5-11-2009

Blind Signal Detection and Identification Over the 2.4GHz ISM Band for Cognitive

Omar Zakaria
University of South Florida

Blind Signal Detection and Identification Over the 2.4GHz ISM Band for Cognitive Radio

by

Omar Zakaria

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Electrical Engineering
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Huseyin Arslan, Ph.D.
Paris Wiley, Ph.D.
Arthur David Snider, Ph.D.

Date of Approval:
May 11, 2009

Keywords: OFDM Estimation, IEEE 802.11, Spectrum Sensing, Joint Time Frequency Analysis, Cyclostationarity Features, Feature Detector, Spectrum Awareness

Dedication

To my wife and parents.

Acknowledgements

First, I would like to sincerely thank my inspirer and my advisor, Dr. Huseyin Arslan for his encouragement, guidance, and support. It has been a great privilege to have the opportunity to work as a member of Dr. Arslan’s research team and to be under his wing. Dr. Arslan, you did not only teach me engineering, you taught me how to be a better person, and for that I give you my greatest respect and acknowledgment.

I also thank Dr. Arthur Snider and Dr. Paris Wiley for their support throughout my studies. I am honored to have their guidance throughout my master program.

Other thanks go to Dr. Srinivas Katkoori and to Catherine Burton for giving me the first chance to be in USF, and for being the first ones who believed in me.

To Ali Gorcin, Mustafa Emin Sahin, Hasari Celebi, Ahmed Hisham, and Hisham Mahmoud: thank you for your technical help, and for your priceless friendship. Special thanks to my friends Sabih Guzelgoz, and Evren Terzi and the entire WCSP group.

I also want to thank my parents, and my uncle Faris for their support, love, and selfless dedication toward me. My deepest gratitude goes to my wife, Dana, for her love and all the sacrifices she has made, for her support, vast patience, and steady encouragement. Dana, many times I felt that this is the end of the line, but you always managed to pull me back on the track and keep me going. For that I give you my heartfelt thanks.

Table of Contents

List of Tables iv

List of Figures v

List of Acronyms viii

Abstract x

Chapter 1 Introduction 1
- 1.1 Organization of the Thesis 3

Chapter 2 Cognitive Radio Model 5
- 2.1 Introduction 5
- 2.2 Cognitive Radio History 7
- 2.3 Spectrum Sensing in Cognitive Radio 10
  - 2.3.1 Matched Filter 12
  - 2.3.2 Energy Detector 14
  - 2.3.3 Cyclostationarity Detector 17
- 2.4 Proposed Model 18
  - 2.4.1 The RF Front End 20
    - 2.4.1.1 The Sampling and Data Conversion Challenge 20
  - 2.4.2 The Energy Detector 22
  - 2.4.3 The Feature Extraction 24
  - 2.4.4 The Central Processing Unit (CPU) 24
  - 2.4.5 Adaptive Transmitter 25
- 2.5 Conclusion 25

Chapter 3 The ISM Band 26
- 3.1 Introduction 26
- 3.2 The Wireless Communication Systems 29
  - 3.2.1 Spread Spectrum 29
  - 3.2.2 Orthogonal Frequency Division Multiplexing (OFDM) 35
    - 3.2.2.1 OFDM System Model 37
    - 3.2.2.2 Cyclic Prefix in OFDM Symbol 39
- 3.3 WiFi IEEE 802.11 Standards 41
  - 3.3.1 WiFi IEEE 802.11b 42
  - 3.3.2 WiFi IEEE 802.11g 47

3.4 IEEE 802.15.1/2 Bluetooth 50
3.5 IEEE 802.15.4 Zigbee Networks 51
3.6 Microwave Ovens 53
3.7 Cordless Phones 55
3.8 Unknown Signals 56
3.9 Conclusion 56

Chapter 4 Features Extraction 58
4.1 Introduction 58
4.2 Feature Detector 59
4.3 Bandwidth and Central Frequency Estimation 61
4.3.1 Heisenberg-Gabor Principle 62
4.4 Power Related Metrics 65
4.4.1 CCDF 66
4.5 Single Carrier versus Multicarrier 68
4.5.1 Moments Based Test 69
4.6 Modulation Order and Type of Single Carrier Signals 75
4.7 OFDM Signals Parameters Estimation 76
4.7.1 OFDM Time Parameters Estimation 77
4.7.1.1 Useful Symbol Duration 78
4.7.1.2 Total Symbol Duration 80
4.7.1.3 Cyclic Prefix Duration 82
4.7.2 OFDM Frequency Domain Parameters 83
4.8 Cyclostationarity Features 84
4.8.1 Introduction to Cyclostationarity 85
4.8.2 Cyclostationarity for Signal Detection 90
4.8.2.1 Symbol Rate Detection 91
4.8.2.2 Chip Rate Estimation 99
4.9 Hopping Sequence 101
4.9.1 Joint Time Frequency Analysis 101
4.9.2 Spectrogram 102
4.10 Conclusion 104

