR technology can be exploited by antagonists for purposes of compromising the integrity of a CR network and inducing severe performance degradation. Security threats associated with cognitive ability include licensed user emulation, transmission of false spectrum sensing observations and selfish misbehaviour. Reconfiguration-related threats include the download of malicious software and configuration files. Besides this threat, CRs are prone to all the long-established threats found in traditional wireless networks.

2.8.1 Security requirements

CRNs must support several security objectives, just like all other wireless technologies, the most common of which are as follows [86]:

- **Confidentiality –** ensure that communication cannot be read by unauthorized parties.
- **Integrity –** ensure that all intentional or unintentional changes to data that occur in transit are detected.
- **Availability –** ensure that a network and its resources are accessible to legitimate devices and individuals at all times that they are needed.
- **Access Control –** ensure that access to a network or its resources is restricted in accordance with a policy**.**

The objectives above help to leverage information assurance (IA), defined by the National Security Agency [87] as "measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication confidentiality and non-repudiation". These necessities go beyond protecting data that is stored or sent over a network and include the ability of the communication infrastructure to ensure the services called for in the specification for operation [88]. Security requirements may be derived by making use of the concepts of stakeholders, assets, threats and risk [89].

Stakeholders include users of the communication system, government authorities, network providers or the public. *Assets* are made up of the network components, stored or transmitted information and network services.

A *security vulnerability* is a flaw or a weakness that is present in the design, implementation or operation of a system, which could be used to violate its security.

A *security threat* is a possible security infringement that can be active (involving a change in the state of the system), or passive (where information is disclosed without authorization and without changing the state of the system).

A *security risk* arises when a security threat and a security vulnerability are combined resulting in a loss of data, public confidence, uptime or privacy among others.

Security services mitigate threats and are implemented through an appropriate security mechanism, such as encryption or digital signature algorithm. Examples of general network security threats, services and mechanisms in the CR context are shown in Table 2.3.

In order to produce a secure communication system based on cognitive radios, capabilities should be provided that deal with and avoid compromising certain security requirements, which are defined below [88], [90]:

1. *Verification of identities*: All network entities should be authenticated. No unauthorized party should be able to join the network.
2. *Controlled access to resources*: Access to data, services and network resources should be controlled with a managed access control policy. In CR, this includes controlling access to spectrum and identifying nodes that attempt to access unavailable spectrum, e.g. SU accessing spectrum to the detriment of a PU.
3. *Protection of confidentiality*: Transmitted and stored data must be kept confidential using suitable data encryption techniques. The 'spectrum-hopping' nature of CR should not be seen as a mechanism to prevent unauthorized data interception. Careful consideration must be given to what data in an industrial network requires confidentiality, e.g. low-level configuration data might not appear valuable, but is useful to competitors.
4. *Protection of data and system integrity*: Ensuring data is correct is important in industrial networks. Suitable cryptographic integrity mechanisms must be used to detect intentional modification. Mechanisms for detecting accidental modification/errors, such as CRC codes, are not sufficient, as they can be recreated by attackers to match modified data.
5. *Accountability*: The mechanism must ensure non-repudiation actions and the subsequent effects thereof by entities, e.g. all configuration changes could be digitally signed to indicate the operator who made the change.
6. *Robustness*: Despite the security, the network must ensure required communication services according to an agreements regarding service levels. Industrial networks must maintain timeliness and be resistant to errors/interference; therefore additional security services must be chosen and implemented with this in mind.
7. *Compliance with the regulatory framework*: Network security should adhere to regulations in force in the system's region of operational. For example, Data Protection laws would govern how data are transmitted and stored.

2.8.2 Attacks against cognitive radio networks and detection techniques

2.8.2.1 Primary user emulation attacks

An underlying feature of a CR is its ability to perform spectrum sensing, since it accesses spectrum opportunistically. In opportunistic spectrum access, the CR must leave a licensed region of spectrum if a PU transmission exists. This requires the CR to perform spectrum hand-off as part of spectrum mobility, when seeking different spectrum white spaces for transmissions. Spectrum hand-off has the undesirable effect of degrading CR performance, as more time for spectrum sensing is needed, which reduces the time that can be used for spectrum access. Adversaries can exploit this integral CR procedure by mimicking incumbent signals. There are two categories of nodes that launch primary user emulation attacks (PUEAs) [85]:

- Greedy nodes: These nodes seek to gain sole access to a particular spectrum band by transmitting fake incumbent signals, which forces other nodes to leave the band.

Table 2.3 Other Cognitive Radio Threats and Protection Techniques [88].

Threat Description	**Security Service Required**	**Affected Functionality**	**Protection Mechanism**
Eavesdropping of cognitive control messages	• Confidentiality	• Spectrum sensing • Spectrum sharing	• Encryption • Frequency hopping
Jamming cognitive control messages	• Integrity	• Spectrum sensing • Spectrum sharing	• Frequency hopping
Compromise of a cognitive radio node	• Integrity • Trusted hardware	• Spectrum sharing • Spectrum mobility	• Identification of modified action through signal analysis or reputation systems • Remote attestation

Threat Description	**Security Service Required**	**Affected Functionality**	**Protection Mechanism**
Malicious alteration of cognitive messages	• Integrity • Non-repudiation	• Spectrum sensing • Spectrum sharing	• Data origin authentication with MAC • Non-repudiation with digital signatures
Fake cognitive radio node	• Authentication • Source authentication of messages • Access control	• Spectrum sensing • Spectrum sharing	• Identification of masquerading threats through signal analysis • Authentication of CR Nodes

- Malicious nodes: These are adversarial nodes that intend causing Denial of service (DoS) attacks on SUs (by mimicking incumbent signals) or to PUs (by causing harmful interference). These nodes can form coalitions to cause extensive DoS attacks across several bands, which result in a major disruption in service.

Both attacks disrupt the operation of the CRN and cause unfairness among network nodes. A PUEA can disrupt the operation of all stages of the cognitive cycle in a CRN. Initially the radio-frequency environment is polluted by fake PU signals. This creates a cascading phenomenon that affects spectrum sensing, analysis and decision. Energy detection is the most widely used spectrum sensing technique, due to its simplicity and low computational overhead [56], [91]. Energy detection is most susceptible to PUEAs, due to its poor performance in environments with low SNR. In addition, since creating signals using carrier frequencies of PUs is simple, non-sophisticated adversaries can initiate PUEAs that are targeted at SUs that use energy detection. Learning CRs are more susceptible to PUEAs, since they construct a manner of acting over an extended period, which is founded on measurements recorded from the environment [92].

The FCC has indicated that "*no modification to the incumbent signal should be required to accommodate opportunistic use of the spectrum by SUs.*" As a result, most detection techniques that have been proposed to protect against PUEAs do not involve altering the PU signal. In addition, some approaches presume that information is available regarding the position of the incumbent user's transmitters. Considering this, different contributions to detecting PUEAs can be characterised as follows [85]:

- whether or not the incumbent signal is modified
- cooperation or non-cooperation based
- advantages and disadvantages of use
- location-based or non-location-based
- tested using simulations or real implementations.

2.8.2.2 Spectrum sensing data falsification attacks

It is possible that some of the SUs will send false observations, either intentionally or inadvertently, which results in hampering collaborative spectrum sensing in a spectrum sensing data falsification (SSDF) attack. In much the same way as with PUEAs, misbehaving nodes that carry out SSDF attacks can be classified as:

- Malicious nodes: These nodes send a false observation in order to mislead the fusion center or other nodes into incorrectly determining that an ongoing PU transmission is in progress or that there are no licensed user transmissions, when this is not the case.
- Greedy nodes: These nodes constantly report that a particular band of licensed spectrum is occupied by PUs, so that all other SUs evacuate it and the greedy nodes can then monopolise use of the band.
- Unintentionally misbehaving nodes: These nodes have parts of their software that are malfunctioning, which leads them to report faulty observations on available spectrum.

The majority of approaches to detecting SSDF attacks presume a scenario in which cognitive users send their observations to a fusion center (FC), but the SUs are not trusted beforehand. These approaches propose methods to calculate reputation metrics, the aim being to detect and isolate users that pose a security threat. The FC combines the reports

generated by trusted nodes and does not include reports from identified attackers. These reports can be: (i) continuous (such as the energy detector's power estimation); (ii) binary (such as whether or not a primary transmission is present). If a node misbehaves, but later acts appropriately, some approaches allow the reputation metric to be restored. Different contributions [93], [94], [95] to SSDF detection can be characterised according to:

- fusion rules in use
- the type of reporting
- advantages and disadvantages of use
- whether or not the reputation metric is restored.

2.8.2.3 MAC layer threats

It is of great importance to avoid interference to PUs in CRNs. In order to achieve this, the MAC layer must interact closely with the lower layers. This cross layer operation does not follow the strict boundaries between layers of the waterfall-like concept found in the OSI communications model. There are two categories of CR MAC protocols: (i) standardised, such as the IEEE 802.22 protocol; (ii) application or scenario specific protocols. CR MAC protocols can also be categorised as being: Direct access based (DAB), which do not permit global optimisation, due to sender-receiver pairs maximising their individual optimisation goals; or DSA, which use complicated optimisation techniques to attain a global goal adaptively [96]. These are shown in Figure 2.9. Using a common control channel (CCC) is an important characteristic of CR MAC protocols. The CCC is central to the operation of a CRN and can become the target of DoS attacks from adversaries.

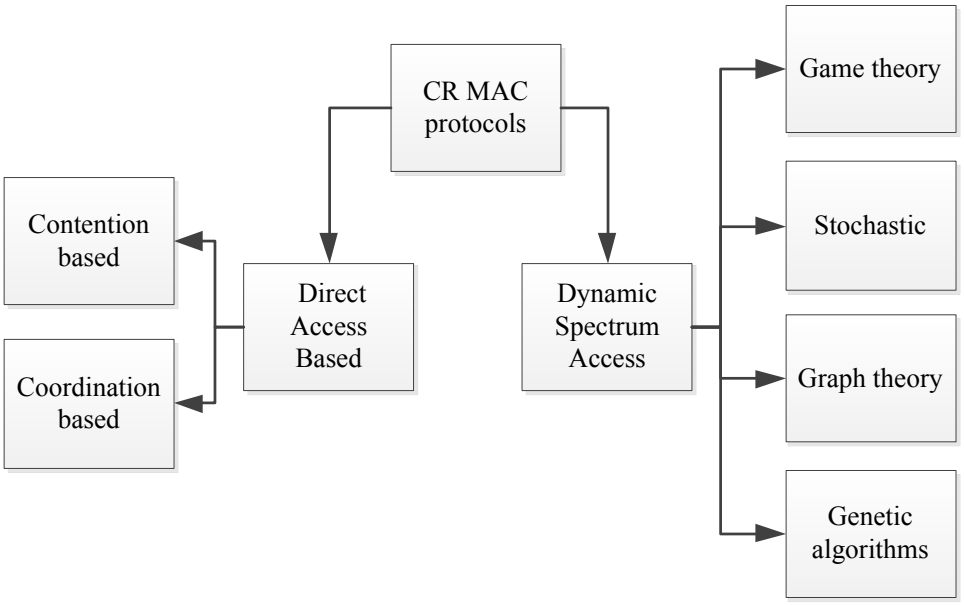


Figure 2.9. Categories of cognitive radio MAC protocols. Republished with permission of IEEE, from [96]; permission conveyed through Copyright Clearance Center, Inc.

2.9 SUMMARY

In this chapter, the potential benefits and current limitations of using cognitive radio techniques in industrial wireless sensor networks were discussed. Cognitive radio approaches can be added to the lower layers of existing industrial network stacks, in order to improve resistance to interference, simplify co-existence with other industrial and consumer networks, and offer additional communication spectrum to allow wideband communication or additional narrow-band channels. Cognitive radio is a developing area and there are still some areas that need to be addressed. These include standardisation, latency and efficiency of spectrum sensing on restricted sensor nodes, the speed of channel selection and dynamic reconfiguration once a channel encounters interference, and compliance with timeliness constraints in industrial applications. The chapter also provided an overview of different techniques for spectrum sensing and spectrum management in cognitive radio networks. The application of game theory for spectrum sharing was explored, and selected security aspects of cognitive radio implementation were discussed.

CHAPTER 3 SPECTRUM MANAGEMENT POLICIES FOR THE EFFICIENT USE OF RADIO SPECTRUM

3.1 INTRODUCTION

Today, the regulation of wireless communication is based on a fixed spectrum assignment policy: government agencies regulate spectrum usage and assign portions of the spectrum over extended periods of time and covering large geographic areas to license holders or for certain services. Large portions of the allocated spectrum are utilized intermittently and spectrum use is congested at particular regions of the spectrum space, while a considerable portion is left under-utilized. The inefficient use and scarcity of spectrum has demanded the adoption of a new paradigm in wireless communication, to ensure that the available wireless spectrum is exploited opportunistically [5].

The radio frequency spectrum is the range of frequencies from 3 kHz to 300 GHz. This spectrum is a finite resource that is used for wireless communication and services. As a finite resource, it is important that it be used and managed carefully. Demand for wireless communication in consumer electronics and personal high data rate networks is increasing continuously, as are the service quality requirements in terms of throughput, reliability and availability of wireless services [97]. It is expected that there will be a considerable increase in the number of devices making use of different wireless standards and technologies in the future. On the one hand, there will be greater provision and access to broadband multimedia services; on the other hand, getting multiple heterogeneous radio systems to co-exist harmoniously in shared spectrum is challenging. Traditionally, network operators have generally been privileged enough to enjoy exclusive rights to access parts of spectrum assigned to them and hence the problems of co-existence and limited spectrum could be ignored. At present, however, it has become necessary to use spectrum more efficiently, so as to facilitate further growth of wireless communication and the future knowledge economy and information society.

3.2 ACCESS TO SPECTRUM AND REGULATION

Access to radio frequency spectrum is regulated by designated regulatory authorities that determine how certain spectrum bands can be used and provide certain rights to licensed and unlicensed users. These regulatory authorities make decisions in the public interest, with the aim of enhancing societal benefit, safety and general welfare. Part of their mandate includes defining regulatory rules that constrain access to radio frequency spectrum as part of a spectrum licensing regime. Such regulation is necessary because radio spectrum is a finite publicly available resource that can be used for a multitude of services, which may create undesirable effects on one another if the system is not coordinated well. For example, radio telescopes such as those used in the Square Kilometre Array (SKA) project are used in astronomy to observe celestial objects in the observable universe. Should the radio frequencies used for radio astronomy be used by another service close to the telescopes, then interference may be created that can affect the quality of scientific observations detrimentally. Such a problem exists with other types of wireless services when there is the emission of electromagnetic radiation at radio frequencies which may result in radio frequency interference; regulation of radio spectrum mitigates undesirable effects like these and makes reliable and efficient spectrum use possible.

3.3 LICENSED AND UNLICENSED SPECTRUM

3.3.1 Licensed

Licensed spectrum is the part of the radio frequency spectrum that is allocated to some radio services for exclusive use. Licensed spectrum can be accessed for exclusive access or shared access of the same type of radio service. License holders usually pay a fee for these spectrum access rights and receive protection from unwanted interference from other radio systems. Licensed spectrum is valuable because of the benefits it provides such as addressing the problem of spectrum scarcity. In addition, license holders charge their customers a fee to use it and they therefore make a profit. License holders are required to ensure that certain conditions are met, such as the use of a particular transmission technology and reaching a certain fraction of the population within a given time period.

The sale of spectrum licenses often takes place by way of auctions. It is a very expensive process, due to the time and difficulty involved. Under-utilised or unused spectrum cannot be used if a license is held on it, which leads to spectrum inefficiency. Licenses typically expire after a decade, but there is an option for renewal.

3.3.2 Unlicensed

Some parts of the radio frequency spectrum are reserved as unlicensed spectrum and are open for inclusive use. Despite this, unlicensed spectrum is still stringently regulated with usage of the spectrum being permitted provided wireless communication devices meet the specified technical rules or standards put in place to limit possible harmful interference arising from transmissions from other devices. Flexibility is provided in terms of usage rights and there is no particular method of accessing spectrum that is defined or mandated. The most common license exempt band is the ISM band, which is between 2400 MHz and 2483.5 MHz. The success of technologies such as Wi-Fi and Bluetooth in the license-free ISM band is evidence of the economic advantage of unlicensed spectrum and show that it is possible to use spectrum more efficiently than is typically the case in licensed bands.

3.4 SPECTRUM SCARCITY, REAL AND ARTIFICIAL

In order to guard against interference from other radio systems, a wireless service provider can license spectrum for exclusive use from the regulatory authority. As more and more spectrum is licensed, a problem of spectrum scarcity arises as there will be less and less spectrum available for licensing. This scarcity of spectrum is, however, artificial in some cases. There are several reasons for this, the first of which is that some licensed radio services and systems may suffer economic failure, resulting in the licensed spectrum not being utilised. An example of this is WiMAX, which appears to have not taken off commercially. Spectrum for WiMAX has been allocated and licensed in many countries, but network operators appear to not be using it. Unless WiMAX spectrum usage picks up, it is largely wasted spectrum. A second reason for artificial spectrum scarcity is that some spectrum is reserved for occasional military radio and public safety use. This spectrum may be used only rarely. Advances in technology are the third reason why there can be

artificial spectrum scarcity. Recently, there has been the migration of television broadcasts from analogue to more the efficient digital broadcast system. This has resulted in less spectrum being required to provide the same service. All this means that some of what can be considered as spectrum scarcity is actually due to inefficient use of spectrum, while the demand for additional spectrum is rising faster than the rate at which new technology has increased spectrum efficiency.

In unlicensed spectrum bands such as the ISM band, however, it is common to find multiple heterogeneous radio systems operating in overlapping spatiotemporal regions. There is notable spectrum congestion in such unlicensed bands and the scarcity of spectrum in such cases is real. It has been established that usage of spectrum in assigned bands varies temporally and geographically between 15% and 85% [98]. It is therefore necessary to develop new methods of spectrum access that will result in more efficient spectrum usage and alleviate spectrum congestion in certain bands.

Experiments were conducted to determine utilisation of spectrum, with readings taken in an office environment. The figures below show spectrum utilisation in popular spectrum bands. The Python scripting language and the GNU radio software development kit were used to create a spectrum analyser program and to generate the graphs shown. The hardware used was the Ettus Research USRP software radio. The following chapter contains more details on the typical setup used for experiments in this research study; in this section, only the measurements obtained are presented. At the time the readings were taken, spectrum occupancy of 42% was observed in the bands predominantly reserved for analogue television, and: 23% in bands that include spectrum touted for LTE communication; 52% in the mobile cellular telephony bands; and 24% in the 2.4 GHz LTE band. See Figure 3.1, Figure 3.2, Figure 3.3 and Figure 3.4.

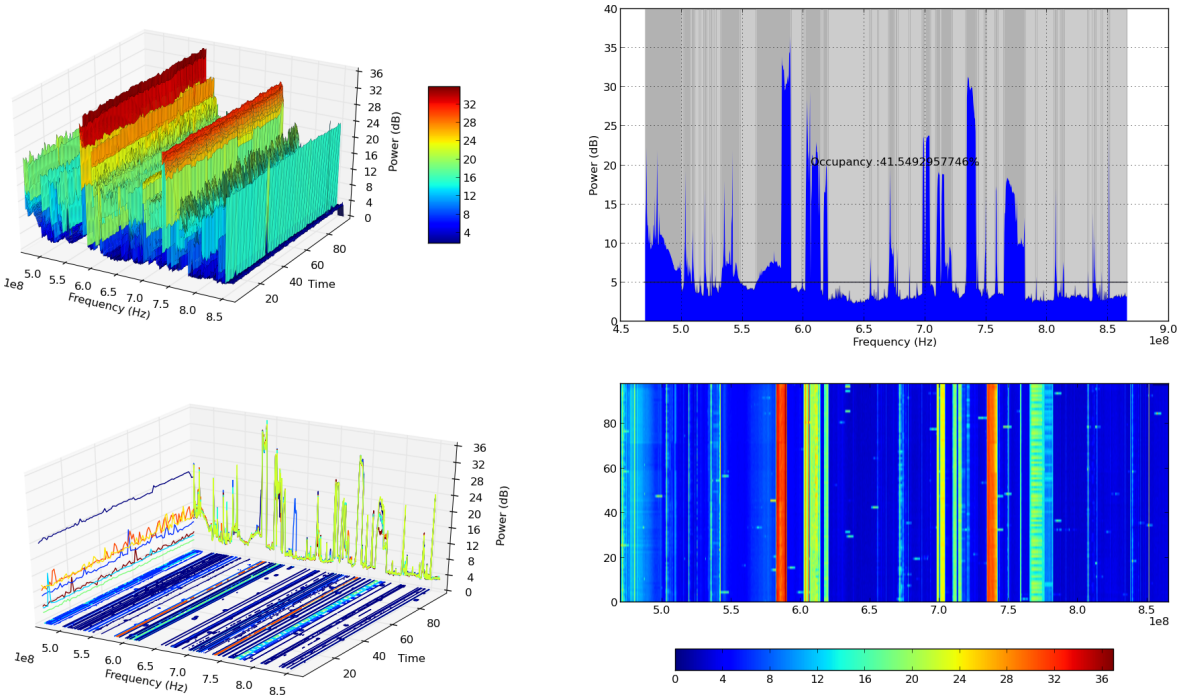


Figure 3.1. Measured spectrum usage in predominantly UHF-TV bands.

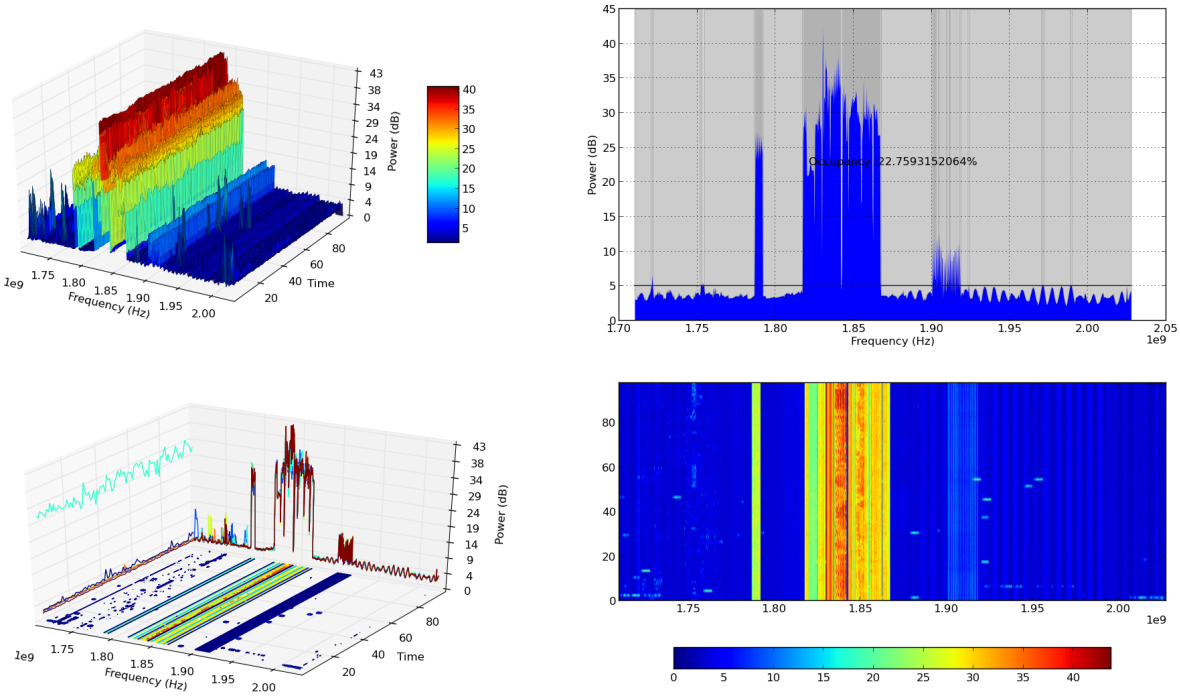


Figure 3.2. Measured spectrum usage in spectrum that includes potential LTE bands.

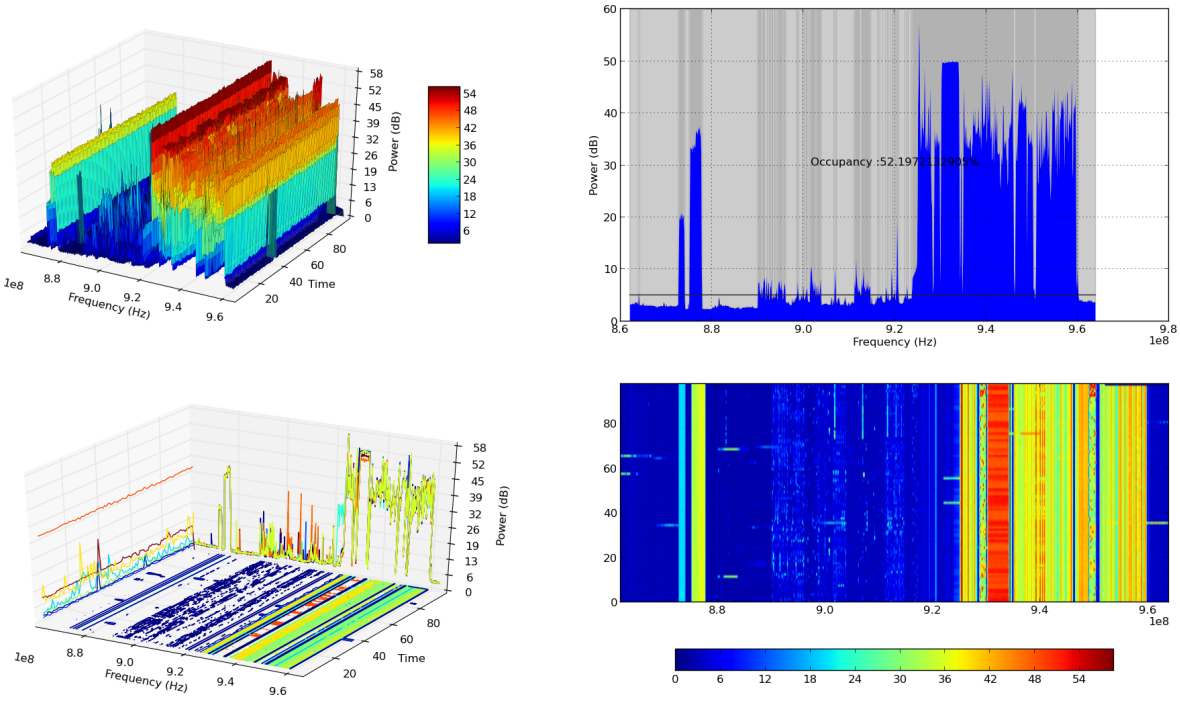


Figure 3.3. Measured spectrum usage in predominantly mobile cellular bands.

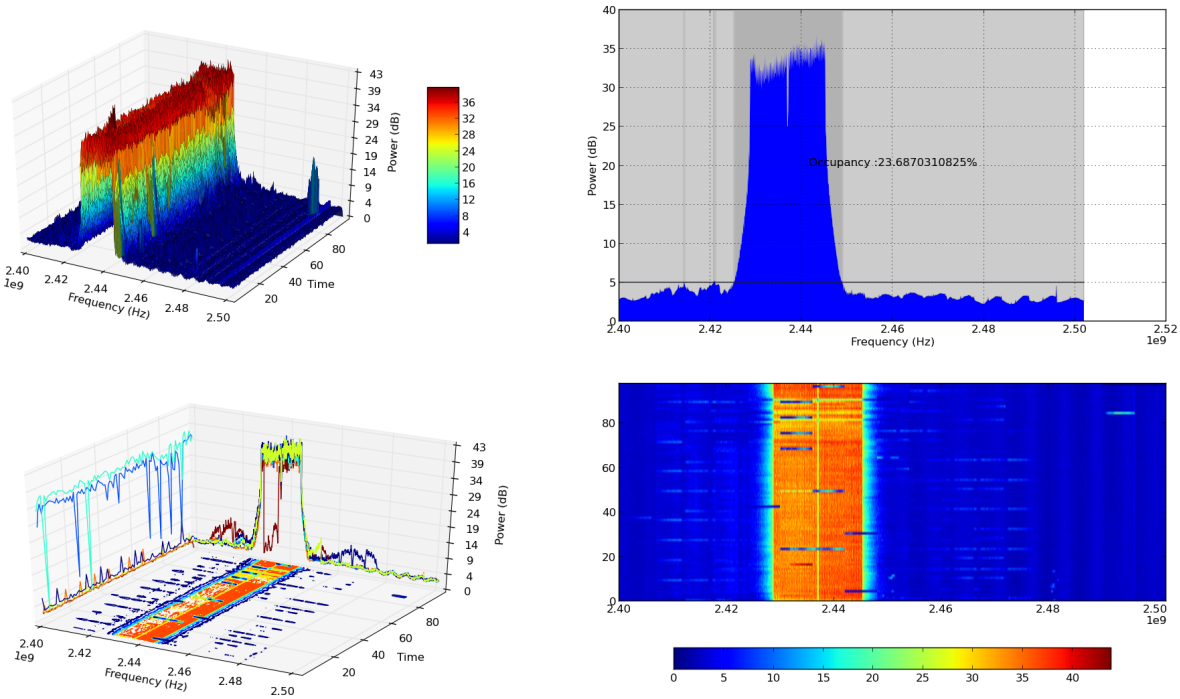


Figure 3.4. Measured spectrum usage in 2.4 GHz ISM band.

3.5 GUIDING PRINCIPLES AND APPROACHES TO REGULATION

3.5.1 Approaches

There are four basic approaches to regulating spectrum, including licensed and unlicensed spectrum [99]. The first approach is licensed spectrum for exclusive usage. With this approach, a licensee has exclusive and transferable rights for certain spectrum bands. This is used, for example, in Europe for the Universal Mobile Telecommunication System (UMTS). The regulator enforces and protects usage of the spectrum.

The second approach is licensed spectrum for shared usage. Here, access is restricted to a particular technology. Examples include the use of Digital Enhanced Cordless Telecommunication (DECT) in Europe and public safety services.

A third approach to regulation is unlicensed spectrum. With this approach, open access is granted by the regulator to all radios that function in accordance with certain spectrum etiquette rules. There is no privilege for interference protection in license-exempt spectrum. Wi-Fi and Bluetooth are examples of technologies that operate using unlicensed spectrum.

There is a fourth approach that can also be followed, i.e. open spectrum. This allows anyone to access any spectrum band without restriction, subject to a minimal collection of guidelines for spectrum sharing derived from technical standards or accepted etiquette.

3.5.2 Guiding principles

Six objectives of spectrum access standards that are influenced by regulation and need to be balanced are as follows:

1. Quality of service – Adequate QoS must be possible for all radio systems, according to their applications.
2. Availability – A radio should not be denied access to spectrum and transmission for an extended period of time.

3. Innovation promotion – Innovations in fast-changing and economically successful wireless communication markets must not be impeded by spectrum regulation.
4. Efficient use – There must not be wastage of spectrum and there must be high spatial re-use of it.
5. Dynamic use – The existing local radio frequency environment and spectrum usage policies must be taken into consideration, so as to use spectrum in an adaptive and dynamic way.
6. Cost effectiveness – Radio regulation must not increase the cost of commercial wireless communication devices because of the techniques required by regulation.

3.6 REGULATORY AUTHORITIES WORLDWIDE

3.6.1 Globally

Regulation of spectrum usage is done by national and international institutions. These regulators license spectrum for exclusive or shared usage in a process known as spectrum allocation or frequency allocation. It is necessary to harmonise the process of allocating spectrum globally; this is done with the assistance of the radio communication sector of the International Telecommunication Union (ITU-R), which is an agency of the United Nations. The ITU-R endeavours to guarantee efficient, equitable, rational and economical radio frequency usage by all wireless communication services.

ITU agreements regarding spectrum allocation can be found in the ITU radio regulations (ITU RR). These agreements have treaty status and regulate radio frequency spectrum usage internationally. They also provide a common framework for national and regional planning. Every three to four years there are world radio communication conferences (WRCs), at which the ITU RRs are revised. The ITU has divided the world into 3 regions for the purpose of apportioning frequencies, as shown in Figure 3.5.

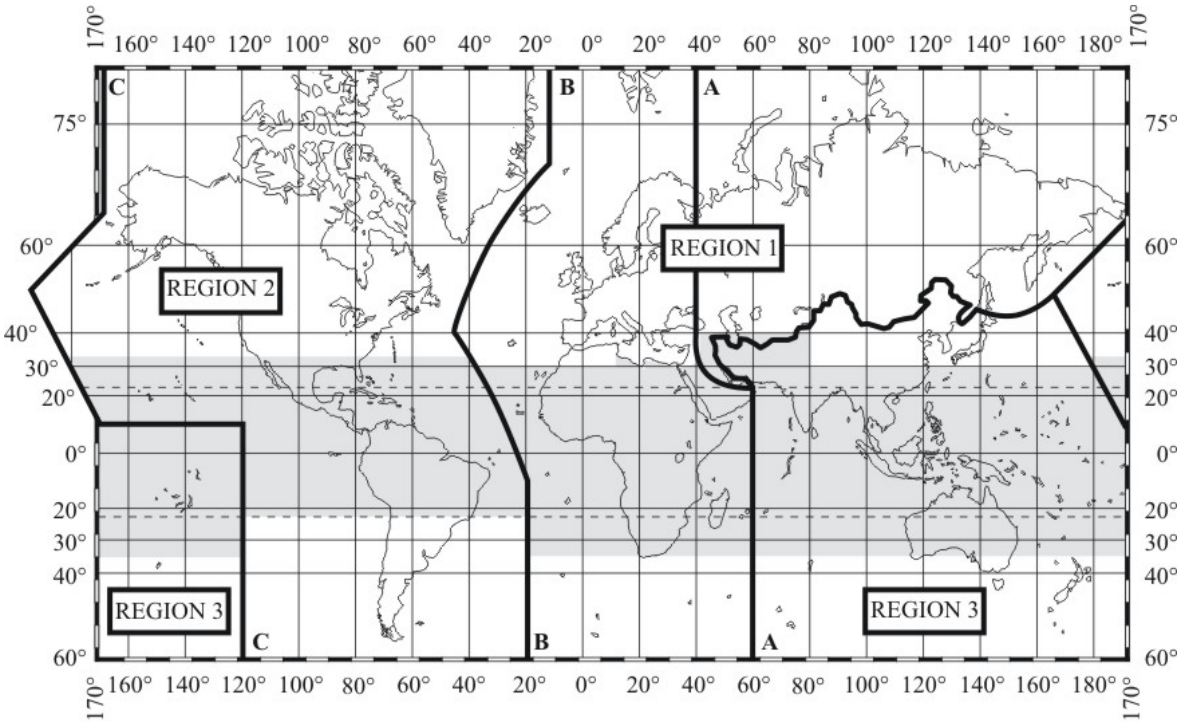


Figure 3.5. ITU-R radio regions. Taken from [100], with permission.

3.6.2 South Africa

In South Africa, the regulatory authority is the Independent Communications Authority of South Africa (ICASA). Historically, this has not always been the case: before 1994, operators such as SABC (for broadcasting) and Telkom (for telecommunications) were themselves responsible for managing spectrum. Independent management of spectrum began after the passing of the Independent Broadcasting Authority Act (Act No. 153 of 1993), which paved the way for the establishment of the Independent Broadcasting Authority (IBA). The South African Telecommunications Regulatory Authority (SATRA) was established after the passing of the Telecommunications Act (Act No. 103 of 1996). IBA was responsible for the regulation of broadcasting whereas SATRA regulated telecommunication. ICASA was established in July 2000 and merged SATRA with IBA. ICASA was formed as a result of the Independent Communication Authority Act of South Africa Amendment Act (Act No. 13 of 2000). The ITU has divided the world into three different regions for the purpose of allocating frequencies and South Africa falls into ITU

region 1. ICASA therefore aligns its frequency allocations with those of ITU region 1 in the ITU RR.

3.6.3 Other countries

Each country has its own regulatory bodies governing spectrum usage. In the United States of America (USA), the FCC and the National Telecommunications and Information Administration (NTIA) are responsible for regulating spectrum. The FCC handles non-governmental use of spectrum, whilst the NTIA looks at spectrum used by government. In Europe, the Electronic Communications Committee (ECC) of the European Conference of Post and Telecommunications Administrators (CEPT) is responsible for regulation. CEPT had 48 member countries as at 2014, each of which generally implement what the ECC decides. Matters relating to spectrum allocation are attended to by the frequency management working group, whilst radio regulation and spectrum engineering issues are attended to by other coordinating committees. The Office of Communication (Ofcom) is the body mandated with the regulation, assignment, licensing and management of radio spectrum in the United Kingdom (UK). In Japan, the Ministry of Internal Affairs and Communication is the regulatory authority, whilst in China the role is fulfilled by the Ministry of Information Industry (at a national level) and local radio regulatory authorities (at the provincial level).

3.7 RADIO FREQUENCY PLAN FOR SOUTH AFRICA

The chart in Addendum A is a one-of-a-kind chart that was developed as part of this research; it shows how frequency is allocated in South Africa, as contained in the National Radio Frequency Plan [101]. In some cases, once spectrum has been allocated, it is necessary to undergo a process of radio frequency migration. Radio frequency migration is defined as “the movement of users or uses of radio frequency spectrum from their existing radio frequency spectrum location to another” [102]. This can happen when a change in the use of a radio frequency band is needed, so as to harmonise the South African National Radio Frequency Plan with the ITU-RR or the final acts of the most recent WRC. Another reason could be harmonisation with the frequency allocation plan of the Southern African

Development Community (SADC). In some cases, ICASA can determine that a change in the use of a spectrum band is needed to enable more efficient spectrum usage or to meet legal objectives. The regulator can also decide that the assignment of frequencies within a radio frequency band to a certain spectrum licensee needs to be changed, in order to provide for greater efficiency in the use of spectrum, which also results in radio frequency migration. Related to spectrum migration is spectrum re-farming, which is defined as "the process by which the use of a radio frequency spectrum band is changed following a change in allocation; this may include a change in the specified technology and does not necessarily mean that the licensed user has to vacate the frequency". Two South African Band Re-planning Exercises (SABRE) were carried out in 1997 and 2001. These were followed by two national radio frequency plans in 2004 and 2010. The National Frequency Migration Plan of 2012 and National Radio Frequency Plan of 2013 were developed subsequently.

The ITU has specified that the radio spectrum will be divided into a total of 9 frequency bands, which are as shown in Table 3.1. Different radio communication services are allowed for each range of frequency. This includes both current and possible future use.

Table 3.1. ITU Band Segmentation [100].

Band	**Symbol**	**Frequency range**	**Metric**
Very Low Frequency	VLF	3 kHz to 30 kHz	Myriametric waves
Low Frequency	LF	30 kHz to 300 kHz	Kilometric waves
Medium Frequency	MF	300 kHz to 3 MHz	Hectometric waves
High Frequency	HF	3 MHz to 30 MHz	Decametric waves
Very High Frequency	VHF	30 MHz to 300 MHz	Metric waves
Ultra High Frequency	UHF	300 MHz to 3 GHz	Decimetric waves
Super High Frequency	SHF	3 GHz to 30 GHz	Centimetric waves
Extremely High Frequency	EHF	30 GHz to 300 GHz	Millimetric waves
Tremendously High Frequency	THF	300 GHz to 3000 GHz	Decimillimetric waves

3.7.1 List of services

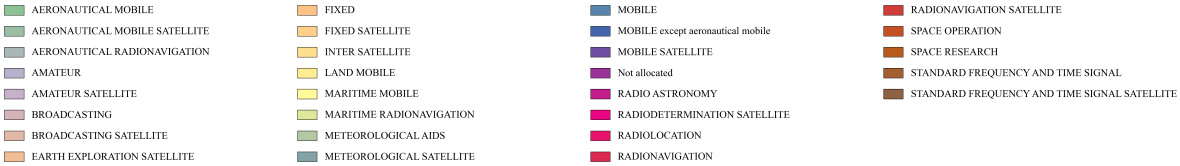


Figure 3.6. Radio services colour legend.

3.7.2 Frequency allocations in different bands

The allocation of frequencies to different services in South Africa is shown in Figure 3.7 to Figure 3.14.

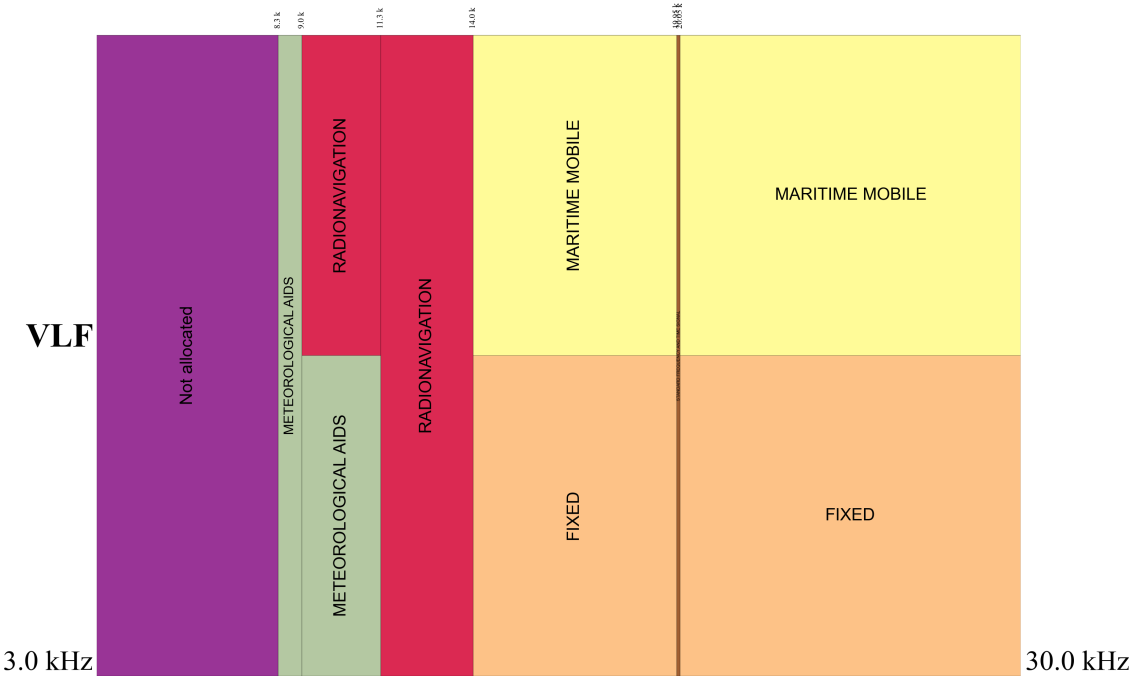


Figure 3.7. VLF band frequency allocations.

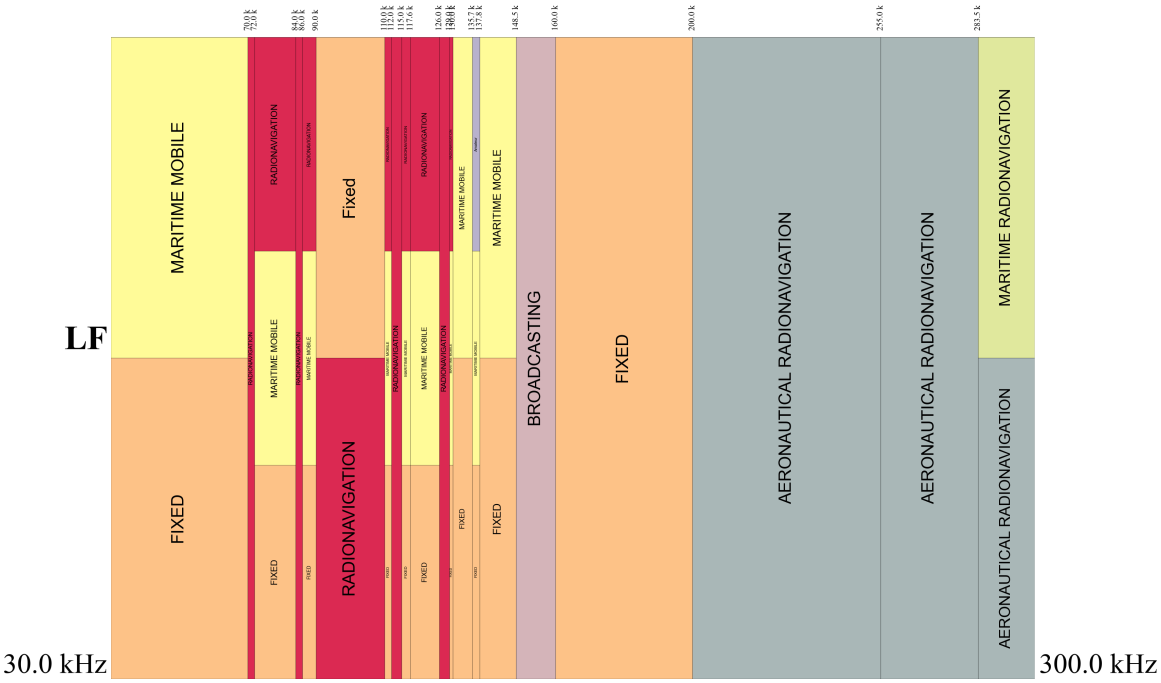


Figure 3.8. LF band frequency allocations.

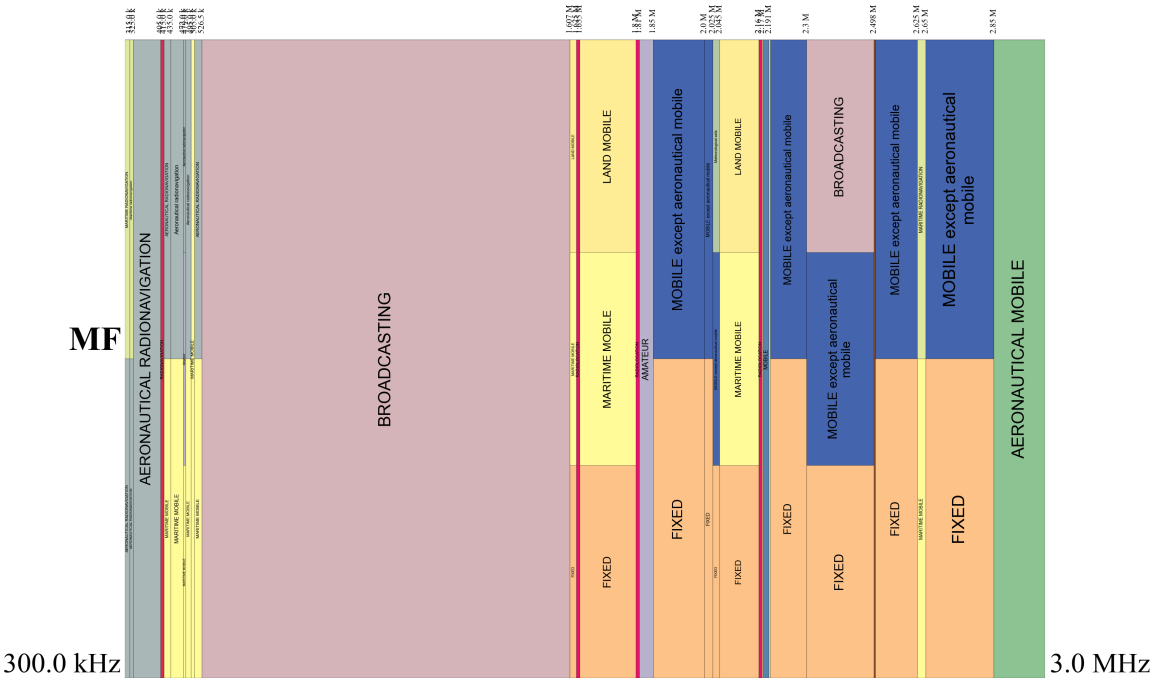


Figure 3.9. MF band frequency allocations.

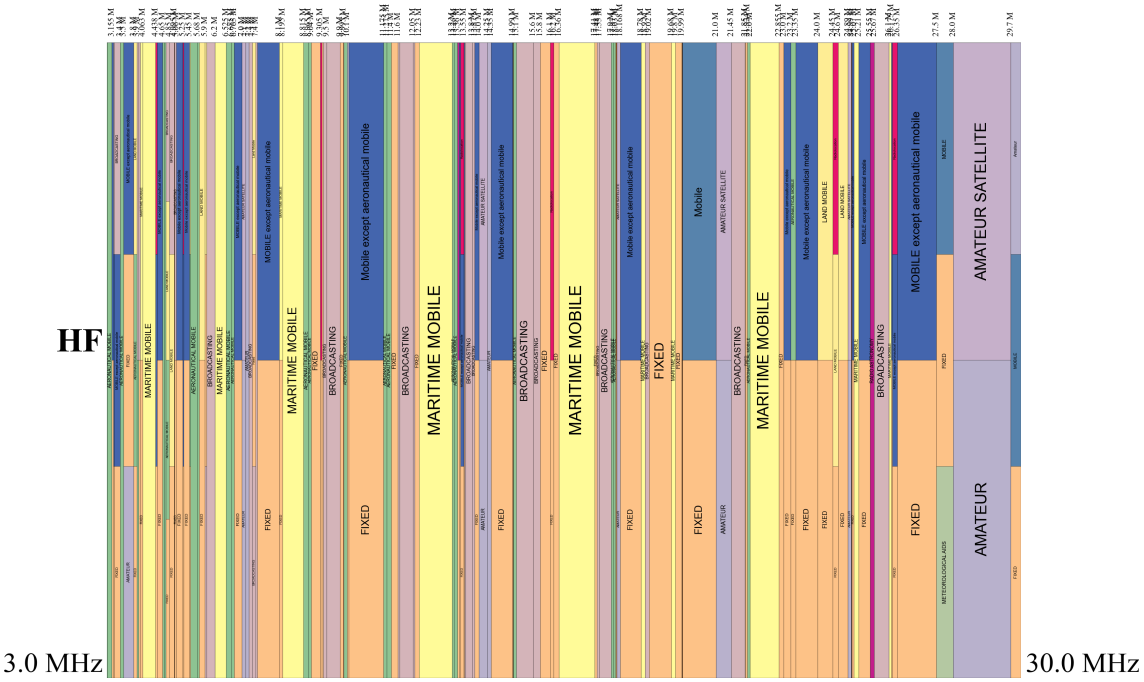


Figure 3.10. HF band frequency allocations.

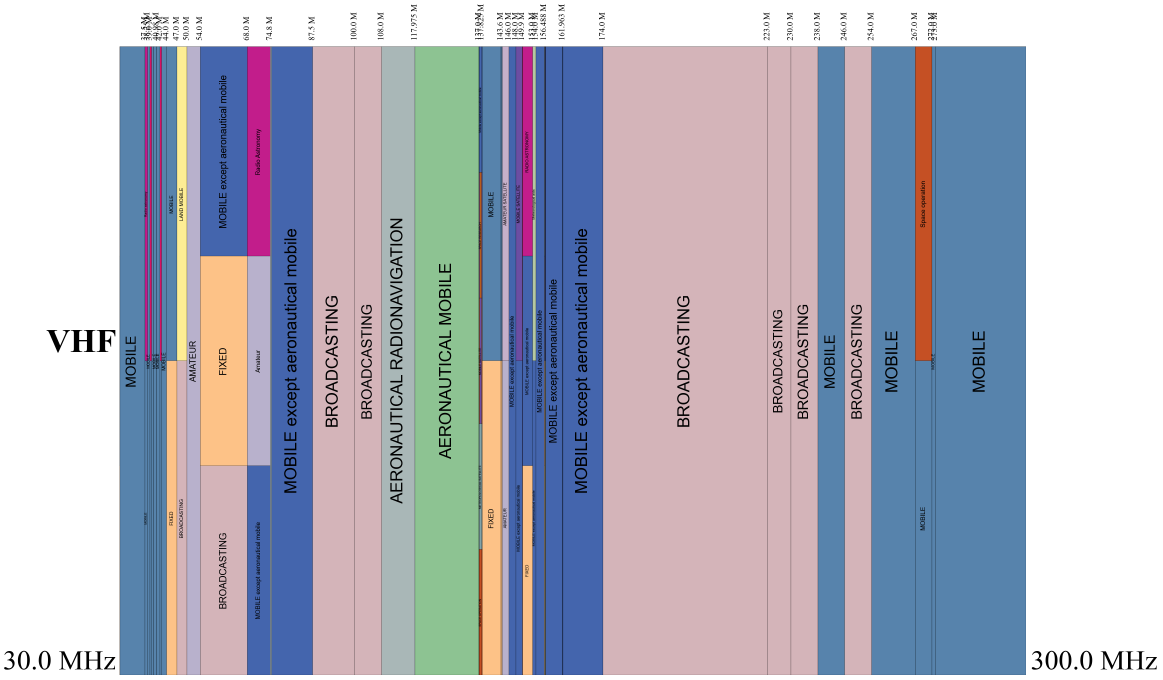


Figure 3.11. VHF band frequency allocations.

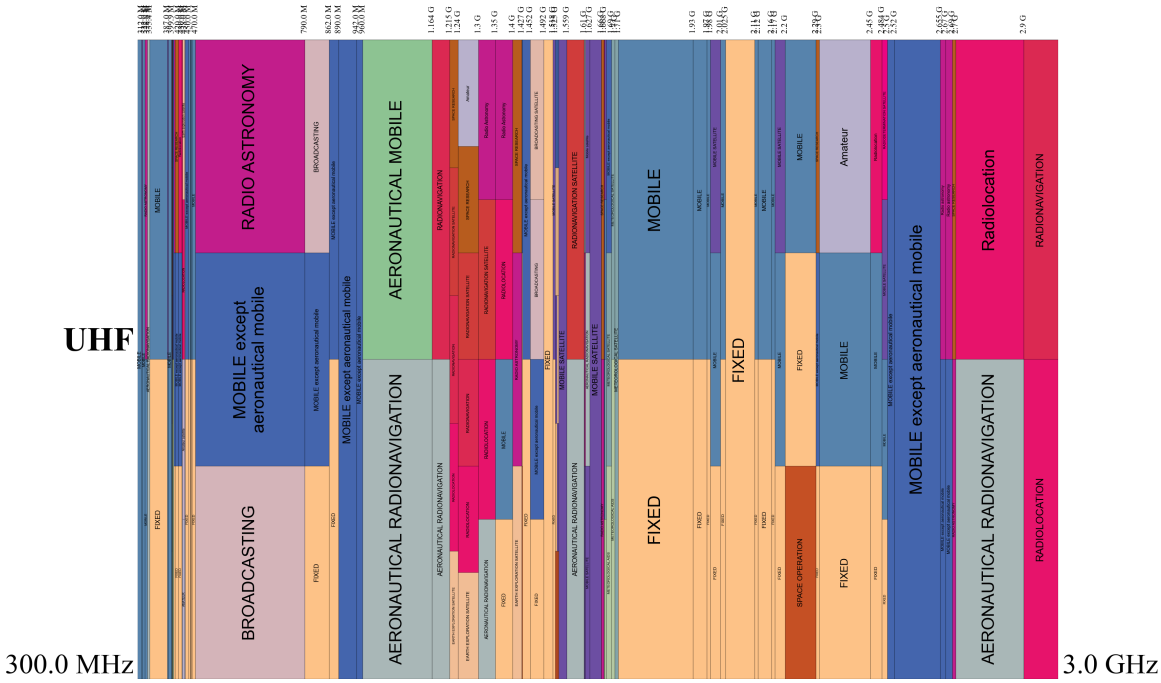


Figure 3.12. UHF band frequency allocations.

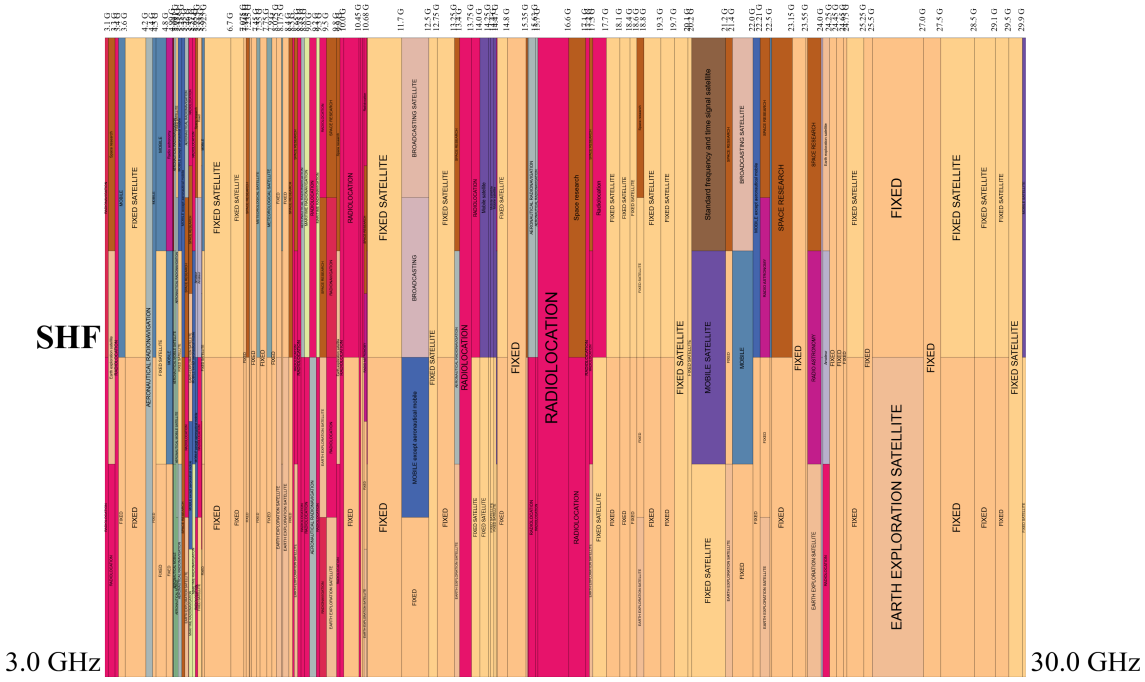


Figure 3.13. SHF band frequency allocations.