Chapter 5 Decision Making Algorithm 105
5.1 Introduction 105
5.2 The Proposed Framework 106
5.3 The Decision Making 108
5.3.1 FCC Regulations for the ISM Band 110
5.3.2 Control and Execution 111
5.3.3 Fuzzy Logic and Soft Decision Algorithm 113
5.4 Location and Time of Occurrence 119
5.5 Conclusion 120

Chapter 6 Summary and Conclusions 121
6.1 Summary of Works and Contributions 121
6.2 Conclusions 123

6.3 Future Work 124

References 126

List of Tables

Table 3.1 The three main branches of the IEEE 802.11 standard 42

Table 3.2 The 11 channels assigned by the FCC to the ISM band 43

Table 3.3 IEEE 802.11b data rate specifications 44

Table 3.4 Possible Barker codes 44

Table 3.5 The generation of the CCK codes depending on the data bits 46

Table 3.6 Data rate modes and modulation for IEEE 802.11g standard 48

Table 3.7 Three defined power categories for Bluetooth transmission 51

Table 4.1 Ideal values for k_{20} and k_{30} 71

Table 4.2 Ideal values for m_{20} and m_{30} 72

Table 5.1 The identifying features for each wireless standard 109

Table 5.2 The FL decision tree of Example 1 115

Table 5.3 The FL decision tree of Example 2 117

Table 5.4 The algorithm performance results of success rate detection 118

List of Figures

Figure 2.1: The frequency spectrum allocation in the US [32] 6

Figure 2.2: Cognitive radio transceiver (courtesy of the author [43]) 10

Figure 2.3: The detection probability of the energy detector in different SNR values 17

Figure 2.4: Spectrum awareness engine 19

Figure 2.5: Frequency domain energy detector 24

Figure 3.1: The ISM and U-NII bands [7] 26

Figure 3.2: The process of spreading the information spectrum 30

Figure 3.3: Illustration showing the DSSS immunity to narrow band interference 31

Figure 3.4: Basic DSSS communication system 33

Figure 3.5: Frequency hopping spread spectrum basic transceiver 34

Figure 3.6: Spectrum of hopping signal 34

Figure 3.7: OFDM signal of six subcarriers 36

Figure 3.8: Typical OFDM system 39

Figure 3.9: Illustration of cyclic prefix extension 40

Figure 3.10: Illustration of the condition for two codes to be complementary to each other 45

Figure 3.11: A typical IEEE 802.11b receiver 47

Figure 3.12: The spectrum of a microwave oven signal 54

Figure 3.13: Microwave oven time domain signal 54

Figure 4.1: The proposed model 60

Figure 4.2: Bandwidth estimation error with SNR values 65

Figure 4.3: CCDF implementation 67

Figure 4.4: CCDF curves for different modulation schemes 68

Figure 4.5: Moments test performance with different SNR values 74

Figure 4.6: Moments test for FSK signals with different orders in 10 tabs channel, SNR=0 76

Figure 4.7: The structure of the OFDM symbols 78

Figure 4.8: Useful symbol duration estimation algorithm results over different SNR values for 10 OFDM symbols with useful symbol duration of 512 samples 80

Figure 4.9: The sliding window technique for estimating the total symbol duration 81

Figure 4.10: The result of the sliding window correlation based algorithm when tested on the same OFDM symbols for different CP lengths 82

Figure 4.11: The success rate of the time parameters estimation 83

Figure 4.12: The cyclostationary detector results for three different cyclostationary signals 88

Figure 4.13: PSD of $a(t)$ and $x(t)$ 92

Figure 4.14: PSD of $b(t)$ and $y(t)$ 93

Figure 4.15: The pulse-shaping process 94

Figure 4.16: PSD of the pulse-shaped signal $x(t)$ 94

Figure 4.17: PSD of $y(t)$ 96

Figure 4.18: Symbol rate estimation without and with using Welch periodogram 97

Figure 4.19: Symbol rate estimation algorithm performances with respect to SNR 98

Figure 4.20: WLAN IEEE 802.11b DSSS signal when tested using the nonlinear algorithm 100

Figure 4.21: Typical WLAN DSSS transmitter 100

Figure 4.22: Spectrogram representation of a Bluetooth signal 103

Figure 5.1: The spectrum awareness engine flow chart 107

Figure 5.2: Feature detection and decision making flow chart 112

Figure 5.3: The algorithm response for a WLAN 802.11g input signal 114

Figure 5.4: The algorithm response for a Bluetooth input signal 116

List of Acronyms

Federal Communications Commission (FCC)

National Information Infrastructure (NII)

The International Telecommunications Union (ITU)

Industrial Scientific and Medical (ISM)

Spectrum Policy Task Force (SPTF)

Central Processing Unit (CPU)

Unlicensed-NII (U-NII)

Pseudo Noise Code (PN code)

Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

Orthogonal Frequency Division Multiplexing (OFDM)

Frequency Division Multiplexing (FDM)

Peak-to-Average Power Ratio (PAPR)

Digital Audio Broadcasting (DAB)

Wireless Local Area Networks (WLAN)

Asymmetric Digital Subscriber Line (ADSL)

Fast Fourier Transforms (FFT)

Discrete Fourier Transforms (DFT)

Phase Shift Keying (PSK)

Quadrature Amplitude Modulation (QAM)

Inter-Carrier Interference (ICI)

Inter-Symbol interference (ISI)

Cyclic Prefix (CP)

Time Division Duplex (TDD)

Microwave Oven (MWO)

Complementary Cumulative Distribution Function (CCDF)

Minimum Mean Squared Error (MMSE)

Power Spectrum Density (PSD)

Fuzzy Logic (FL)

Blind Signal Detection and Identification Over the 2.4GHz ISM Band for Cognitive Radio

Omar Zakaria

ABSTRACT

“It is not a lack of spectrum. It is an issue of efficient use of the available spectrum”--conclusions of the FCC Spectrum Policy Task Force.

There is growing interest towards providing broadband communication with high bit rates and throughput, especially in the ISM band, as it was an ignition of innovation triggered by the FCC to provide, to some extent, a regulation-free band that anyone can use. But with such freedom comes the risk of interference and more responsibility to avoid causing it. Therefore, the need for accurate interference detection and identification, along with good blind detection capabilities are inevitable. Since cognitive radio is being adopted widely as more researchers consider it the ultimate solution for efficient spectrum sharing [1], it is reasonable to study the cognitive radio in the ISM band [2].

Many indications show that the ISM band will have less regulation in the future, and some even predict that the ISM may be completely regulation free [3]. In the dawn of cognitive radio, more knowledge about possible interfering signals should play a major role in determining optimal transmitter configurations.

Since signal identification and interference will be the core concerns [4], [5], we will describe a novel approach for a cognitive radio spectrum sensing engine, which will be essential to design more efficient ISM band transceivers.

In this thesis we propose a novel spectrum awareness engine to be integrated in the cognitive radios. Furthermore, the proposed engine is specialized for the ISM band, assuming that it can be one of the most challenging bands due to its free-to-use approach. It is shown that characterization of the interfering signals will help with overcoming their effects. This knowledge is invaluable to help choose the best configuration for the transceivers and will help to support the efforts of the coexistence attempts between wireless devices in such bands.

Chapter 1

Introduction

“Are you ready?” This was the message content of the first wireless transmission on May 13, 1897 by Marconi [16]. From that early time, people began to realize the importance of wireless communication and the scarcity of the electromagnetic spectrum. Wireless networks in the US can only operate in the band of frequencies allowed by the Federal Communications Commission (FCC), and must follow the rules regulating the way that spectrum can be used. The FCC regulations are designed to set usage rules, increase the spectrum resource usage efficiency, and to prevent interference. Until 1985 a large portion of the spectrum in the US was leased to individuals exclusively for particular services such as cellular or TV broadcasting. At that time, interference was not a large problem, as long as the users stayed within their assigned band of frequency spectrum.

In 1985 the FCC put in place a creative plan by opening an unlicensed band of 2.4GHz for wireless networks. This band was regulated by the FCC Part 15 rules [1]. These rules allow new and existing technologies to share the same frequency band and try to coexist and operate together. The FCC explained that creativity and better spectrum efficiency usage would be the results from opening a shared portion of the spectrum for the uncoordinated wireless devices.

In 1995, Apple Company petitioned the FCC to create a new unlicensed 5GHz band called National Information Infrastructure (NII). Differing from the 2.5GHz unlicensed band, the NII technologies rules restrict possible uses of the NII band to wireless networks that use wideband communications. The International Telecommunication Union (ITU) announced a number of bands for industrial, scientific and medical (ISM) applications and services that are not restricted to any specific wireless technologies. The ITU develops frequency assignments that are adopted by countries in all regions by international treaty [4].

From the early beginnings of the ISM band, it became one of the popular destinations for wireless system manufacturers. With the increasing demand for the wireless networks, especially with today's applications and services that need high bit rate like video streaming, there was an increasing need for frequency spectrum resource availability, not to mention the importance of peaceful coexistence between wireless users. Therefore the FCC began to encourage innovation and creativity to enhance spectrum usage, and it began with the ISM band. FCC was open to new approaches and techniques to efficiently share the spectrum in the ISM band. One of the more promising techniques that were looked at with hope was the cognitive radio. Cognitive radio has the ability to sense, adapt and learn to overcome environment changes and possible interference [36]. The biggest challenges with cognitive radio are the ability to identify the existence of the primary users and avoid interfering with them or with other cognitive radios. To have this ability, cognitive radio needs to constantly sense the spectrum and identify possible wireless users and based on the identification result, make the appropriate decision to overcome their effect as interference.

1.1 Organization of the Thesis

The main topics covered in this thesis can be summarized as follows:

a. Cognitive radio, models and applications (Chapter 2)

b. The ISM band and its players, descriptions and analysis (Chapter 3)

c. Wireless signals features, analysis and extractions (Chapter 4)

d. Smarter decision making in spectrum sensing (Chapter 5)

The outlines of these chapters are as follows. In Chapter 2, the cognitive radio concept is provided with a brief historical look into cognitive radio evolution over the last decade. A conventional model of cognitive radio transceivers [43] is described, and analyzed. A detailed description for various spectrum sensing techniques is provided, with an evaluation of each technique's performance. A proposal for a spectrum awareness engine is described, to be integrated in the cognitive radio transceivers model. A description of the first two stages (the RF front end and the energy detector) of the proposed model is provided.