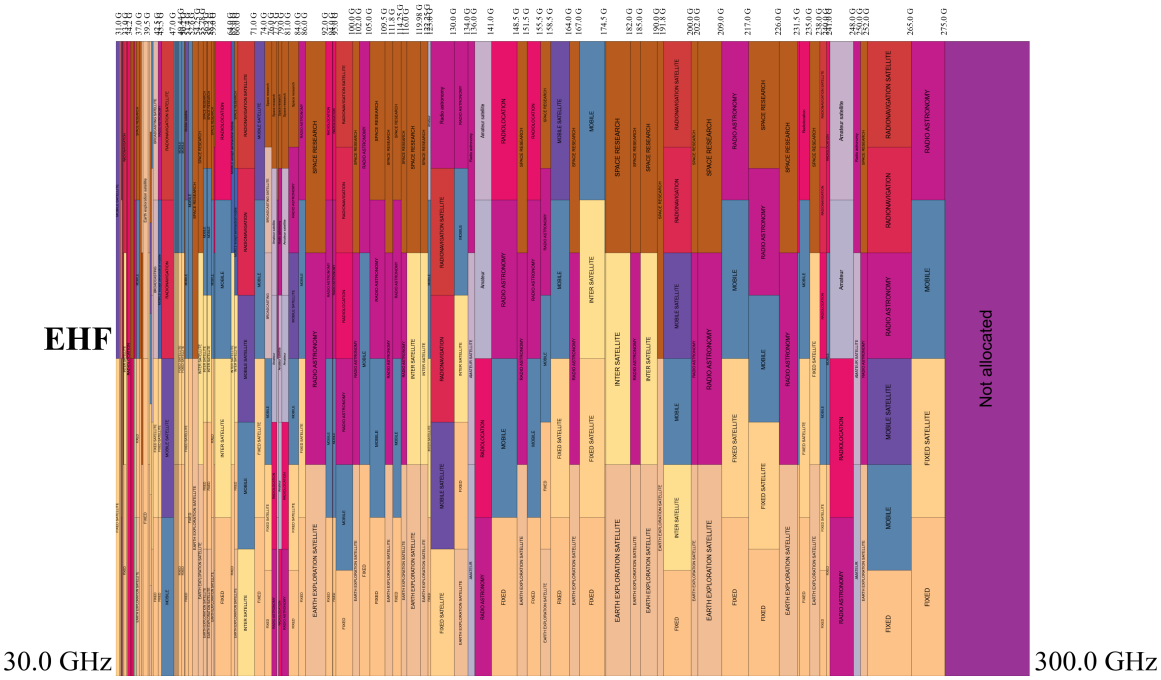


Figure 3.14. EHF band frequency allocations.

3.8 DYNAMIC SPECTRUM ACCESS

The inefficient use and scarcity of spectrum has resulted in a push for the adoption of flexible spectrum access policies by radio frequency spectrum regulatory bodies. Optimal spectrum usage can be realised through the use of the dynamic spectrum access concept: network licenses and priorities are not set at design time, instead radios are allowed to negotiate use of spectrum locally for a given time window. A first step to realising DSA is opportunistic spectrum access (OSA), as radios can search for unused spectrum in licensed bands (referred to as white spaces or spectrum holes) and proceed to use them.

OSA can be realised using a CR technology. Some regulators, such as the FCC in the US, have allocated bands for testing CR, in order to facilitate the development of CR technologies; many other regulators worldwide are faced with the choice of whether or not to allocate spectrum for CR testing in a similar way. Determination of safety criteria for CR equipment will be beneficial in instances where CRs share bands with other types of technology. In OSA with CRs, band sharing can either be authorized by the regulator or

primary spectrum license holders can enter into an agreement with secondary unlicensed users without regulatory involvement.

3.9 SUMMARY

Regulatory authorities worldwide make decisions that determine how different radio frequency spectrum bands are accessed. In order to overcome problems associated with real and artificial scarcity of radio spectrum, new paradigms for spectrum assignment policy should be explored. Dynamic spectrum access can be used to enable optimal spectrum usage. A first step in this regard is opportunistic spectrum access, which can be realized using cognitive radio technology, the end result being more efficient use of radio spectrum.

CHAPTER 4 COGNITIVA – A COGNITIVE INDUSTRIAL WIRELESS NETWORK PROTOCOL

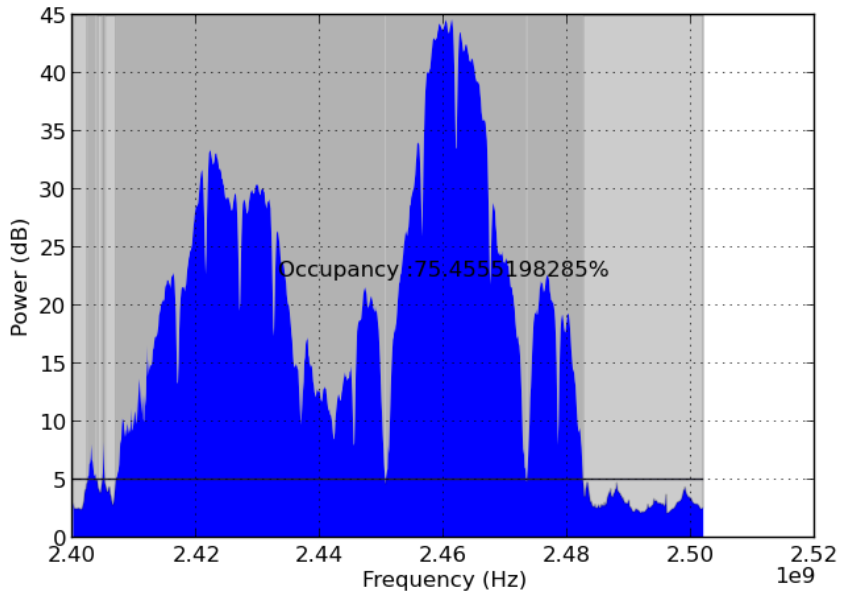
4.1 INTRODUCTION

Using CRs for opportunistic spectrum access, such as in in the lower sub-1 GHz frequencies, can result in enhanced spatial re-use, extended communication range, and greater energy efficiency [103, 104]. As an unlicensed band, the ISM band is prone to radio frequency interference from different radio signals, which can affect reliability of communication adversely. To illustrate this, Figure 4.1 shows readings that were taken to indicate spectrum usage in the 2.4 GHz ISM and UHF TV bands.

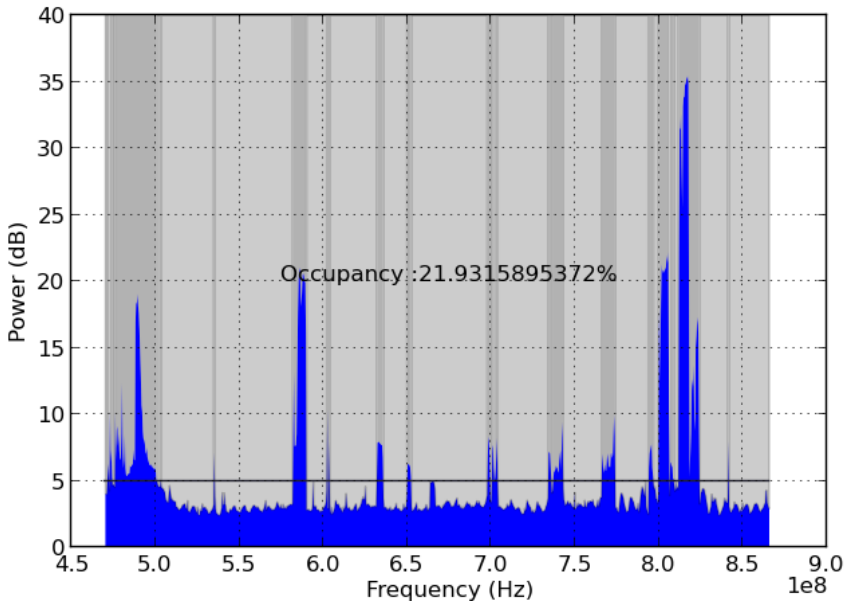
In this chapter, the design of Cognitiva, an industrial wireless protocol that is based on CR principles covering the PHY and MAC layers is presented. The implementation of a software defined radio testbed for the protocol is also described. Cognitiva can be used for reliable wireless communication and is designed with support for multi-channel inter-band and intra-band operation involving TVWS and the 2.4 GHz ISM band. Cognitiva caters for the growing trend of machine-to-machine (M2M) communication and Internet-of-things (IoT) type applications [9], which did not exist a few years ago. This was borne out of a need to connect a wide variety of different devices that run different applications using global communication solutions through the application of Internet Protocol Version 6 (IPv6) [7].

The testbed can be used for rapid prototyping and testing the real world performance of new communication algorithms, such as cooperative spectrum sensing and dynamic spectrum Access. The implementation approach is Open Source and this is freely available to students, researchers, engineers and wireless enthusiasts. This chapter begins with an overview of the design of the Cognitiva protocol, followed by an outline of the testbed

implementation process. Performance characteristics are then presented, related work outlined and comparisons of this work with previous work provided.



(a)



(b)

Figure 4.1. Spectrum occupancy in the (a) 2.4 GHz ISM band and the (b) UHF broadcast television bands.

4.2 DESIGN

The goal in designing the Cognitiva protocol was to create a protocol that can overcome the problem of interference and spectrum scarcity that arises when operating in unlicensed bands. The protocol was supposed to be suitable for use in industrial networks [11] and IoT type deployments. It was supposed to provide efficient spectrum use, multiple access, reliability, interference mitigation, and easy integration with IoT applications. Several techniques were identified to achieve this, including DSM, CSMA, automatic repeat request (ARQ), dynamic frequency selection, spectrum sensing, spread spectrum and large packet payloads. The design was supposed to be flexible enough to allow additional features to be added if desired, such as transmit power control, adaptive rate adaptation and encryption. In the following sections, a description will be provided of the design of the physical layer, the MAC layer and the packet formats.

4.2.1 Physical layer

The protocol was designed to work with low cost, low power and low complexity devices, as is typically found in industrial wireless networks. At the same time, with the passage of time, hardware becomes more and more powerful, which provides room to implement more advanced features on low cost hardware. Two different PHY versions are defined: one uses Offset Quadrature Phase Shift Keying (O-QPSK) modulation; the other uses Gaussian Mean Shift Keying (GMSK). The symbol rate for both of these is 4 MHz. Direct sequence spread spectrum is used as part of the interference mitigation strategy. Data symbols are mapped to a 32-chip PN sequence. The first PHY is similar to the 802.15.4 PHY in terms of modulation and spreading. The second PHY uses a Kasami sequence with generator polynomial $x^{10} + x^3 + 1$ as the spreading sequence. The large Kasami sequence has good properties that make it suitable for a wide range of applications [105].

Multi-band operation is provided for, with the first band of operation being the 2.4 GHz ISM band; the other is the licensed spectrum reserved for TV broadcast. The idea is to have a mode of operation that uses TVWS opportunistically, while avoiding interference

with licensed users. The modulation and spreading of the Cognitiva PHY are shown in Figure 4.2 and the different rates are indicated.

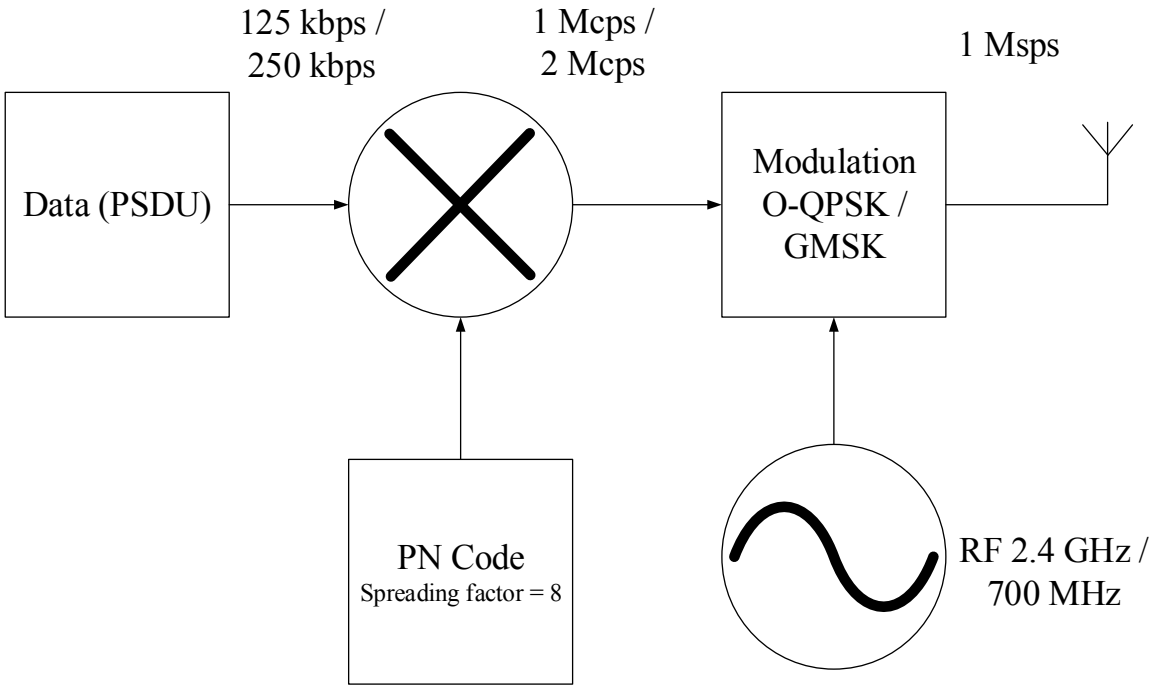


Figure 4.2. Cognitiva PHY spreading and modulation.

Each channel is 2 MHz in width and the channel spacing is 4 MHz. There are 23 channels defined for each band. Figure 4.3 below shows the channels in the 2.4 GHz band. The same scheme is used in the TV band between 690 MHz and 790 MHz.

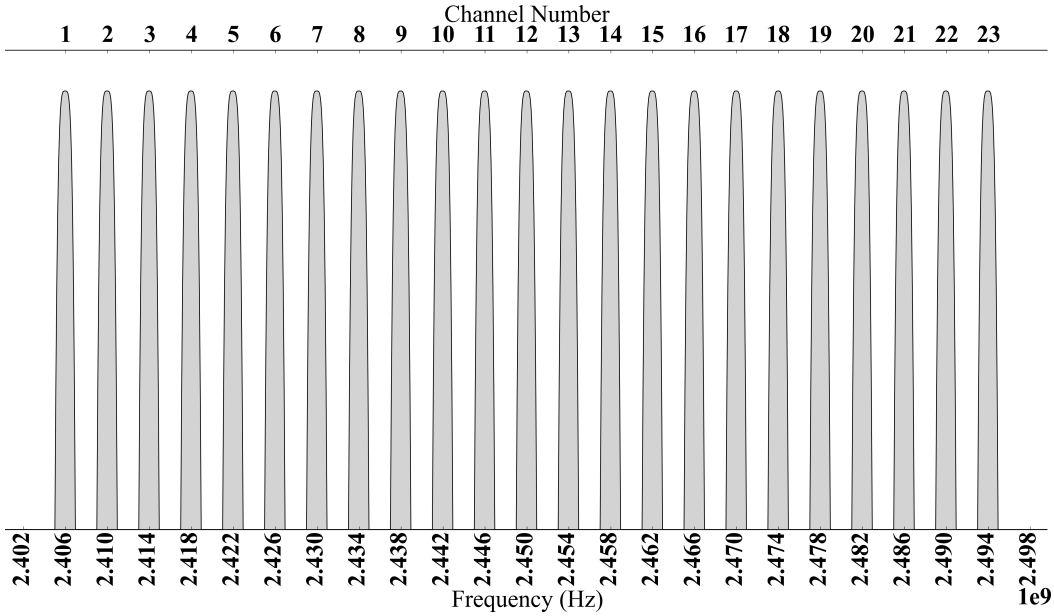


Figure 4.3. Cognitiva channels in the 2.4 GHz ISM band.

Both bands have a bandwidth of 100 MHz. Table 4.1 below shows some of the main properties of the PHY layer.

Table 4.1 PHY Layer Characteristics.

Modulation	O-QPSK	GMSK
Channel bandwidth	2 MHz	2 MHz
Samples per symbol	4	4
Symbol rate	1 MHz	1 MHz
Bits per symbol	2	1
Chip rate	2 Mcps	1 Mcps
Chips per bit	8	8
Data rate	250 kbps	125 kbps

4.2.2 MAC layer

The MAC layer was designed to improve the reliability of wireless communication. Cross-layer design between the PHY and the MAC layer enabled advanced features to be implemented. Stop and wait ARQ was chosen for better reliability, which is a critical requirement in IWSNs, with the MAC layer playing an important role [106]. Such a feature

is not available in 802.15.4, which is used in a number of industrial wireless network standards. Clear channel assessment was used to achieve multiple access through carrier sensing and energy detection; this is similar to the approach used in 802.11 (Wi-Fi).

Four CCA modes were defined, as follows:

1. ALOHA - the channel is always reported as idle.
2. CCA-ED - Energy detection is used to determine if the channel is busy/idle.
3. CCA-CS - Carrier sensing is employed to determine if the channel is busy/idle. This is based on identification of the protocol's synchronization header (SHR) / preamble.
4. CCA-ED-CS - Carrier sensing and energy detection is used. The channel is reported as busy if energy above a certain threshold is detected and a protocol compliant preamble is observed.

The clear channel assessment for 802.11 also includes a ready-to-send (RTS) clear-to-send (CTS) handshake. RTS/CTS introduces an additional overhead, which reduces throughput, and the benefit of reducing retransmissions in the case of a hidden node (through the use of RTS/CTS) may not be worth the additional RTS/CTS frame overhead. Cognitiva provides for RTS/CTS as an option, which may be used if desired. At the MAC layer, a 32-bit CRC checksum is calculated and appended as the trailing field. The checksum is used to detect corrupt packets, which will be dropped.

The flowchart in Figure 4.4 below shows how packets are sent. When using collision avoidance and the transmit state is TX_WAIT or TX_DEFER (which happens when the medium is detected as being busy), then transmission will back-off for a duration derived from the time it takes to send the largest possible packet and obtain an acknowledgement. A random value is added to this inter-packet delay, such that it increases by 50% at most.

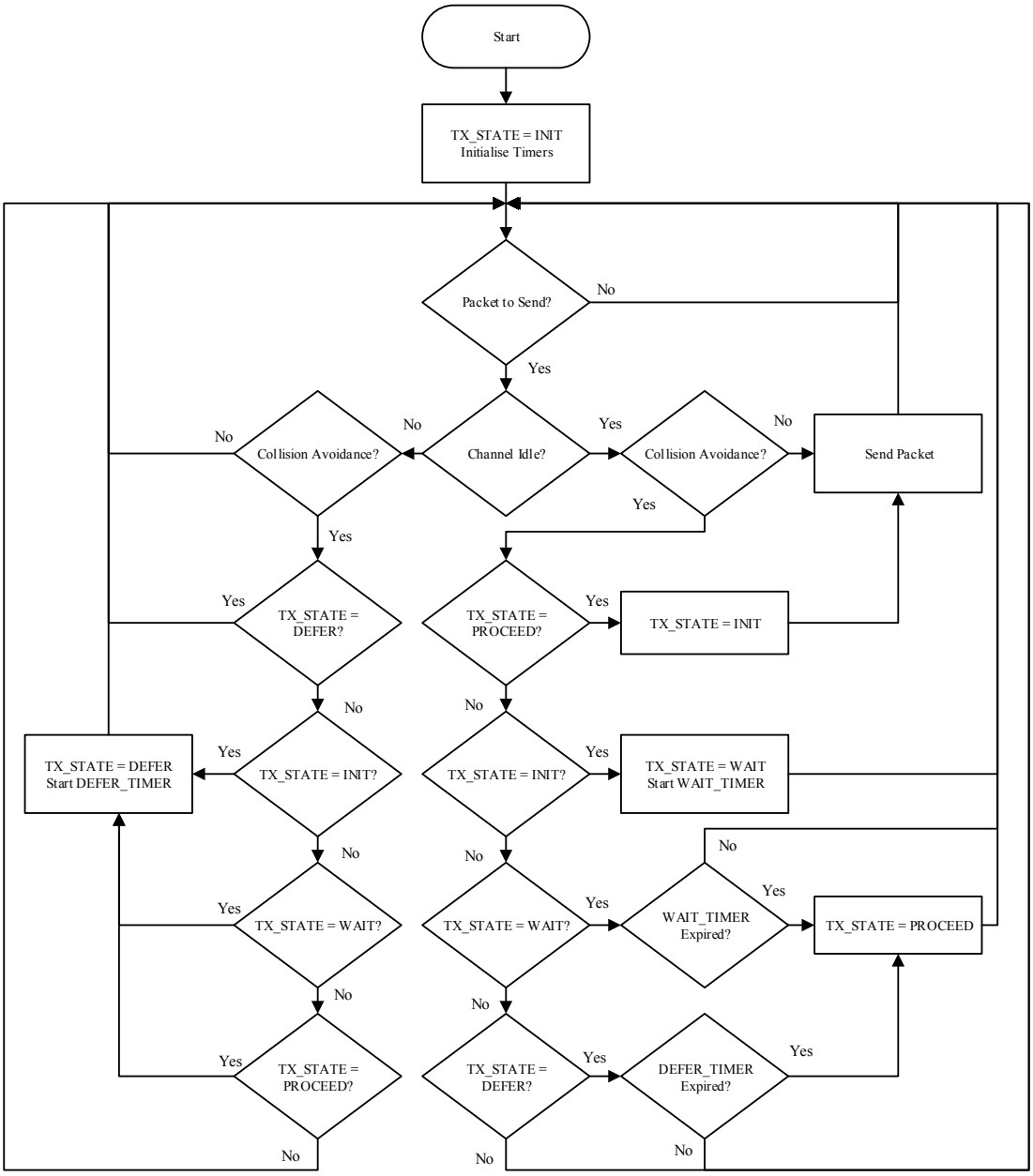


Figure 4.4. Flowchart showing how packets are sent.

4.2.3 Cross layer design

For operation in TVWS, it is necessary to perform spectrum sensing in the licensed spectrum bands and to employ DSM to decide on which spectrum it is best to use. This is in line with what is expected of CRNs. Several algorithms can be developed and used for

DSM. CR is a relatively new field and the goal was to make Cognitiva also serve as a basis for experimenting with different methods of DSA. As such, a cross-layer message passing system was implemented, which can be used to achieve this. Control messages were defined and are passed between the PHY and MAC layers. The PHY layer can send spectrum sensing messages that include a measure of the energy detected in a certain spectrum band, as well as carrier sensing information, which becomes available when a waveform is found that is compliant with the protocol. The MAC layer can send messages about the mode of spectrum sensing to be carried out, as well as the desired band of operation. The messages are summarized in Figure 4.5 below.

4.2.4 Packet format

The maximum packet size defined for Cognitiva is 2048 bytes. The PHY overhead is 10 bytes, which leaves a maximum PHY payload size of 2038 bytes. The MAC overhead is 32 bytes, which leaves a maximum MAC payload size of 2006 bytes. Based on the design, the maximum protocol packet size can be extended to up to 65536 bytes, but the limit is currently set to 2048 bytes, so as to limit packet air-time, which can severely limit network performance, given the modest data rates. The total protocol overhead is 42/2048 = 2.1%.

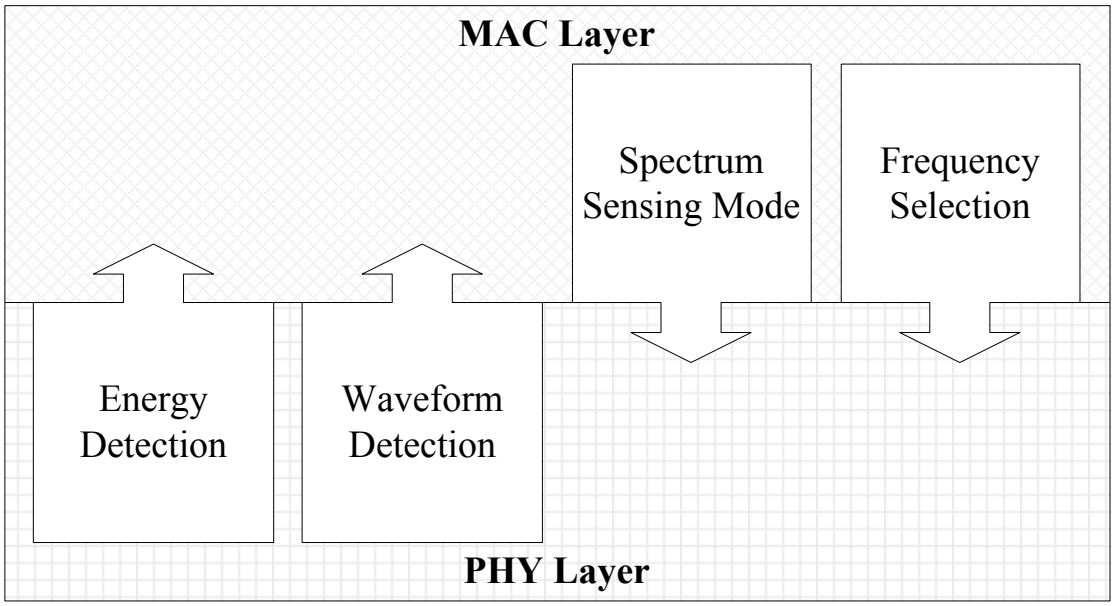


Figure 4.5. Cross layer control messages.

4.2.4.1 PHY protocol data unit

The physical layer protocol data unit (PPDU) comprises a synchronisation header with a preamble sequence of length 6 bytes, followed by a start of frame delimiter that is 2 bytes long. The synchronisation header is followed by a length field of 2 bytes and then the MAC layer protocol data unit (MPDU), which varies in length from 32 bytes to 2038 bytes. The preamble is a sequence of zeros, whereas the start of frame delimiter is 0xF3A0.

4.2.4.2 MAC protocol data unit

The MAC layer protocol data unit comprises a 2-byte frame control field, then a 2-byte sequence number, followed by a source and destination address (MAC address) of 6 bytes each. Two 6-byte network addresses are catered for to implement infrastructure-based networks if desired. Next is the data payload, which can range from 0 bytes to 2006 bytes. Finally, there is a 32-bit frame check sequence for error checking.

4.2.4.3 IoT and IPv6

Global adoption of IPv6 in the future is required for successful deployment of the IoT. IPv6 uses 16-byte addresses and the default IPv6 minimum transmission unit (MTU) is 1280 octets. Cognitiva allows for 6-byte MAC addresses and a maximum data payload size of 2006 bytes, which enables it to carry IPv6 traffic without the need for fragmentation, as is the case, for example, in 6LowPAN.

4.2.4.4 Packet Types

Three packet types are defined, namely data, control and management packets. Each packet type has its own sub-types, as shown in Figure 4.6 below.

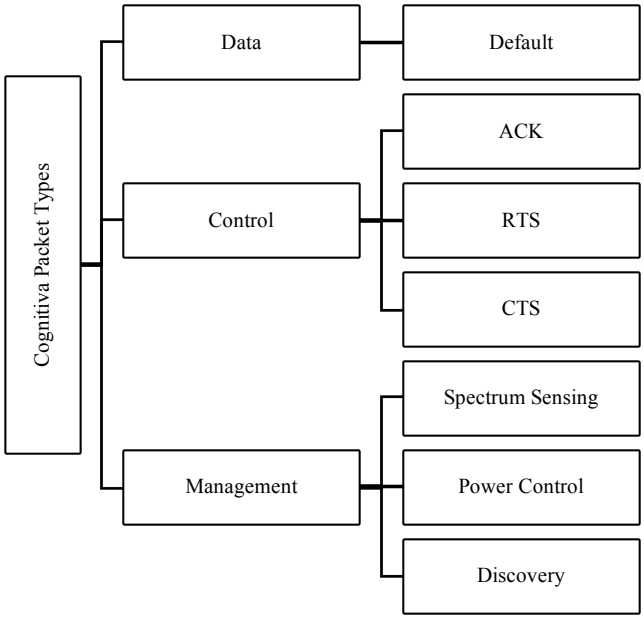


Figure 4.6. Cognitiva packet types.

There is provision for RTS and CTS packets. The breakdown of the different packet fields at the PHY and MAC layer are shown in Figure 4.7. The FCF is further broken down into more fields, as shown in Figure 4.8.

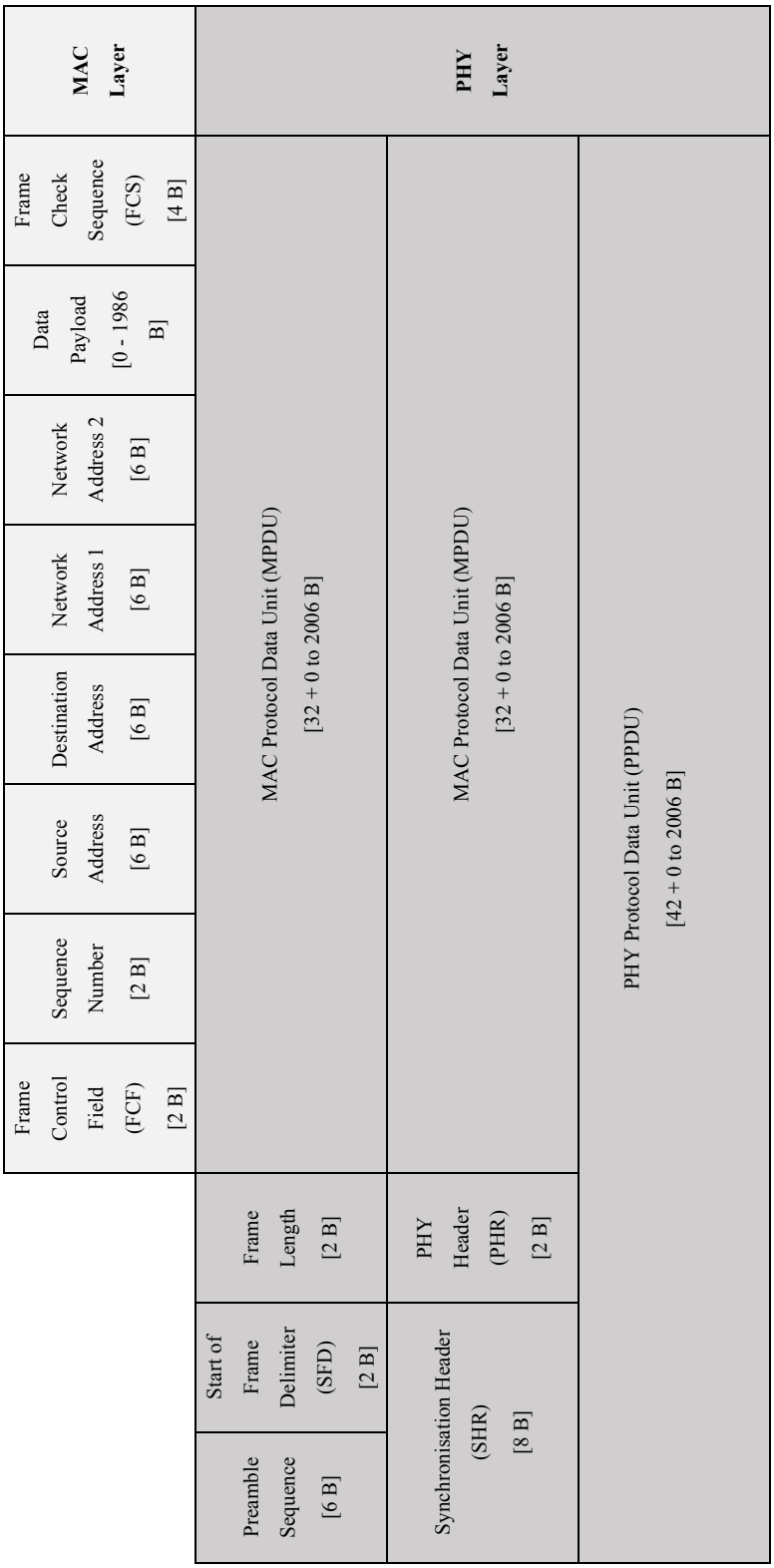


Figure 4.7. Cognitiva packet fields.

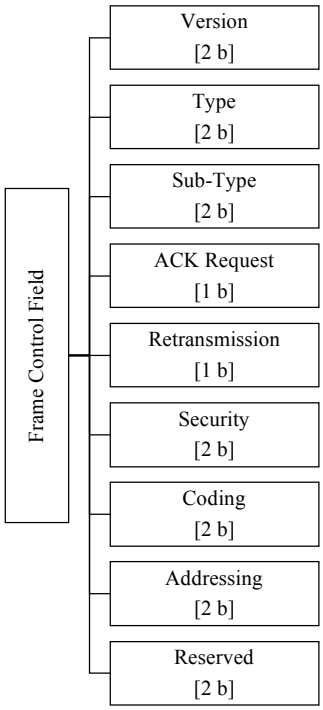


Figure 4.8. Sub-fields of the frame control field.

The **version** field identifies the MAC layer version; the **type** and **sub-type** fields identify the packet type according to the types in Figure 4.6. The **ACK request** field is used if a node requires acknowledgement of the packet sent. The **retransmission** field is used to denote that a packet is being sent again, e.g. when an ACK is not received within the given ARQ interval. The **security** field is used to identify different security mechanisms that may be employed, e.g. a particular type of encryption. The **coding** field is set if a particular type of source coding is applied to the payload. The **addressing** field is for identifying different addressing modes and the last 2 bits of the FCF are reserved for possible future use.

4.3 RELATED WORK

4.3.1 GNU radio based SDR

The authors in [107] presented a SDR testbed based on an IEEE 802.15.4 transceiver. The testbed was open source and interoperable with off-the-shelf TelosB devices. The authors only implemented a minimal 802.15.4 MAC layer that is focused on the most basic

functionality required for connectivity. No CSMA/CA was implemented. The authors in [108] presented an implementation demonstration of an open source IEEE 802.11p stack for broadcast transmissions using SDR. They showed that the performance of their system matched commercial IEEE 802.11p cards. They saw it as a first step towards open source stacks for wireless access in vehicular environments (WAVE) or intelligent transport systems (ITS) G5. The authors later extended their work to demonstrate standards-compliant channel access in [109] by making marginal FPGA modifications, whilst keeping the advantages of a software-based architecture. The latency of SDR systems that can affect standards compliance was studied in [110]. A performance evaluation of 802.11 was presented by [111].

In [112], the authors developed and implemented algorithms for stand-alone detection of UHF TV White Spaces using GNU Radio and Ettus USRP-E110 hardware, the results of which could be accessed remotely using IP networks. An efficient routing protocol for use in a setup with directional antennas in CRNs was investigated in by [113]. They made use of GNU Radio and USRPs to show how sensing results differ with direction at boundary nodes.

In [114], the authors presented a wireless body area network (WBAN) prototype system using GNU Radio and USRP. The prototype could be used to determine the requirements for a system on chip (SoC) solution. Many adjustable parameters were available, including the frequency band, modulation mode, channel number and spreading factor. In [115], the authors developed an adaptive interference avoidance system using SDR and CR principles and demonstrated seamless real-time video transmission using the system.

4.3.2 Industrial wireless network protocols

Popular wireless standards used in industrial networks include ZigBee, WirelessHART, ISA 100.11a and WISA [18, 19]. These protocols offer low to moderate data rates and are mostly based on either the IEEE 802.15.4 or the IEEE 802.15.1 protocols. These protocols are well suited to low power, low cost and low complexity devices. Both of them operate

in the license free 2.4 GHz ISM band and are not designed to operate in TV bands. Recently, IEEE 802.15.4 formed the IEEE 802.15.4m task group that will specify technologies that can enable low rate wireless personal area networks in TVWS [48]. IEEE 802.22 [49] was the first CR standard to be developed, but it is targeted at WRANs and not industrial networks.

One of the design goals of Cognitiva is multi-band operation between TV and ISM bands, which is unlike other IWSN protocols. It is also designed with the IoT in mind. These features may also be incorporated into other IWSN protocols in future; recently Bluetooth 4.2 was released with the addition of key IoT features to the standard. Some of the salient features of Cognitiva are compared with other protocols used as the basis for popular IWSN standards in the Table 4.2. The broad goal was to develop DSA techniques using Cognitiva and the testbed that was developed, which can be integrated with other industrial protocols.

Table 4.2 Comparison of Cognitiva, 802.15.4 and Bluetooth.

	Cognitiva	**IEEE 802.15.4**	**Bluetooth**
Bandwidth	2 MHz	2 MHz	1 MHz/ 2MHz
Channels	23/46	16	40/79
Data Rate	125/250 kbps	250 kbps	1 Mbps
Frequency Bands	2.4 GHz, 690 MHz	2.4 GHz	2.4 GHz

Most SDR protocol implementation that use GNU Radio focus on the physical layer and are stream-based. There has not been a lot of work done on the packed-based mode of communication, but with the recent addition of asynchronous messages in GNU Radio, this is beginning to change; this also allows more work to be done on the MAC layer, as was done in this study. The testbed is compared with other low data rate WPAN SDR implementations in Table 4.3 below.

Table 4.3 Comparison of Cognitiva SDR Testbed and Similar SDR Protocol Implementations.

	Cognitiva	**Schmid** [116]	**Bloessl** [107]
PHY	IEEE 802.15.4 / Custom	IEEE 802.15.4	IEEE 802.15.4
MAC	Extensive	None	Minimal
CSMA	Yes	No	No
ARQ	Yes	No	No
Max. Payload	1988 bytes	245 Bytes	245 Bytes
DFS	Yes	No	No
SS	Yes	No	No

4.4 IMPLEMENTATION

In order to prototype the protocol, a testbed was created using software defined radio. The software is open-source and is freely available online.[1] To create a SDR, it is necessary to have a hardware front-end that can send and receive waveforms. It is also necessary to have software that performs signal processing and message passing. For this purpose, use was made of the USRP™ from Ettus Research as the hardware front-end, and GNU Radio as the software toolkit. The interaction between the two is shown in Figure 4.9 below.

[1] Online source code repository: https://github.com/tchiwewe/cognitiva

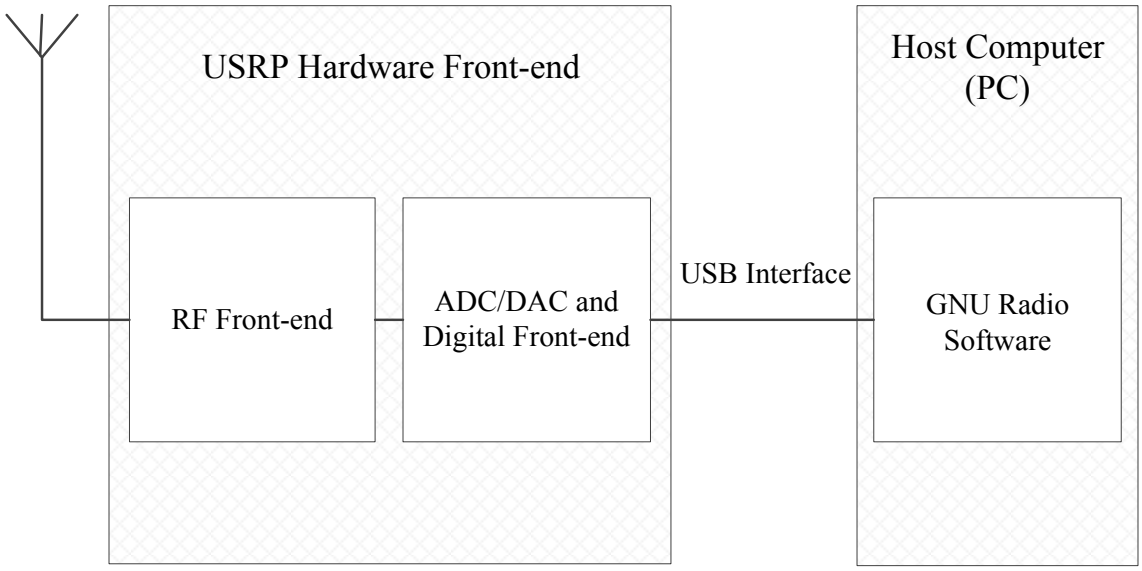


Figure 4.9. USRP and GNU Radio interaction.

GNU Radio is a software development kit (SDK) that provides signal processing and message passing blocks to implement software defined radio. It is free and open source and can be extended with out-of-tree modules, if required [117]. Programs that were written using GNU Radio were then tested on hardware, i.e. USRP devices from Ettus research [117], [118]. The USRPs are comparatively inexpensive hardware platforms for software radio, which have found widespread use. The USRP B100 and USRP B200 models were used; these are shown in Figure 4.10 and Figure 4.11 respectively.

Figure 4.10. USRP B100.

Figure 4.11. USRP B200 in 3rd party enclosure.

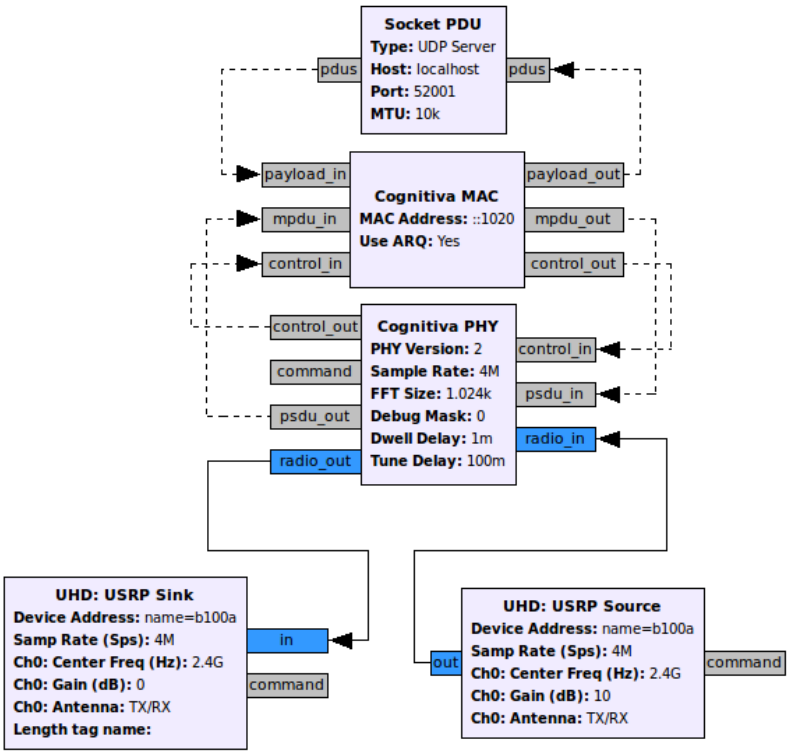


Figure 4.12. A Cognitiva SDR Transceiver in GNU Radio.

These models make use of a USB interface between a host computer and themselves. Several custom GNU Radio blocks were written to implement the Cognitiva design. Figure 4.12 shows a GNU Radio flow graph that was used to create a fully working Cognitiva wireless node. The Cognitiva MAC layer design caters for an ad-hoc wireless mesh network. In Figure 4.13, a dialog is shown of the different properties at the MAC layer that can be adjusted, if desired. The typical experimental set-up consisted of a PC connected to a USRP, which was connected to a suitable antenna. Version 3.7.4 of GNU Radio was used. In the set-up shown in Figure 4.14 below, an Apple MacBook Pro computer with a quad-core 2.4 GHz Intel core i7 processor running Ubuntu 12.04 and a test Cognitiva GNU Radio program was connected to a USRP B100 and a high-gain wideband antenna mounted on a tripod.

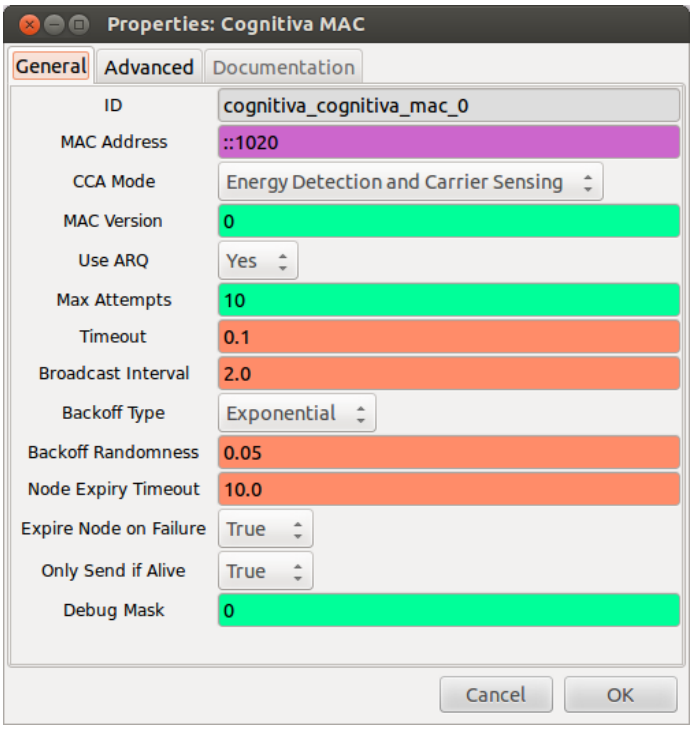


Figure 4.13. GNU Radio dialog showing Cognitiva MAC layer properties that can be set.

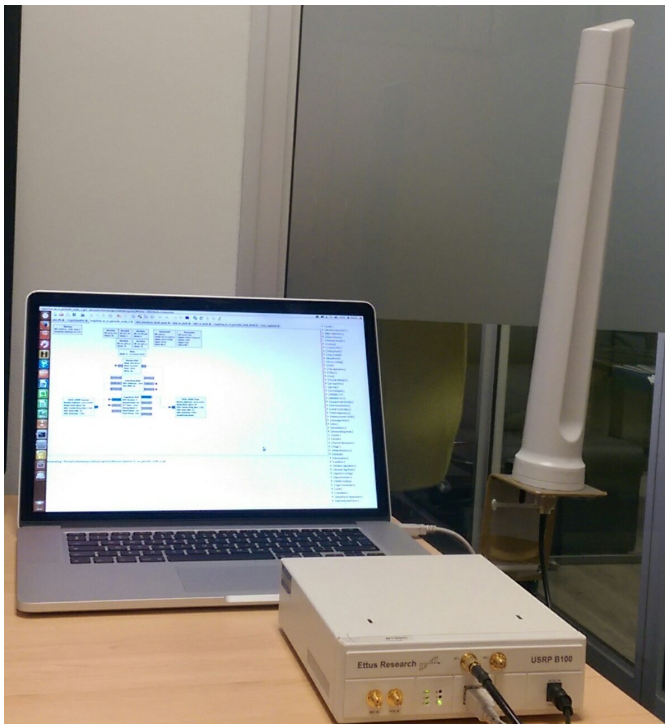


Figure 4.14. Typical setup of a Cognitiva node.

4.5 PERFORMANCE

4.5.1 Choice of parameters

The smallest packet that can be sent is 42 bytes, which is for an acknowledgement (ACK) packet. When using the PHY version with GMSK modulation, this takes 0,002688s to send at 125 kbps. The largest packet of 2048 bytes takes 0,131072s to send. The processing and propagation delay is minimal in comparison. The ARQ timeout must cater for at least the largest packet and an ACK to be sent. The ARQ timeout was set to the time it would take to send the largest packet and two ACKs, which was 0,136448s. Likewise, for energy detection, the detector must at least be able to detect a burst of the smallest packet. This means the dwell delay, which is the time it takes for complex samples to be collected, and their FFTs calculated and averaged, must be a maximum of 0,002688s. A larger dwell delay means that averaging happens over a longer period and fewer cross-layer energy detection messages will be sent for long packets or long energy bursts. The dwell delay was set to 0.002688s, which is the time required to send the smallest packet.

4.5.2 Round-trip times

Table 4.4 Round-Trip Time Required for Different Size Payloads.

Data Payload (bytes)	RTT (s)
200	0.020272
400	0.032622
600	0.045774
800	0.058525
1000	0.071063
1200	0.084119
1400	0.096669
1600	0.109975
1800	0.122638

In Table 4.4, the measured round-trip time for a node to send a packet with a certain payload size and receive an ACK of receipt is given. The nodes were placed 7 meters apart, with line of sight between them.

4.5.3 Packet error rate

In Figure 4.15 below, the measured packet error rates (PERs) for different payload sizes in the ISM and TV bands are shown. In the experiment, 1000 packets were sent when using ALOHA without ARQ. When ARQ was used, 400 packets were sent.

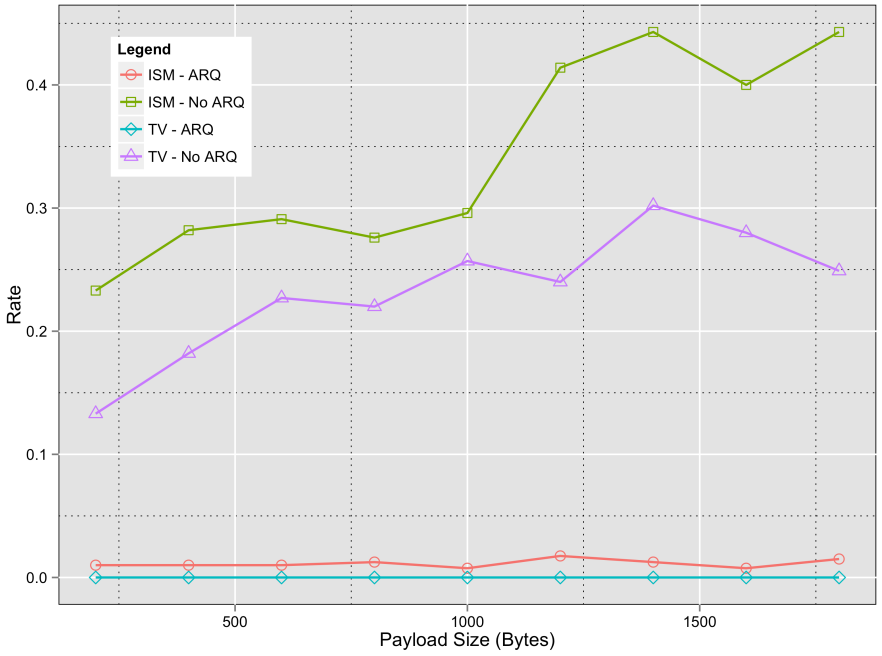


Figure 4.15. Measured PER for different payload sizes in TV and ISM bands, with and without ARQ.

As can be seen above, the packet error rate decreases substantially when ARQ is used, as is to be expected. Some insights can be gathered when looking at the number of packets that actually get retransmitted to achieve such a low PER. This is shown in Figure 4.16 below. The PER measured is dependent on the existing channel conditions. The ISM band is unlicensed and it is to be expected that there will be considerable co-channel interference in this band, hence the PER is higher than in the TV band, which is licensed. A simulation

without the USRP hardware in GNU Radio was run to get an idea of how bad the co-channel interference in the different bands was. Here, an additive white Gaussian noise source was added, with its amplitude set to 25% of its maximum value in GNU Radio. The results are shown in Figure 4.17 below.

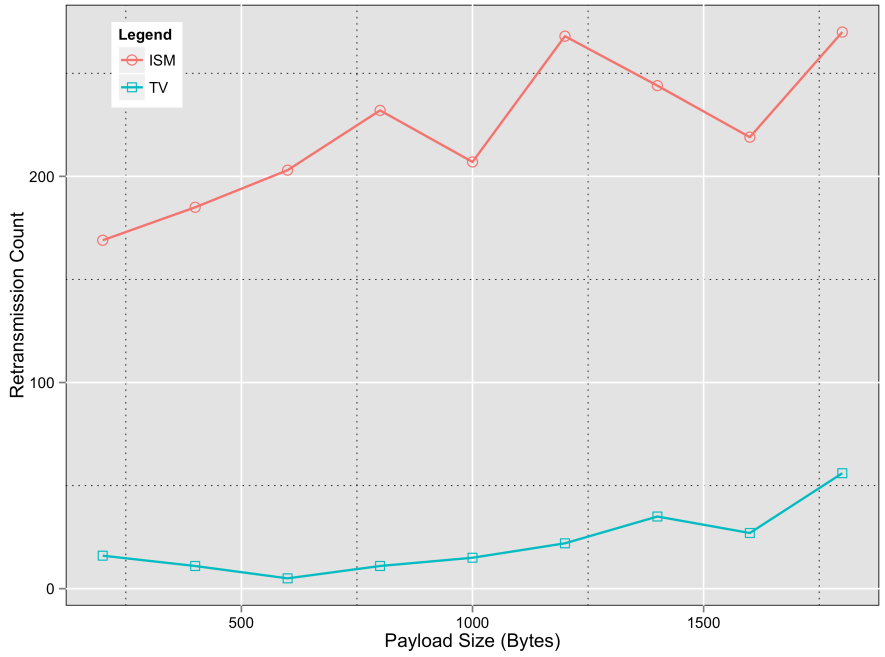


Figure 4.16. Number of ARQ retransmissions recorded in TV and ISM bands.

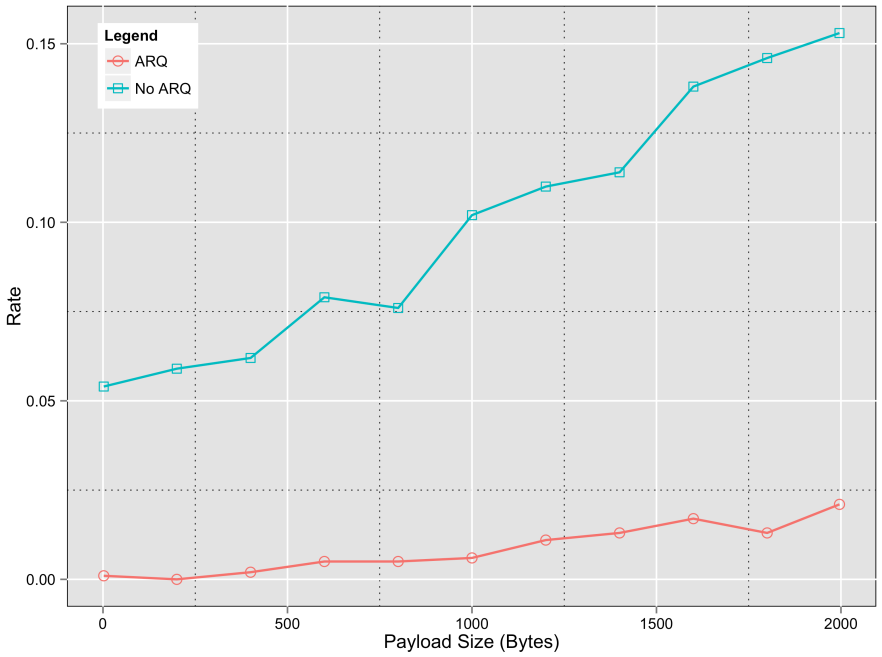


Figure 4.17. Simulated PER for different payload sizes.

Increasing the transmitter gain can be expected to reduce the packet error rate and this was confirmed by the measurements taken in the ISM band, as shown in Figure 4.18.

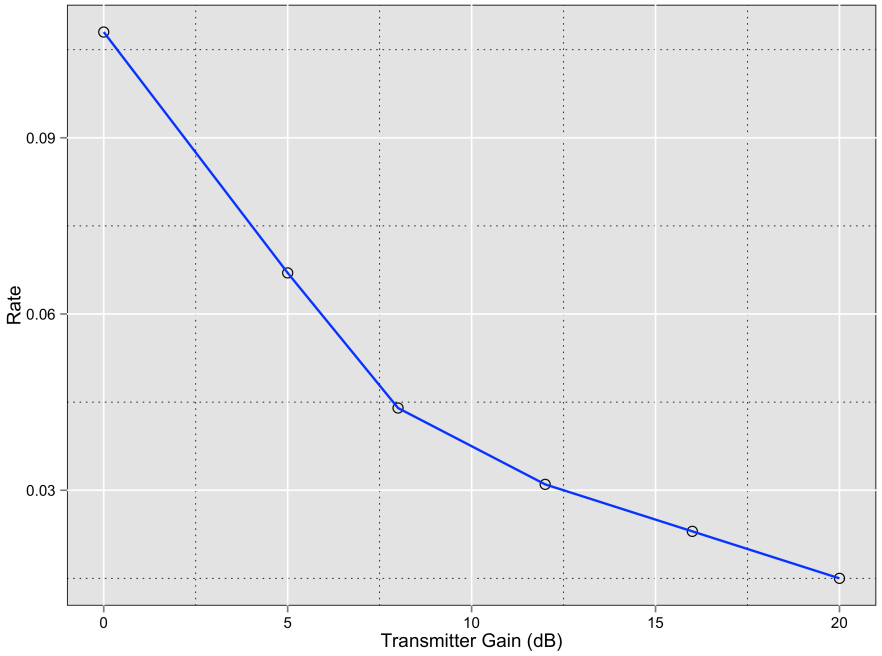


Figure 4.18. Measured PER for different transmitter gains.

4.5.4 Clear channel assessment and collision avoidance

Using techniques such as CCA, ARQ and collision avoidance can increase the reliability of communication, but it results in certain communication overhead.

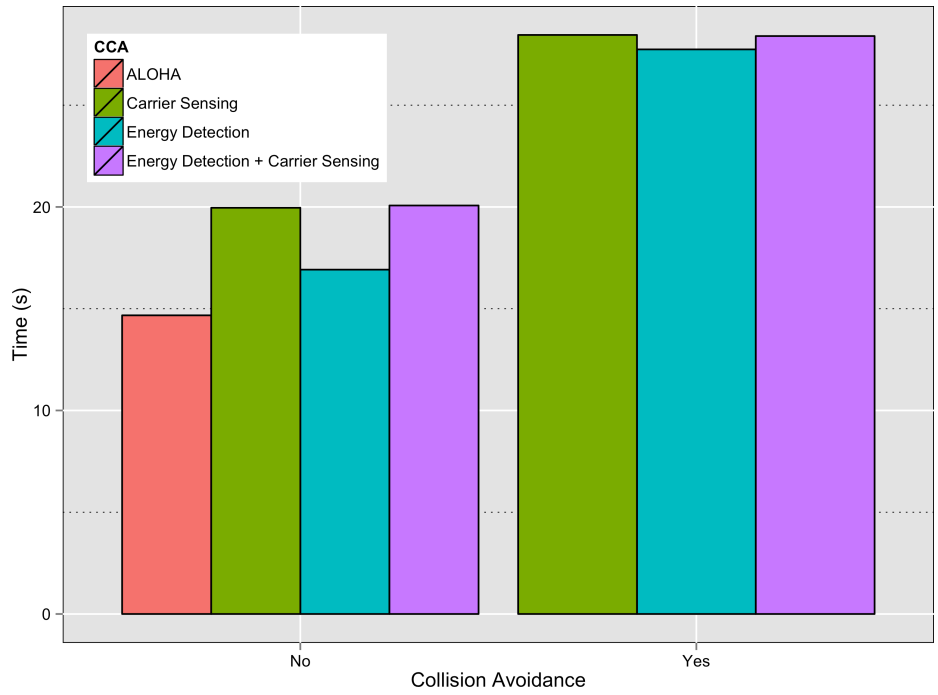


Figure 4.19. Time required to send 100 packets using different combinations of collision avoidance and clear channel assessment modes.

To get an idea of the additional overhead, an observation was made of how long it would take to send 100 packets with a payload size of 1990 bytes when using different combinations of collision avoidance and clear channel assessment modes. The results are shown in Figure 4.19.