An extensive study about the ISM band is provided in Chapter 3, along with thorough analysis of the main wireless standards that are active in the ISM band. A brief description of the main modulation schemes that are commonly used in the ISM band is also provided in this chapter.

In Chapter 4, a description of the ISM band spectrum sensing feature detector is proposed. We submit a list of wireless signal's features that are useful in the process of identifying them. Algorithms are proposed to extract and detect each feature in the list, while maintaining the lowest computational complexity as possible.

In Chapter 5, we demonstrate how different wirelesses standards may inherit similar features which may lead to confusion during the detection process. A novel algorithm is proposed to utilize the extracted features before making the decision, along with a controlling algorithm, to regulate the rest of the spectrum awareness engine's units.

The thesis concludes with Chapter 6, in which we summarize the thesis and discuss open research areas.

Chapter 2

Cognitive Radio Model

In this chapter we discuss the cognitive radio technologies and examine the ideology and the evolutionary history of the cognitive radios. We will choose one of the proposed architecture and try to design a realistic model to be integrated in the proposed cognitive radio architecture.

2.1 Introduction

With the increased number of wireless devices and the number of users, the awareness of the frequency spectrum scarcity increased. From the early dawn of the wireless communications era, engineers realized the importance of utilizing the spectrum to increase the number of users and provide better quality of service. A closer look at the frequency spectrum allocation by the FCC shows that the spectrum is greatly underutilized [32]. Figure 2.1 shows the current frequency spectrum allocation in the US.

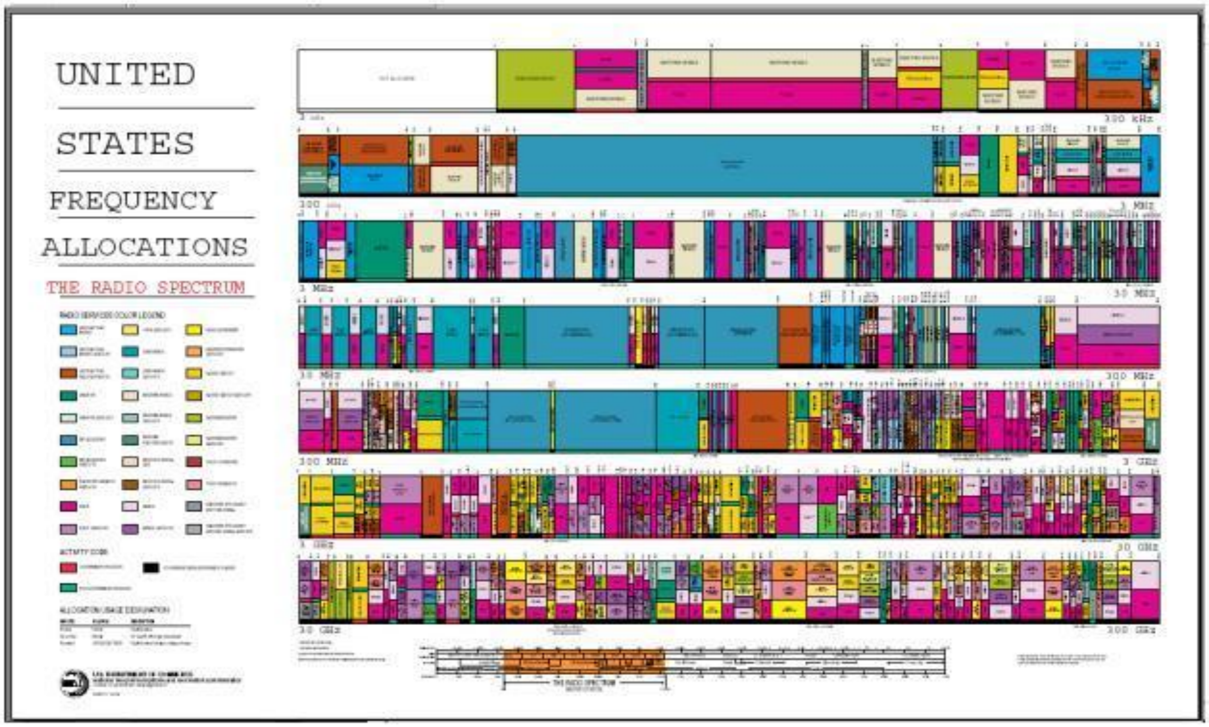


Fig 2.1 The frequency spectrum allocation in the US [32]

In June 2002, the Spectrum Policy Task Force (SPTF) was established to assist the FCC in the process of identifying and evaluating changes in spectrum policy to help increase the public benefits derived from the use of the radio spectrum [33]. The SPTF released a report in November 2002 [34]. In this report, the SPTF demonstrated that the current usage for the spectrum is not very efficient and recommended rules and regulations for the efficient use of the radio spectrum and ways to improve the existing spectrum usage. Cognitive radio is being widely adapted, as many researchers look to it as the ultimate solution for efficient spectrum sharing [35]-[41]. Even though there is no formal definition of cognitive radio, the concept is being addressed by researchers in various contexts as well as many efforts to standardize it [42]. The FCC attempts to define cognitive radio as, “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 [to] maximize throughput, mitigate interference, facilitate interoperability, [and] access secondary markets." [47]

The main works of this chapter are to:

a. Define cognitive radio and analyze its functionalities.

b. Study one conceptual cognitive radio architecture extensively.

c. Propose a novel and realistic design for the spectrum awareness engine in the mentioned architecture.

d. Propose a combination of spectrum sensing algorithms to blindly identify primary signals.