4.6 SUMMARY

In this chapter Cognitiva, a wireless protocol for industrial wireless networks that can exploit Television White Spaces for less interference and greater reliability was presented. The Open Source software radio testbed that was developed, which allows the protocol to be tested and different cognitive radio techniques to be investigated with reduced development time, through the re-use of software components, was also covered. New

developments in wireless communications in terms of technology and use cases that call for advances in industrial wireless protocols were highlighted.

CHAPTER 5 FAST CONVERGENCE DYNAMIC SPECTRUM ACCESS

5.1 INTRODUCTION

The radiofrequency spectrum that comprises frequencies from 3 kHz to 300 GHz is regulated by government agencies worldwide, using a fixed spectrum assignment policy, with usage of spectrum being controlled and certain sections of the spectrum being assigned to license holders or to certain services [5]. These restrictions cover prolonged time periods and vast geographic areas. What has been observed is that most of the spectrum is used on an on-off basis and usage tends to be congested in certain sections of the spectrum. This is despite there being spectrum scarcity, as most of the available radiofrequency spectrum has been allocated and the demand for wireless communication is increasing. There are therefore cases of both real and artificial spectrum scarcity [99]. This situation, of spectrum being managed inefficiently due to fixed spectrum assignment schemes, can be overcome by adopting opportunistic approaches to accessing spectrum.

These approaches to reforming the way spectrum is accessed are referred to as Dynamic Spectrum Access strategies. Spectrum management schemes can be categorised as: (i) licensed spectrum for exclusive usage; (ii) licensed spectrum for shared usage; (iii) unlicensed spectrum; and (iv) open spectrum. Traditional spectrum management schemes fall under the first three categories and DSA schemes fall into the fourth category. DSA schemes can be further classified as: (i) dynamic exclusive use; (ii) open sharing; and (iii) hierarchical access.

In the dynamic exclusive use model, portions of the spectrum are licensed for exclusive use by services and users. This is similar to current spectrum regulation policy. There is a difference, however, in that some of the approaches that have been proposed call for spectrum property rights, whereby license holders are free to sell and trade their spectrum and to select the technology they use. Other approaches in this model call for dynamic spectrum allocation, whereby spatio-temporal properties of distinct services are exploited

to improve spectrum efficiency. In the open sharing (spectrum commons) model, all users are peers with the same spectrum access rights and open sharing is employed; this is similar to the operation that currently exists of devices in the ISM radio band. With the hierarchical access model, there is a hierarchy in the network, with primary users (licensees) having special access rights, but secondary users do not and instead they are allowed access to licensed spectrum provided they minimise interference to primary users. The overlay and underlay approaches to spectrum sharing, with spectrum whitespaces being exploited opportunistically and low transmission power being used respectively, fall under this model. The hierarchical model lends itself well to use with legacy wireless systems, whilst allowing for the adoption of dynamic spectrum access techniques.

Dynamic spectrum access is an important application of Cognitive Radio and covers many spectrum management aspects, as shown in Figure 5.1. In this chapter, a scalable dynamic spectrum access scheme is presented that allows for opportunistic spectrum access. As a basis, the work on a hedonic coalition formation game for cooperative spectrum sensing and channel access by [83] is used and improvements to the proposed technique for better performance are presented.

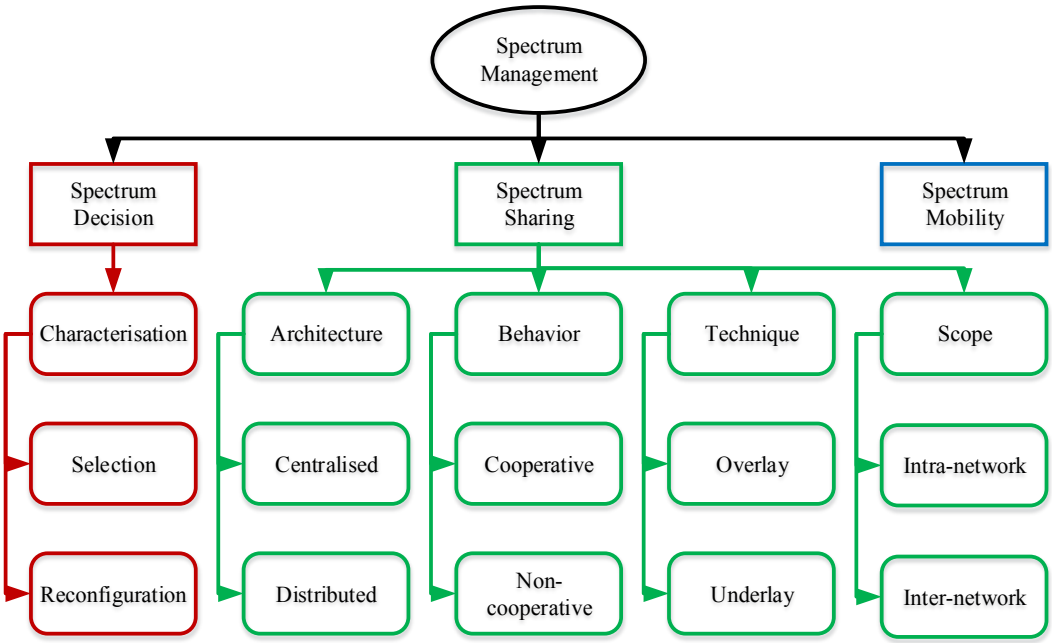


Figure 5.1. Spectrum management aspects.

5.2 SYSTEM MODEL

5.2.1 Network architecture

The network architecture is composed of two types of users: primary users that are licensed; and secondary users that are unlicensed. The SUs opportunistically use spectrum bands that are licensed for use by PUs. The spectrum bands are divided into a number of channels with each having a fixed frequency bandwidth. There are C non-overlapping licensed channels in total and D SUs in the network ($D \geq C$). The set of PUs is $\mathcal{C} \in \{1, \ldots, C\}$ and the set of SUs is $\mathcal{D} \in \{1, \ldots, D\}$. Each licensed channel has a PU operating in it that can either be active or inactive - denoted by $PU_i, i \in \mathcal{C}$ - and the channel bandwidth is B_i. Different example network configurations are shown in Figure 5.2, Figure 5.3 and Figure 5.4.

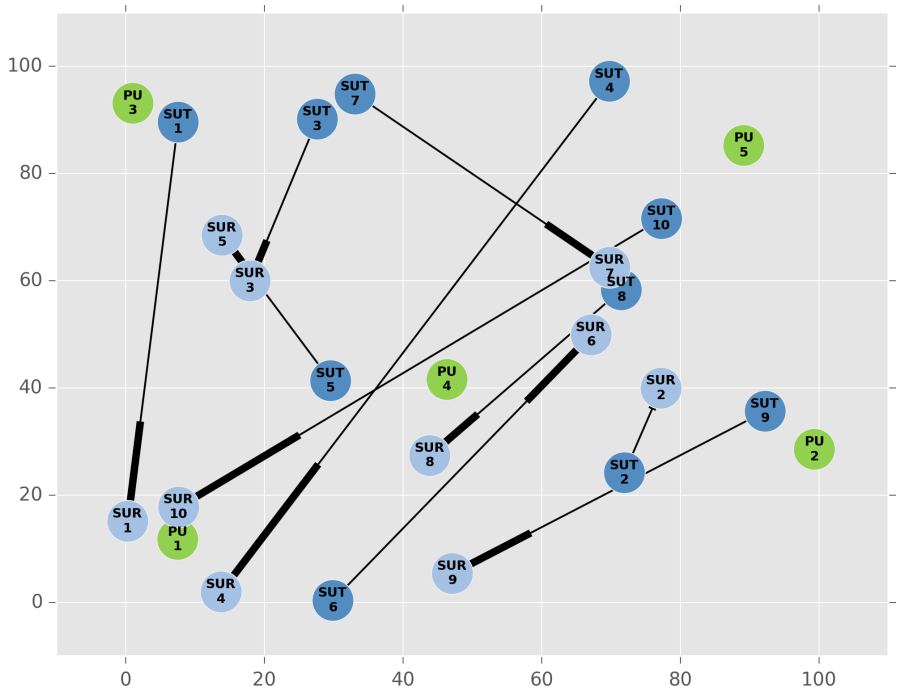


Figure 5.2. Network with 5 PUs and 10 SUs.

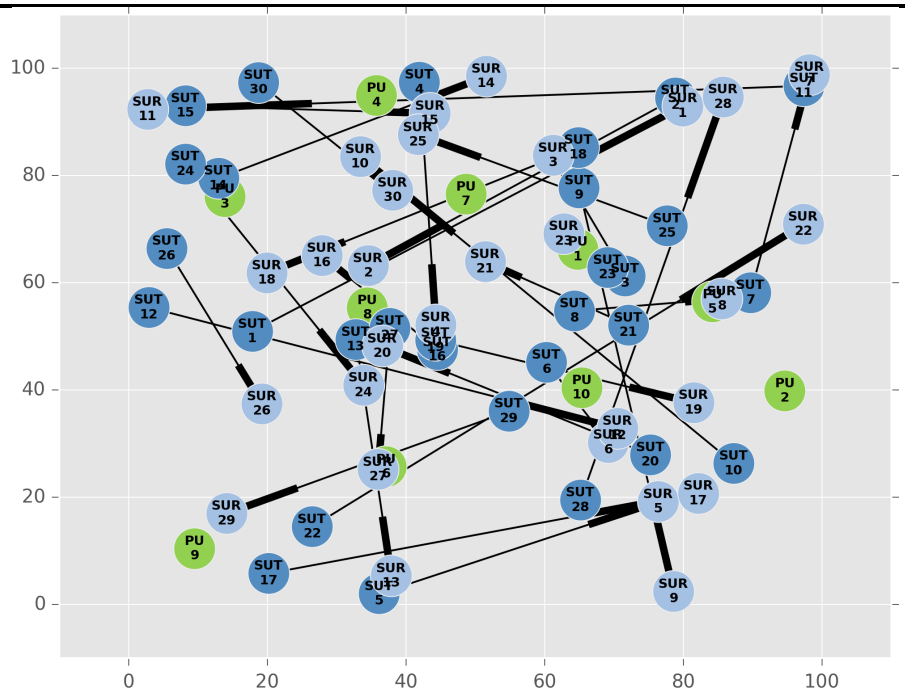


Figure 5.3. Network with 10 PUs and 30 SUs.

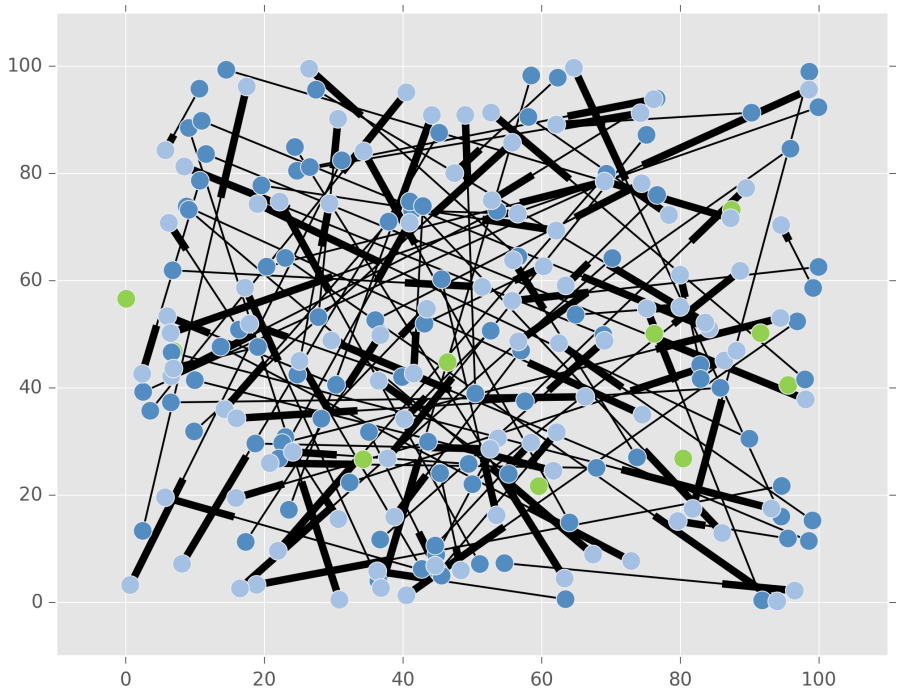


Figure 5.4. Network with 10 PUs and 100 SUs.

5.2.2 Channel occupancy model

The status of each channel is represented using a usage model in which the channel switches between being busy and being idle. To detect spectrum holes and avoid causing interference to PUs, it is necessary for SUs to perform spectrum sensing before transmission. The SUs are located in the vicinity of the PUs and each SU is denoted by $SU_j, j \in \mathcal{D}$. A SU accesses one of the C channels only when it is idle. If PU_i is present in the channel of interest i, $i \in \mathcal{C}$ this is denoted by $H_{1,i}$; if PU_i is absent, this is denoted by $H_{0,i}$. An assumption is made that a SU always has data to send. Another assumption is that each user has a single transceiver that operates in half duplex mode in a single channel at any instance. Each SU is required to have spectrum agility and to be capable of dynamic frequency selection and able to change channels with minimal latency. The probability that PU_i is active is denoted as $P_{H_{1,i}}$; the probability that it is idle is denoted as $P_{H_{0,i}}$. It follows that $P_{H_{1,i}} + P_{H_{0,i}} = 1$. The status of a given channel, i, is described in the Markov chain shown in Figure 5.5.

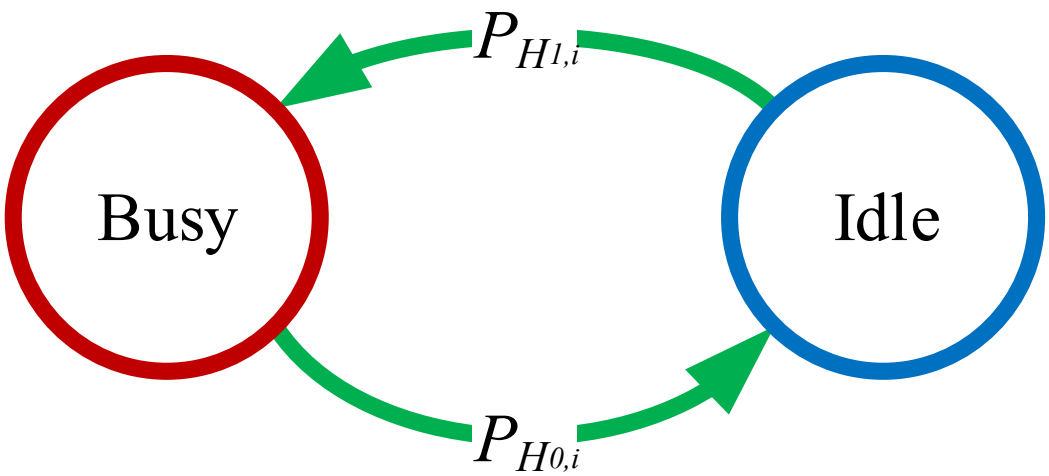


Figure 5.5. Markov chain for channel status.

5.3 SPECTRUM SENSING

5.3.1 Individual spectrum sensing

To determine the status of channels, spectrum sensing is performed. Energy detection is used as the spectrum sensing technique, due to its low implementation complexity and minimal runtime overhead [119]. When using energy detection for spectrum sensing, and given a detection threshold ε with test statistic y, the *probability of detection* and the *probability of false alarm* are defined as:

$$P_d = \Pr(y > \varepsilon | H_{1,i}), P_f = \Pr(y > \varepsilon | H_{0,i}). \quad (5.1)$$

The case under consideration is that of complex valued Phase Shift keying (PSK) signals, Circularly Symmetric Complex Gaussian (CSCG) noise that is an independent and identically distributed random process in each channel $i, i \in \mathcal{C}$ with a mean of zero and a variance of $\sigma_{n,i}^2$. The bandwidth of each channel is B_i and the power spectral density is N_0, which gives $\sigma_{n,i}^2 = N_0 B_i$. Each PU signal $PU_i, i \in \mathcal{C}$ is an independent and identically distributed random process, with a zero mean and a variance of $\sigma_{s,i}^2$. The signal to noise ratio of PU_i measured by a given secondary user, $SU_j, j \in \mathcal{D}$, under the hypothesis $H_{1,i}$; an average channel gain between PU_i and SU_j of $|g_{i,j}|^2$ is given by $\gamma_{i,j} = |g_{i,j}|^2 \sigma_{s,i}^2 / \sigma_{n,i}^2$. Narrowband sensing is considered where each SU senses one channel per time frame. Each frame has a duration of T and each SU has a sensing duration δ, which is non-zero and less than T. The time left for data transmission is therefore $T - \delta$. The sampling frequency for received signals is f_s and the sensing duration and frame duration are multiples of the sample time, i.e. $\frac{1}{f_s}$. It follows that the number of samples during spectrum sensing is δf_s.

Given the above, the probability of false alarm for a channel $i, i \in \mathcal{C}$ and $SU_j, j \in \mathcal{D}$ is given by

$$P_{f,i,j}(\varepsilon, \delta, \sigma_{n,i}^2) = \Pr(y_{j,i} > \varepsilon | H_{0,i}) = Q((\varepsilon/\sigma_{n,i}^2 - 1)\sqrt{\delta f_s}). \quad (5.2)$$

In the above equation: $Q(.)$ is the complementary distribution function of the standard Gaussian; and $y_{j,i}$ is the test statistic for the energy detector of SU_j in channel $i \in \mathcal{C}$. Given the same sensing duration δ and detection threshold ε for all SUs and the same bandwidth

B_i for all PUs, then the probability of false alarm $P_{f,i,j}(\varepsilon, \delta, \sigma_{n,i}^2)$ is the same for all channels and all SUs, i.e. $\forall i \in \mathcal{C}, \forall j \in \mathcal{D}$. The probability of detection for a channel $i, i \in \mathcal{C}$ and $SU_j, j \in \mathcal{D}$ given by

$$P_{d,i,j}(\varepsilon, \delta, \sigma_{n,i}^2, \gamma_{i,j}) = \Pr(y_{j,i} > \varepsilon | H_{1,i}) = Q((\varepsilon/\sigma_{n,i}^2 - \gamma_{i,j} - 1)\sqrt{\delta f_s/(2\gamma_{i,j} + 1)}). \quad (5.3)$$

The receiver operating characteristic (ROC) curve for energy detector based spectrum sensing is shown in: Figure 5.6 for different SNR values; Figure 5.7 for different values of sensing duration, where a higher sensing duration implies that a higher number of samples is collected. It can be seen that a higher SNR and a greater number of samples results in better performance of the energy detector.

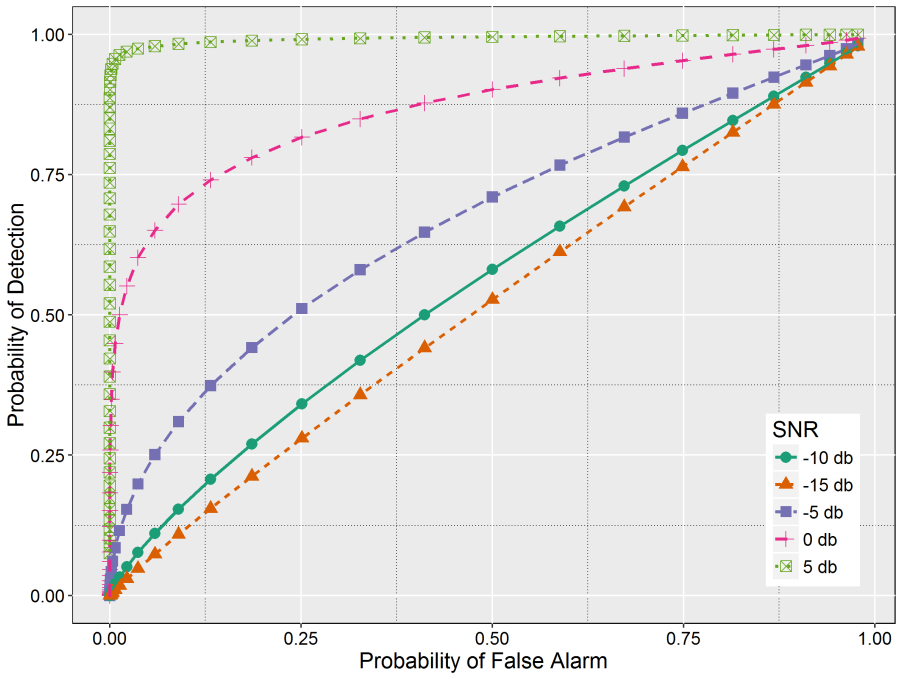


Figure 5.6. ROC for spectrum sensing at different values of SNR.

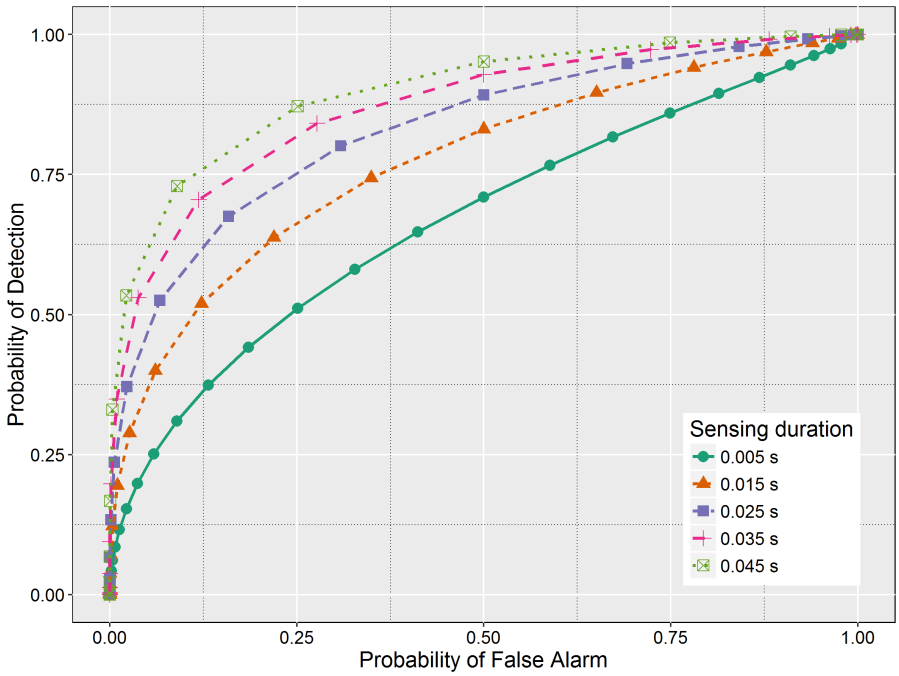


Figure 5.7. ROC for spectrum sensing at different values of sensing duration.

5.3.2 Cooperative spectrum sensing

Cooperative spectrum sensing, where SUs cooperate with one another, can be used to increase the performance of spectrum sensing [120]. CSS can help overcome the problems of fading, shadowing and hidden terminals. Each channel has a decision node (DN) that is selected in each time-frame on expiry of the sensing period. The decision node is selected from among the SUs in a given channel i, the set of which is denoted by $\mathcal{A}_i$ with $\mathcal{A}_i \subseteq \mathcal{D}, \forall i \in \mathcal{C}$ and $\bigcup_{i\in\mathcal{C}} \mathcal{A}_i = \mathcal{D}$. $DN_i, i \in \mathcal{C}$ is responsible for determining whether the channel i, is busy or idle, based on sensing results from other SUs that sense the channel. Different decision fusion rules can be used including the: AND rule, OR rule, soft combination rule, majority rule, and the *k*-out-of-*n* rule [121]. The *k*-out-of-*n* rule becomes the AND rule, OR rule and majority rule when *k* is *1*, *n* and $\geq$ *n/2* respectively.

Considering the OR rule, if at least one SU presumes that a PU is present in a channel, then the channel is considered to be busy. In this case, for channel $i, i \in \mathcal{C}$, the *probability of detection* and the *probability of false alarm* are defined as

$$P_{f,i} = 1 - \prod_{j \in \mathcal{A}_i} (1 - P_{f,i,j}(\varepsilon, \delta, \sigma_{n,i}^2)), \tag{5.4}$$

$$P_{d,i} = 1 - \prod_{j \in \mathcal{A}_i} (1 - P_{d,i,j}(\varepsilon, \delta, \sigma_{n,i}^2, \gamma_{i,j})). \tag{5.5}$$

Considering the AND rule, there needs to be consensus among SUs that a PU is present in a channel for it to be considered as being busy. For a channel $i, i \in \mathcal{C}$ the *probability of detection* and *probability of false alarm* are defined as

$$P_{f,i} = \prod_{j \in \mathcal{A}_i} (P_{f,i,j}(\varepsilon, \delta, \sigma_{n,i}^2)), \tag{5.6}$$

$$P_{d,i} = \prod_{j \in \mathcal{A}_i} (P_{d,i,j}(\varepsilon, \delta, \sigma_{n,i}^2, \gamma_{i,j})). \tag{5.7}$$

The OR rule is suitable for a conservative approach where high priority is placed on protecting PUs, whereas the AND rule is suitable for an aggressive approach that seeks to maximise spectrum access opportunities for SUs. Making use of the OR rule gives a higher probability of detection, whereas making use of the AND rule gives a lower probability of false alarm. If DN_i decides that PU_i is active, then all SUs, $SU_j, \forall j \in \mathcal{A}_i$ operating in the channel are not permitted to transmit during the time-frame period. If, on the other hand, DN_i decides that the channel is idle, then all the SUs operating in the channel have an equal opportunity to access the channel, i.e. the probability of transmitting for each SU, $SU_j, \forall j \in \mathcal{A}_i$ is $1/|\mathcal{A}_i|$.

5.4 SPECTRUM SHARING

5.4.1 Hedonic coalition formation

In [83], the authors present a multi-channel coalition formation game for spectrum sensing and access, which terminates at a final partition that is individually stable and Nash stable. Considering a channel i with a SU transmit power of P_{su}, a SU sensing power of P_{ss}, a noise power of $\sigma_{n,i}^2$, and an average channel gain of $|h_{j,i}|$ between a SU transmitter and receiver pair j in channel i, the rate of transmission can be represented as [83]:

$$R_{j,i} = B\ log_2\left(1 + |h_{j,i}|^2 \frac{P_{su}}{\sigma_{n,i}^2}\right). \tag{5.8}$$

For a set $\mathcal{A}_i$, the payoff is the difference between the reward and the penalty, where: the reward is defined as the amount of data that is transmitted by the SUs in $\mathcal{A}_i$; and the penalty is given by λ, where $\lambda > 0$ is defined as the unity penalty factor per second that is applied when a PU transmission is interfered with. The 4 possible scenarios in channel i regarding the decision of DN_i and the activity of PU_i are:

1. DN_i makes a decision that channel i is idle and PU_i is silent, i.e. a true negative, which occurs with probability $P_{0|0,i} = P_{H_{0,i}}(1 - P_{f,i})$.
2. DN_i makes a decision that channel i is busy and PU_i is silent, i.e. a false positive, which occurs with probability $P_{1|0,i} = P_{H_{0,i}}P_{f,i}$.
3. DN_i makes a decision that channel i is idle and PU_i is active, i.e. a false negative, which occurs with probability $P_{0|1,i} = P_{H_{1,i}}(1 - P_{d,i})$.
4. DN_i makes a decision that channel i is busy and PU_i is active, i.e. a true positive, which occurs with probability $P_{1|1,i} = P_{H_{1,i}}P_{d,i}$.

In the first scenario, which corresponds to a true negative decision by the decision node, the SU transmission proceeds successfully and there is no penalty, since no PU transmission is interfered with. The payoff in this scenario for set $\mathcal{A}_i$ is $r_{0|0}(\mathcal{A}_i) = \frac{\sum_{j\in\mathcal{A}_i} R_{j,i}}{|\mathcal{A}_i|}(T - \delta)$ and the energy consumption for the set is $e_{0|0}(\mathcal{A}_i) = P_{ss}|\mathcal{A}_i|\delta + P_{su}(T - \delta)$.

In the second scenario, which corresponds to a false positive decision being made by the decision node, there is no SU transmission, resulting in no reward, and there is no penalty, since no PU transmission is interfered with. The payoff in this scenario for set $\mathcal{A}_i$is $r_{1|0}(\mathcal{A}_i) = 0$ and the energy consumption for the set is $e_{1|0}(\mathcal{A}_i) = P_{ss}|\mathcal{A}_i|\delta$.

In the third scenario, which corresponds to a false negative decision being made by the decision node, the SU transmission proceeds at the same time as PU transmission and they interfere with one another. As a result, there is no reward and a penalty is applied. The payoff in this scenario for set $\mathcal{A}_i$ is $r_{0|1}(\mathcal{A}_i) = -\lambda(T - \delta)$ and the energy consumption for the set is $e_{0|1}(\mathcal{A}_i) = P_{ss}|\mathcal{A}_i|\delta + P_{su}(T - \delta)$.

In the fourth scenario, which corresponds to a true positive decision being made by the decision node, there is no SU transmission and PU transmission proceeds with no interference. As a result, there is no reward or penalty. The payoff in this scenario for set $S_i$is $r_{1|1}(\mathcal{A}_i) = 0$ and the energy consumption for the set is $e_{1|1}(\mathcal{A}_i) = P_{ss}|\mathcal{A}_i|\delta$.

The payoff that is expected in each frame, when considering all four scenarios, is:

$$\begin{aligned} r(\mathcal{A}_i) &= \sum_{a=0}^{1}\sum_{b=0}^{1} P_{a|b,i} r_{a|b}(\mathcal{A}_i) \\ &= P_{0|0,i}\frac{\sum_{j\in\mathcal{A}_i} R_{j,i}}{|\mathcal{A}_i|}(T-\delta) - P_{0|1,i}\lambda(T-\delta). \end{aligned} \tag{5.9}$$

The expected energy consumption per frame is as follows, when taking into account all four scenarios:

$$\begin{aligned} e(\mathcal{A}_i) &= \sum_{a=0}^{1}\sum_{b=0}^{1} P_{a|b,i} e_{a|b}(\mathcal{A}_i) \\ &= P_{ss}|\mathcal{A}_i|\delta + \left(P_{0|0,i} + P_{0|1,i}\right)P_{su}(T-\delta). \end{aligned} \tag{5.10}$$

The value function of set $\mathcal{A}_i$ is defined as the ratio of the expected payoff to the expected energy consumption; this is given by:

$$\begin{aligned} v(\mathcal{A}_i) &\triangleq \frac{r(\mathcal{A}_i)}{e(\mathcal{A}_i)} \\ &= \frac{P_{0|0,i}\sum_{j\in\mathcal{A}_i} R_{j,i}\,(T-\delta) - |\mathcal{A}_i|P_{0|1,i}\lambda(T-\delta)}{|\mathcal{A}_i|\left(P_{ss}|\mathcal{A}_i|\delta + \left(P_{0|0,i} + P_{0|1,i}\right)P_{su}(T-\delta)\right)}. \end{aligned} \tag{5.11}$$

Since all SUs in a given channel sense and access the channel with the same probability, the utility that they receive is the same, and the utility function is defined as:

$$u_j^{\mathcal{A}_i} = \frac{v(\mathcal{A}_i)}{|\mathcal{A}_i|}. \tag{5.12}$$

5.4.2 Coalition formation algorithm

The problem of cooperative multi-channel spectrum sensing and access can be modelled using coalition game theory. The set $\mathcal{A}_i$ represents coalition i and there are C coalitions in

total. Each SU is a member of one coalition and there is one coalition per channel. The basic components of the game are as follows:

- A set of $\mathcal{D}$ players, which are the SUs $SU_j, j \in \mathcal{D}$.
- A set of strategies for each SU, which is the channel it decides to sense and access.
- A utility function, which is given in (5.12) for each SU.

The algorithm for channel sensing and access is given below.

Algorithm 5.1 Coalition formation algorithm
Executed by $SU_j, j \in \mathcal{D}$

Initialisation: $\mathcal{A}_1^0 \coloneqq \mathcal{D}, \mathcal{A}_l^0 \coloneqq \emptyset, \forall l \in \mathcal{C}\{1\}$

for iteration r:= 1 to *MAX* **do**

$\mathcal{A}_j^{(r)} \coloneqq \mathcal{A}_j^{(r-1)}$ where $i \in \mathcal{C}$ and $\mathcal{A}_j^{(r)} j \in \mathcal{A}_i^{(r)}$

SU_j generates θ_j which is a standard normal random variable

SU_j selects a random channel α_j other than its current channel such that $\alpha_j \in \mathcal{C}$ and $\alpha_j \neq i$

SU_j broadcast details on θ_j and α_j to other SUs, $SU_k, \forall k \in \mathcal{D}, k \neq j$

SU_j receives details on θ_k and α_k from other SUs, $SU_k, \forall k \in \mathcal{D}, k \neq j$

SU_j requests and receives details on $\mathcal{S}_l^{(r)} \forall l \in \mathcal{C}, l \neq i$

m:=arg $\max_w \theta_w, \forall w \in \mathcal{A}_i^{(r)}$

if $SU_j = SU_m$ **then**

$\mathcal{Z} \coloneqq \emptyset$

$\mathcal{Z} \coloneqq \mathcal{Z} \cup \{q\}$, q:=arg $\max_q \theta_q, \forall q \in \mathcal{A}_k^{(r)}, \forall k \in \mathcal{D}, k \neq i$

$\mathcal{Z} \coloneqq \mathcal{Z} \backslash \{p\}, \forall p \in \mathcal{Z}, \theta_p < \theta_j$

if $i \neq \alpha_k \forall k \in \mathcal{Z}$ **then**

if $\alpha_j \neq \alpha_k \forall k \in \mathcal{Z}$ **then**

SU_j computes $x_j^{\mathcal{S}_i^{(r)}} \coloneqq v(\mathcal{A}_i^{(r)})/|\mathcal{A}_i^{(r)}|$

$\mathcal{A}_i^{(r)} \coloneqq \mathcal{A}_i^{(r)} \backslash \{j\}$

$\mathcal{A}_{\alpha_j}^{(r)} \coloneqq \mathcal{A}_{\alpha_j}^{(r)} \cup \{j\}$

if $\mathcal{A}_{\alpha_j}^{(r)} \in h(j)$ **then**

$\mathcal{A}_{\alpha_j}^{(r)} \coloneqq \mathcal{A}_{\alpha_j}^{(r)} \backslash \{j\}$

$\mathcal{A}_i^{(r)} \coloneqq \mathcal{A}_i^{(r)} \cup \{j\}$

else

SU_j computes $u_j^{\mathcal{A}_{\alpha_j}^{(r)}} \coloneqq v(\mathcal{A}_{\alpha_j}^{(r)})/|\mathcal{A}_{\alpha_j}^{(r)}|$

if $u_j^{\mathcal{A}_{\alpha_j}^{(r)}} \leq u_j^{\mathcal{A}_i^{(r)}}$ **then**

25: $\mathcal{A}_{\alpha_j}^{(r)} := \mathcal{A}_{\alpha_j}^{(r)} \backslash \{j\}$

26: $\mathcal{A}_i^{(r)} := \mathcal{A}_i^{(r)} \cup \{j\}$

27: **end if**

28: **end if**

29: **end if**

30: **end if**

31: **end if**

32: SU_j adds its current coalition to $h(j)$

33: **end for**

The algorithm above provides some improvements to the hedonic coalition formation algorithm on which it is based. The key improvement is faster convergence time. This is achieved by allowing multiple SUs to perform channel sensing and access during one time frame. Multiple SUs can perform channel sensing and access at the same time, without sensing and accessing the same channels. As a result, there is no contention or instability in the network. Additional message passing needs to occur. In particular, apart from SUs sharing a standard random standard normal number that they each generate, they also share details on the channels they would like to sense. In addition, instead of a node requesting and acquiring information on the coalition it would like to join, it must do so for all coalitions.

5.5 PERFORMANCE

5.5.1 Simulation parameters

The nodes in the network were randomly distributed in a square area with dimensions 100m x 100m. The original algorithm was compared to the new algorithm for dynamic spectrum sensing and access. The main metric used for comparison was the average utility of SUs in the network. Different simulation parameters were varied to determine their effect on the average network SU utility. The default simulation parameters that were used are shown in Table 5.1.

When investigating the effect of the number of iterations on the average network utility, the algorithms were run up to 300 iterations, where it was observed that they were close to converging to a point of equilibrium where the average utility remains stable. The simulations were run 1000 times and the results were averaged. When investigating the effects of varying some of the simulation parameters, the algorithms were run to 200 iterations, where it was observed that they were not yet close to a point of equilibrium and the benefit of using one algorithm over the other was more pronounced. The original algorithm for dynamic spectrum sensing and access is denoted DSSA, while the fast convergence dynamic spectrum sensing and access algorithm is denoted DSA-FC. The versions of the algorithms that make use of the AND rule are denoted DSSA* and DSA-FC* respectively.

Table 5.1 Simulation Parameters.

Parameter	**Description**	**Value**
C	Number of channels	50
D	Number of secondary users	100
B	Channel bandwidth	10 MHz
T	Frame duration	100 ms
f_s	Sample frequency	1 kHz
P_{su}	SU transmit power	100 mW
$\sigma_{s,i}^2$	PU transmit power	100 mW
P_{ss}	SU sensing power	100 mW
ε	Detector threshold	0.2 mW
$\sigma_{n,i}^2$	Noise power	0.1 mW
$P_{H_{1,i}}$	Probability PU_i is active	0.8
δ	Sensing duration	5 ms
λ	Unit penalty per second	100
$\lvert g_{i,j} \rvert^2$	Average channel gain between PU_i and SU_j with a distance of $d_{i,j}$ between them and a path loss exponent γ set to 2	$\frac{1}{d_{i,j}^{\gamma}}$

Parameter	Description	Value
$\lvert h_{i,j} \rvert^2$	Average channel gain between secondary user transmitter receiver pair SU_j in channel i with distance of $d_{j,i}$ between them and a path loss exponent γ set to 2	$\frac{1}{d_{j,i}^{\gamma}}$

5.5.2 Coalition formation

The number of coalitions available to join corresponds with the number of channels available. Nodes in the same coalition operate in the same channel. To visualise the coalitions that were formed, graphs showing the PUs and SUs in the network were generated and the colour of the node depicts the coalition that the node is a part of. Coalitions formed after 300 iterations for networks with 5 PUs are shown in Figure 5.8, Figure 5.9 and Figure 5.10 for 30, 100 and 300 SUs, respectively.

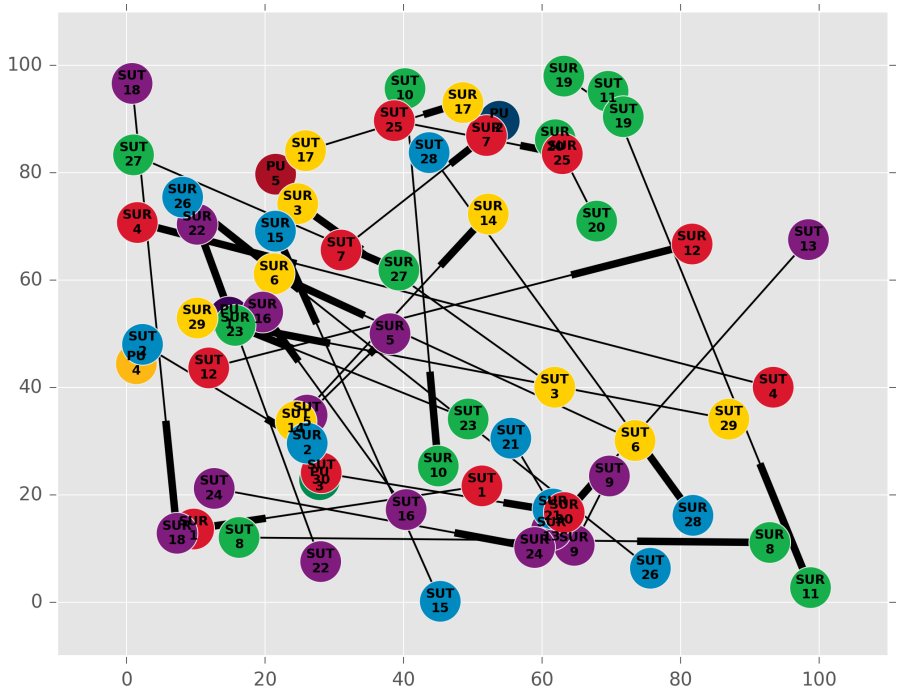


Figure 5.8. Coalitions formed in networks with 5 PUs and 30 SUs.

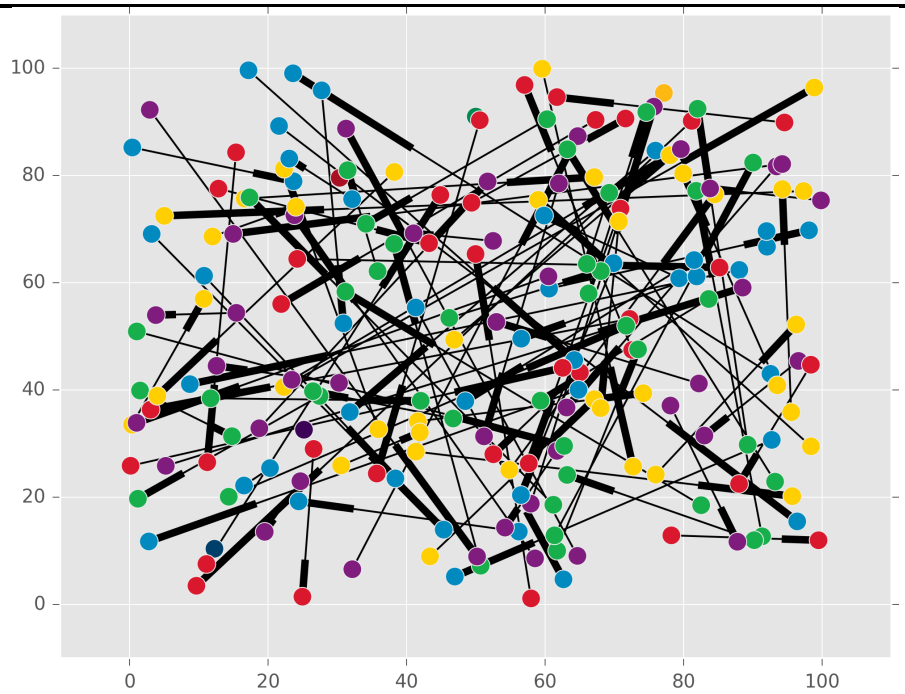


Figure 5.9. Coalitions formed in networks with 5 PUs and 100 SUs.

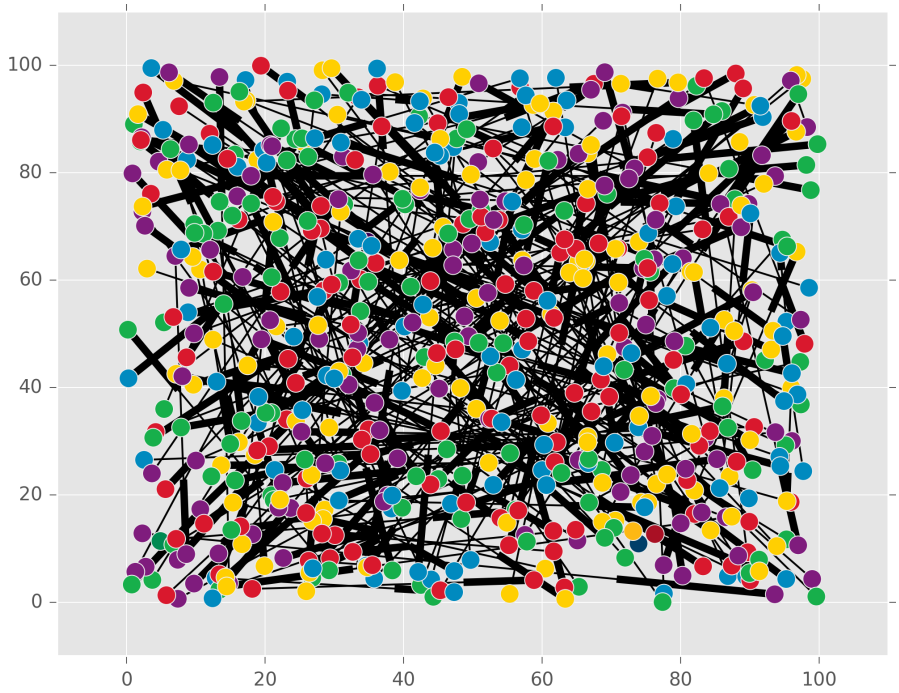


Figure 5.10. Coalitions formed in networks with 5 PUs and 300 SUs.

Coalitions formed after 300 iterations for networks with 10 PUs are shown in Figure 5.11, Figure 5.12 and Figure 5.13 for 30, 100 and 300 SUs, respectively.

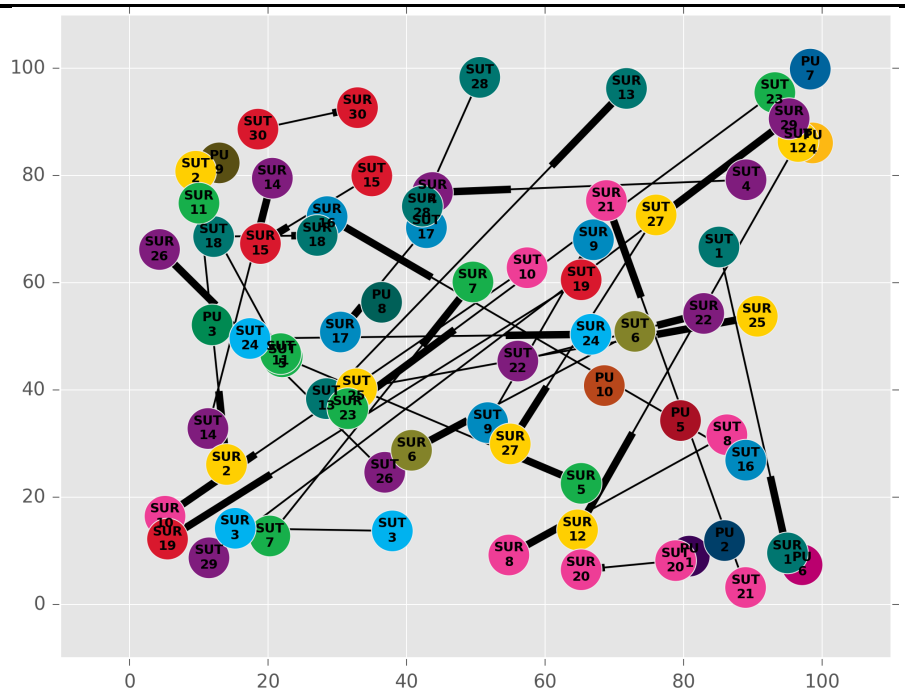


Figure 5.11. Coalitions formed in networks with 10 PUs and 30 SUs.

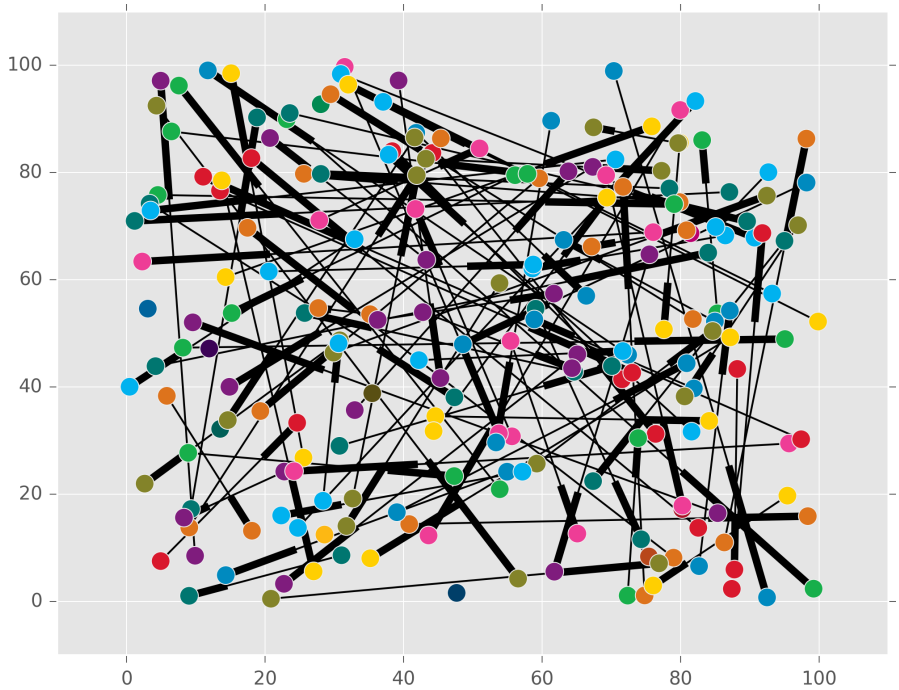


Figure 5.12. Coalitions formed in networks with 10 PUs and 100 SUs.

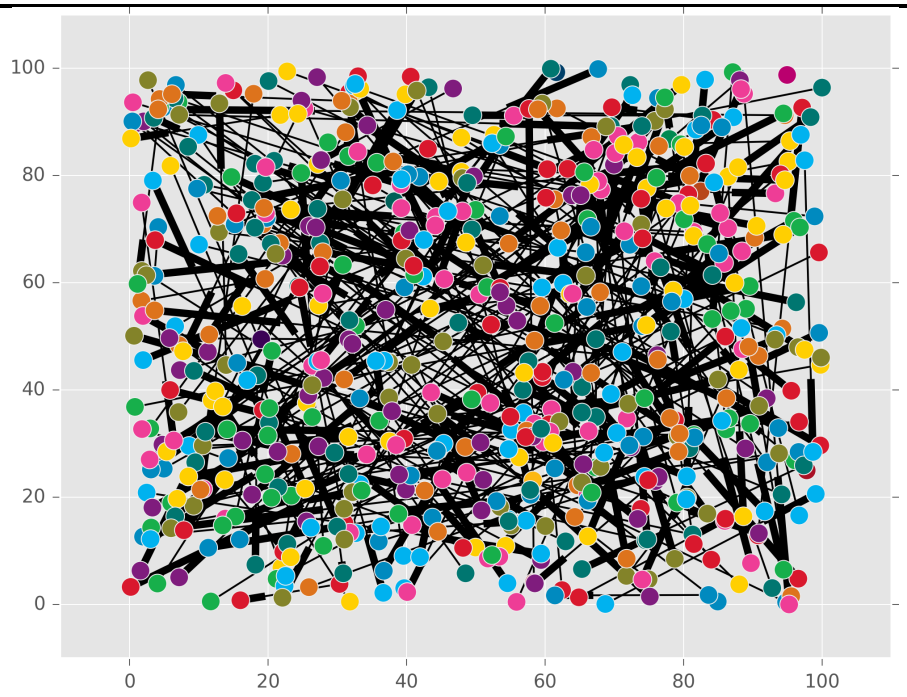


Figure 5.13. Coalitions formed in networks with 10 PUs and 300 SUs.

Initially, all SUs are in the same coalition. As more iterations of the algorithm are run, the SUs get spread out among the different coalitions. The distribution of SUs among the different coalitions is shown in Figure 5.14, Figure 5.15 and Figure 5.16 for networks with 5, 10 and 50 coalitions respectively. This is an indication of how many SUs are in each coalition, but does not show which SUs are in each coalition. The organisation of SUs across the coalitions is what the spectrum sensing and access algorithm seeks to optimise and is reflected in the average utility of the network.

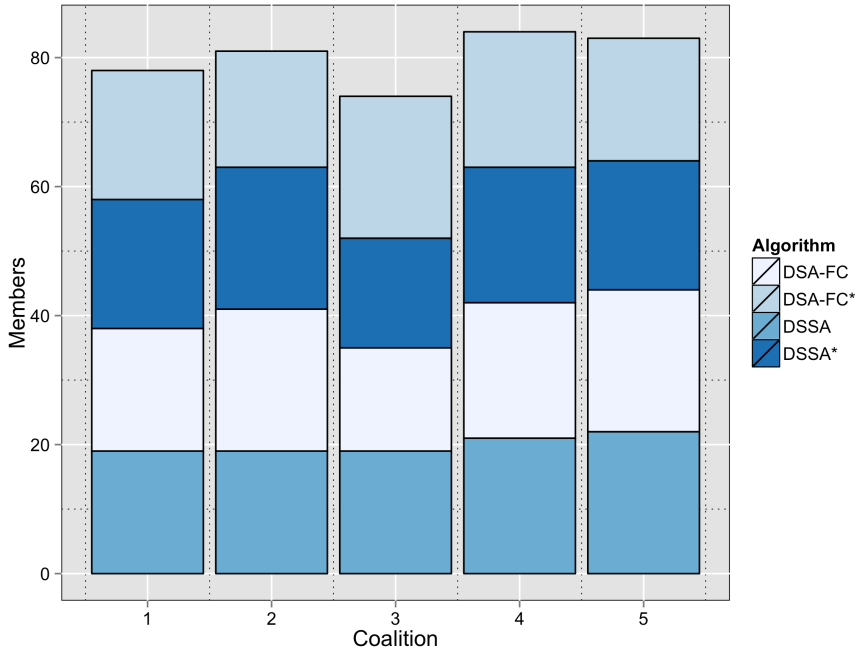


Figure 5.14. Membership of coalitions formed in networks with 5 PUs and 300 SUs.

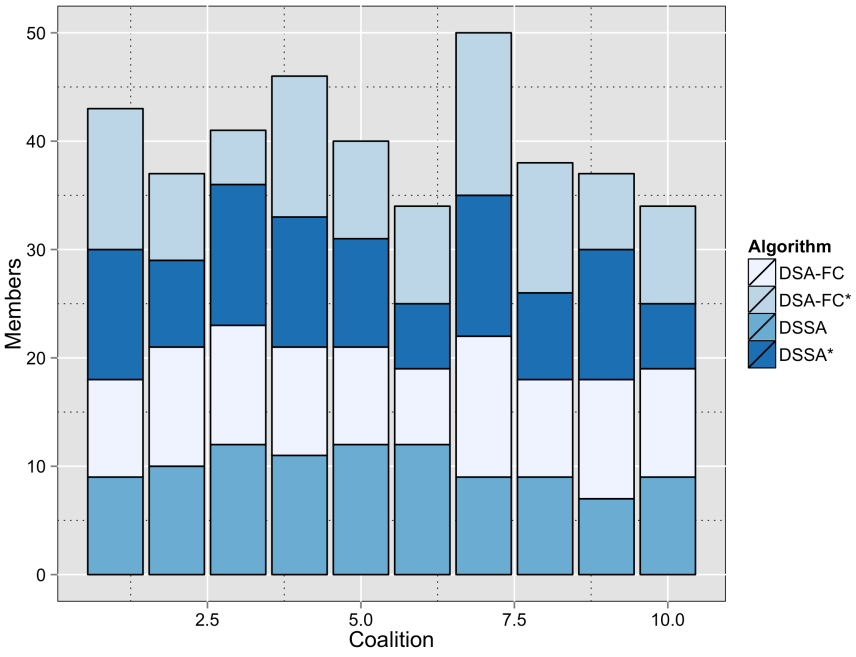


Figure 5.15. Membership of coalitions formed in networks with 10 PUs and 300 SUs.

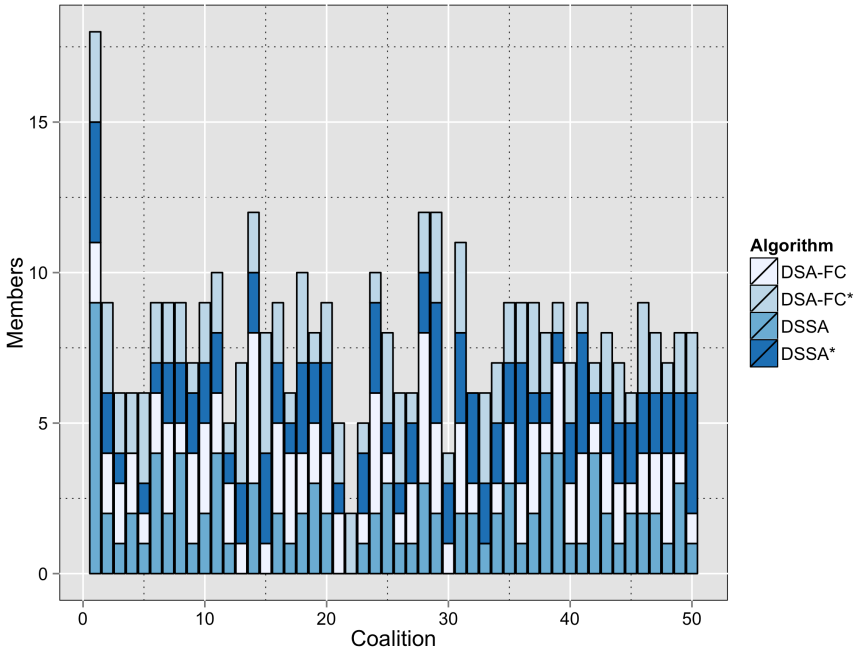


Figure 5.16. Membership of coalitions formed in networks with 50 PUs and 300 SUs.

5.5.3 Average utility per iteration

The average SU utility per iteration is shown for both algorithms in Figure 5.17 and Figure 5.18 when using the OR and AND rules for decision fusion, respectively.

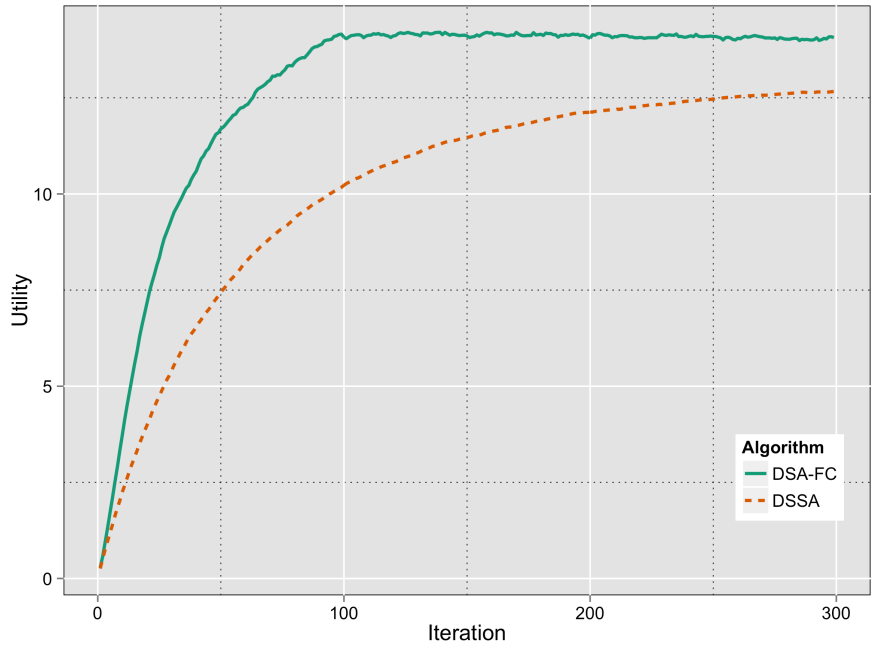


Figure 5.17 Average SU utility vs iteration when using OR decision rule.