2.2 Cognitive Radio History

Cognitive radio is a relatively new concept proposed by Joseph Mitola [35] in 1999. The concept aims to create a new smart generation of communication systems that dynamically interact with the environment in real time to modify its parameters, such as band of operation, central frequency, waveforms, and the used modulation. It aims to establish wireless systems with a state of awareness that will efficiently utilize the spectrum, with the ability to sense, learn and adapt [36]. Cognitive radio provides a solution for the spectrum underutilization problem, through an opportunistic spectrum usage [37], [38], [40]. The main idea is to temporarily use the frequency channels that are currently not occupied by the licensed user (primary) through cognitive radios (secondary) who are constantly looking for opportunities in the spectrum without disturbing the primary user.

In 1999 Mitola described the cognitive radio's capabilities through a cognition cycle [35], where the cognitive radios interact with the outside world through:

a. Observation through the cognitive radio sensors

b. Orientation, to establish priorities

c. Planning, to develop the appropriate possible set of actions

d. Decision, to choose the best plan for the current set of factors

e. Action, to execute the decision that been taken

f. Learning. This function is a cross function between observing, planning and deciding, to enable the cognitive radio to learn from the past in order to better plan in the future.

In 2005 a simplified understanding of the cognitive cycle was proposed by Haykin [36], where the focus is on three basic units:

a. Spectrum sensing unit, which mainly deals with spectrum sensing analysis and white holes detection

b. Channel identification unit, which deals with channel estimation

c. Dynamic spectrum managements unit, to cognitively manage the spectrum resources

The publisher explained that spectrum sensing and channel identification functionalities are part of the receiver responsibilities, while the dynamic spectrum management's function is carried out by the transmitter.

In 2008 a novel cognitive radio model was proposed [43]. This model describes a cognitive radio transceiver form that consists of mainly four engines:

a. Cognitive engine
b. Spectrum awareness engine
c. Location awareness engine
d. Environment awareness engine

The author considered the cognitive engine to be the main entity that controls and monitors the other entities in the model in order to have goal-driven and self-directed task results. In the four-engine model, all the information generated by the engines goes to the cognitive engine so that the proper system configuration, for example, the proper waveform, will be decided by the cognitive engine.

The main responsibility of spectrum awareness engine is to handle any job related to the frequency spectrum usage and efficiency, not to mention the most important role for this engine, the sensing part, where the success of the cognitive radio will greatly depend on its ability to detect unoccupied spectrum. Figure 2.2 demonstrates the cognitive system model we will adopt in our research.