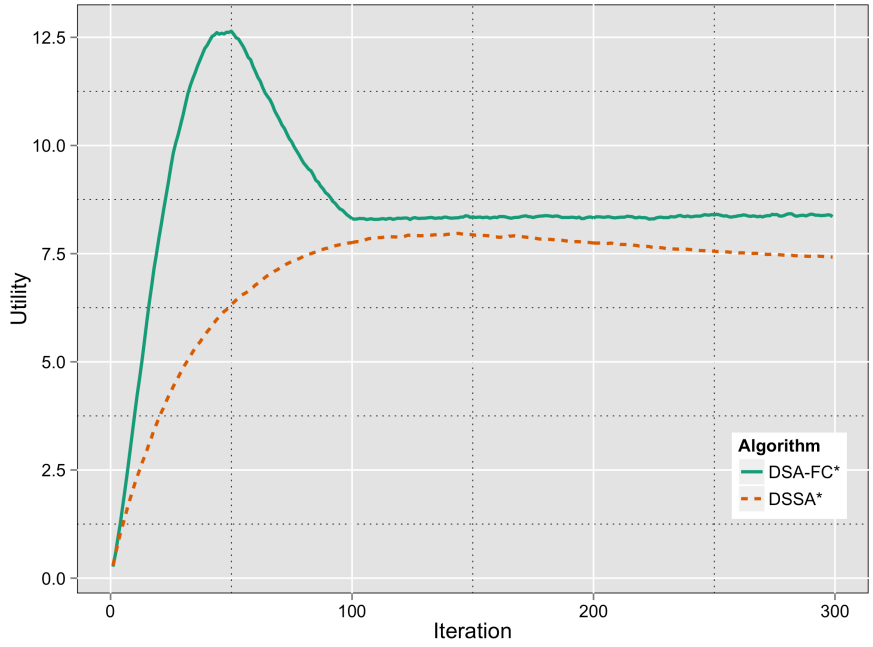


Figure 5.18 Average SU utility vs iteration when using AND decision rule.

5.5.4 Average utility with number of channels

The average SU utility for different channel counts is shown in Figure 5.19 and Figure 5.20 when using the OR and AND decision rules, respectively.

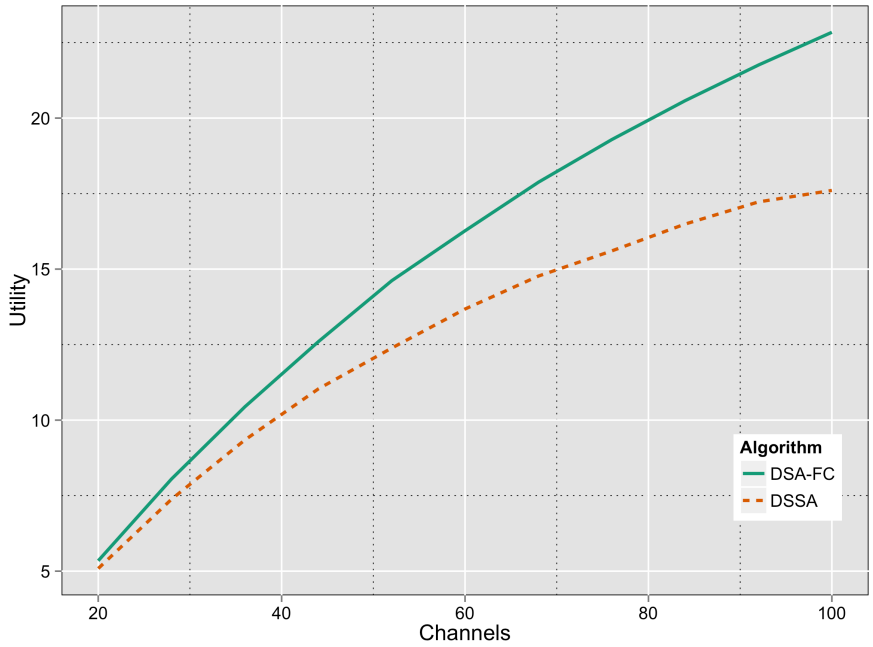


Figure 5.19 Average SU utility vs number of channels when using OR decision rule.

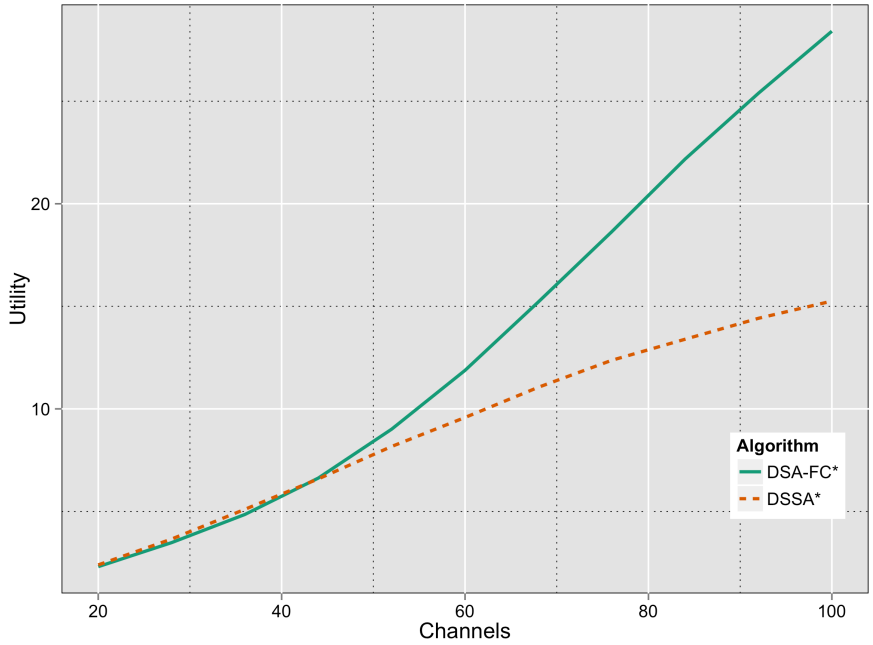


Figure 5.20 Average SU utility vs number of channels when using AND decision rule.

5.5.5 Average utility with number of secondary users

The average SU utility for different numbers of SUs in the network is shown in Figure 5.21 and Figure 5.22 when using the OR and AND decision rules, respectively.

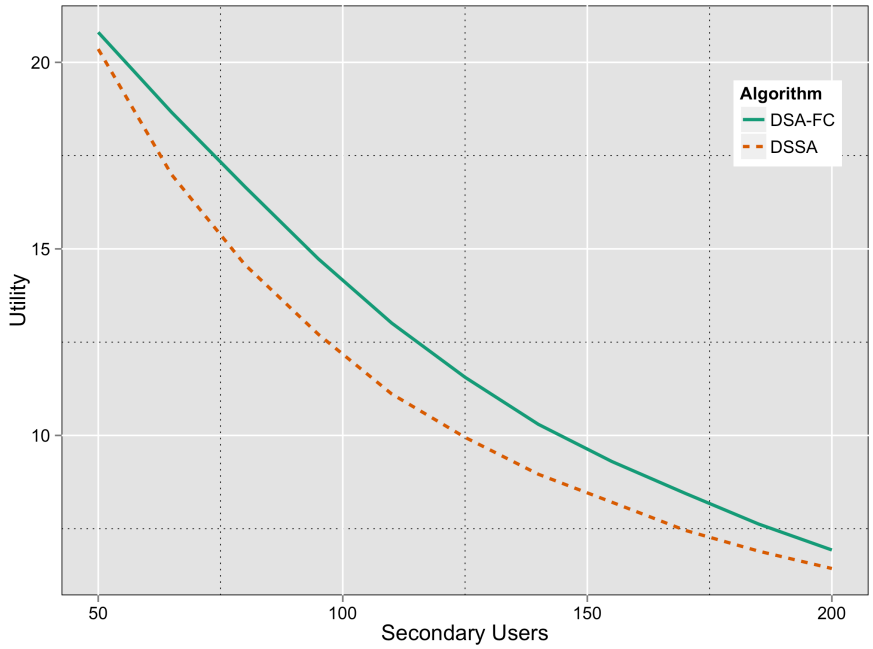


Figure 5.21 Average SU utility vs number of SUs when using OR decision rule.

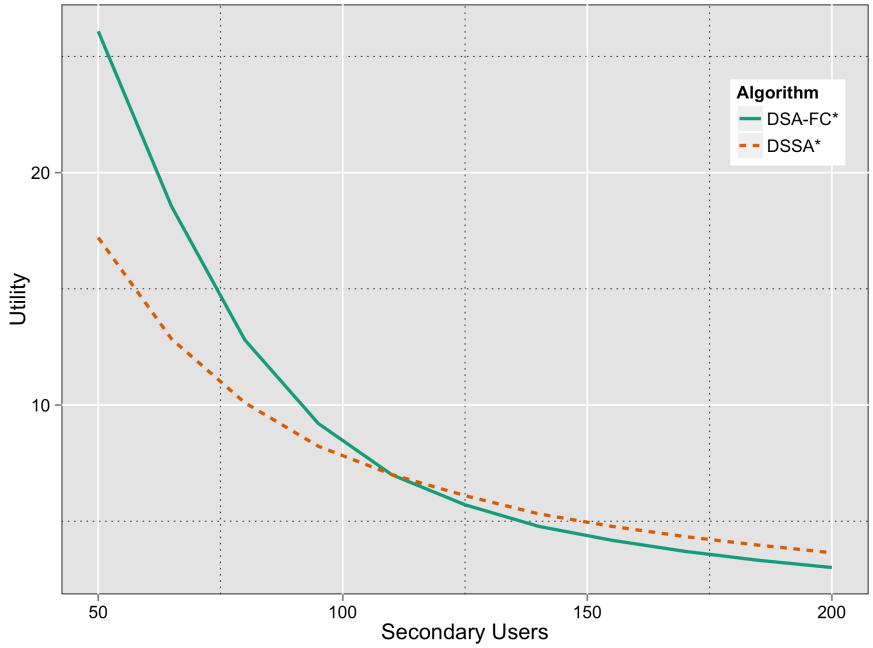


Figure 5.22 Average SU utility vs number of SUs when using AND decision rule.

5.5.6 Average utility with probability of primary user activity

The average SU utility for different probabilities of primary users being active is shown in Figure 5.23 and Figure 5.24 when using the OR and AND decision rules, respectively.

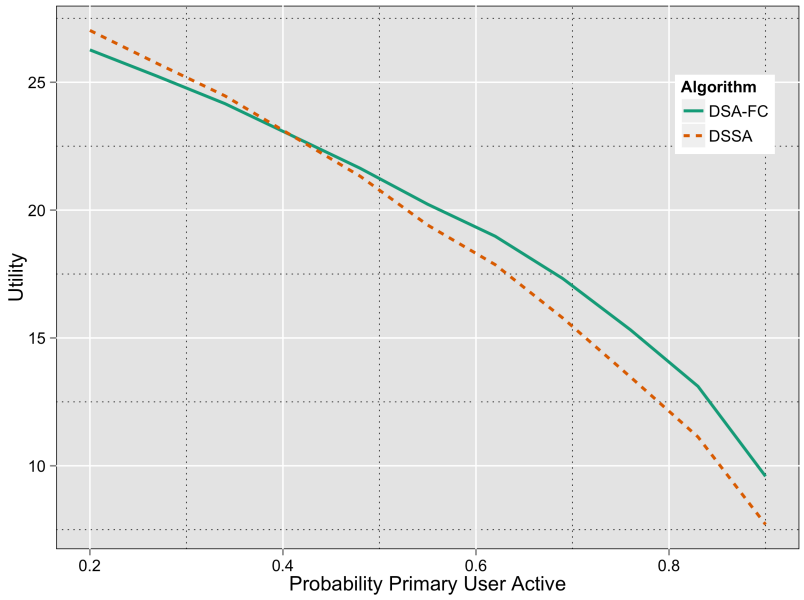


Figure 5.23 Average SU utility vs probability of primary users being active when using OR decision rule.

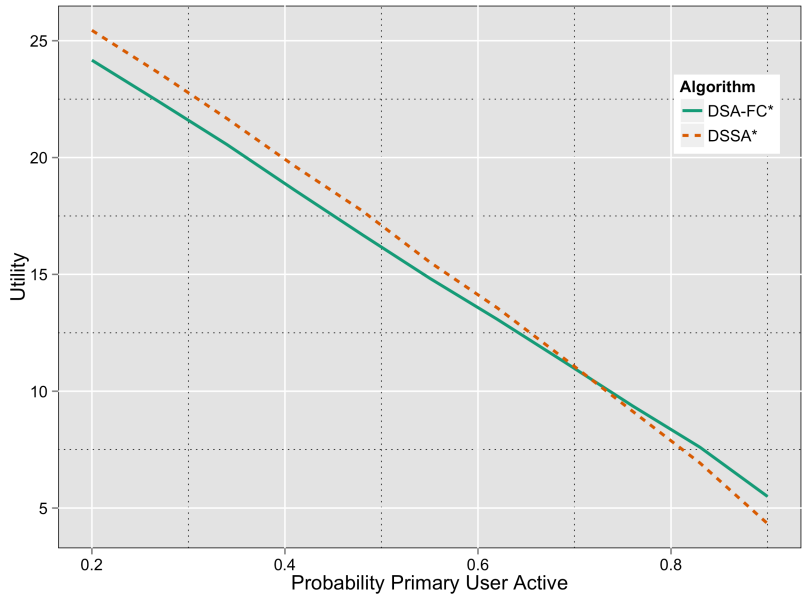


Figure 5.24 Average SU utility vs probability of primary users being active when using AND decision rule.

5.5.7 Average utility with sensing time

The average SU utility for different sensing durations and, as a result, the different number of sensing samples collected, is shown in Figure 5.25 and Figure 5.26 when using the OR and AND decision rules respectively.

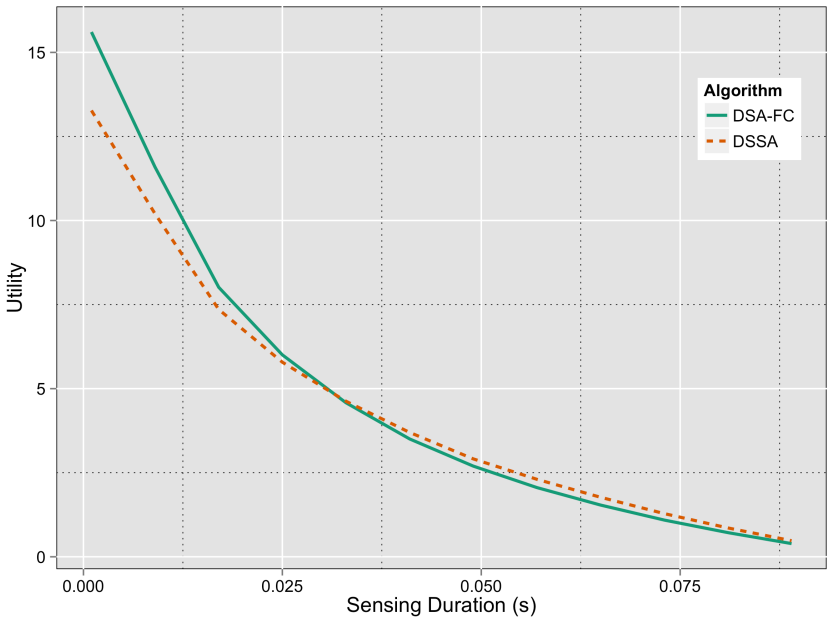


Figure 5.25 Average SU utility vs sensing duration when using OR decision rule.

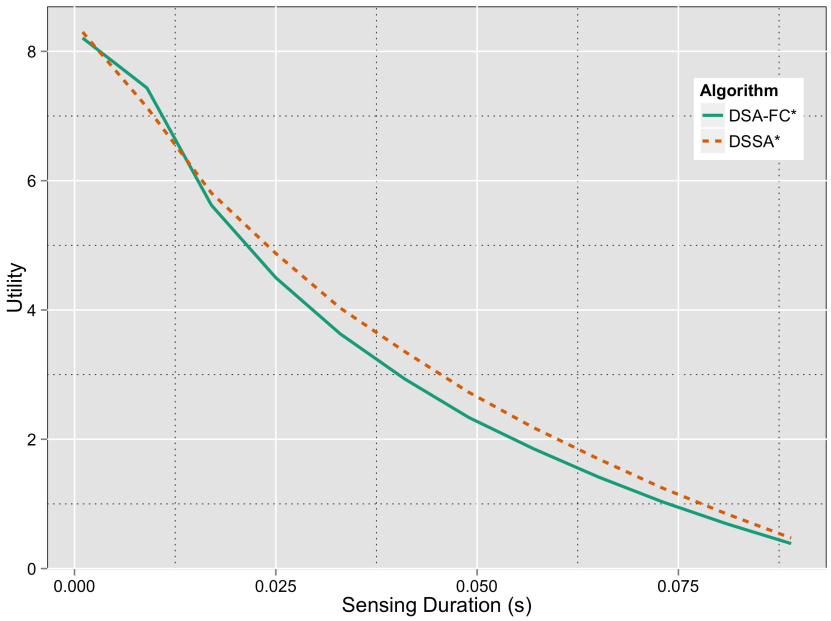


Figure 5.26 Average SU utility vs sensing duration when using AND decision rule.

5.6 DISCUSSION

There are several insights that can be gleaned from the performance results that were obtained. When considering how coalitions are formed, it can be seen in Figure 5.14 to Figure 5.16 that there is not an even distribution of SUs among the different coalitions; however, the number of SUs in each coalition is quite similar. This is likely because the utility that SUs will obtain is based on channel characteristics as well as coalition membership. A coalition in which the PU is far away from a particular SU is generally undesirable, because of the relatively low channel gain; however, should the channel be largely unoccupied, then this makes it attractive. There is, therefore, an interplay between the channel gain and how congested a channel is. The net effect observed is that the Nash stable partition spreads SUs across the different channels fairly evenly, which suggests that SUs will be part of a coalition where the PU is closer to them and they receive a higher channel gain and therefore higher utility.

When looking at the average utility per iteration in Figure 5.17 and Figure 5.18 it can be seen that the new algorithm does converge faster than the original one. After several iterations, the partitions for both the new and the original algorithms are Nash stable and

the utility is the same. The advantage here is fast convergence. When looking at the algorithm, this result it is to be expected, as going from just one SU performing channel sensing and access per time-frame to multiple SUs performing this action in a time-frame suggests that the coalition game should converge faster. Apart from fast convergence, the fact that the multi-user channel sensing and access is done in a way that ensures that there is no contention and instability in the coalition game is advantageous. What happens is that if a channel has members that are part of its coalition, one of them will have an opportunity to do sensing in that channel. This is in contrast with sensing being performed in one channel across the whole network. The new algorithm also ensures that there is no likelihood of a SU migrating to a channel that another SU has chosen to migrate to, which would result in contention and inaccurate expected utility in the new channel.

An interesting result is obtained when considering the average utility as the number of channels increases. Figure 5.19 and Figure 5.20 show that the new fast convergence algorithm scales much better than the original one. Here the benefits of fast convergence are amplified. The original algorithm takes longer and longer to converge as the number of channels increases, and the difference in average utility after a given number of iterations keeps increasing as the number of channels increases. This shows clearly that the new algorithm scales well and out-performs the original one significantly in this regard.

The difference is less pronounced when considering the average SU utility with different values for the number of SUs, the primary user activity and the sensing time, as shown in Figure 5.21 to Figure 5.26. The results indicate that the number of secondary users does not have a major effect on the average SU utility. The new algorithm has a higher average utility, but as the number of SUs increases, this difference is less pronounced. This suggests that a Nash-stable partition is reached much sooner, as the number of SUs increases. When the primary user activity is low, a higher average utility is achieved using the original algorithm, whereas the new algorithm performs better when it is high. The sensing duration seems to have even less of an effect when comparing the two algorithms.

The choice of decision rule is shown to have a marked difference in the results obtained. The OR rule is a more conservative rule to use that seeks to protect PUs more and it results in a much higher average utility than when using the AND rule. When using the AND rule, it can be seen that the fast convergence algorithm gives a rapid increase in utility in the early stages of the iterations, before dropping and finally settling to the Nash-stable partition. The highest utility is obtained before equilibrium is reached.

5.7 SUMMARY

In this chapter, approaches to open spectrum sharing were outlined and detailed. A spectrum model for multi-channel dynamic spectrum access was presented and an in-depth analytical account of spectrum sensing was given. The details of a collaborative spectrum sharing game were then presented from an analytical perspective, and an algorithm for fast convergence in a hedonic coalition game was given. Finally, the performance of the algorithm was shown and discussed.

CHAPTER 6 CONCLUSION

Cognitive radio networks show a lot of promise and are the next frontier in wireless communication. They can reduce the problems of spectrum scarcity - real and artificial. They can provide reliable communication in challenging environments. They can help achieve the vision of good quality service for wireless communication wherever and whenever needed. There is a road to travel before this vision is realised. In this study, a part of that road has been travelled.

A concise one-of-a-kind chart that shows the allocation of radiofrequency spectrum in South Africa was developed in chapter 3. This chart shows that, from a regulatory perspective, the RF spectrum has been allocated to different services and applications in its entirety. Readings that were taken of actual spectrum usage reveal that even though spectrum has been allocated, it is not being used in its entirety. There are variations over time and geographic areas, in terms of how it is used. The opportunity to use cognitive radio is laid bare. In addition, with the current effort at digital migration of television broadcast signals, there are Television White Spaces that are being created, which present an opportunity to use cognitive radio.

In chapter 4, a novel cognitive radio protocol was developed with a specification that covers the physical layer and the MAC layer. The protocol was implemented using software radio and its real-world performance was characterised. The implementation was made available online for download by those who are interested in trying the testbed for the protocol themselves. This was done to make the research more transparent. In addition to this, cognitive radio can be a far-removed abstract concept for some people. What was demonstrated was a real-world working cognitive radio protocol. The protocol allows other members of the research community to develop their own algorithms for dynamic spectrum allocation and to test these in real-life situations. A lot of the groundwork that normally has to be done has already been done for interested parties, so that they can focus on the main objectives of their research.

Dynamic spectrum access is one of the key capabilities of cognitive radio. In chapter 5 an algorithm for fast convergence dynamic spectrum access was presented, which improves on a previously developed algorithm for dynamic spectrum sensing and allocation. It was demonstrated that the new algorithm converges faster than the original one. Also, it is more scalable when the network gets more and more dense.

What has been achieved in this study is to lay bare the state of radio-frequency spectrum utilisation. The idea of cognitive radio was made real by developing a novel cognitive radio protocol and demonstrating it in real-life situations. A testbed was created for developing and experimenting with different cognitive radio techniques using software radio. Also, a dynamic spectrum access algorithm was developed and benchmarked against other algorithms and it was demonstrated that it performed well. Cognitive radio was brought to life in this study and it is hoped that the humble contributions of this study will find further life in the work of others.

Future work that can be done includes testing the spectrum sharing algorithm that was developed using the cognitive radio testbed that was created, to show how it performs in the real world. There is also a lot of work that can be done to extend the Cognitiva protocol, particularly when it comes to the upper layers of the protocol stack, such as the networking layer and the application layer.

REFERENCES

[1] K. R. Liu, "Cognitive radio games," *IEEE Spectrum,* vol. 48, no. 4, pp. 40-56, 2011.

[2] I. F. Akyildiz, W. -Y. Lee, M. C. Vuran and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.,* vol. 46, no. 4, pp. 40-48, 2008.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Select. Areas Commun.,* vol. 23, no. 2, pp. 201-220, 2005.

[4] F. K. Jondral, "Software-defined radio - Basics and evolution to cognitive radio," *Eurasip Journal on Wireless Communications and Networking,* vol. 2005, no. 3, pp. 275-283, 2005.

[5] T. Chiwewe and G. Hancke, "A look at spectrum management policies for radio spectrum," *EngineerIT,* no. March, pp. 47-49, 2015.

[6] T. M. Chiwewe, C. F. Mbuya and G. P. Hancke, "Using Cognitive Radio for Interference-Resistant Industrial Wireless Sensor Networks: An Overview," *IEEE Trans. Ind. Informat.,* vol. 11, no. 6, pp. 1466-1481, 2015.

[7] T. M. Chiwewe and G. P. Hancke, "Cognitiva - A cognitive industrial wireless network protocol: Protocol design and testbed implementation," in *2016 IEEE International Conference on Industrial Technology (ICIT),* 2016, pp. 2042-2047.

[8] A. Willig, "Recent and emerging topics in wireless industrial communications: A selection," *IEEE Trans. Ind. Informat.,* vol. 4, no. 2, pp. 102-122, 2008.

[9] J. Chen, X. Cao, P. Cheng, Y. Xiao and Y. Sun, "Distributed collaborative control for industrial automation with wireless sensor and actuator networks," *IEEE Trans. Ind. Electron.,* vol. 57, no. 12, pp. 4219-4230, 2010.

[10] J. Silvestre-Blanes, L. Almeida, R. Marau and P. Pedreiras, "Online QoS management for multimedia real-time transmission in industrial networks," *IEEE Trans. Ind. Electron.,* vol. 58, no. 3, pp. 1061-1071, 2011.

[11] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.,* vol. 56, no. 10, pp. 4258-4265, 2009.

[12] G. Cena, L. Seno, A. Valenzano and C. Zunino, "On the performance of IEEE 802.11e wireless infrastructures for soft-real-time industrial applications," *IEEE Trans. Ind. Informat.,* vol. 6, no. 3, pp. 425-437, 2010.

[13] F. P. Rezha and S. Y. Shin, "Performance analysis of ISA 100.11a under interference from an IEEE 802.11b wireless network," *IEEE Trans. Ind. Informat.,* vol. 10, no. 2, pp. 919-927, 2014.

[14] K. Ahmad, P. -B. Ostfeld, U. Meier and H. Kwaśnicka, "Exploitation of multiple hyperspace dimensions to realize coexistence optimized wireless automation systems," *IEEE Trans. Ind. Informat.,* vol. 6, no. 4, pp. 758-766, 2010.

[15] Federal Communications Commission, "Notice of proposed rulemaking and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies," vol. ET Docket No. 03-108, Feb 2005.

[16] B. Wang, Y. Wu and K. J. R. Liu, "Game theory for cognitive radio networks: An overview," *Computer Networks,* vol. 54, no. 14, pp. 2537-2561, 2010.

[17] G. Gamba, F. Tramarin and A. Willig, "Retransmission strategies for cyclic polling over wireless channels in the presence of interference," *IEEE Trans. Ind. Informat.,* vol. 6, no. 3, pp. 405-415, 2010.

[18] P. Gaj, J. Jasperneite and M. Felser, "Computer Communication Within Industrial Distributed Environment—a Survey," *IEEE Trans. Ind. Informat.,* vol. 9, no. 1, pp. 182-189, 2013.

[19] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.,* vol. 5, no. 4, pp. 23-34, 2011.

[20] T. Kaiser, M. D. Pérez-Guirao and A. Wilzeck, "Cognitive radio & networks in the perspective of industrial wireless communications," in *2009 2nd International Workshop on Cognitive Radio and Advanced Spectrum Management, CogART 2009,* 2009, pp. 24-29.

[21] R. L. Kirlin, C. Lascu and A. M. Trzynadlowski, "Shaping the noise spectrum in power electronic converters," *IEEE Trans. Ind. Electron.,* vol. 58, no. 7, pp. 2780-2788, 2011.

[22] O. Staub, J. Zurcher, P. Morel and A. Croisier, "Indoor propagation and electromagnetic pollution in an industrial plant," in *IECON Proceedings (Industrial Electronics Conference),* 1997, pp. 1198-1203.

[23] K. S. Low, W. N. N. Win and M. J. Er, "Wireless sensor networks for industrial environments," in *Proceedings - International Conference on Computational Intelligence for Modelling, Control and Automation, CIMCA 2005 and International Conference on Intelligent Agents, Web Technologies and Internet,* 2005, pp. 271-276.

[24] R. Steigmann and J. Endresen, "Introduction to WISA: WISA–Wireless Interface for Sensors and Actuators," *White Paper, ABB,* 2006.

[25] R. Jurdak, C. V. Lopes and P. Baldi, "A survey, classification and comparative analysis of medium access control protocols for ad hoc networks," *IEEE Commun. Surveys & Tutorials,* vol. 6, no. 1, pp. 2-16, 2004.

[26] S. Stanczak, M. Wiczanowski and H. Boche, *Fundamentals of Resource Allocation in Wireless Networks: Theory and Algorithms.* Springer, 2009.

[27] G. M. Dousoky, M. Shoyama and T. Ninomiya, "FPGA-Based spread-spectrum schemes for conducted-noise mitigation in DCDC power converters: Design,

implementation, and experimental investigation," *IEEE Trans. Ind. Electron.,* vol. 58, no. 2, pp. 429-435, 2011.

[28] J. Wang, Q. Gao, Y. Yu, H. Wang and M. Jin, "Toward robust indoor localization based on Bayesian filter using chirp-spread-spectrum ranging," *IEEE Trans. Ind. Electron.,* vol. 59, no. 3, pp. 1622-1629, 2012.