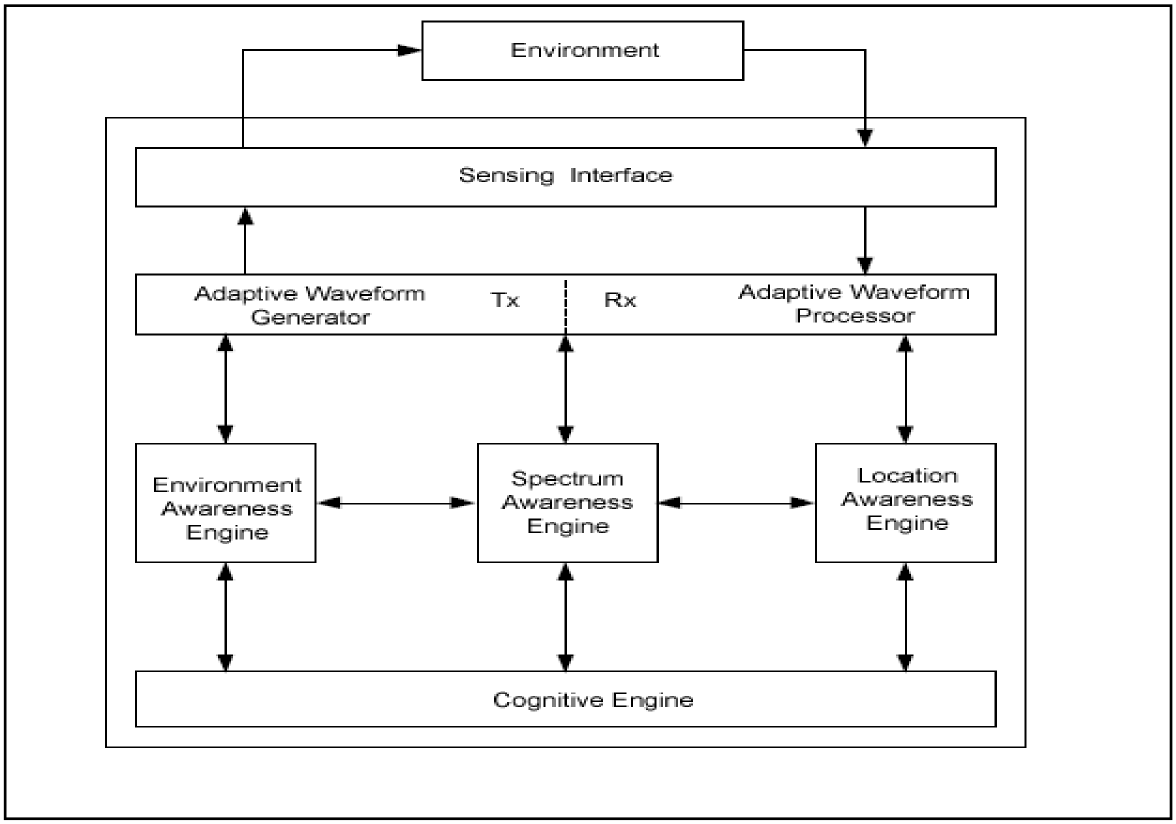

Environment
Sensing Interface
Adaptive Waveform Generator
Tx
Rx
Adaptive Waveform Processor
Environment Awareness Engine
Spectrum Awareness Engine
Location Awareness Engine
Cognitive Engine

Fig 2.2 Cognitive radio transceiver (courtesy of the author [43])

2.3 Spectrum Sensing in Cognitive Radio

To achieve the main goal of the cognitive radio, which is utilizing spectrum usage, the system needs to continuously monitor the spectrum and identify any white spaces that may become available. A brief literature scan shows that there are three common techniques that can be used for spectrum sensing:

a. Matched filter

b. Energy detector

c. Cyclostationarity detector

Before we explain more about the three techniques, let us assume the following hypothesis for detecting a signal:

$$H_0 : y[n] = \ w[n] \qquad\qquad n = 0,1 \ldots, N-1 \tag{1}$$

$$H_1 \ : y[n] = \ x[n] + \ w[n] \qquad n = 0,1 \ldots, N-1 \tag{2}$$

where $x[n]$ is the transmitted signal, and $w[n]$ is the added white noise. The white noise is usually modeled as a Gaussian zero mean distribution density $w[n] \sim Normal(0, {\sigma_w}^2)$; therefore the spectral density of the noise is assumed to be σ^2. H_0 represents the null hypothesis, and H_1 represents the detection hypothesis. That means that $x[n]$ equal zero in case of H_0 .

The performance of the detection system can be characterized by two probabilistic measurements, the probability of detection P_D and probability of false alarm P_{FA}. The probability P_D describes the probability of detecting the desired signal on the spectrum when the signal is truly present. Needless to say, we desire the largest probability. On the other hand, P_F represents the probability that the test incorrectly decides that the signal exists when it does not. Therefore we try to minimize the false detection probability value as much as we can. It is important to point out that usually in detection systems, increasing the P_D will increase the P_{FA} as well, and vice versa. Therefore it is important to find the optimum balance between these probabilities in any detection algorithm [50].

2.3.1 Matched Filter

Matched filter is a filter that maximizes the signal to noise ratio. The main strength of this filter is that due to the coherency; the filter does not need a long time to achieve high processing gain [44]. In the case that the receiver has perfect knowledge of the transmitted signal, the matched filter will be the optimal detector [45]; in this case the optimal detector test statistic will be [48]:

$$T(y) = \sum_{N} y[n]x[n] \tag{3}$$

This test equation, along with a predefined threshold, γ, will be used in the signal detection process, where $H_1 = T > \gamma$ represents the presence of the signal, and $H_0 = T < \gamma$ represents the absence of the signal. The value of threshold γ is critical as it impacts the desired detection and false alarm probabilities. The proof is in the following analysis.

As shown previously, $y[n]$ is a jointly Gaussian random variable. Since T is a result of linear operation of jointly Gaussian random variables, consequently it is Gaussian. Therefore, if we define P as the average power of the sampled signal [48], which is

$$P = \frac{1}{N}\sum_{N}(X[n])^2 \tag{4}$$

then:

$T{\sim}Normal(0,\frac{1}{N}{\sigma_w}^2P)$ in the case of H_0 (5)

and

$T{\sim}Normal(P,\frac{1}{N}{\sigma_w}^2P)$ in the case of H_1 (6)

So the $P_D = P(T(Y) > \gamma|H_1)$

$$P_D = Q\left(\frac{\gamma - P}{\sqrt{\frac{P{\sigma_w}^2}{N}}}\right) \tag{7}$$

In the same way,

$$P_{FA} = \mathrm{P(T(Y)} > \gamma|H_0) \tag{8}$$

$$P_{FA} = Q\left(\frac{\gamma}{\sqrt{\frac{P{\sigma_w}^2}{N}}}\right) \tag{9}$$

In [48] it is shown that the minimum number of samples needed for a successful detection is a function of the Signal to Noise Ratio (SNR) and SNR = $\frac{{\sigma_X}^2}{{\sigma_W}^2}$. Therefore,

$$N = [Q^{-1}(\,P_{FA}) - Q^{-1}(\,P_D)]^2 SNR^{-1} \tag{10}$$

$$N = \mathrm{O}(\mathrm{SNR}^{-1}) \tag{11}$$

where the O notation represents the limiting behavior of the original number of samples function simplified to focus on its growth rate. Thus, 1/SNR is considered the lower bound on the number of samples which is related to the sensing time. As we mentioned before, in the case that the receiver already has satisfactory knowledge of the transmitted signal, the matched filter will be the optimal detector. However, this is usually not the case, as we often do not have prior information about the signal. Also since the cognitive radio will employ matched filter techniques to perform the detection, it will need a receiver design for each possible signal, making it difficult to implement in real life [46].

2.3.2 Energy Detector

Opposite to the matched filter method, the energy detector is used when there is no prior information about the signal. It also has low computational and implementation complexity. For all these reasons, it is one of the common detectors [48], [49], [50], [51], [52]. In this detector the signal energy is compared to a predefined threshold to decide if the signal is present or absent. This threshold can be adjustable in an adaptive way depending on the noise variance and the channel [50], [75].

Using the same assumption for the H_0 and H_1 in the previous sections, we know that the noise variance is ${\sigma_w}^2$. Since we do not have prior information about the signal, we can model the samples of the signal $x[n]$ as a Gaussian random process with variance of ${\sigma_X}^2$.

The detector test statistic will be:

$$T(y) = \sum_{N} (y[n])^2 \tag{12}$$

This test equation, along with a predefined threshold, γ, will be used in the signal detection process, where $H_1 = T > \gamma$ represents the presence of the signal, and $H_0 = T < \gamma$ represents the absence of the signal. The value of threshold γ is critical as it impacts the desired detection and false alarm probabilities.

Therefore the P_D

$$P_D = P(T(y) > \gamma | H_1) \tag{13}$$

$$P_D = Q\left(\frac{\frac{\gamma}{\sigma_w{}^2} - N}{\sqrt{2N}}\right) \tag{14}$$

In the same way:

$$P_{FA} = \mathrm{P}(\mathrm{T(y)} > \gamma | H_0) \tag{15}$$

$$P_{FA} = Q\left(\frac{\frac{\gamma}{\sigma_w{}^2} - \gamma - N}{\sqrt{4\gamma + 2N}}\right) \tag{16}$$

Closed form expressions for probability of detection under AWGN and fading (Rayleigh, Nakagami, and Ricean) channels are derived. Average probability of detection for energy detector based sensing algorithms under log-normal shadowing and Rayleigh fading channels is derived in [76].

Also it is proven that the minimum number of sampled required is

$$N = [Q^{-1}(\,P_{FA}) - Q^{-1}(\,P_D)]^2 SNR^{-2} \tag{17}$$

$$N = \mathrm{O}(\mathrm{SNR}^{-2}) \tag{18}$$

It is obvious for this kind of detector we need a higher number of samples in case of low SNRs compared to the matched filter detector. Some of the difficulties with the spectrum sensing based on the energy detector alone are:

a. The threshold value selection

b. The inability to distinguish interference from primary signal

c. Poor performance under low SNR values [74]

The performance of the energy detector for 10 OFDM symbols in a Gaussian noise channel is shown in Figure 2.3.