[29] A. Bachir, M. Dohler, T. Watteyne and K. K. Leung, "MAC essentials for wireless sensor networks," *IEEE Commun. Surveys & Tutorials,* vol. 12, no. 2, pp. 222-248, 2010.

[30] V. C. Gungor, B. Lu and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. Ind. Electron.,* vol. 57, no. 10, pp. 3557-3564, 2010.

[31] I. F. Akyildiz, W. -Y. Lee and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks,* vol. 7, no. 5, pp. 810-836, 2009.

[32] A. Khattab, D. Perkins and M. A. Bayoumi, "Opportunistic spectrum access: From theory to practice," *IEEE Veh. Technol. Mag.,* vol. 7, no. 2, pp. 62-68, 2012.

[33] Hyung-Jung Kim, Jin-Up Kim, Jae-Hyung Kim, Hongmei Wang and In-Sung Lee, "The Design Method and Performance Analysis of RF Subsampling Frontend for SDR/CR Receivers," *IEEE Trans. Ind. Electron.,* vol. 57, no. 5, pp. 1518-1525, 2010.

[34] T. Ulversoy, "Software defined radio: Challenges and opportunities," *IEEE Commun. Surveys & Tutorials,* vol. 12, no. 4, pp. 531-550, 2010.

[35] K. Nishimori, H. Yomo and P. Popovski, "Distributed Interference Cancellation for Cognitive Radios Using Periodic Signals of the Primary System," *IEEE Trans. Wireless Commun.,* vol. 10, no. 9, pp. 2971-2981, 2011.

[36] G. M. Shrestha, K. Ahmad and U. Meier, "Statistical analysis and predictive modeling of industrial wireless coexisting environments," in *IEEE International*

Workshop on Factory Communication Systems - Proceedings, WFCS, 2012, pp. 125-134.

[37] N. Devroye, M. Vu and V. Tarokh, "Cognitive radio networks: Highlights of information theoretic limits, models, and design," *IEEE Signal Process. Mag.,* vol. 25, no. 6, pp. 12-23, 2008.

[38] Chang-Jiang You, Xiao-Wei Zhu, Xiao-Dong Zhang, Jing Liu, Zhi-Gang Cao, Jia Chen, Luong Ngoc Quyen and Wei-Yu Zong, "Study of RF Subsystem Used in Dynamic Spectrum Sharing System at TV Band," *IEEE Trans. Ind. Electron.,* vol. 60, no. 6, pp. 2346-2357, 2013.

[39] G. P. Villardi, G. Thadeu Freitas De Abreu and H. Harada, "TV white space technology: Interference in portable cognitive emergency network," *IEEE Veh. Technol. Mag.,* vol. 7, no. 2, pp. 47-53, 2012.

[40] Muhammad Faisal Amjad, B. Aslam and C. C. Zou, "Transparent cross-layer solutions for throughput boost in cognitive radio networks," in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE,* 2013, pp. 580-586.

[41] Chen Sun, G. P. Villardi, Zhou Lan, Y. D. Alemseged, H. -N. Tran and H. Harada, "Optimizing the Coexistence Performance of Secondary-User Networks Under Primary-User Constraints for Dynamic Spectrum Access," *IEEE Trans. Veh. Technol.,* vol. 61, no. 8, pp. 3665-3676, 2012.

[42] M. Cesana, F. Cuomo and E. Ekici, "Routing in cognitive radio networks: Challenges and solutions," *Ad Hoc Networks,* vol. 9, no. 3, pp. 228-248, 5, 2011.

[43] T. M. Chiwewe and G. P. Hancke, "A Distributed Topology Control Technique for Low Interference and Energy Efficiency in Wireless Sensor Networks," *IEEE Trans. Ind. Informat.,* vol. 8, no. 1, pp. 11-19, 2011.

[44] G. A. Shah, V. C. Gungor and O. B. Akan, "A Cross-Layer QoS-Aware Communication Framework in Cognitive Radio Sensor Networks for Smart Grid Applications," *IEEE Trans. Ind. Informat.,* vol. 9, no. 3, pp. 1477-1485, 2013.

[45] T. Zheng, Y. Qin, H. Zhang and S. -Y. Kuo, "A self-configurable power control algorithm for cognitive radio-based industrial wireless sensor networks with interference constraints," in *IEEE International Conference on Communications,* 2012, pp. 98-103.

[46] P. T. A. Quang and D. -S. Kim, "Throughput-aware routing for industrial sensor networks: Application to ISA100.11a," *IEEE Trans. Ind. Informat.,* vol. 10, no. 1, pp. 351-363, 2014.

[47] J. Hu, L. -L. Yang and L. Hanzo, "Maximum average service rate and optimal queue scheduling of delay-constrained hybrid cognitive radio in nakagami fading channels," *IEEE Trans. Veh. Technol.,* vol. 62, no. 5, pp. 2220-2229, 2013.

[48] C. -S. Sum, G. Villardi, M. A. Rahman, T. Baykas, H. Tran, Z. Lan, C. Sun, Y. Alemseged, J. Wang, C. Song, C. -. Pyo, S. Filin and H. Harada, "Cognitive communication in TV white spaces: An overview of regulations, standards, and technology," *IEEE Commun. Mag.,* vol. 51, no. 7, pp. 138-145, 2013.

[49] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.,* vol. 47, no. 1, pp. 130-138, 2009.

[50] C. -S. Sum, M. -T. Zhou, L. Lu, R. Funada, F. Kojima and H. Harada, "IEEE 802.15.4m: The first low rate wireless personal area networks operating in TV white space," in *IEEE International Conference on Networks, ICON,* 2012, pp. 326-332.

[51] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Pers. Commun.,* vol. 6, no. 4, pp. 13-18, 1999.

[52] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys & Tutorials,* vol. 11, no. 1, pp. 116-130, 2009.

[53] P. Kolodzy, "Next generation communications: Kickoff meeting," in *Proc. DARPA,* 2001, .

[54] L. Drozd, "Computational electromagnetics applied to analyzing the efficient utilization of the RF transmission hyperspace," in *Proc. IEEE/ACES Int. Conf.* 2005, pp. 1077-1085.

[55] H. Tang, "Some physical layer issues of wide-band cognitive radio systems," in *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005,* 2005, pp. 151-159.

[56] F. F. Digham, M. -S. Alouini and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. Commun.,* vol. 55, no. 1, pp. 21-24, 2007.

[57] T. Yucek and H. Arslan, "Spectrum characterization for opportunistic cognitive radio systems," in *Military Communications Conference,* 2006, pp. 1-6.

[58] S. Shankar, C. Cordeiro and K. Challapali, "Spectrum agile radios: Utilization and sensing architectures," in *Proc. IEEE DySPAN,* 2005, pp. 160-169.

[59] Q. Peng, K. Zeng, J. Wang and S. Li, "A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context," in *IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications,* 2006, pp. 1-5.

[60] E. Axell, G. Leus, E. G. Larsson and H. V. Poor, "Spectrum sensing for cognitive radio : State-of-the-art and recent advances," *IEEE Signal Process. Mag.,* vol. 29, no. 3, pp. 101-116, 2012.

[61] A. Fehske, J. Gaeddert and J. H. Reed, "A new approach to signal classification using spectral correlation and neural networks," in *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005,* 2005, pp. 144-150.

[62] T. Farnham, G. Clemo, R. Haines, E. Seidel, A. Benamar, S. Billington, N. Greco, N. Drew, Truong Hong Le, B. Arram and P. Mangold, "IST-TRUST: A perspective on the reconfiguration of future mobile terminals using software download," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC,* 2000, pp. 1054-1059.

[63] J. Palicot and C. Roland, "A new concept for wireless reconfigurable receivers," *IEEE Commun. Mag.,* vol. 41, no. 7, pp. 124-132, 2003.

[64] A. Sahai, R. Tandra, S. M. Mishra and N. Hoven, "Fundamental design tradeoffs in cognitive radio systems," in *Proc. of Int. Workshop on Technology and Policy for Accessing Spectrum,* 2006, .

[65] R. Tandra and A. Sahai, "Fundamental limits on detection in low SNR under noise uncertainty," in *2005 International Conference on Wireless Networks, Communications and Mobile Computing,* 2005, pp. 464-469.

[66] D. Cabric, S. M. Mishra and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Conference Record - Asilomar Conference on Signals, Systems and Computers,* 2004, pp. 772-776.

[67] K. Challapali, S. Mangold and Z. Zhong, "Spectrum agile radio: Detecting spectrum opportunities," in *Proc. Int. Symp. Advanced Radio Technologies,* 2004, pp. 61-65.

[68] Z. Tian and G. B. Giannakis, "A wavelet approach to wideband spectrum sensing for cognitive radios," in *Proc. IEEE Int. Conf. Cognitive Radio Oriented Wireless Networks and Commun. (Crowncom),* 2006, pp. 1054-1059.

[69] Y. Hur, J. Park, W. Woo, K. Lim, C. -H. Lee, H. S. Kim and J. Laskar, "A wideband analog multi-resolution spectrum sensing (MRSS) technique for cognitive radio (CR) systems," in *Proceedings - IEEE International Symposium on Circuits and Systems,* 2006, pp. 4090-4093.

[70] R. Umar and A. U. H. Sheikh, "A comparative study of spectrum awareness techniques for cognitive radio oriented wireless networks," *Phys. Commun.,* vol. 9, pp. 148-170, 2013.

[71] M. T. Masonta, M. Mzyece and N. Ntlatlapa, "Spectrum decision in cognitive radio networks: A survey," *IEEE Commun. Surveys & Tutorials,* vol. 15, no. 3, pp. 1088-1107, 2013.

[72] M. B. Pursley and T. C. Royster IV, "Low-complexity adaptive transmission for cognitive radios in dynamic spectrum access networks," *IEEE J. Select. Areas Commun.,* vol. 26, no. 1, pp. 83-94, 2008.

[73] C. Peng, H. Zheng and B. Y. Zhao, "Utilization and fairness in spectrum assignment for opportunistic spectrum access," *Mobile Networks and Applications,* vol. 11, no. 4, pp. 555-576, 2006.

[74] R. Menon, R. M. Buehrer and J. H. Reed, "Outage probability based comparison of underlay and overlay spectrum sharing techniques," in *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005,* 2005, pp. 101-109.

[75] F. Khozeimeh and S. Haykin, "Self-organizing dynamic spectrum management for cognitive radio networks," in *CNSR 2010 - Proceedings of the 8th Annual Conference on Communication Networks and Services Research,* 2010, pp. 1-7.

[76] H. Zheng and C. Peng, "Collaboration and fairness in opportunistic spectrum access," in *IEEE International Conference on Communications,* 2005, pp. 3132-3136.

[77] Q. Yu, "A Survey of Cooperative Games for Cognitive Radio Networks," *Wireless Personal Communications,* pp. 1-18, 2013.

[78] J. Elias, F. Martignon, A. Capone and E. Altman, "Non-cooperative spectrum access in cognitive radio networks: A game theoretical model," *Computer Networks,* vol. 55, no. 17, pp. 3832-3846, 12/1, 2011.

[79] S. M. M. Toroujeni, S. M. -S. Sadough and S. A. Ghorashi, "An auction-based approach for spectrum leasing in cognitive radio networks," in *2011 Wireless Advanced, WiAd 2011,* 2011, pp. 106-109.

[80] D. Xu, X. Liu and Z. Han, "Decentralized bargain: A two-tier market for efficient and flexible dynamic spectrum access," *IEEE Trans. Mobile Comput.,* vol. 12, no. 9, pp. 1697-1711, 2013.

[81] Q. Ni and C. C. Zarakovitis, "Nash bargaining game theoretic scheduling for joint channel and power allocation in cognitive radio systems," *IEEE J. Select. Areas Commun.,* vol. 30, no. 1, pp. 70-81, 2012.

[82] W. Saad, Z. Han, R. Zheng, A. Hjørungnes, T. Basar and H. V. Poor, "Coalitional games in partition form for joint spectrum sensing and access in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.,* vol. 6, no. 2, pp. 195-209, 2012.

[83] X. Hao, M. H. Cheung, V. W. S. Wong and V. C. M. Leung, "Hedonic coalition formation game for cooperative spectrum sensing and channel access in cognitive radio networks," *IEEE Trans. Wireless Commun.,* vol. 11, no. 11, pp. 3968-3979, 2012.

[84] M. Cheminod, L. Durante and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Trans. Ind. Informat.,* vol. 9, no. 1, pp. 277-293, 2013.

[85] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," *IEEE Commun. Surveys & Tutorials,* vol. 15, no. 1, pp. 428-445, 2013.

[86] S. E. Frankel, B. Eydt, L. Owens and K. A. Scarfone, "SP 800-97. establishing wireless robust security networks: A guide to IEEE 802.11i," National Institute of Standards & Technology, Tech. Rep. 2206307, 2007.

[87] National Security Agency. (2015, Feb). *NSA's Information Assurance Definition*. Available: http://www.nsa.gov/ia/.

[88] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Gódor and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys & Tutorials,* vol. 14, no. 2, pp. 355-379, 2012.

[89] International Telecommunication Union., "Security in telecommunications and information technology. an overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications." ITU, 2003.

[90] International Telecommunication Union., "Telecommunication networks security requirements," ITU, 2004.

[91] S. P. Herath, N. Rajatheva and C. Tellambura, "Energy detection of unknown signals in fading and diversity reception," *IEEE Trans. Commun.,* vol. 59, no. 9, pp. 2443-2453, 2011.

[92] C. Clancy, J. Hecker, E. Stuntebeck and T. O'Shea, "Applications of machine learning to cognitive radio networks," *IEEE Wireless Communications,* vol. 14, no. 4, pp. 47-52, 2007.

[93] W. Wang, H. Li, Y. Sun and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proceedings - 43rd Annual Conference on Information Sciences and Systems, CISS 2009,* 2009, pp. 130-134.

[94] A. W. Min, K. G. Shin and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Proceedings - International Conference on Network Protocols, ICNP,* 2009, pp. 294-303.

[95] N. Nguyen-Thanh and I. Koo, "An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context," *IEEE Commun. Lett.,* vol. 13, no. 7, pp. 492-494, 2009.

[96] A. De Domenico, E. Calvanese Strinati and M. -G. Di Benedetto, "A survey on MAC strategies for cognitive radio networks," *IEEE Commun. Surveys & Tutorials,* vol. 14, no. 1, pp. 21-44, 2012.

[97] L. Berlemann and S. Mangold. "Introduction," in *Cognitive Radio and Dynamic Spectrum Access*Anonymous 2009, . DOI: 10.1002/9780470754429.ch1.

[98] I. F. Akyildiz, W. -Y. Lee, M. C. Vuran and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks,* vol. 50, no. 13, pp. 2127-2159, 2006.

[99] L. Berlemann and S. Mangold. "Radio spectrum today - regulation and spectrum usage," in *Cognitive Radio and Dynamic Spectrum Access*Anonymous 2009, . DOI: 10.1002/9780470754429.ch2.

[100] International Telecommunication Union, "Radio regulations (2012)," International Telecommunication Union, Tech. Rep. WRC-12, 2012.

[101] ICASA, "National radio frequency plan 2013," Government Gazette Republic of South Africa, Tech. Rep. 36336, 2013.

[102] ICASA, "Draft frequency migration regulation and frequency migration plan," Government Gazette Republic of South Africa, Tech. Rep. 35598, 2012.

[103] Pham Tran Anh Quang, Soo-Ro Kim and Dong-Sung Kim, "A throughput-aware routing for distributed industrial cognitive radio sensor networks," in *Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop On,* 2012, pp. 87-90.

[104] G. A. Shah, F. Alagoz, E. A. Fadel and O. B. Akan, "A spectrum-aware clustering for efficient multimedia routing in cognitive radio sensor networks," *IEEE Trans. Veh. Technol.,* vol. 63, no. 7, pp. 3369-3380, 2014.

[105] A. Mitra, "On pseudo-random and orthogonal binary spreading sequences," *Int.J.Information Techn,* vol. 4, no. 2, pp. 137-144, 2008.

[106] H. Yan, Y. Zhang, Z. Pang and L. D. Xu, "Superframe planning and access latency of slotted MAC for industrial WSN in IoT environment," *IEEE Trans. Ind. Informat.,* vol. 10, no. 2, pp. 1242-1251, 2014.

[107] B. Bloessl, C. Leitner, F. Dressler and C. Sommer, "A GNU Radio-based IEEE 802.15. 4 Testbed," *12.Gi/Itg Fachgespräch Sensornetze,* pp. 37, 2013.

[108] B. Bloessl, M. Segata, C. Sommer and F. Dressler, "Towards an open source IEEE 802.11p stack: A full SDR-based transceiver in GNU radio," in *IEEE Vehicular Networking Conference, VNC,* 2013, pp. 143-149.

[109] B. Bloessl, A. Puschmanny, C. Sommer and F. Dressler, "Timings matter: Standard compliant IEEE 802.11 channel access for a fully software-based SDR architecture," in *WiNTECH 2014 - Proceedings of the 9th ACM MobiCom Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization,* 2014, pp. 57-63.

[110] T. Schmid, O. Sekkat and M. B. Srivastava, "An experimental study of network performance impact of increased latency in software defined radios," in *Proceedings of the Second ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization,* 2007, pp. 59-66.

[111] T. Vilches and D. Dujovne, "GNUradio and 802.11: Performance evaluation and limitations," *IEEE Network,* vol. 28, no. 5, pp. 27-31, 2014.

[112] L. Sanabria-Russo, J. Barcelo, A. Domingo and B. Bellalta. Spectrum sensing with USRP-E110. *Lecture Notes in Computer Science (Including Subseries Lecture*

Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7642 LNCS, pp. 79-84. 2012.

[113] Y. Dai and J. Wu, "Boundary helps: Efficient routing protocol using directional antennas in cognitive radio networks," in *Proceedings - IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, MASS 2013,* 2013, pp. 502-510.

[114] T. Guan, J. Han and X. Zeng, "Highly flexible WBAN transmit-receive system based on USRP," in *Proceedings of International Conference on ASIC,* 2013, .

[115] W. Zhou, G. Villemaud and T. Risset, "Full duplex prototype of OFDM on GNURadio and USRPs," in *IEEE Radio and Wireless Symposium, RWS,* 2014, pp. 217-219.

[116] T. Schmid. Gnu radio 802.15. 4 en-and decoding. Networked & Embedded Systems Laboratory, UCLA. 2006.

[117] E. Blossom, "GNU radio: Tools for exploring the radio frequency spectrum," *Linux Journal,* vol. 2004, no. 122, 2004.

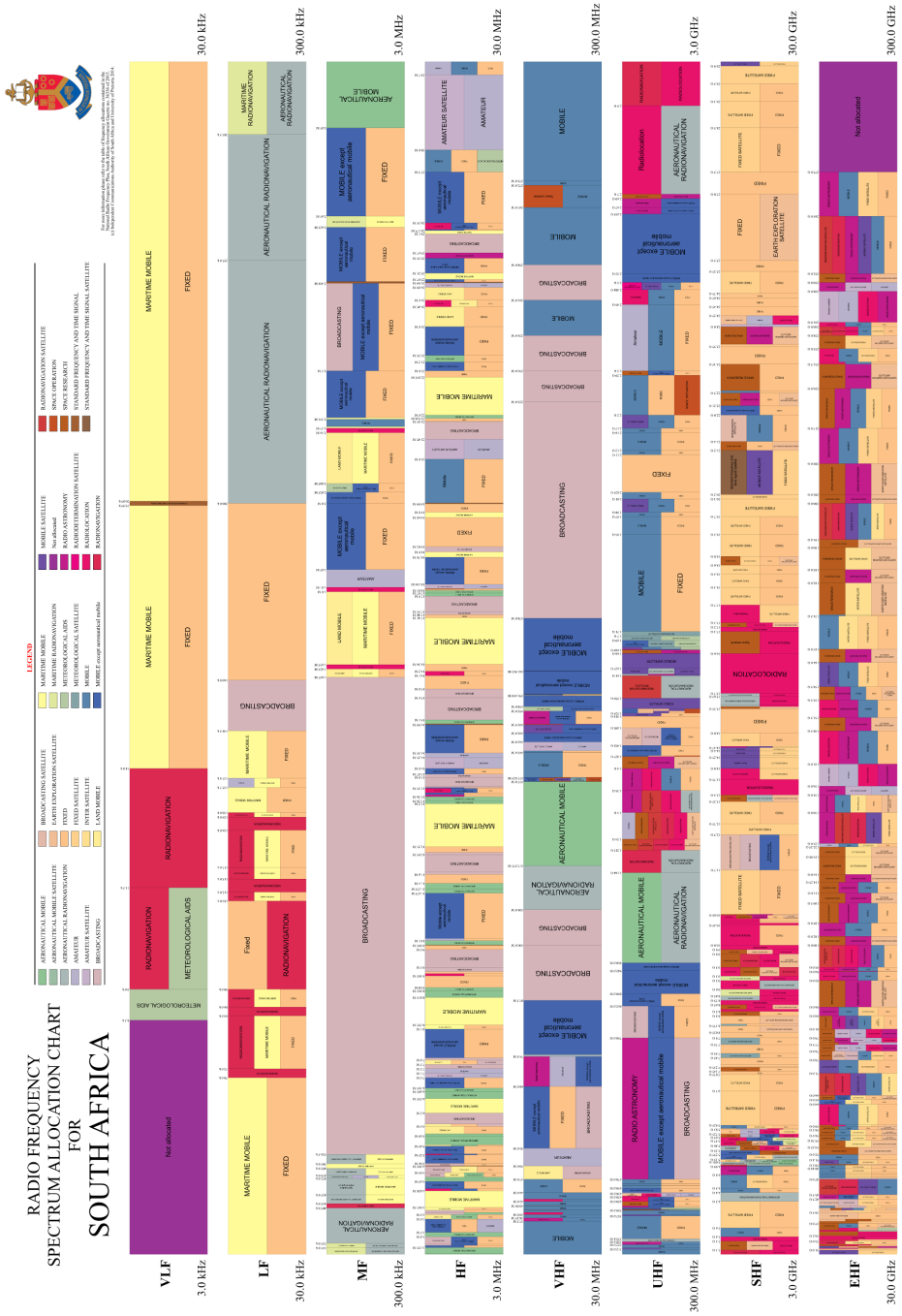
[118] S. Cass, "Hardware for your software radio," *IEEE Spectrum,* vol. 43, no. 10, pp. 51-56, 2006.

[119] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.,* vol. 24, no. 3, pp. 79-89, 2007.

[120] I. F. Akyildiz, B. F. Lo and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication,* vol. 4, no. 1, pp. 40-62, 2011.

[121] N. Zhang, H. Liang, N. Cheng, Y. Tang, J. W. Mark and X. S. Shen, "Dynamic spectrum access in multi-channel cognitive radio networks," *IEEE J Sel Areas Commun,* vol. 32, no. 11, pp. 2053-2064, 2014.

ADDENDUM A RADIOFREQUENCY SPECTRUM ALLOCATON CHART



ADDENDUM B PROOF OF STABLE PARTITION IN HEDONIC COALITION FORMATION GAME

The following is proof that a stable partition exists in the hedonic coalition formation game.

Definition 1: (Switch Rule) For a partition, $\mathcal{A} = \{\mathcal{A}_1, \dots, \mathcal{A}_C\}$, $SU_j, j \in \mathcal{A}_i$ makes a decision to move away from its current coalition $\mathcal{A}_i$ to join another coalition $\mathcal{A}_l$ $(l \neq i)$ if the condition $\mathcal{A}_l \cup \{j\} \succ_j \mathcal{A}_i$ is satisfied. This provides an established process by which a SU can leave its current coalition to join another coalition, provided that the new coalition is preferred to the current one. All SUs make decisions to form coalitions in the network, hence the partition of the hedonic coalition game may change in each time-frame. The initial partition of the hedonic coalition formation game is defined as $\mathcal{A}^{(0)} = \{\mathcal{A}_1^{(0)}, \dots, \mathcal{A}_C^{(0)}\}$ and at the r-th time-frame the partition is defined as $\mathcal{A}^{(r)} = \{\mathcal{A}_1^{(r)}, \dots, \mathcal{A}_C^{(r)}\}$. Should $\mathcal{A}^{(r)} = \mathcal{A}^{(r-1)}$ then no switch iteration was performed in the r-th time-frame.

Definition 2: A partition $\mathcal{A} = \{\mathcal{A}_1, \dots, \mathcal{A}_C\}$ is considered to be *Nash-stable* if $\forall j \in \mathcal{A}_i$ with $\forall i \in \mathcal{C}, \mathcal{A}_i \succcurlyeq_j \mathcal{A}_l \cup \{j\}, \forall l \in \mathcal{C}$. This means that should no other player have a motivation to switch to a coalition other than its current one, then a coalition partition $\mathcal{A}$ is Nash stable. Performing the switch operation does not result in a higher utility when a player is in a Nash-stable partition. Should a partition be Nash-stable, it follows that it is individually stable and no coalition exists that a player prefers to become a member of, and that members of the coalition will not suffer a loss of utility upon the creation of this new coalition.

Definition 3: A partition $\mathcal{A} = \{\mathcal{A}_1, \dots, \mathcal{A}_C\}$ is considered to be *individually stable* should there not be $j \in \mathcal{A}_i$ with $i \in \mathcal{C}$ and a coalition $\mathcal{A}_l$ $(l \neq i)$ in such a way that $\mathcal{A}_l \cup \{j\} \succ_j \mathcal{A}_i$, and $\mathcal{A}_l \cup \{j\} \succcurlyeq_k \mathcal{A}_l$ for all $k \in \mathcal{A}_l$.

Theorem 1: Beginning with any partition $\mathcal{A}^{(0)}$, each of the SUs will always converge to an end partition $\mathcal{A}^* = \{\mathcal{A}_1^*, \dots, \mathcal{A}_C^*\}$ that is individually stable and also Nash-stable.

Proof: Provided the start partition is $\mathcal{A}^{(0)}$, a series of switch operations make up the hedonic coalition game. It follows that there is a series of partitions of the network $\{\mathcal{A}^{(0)}, \mathcal{A}^{(1)}, \mathcal{A}^{(2)}, \dots, \mathcal{A}^{(r)}\}$ following *r* iterations. As per Definition 1 above, joining a new coalition after a switch operation will result in a higher utility for a SU. Each switch operation results in a new partition that has not been visited before. Considering that there are *C* channels and *D* Sus, the number of different partitions is C^D in total, which is a bounded number. It follows that from any initial partition $\mathcal{A}^{(0)}$, after a bounded number of iterations, a point will be reached where the switch operations will terminate; this is where the structure of the coalition converges to the end partition $\mathcal{A}^*$.

Should $\mathcal{A}^*$ not be Nash-stable, as per Definition 2, some switch operations exist that can increase the utility of a SU by migrating it to a different coalition. $\mathcal{A}^*$ will then be updated, which will mean that it is not the end partition that violates the assumption made. Therefore, the end partition $\mathcal{A}^*$ must be Nash-stable. A Nash-partition is individually stable.

ADDENDUM C HARDWARE CALIBRATION

The B100 USRPs from Ettus Research™ were calibrated using self-calibration utility software that minimizes IQ imbalance and DC offset. The utility software performs calibration sweeps that make use of transmit leakage into the receive path. The calibration results are written to a CSV file that is used by the driver software at runtime to apply corrections. The calibration results are unique to each individual RF board - in this case each SBX daughterboard for the B100 USRPs.

There are three utilities used for calibration that ship with the UHD software for the USRP devices. These are listed below.

1. **uhd_cal_rx_iq_balance**: minimises RX IQ imbalance vs LO frequency
2. **uhd_cal_tx_dc_offset**: minimises TX DC offset vs LO frequency
3. **uhd_cal_tx_iq_balance**: minimises TX IQ imbalance vs LO frequency

ADDENDUM D HARDWARE SPECIFICATION

ETTUS RESEARCH USRP™ B100 MANUFACTURER SPECIFICATION

Specification	Type	Unit
Power		
DC Input	6	V
Current Consumption	0.6	A
Conversion Performance and Clocks		
ADC Sample Rate	64	MSPS
ADC Resolution	12	bits
ADC Wideband SFDR	83	dBc
DAC Sample Rate	128	MSPS
DAC Resolution	14	bits
DAC Wideband SFDR	83	dBc
Sample Rate to/from Host (8b/16b)	16/8	MSPS
Frequency Accuracy	2.5	ppm
w/ GPSDO Reference	0.01	ppm
RF Performance (w/ WBX)		
SSB/LO Suppression	35/50	dBc
Phase Noise(1.8 Ghz)		
10 kHz	-80	dBc/Hz
100 kHz	-100	dBc/Hz
1 MHz	-137	dBc/Hz
Power Output	15	dBm
IIP3	0	dBm
Receive Noise Figure	5	dB

ETTUS RESEARCH USRP™ B200 MANUFACTURER SPECIFICATION

Specification	Type	Unit
Power		
DC Input	6	V
Conversion Performance and Clocks		
ADC Sample Rate (max)	61.44	MS/s
ADC Resolution	12	bits
ADC Wideband SFDR	78	dBc
DAC Sample Rate (max)	61.44	MS/s
DAC Resolution	12	bits
Host Sample Rate (16b)	61.44	MS/s
w/ GPSDO Reference	0.01	ppm
RF Performance (single channel)		
SSB/LO Suppression	-35/50	dBc
3.5 GHz	1.0	deg RMS
6 GHz	1.5	deg RMS
Power Output	>10	dBm
IIP3 (@ typ NF)	-20	dBm
Receive Noise Figure	<8	dB