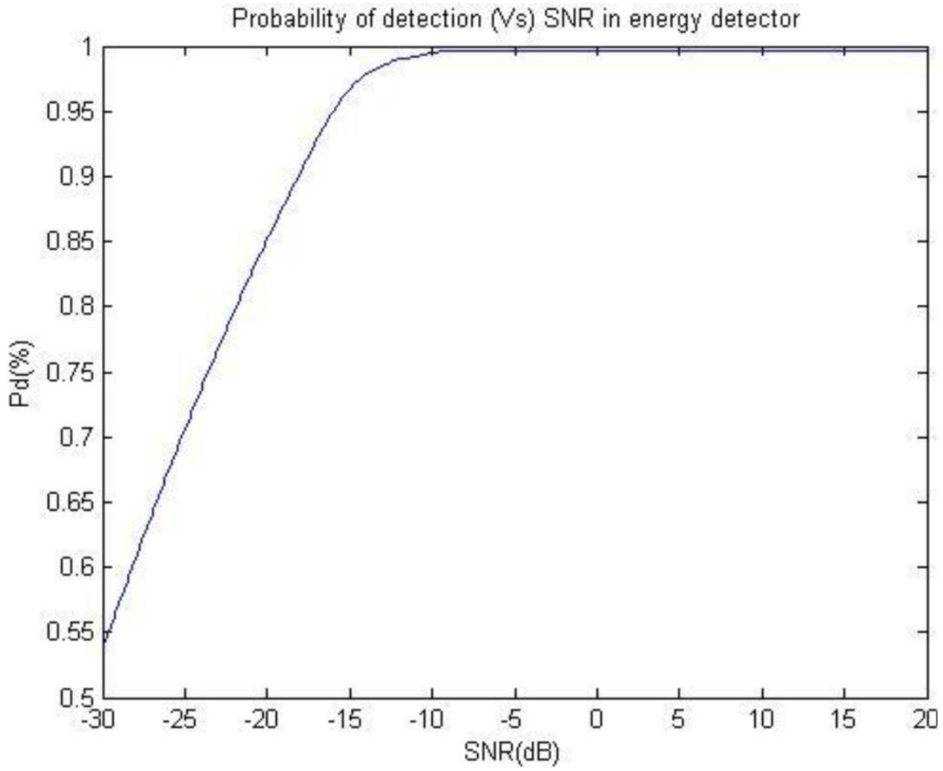


Fig 2.3 The detection probability of the energy detector in different SNR values

2.3.3 Cyclostationarity Detector

Another technique used recently in research is the cyclostationary features searching in signals as a way to identify them. The cyclostationary theory was first introduced by Gardner [54] in his famous paper series about the exploitation of the cyclostationary features in random processes [54]-[63]. Gardner tried to analyze the signals by extracting the hidden frequencies that exist in manmade signals due to modulation, pulse-shaping, shifting in frequency, sampling, repeated spreading codes, and any operation that may introduce a signal through the communication system. The theory explained that the communication processes that are applied on the original source signals introduce hidden frequencies (the author calls these cyclic frequencies) in the result signal. These frequencies can be detected using a mathematical tool developed by Gardner which is the cyclic autocorrelation and the spectral correlation function. In the past, the computational complexity was a large problem in the cyclostationarity analysis operations due to the nature of the estimation [64]. But with the development of FPGAs and microprocessors, this theory became popular is used in many proposed algorithms for signal detections [65]-[70]. We will explain more about the cyclostationary analysis in Chapter 4.

2.4 Proposed Model

Three detection techniques are used in this research for the purposes of spectrum sensing: energy detection, matched filtering, and cyclostationary feature detection. The three techniques are combined in the spectrum awareness engine design. Figure 2.4 describes the proposed spectrum awareness engine.

The proposed model consists mainly of five units:

a. RF front ends

b. Energy detector for initial stage channel sensing

c. Features extraction unit, for detailed detection and identification

d. Processing unit for decision making and controlling the engine component

e. Adaptive waveform generator of the transmitter (included for consistency)

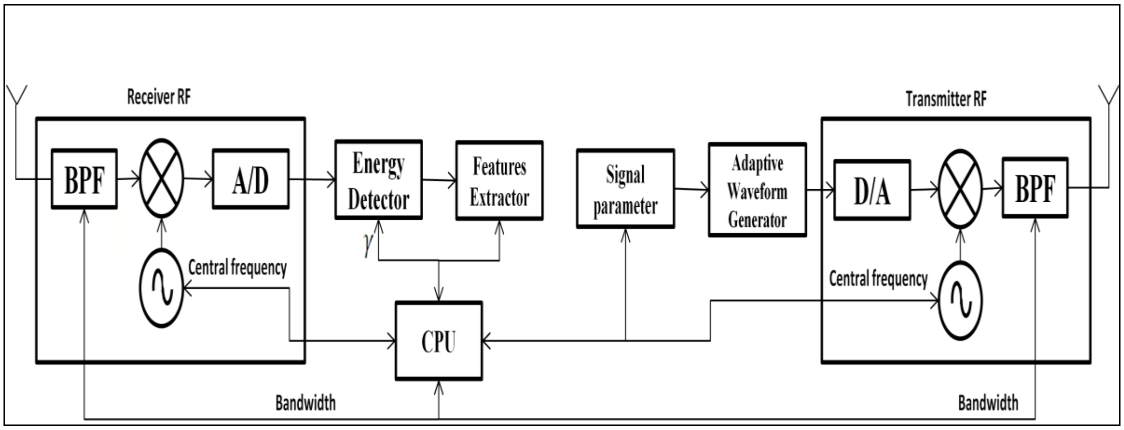


Fig 2.4 Spectrum awareness engine

As shown in [43], the spectrum awareness engine will pass the information to the cognitive engine and both the location awareness and the environment awareness engines. All these engines will cooperate to decide the best configuration for the current situation the cognitive radio is in.

An example on how the spectrum awareness engine can cooperate with the location and/or environment engines can be that the expected range information of the detected signal can be fed to the location awareness engine to participate in the decision making of the location, especially in the case of known wireless standards where usually the average range of the signal is predefined. As for the role of the spectrum engine information on the waveform configuration, it is important to know signal features such as the duty cycle, the used hopping sequence, and the number of subcarriers, in order to design a signal that is robust against interference. In the following subsection we will briefly describe each unit of the spectrum awareness engine.

2.4.1 The RF Front End

From the cognitive radio point of view, having an effective spectrum sensing ability requires cognitive radio to cover a large range of frequencies at the RF front end and then carry on the sampling process through a high speed analog to digital (A/D) converter. This particular task became more possible after the development of sub-sampling theorem and techniques.

2.4.1.1 The Sampling and Data Conversion Challenge

In cognitive radio applications, RF signals need to be directly digitized by the cognitive radio RF front end [35], [40]. According to Nyquist, in order to successfully reconstruct a sampled signal, we must sample the signal at no less than twice the frequency of its highest frequency components. Cognitive radio will deal with a wide range of frequencies, especially in the range of Giga-Hertz like the ISM band. This means that the ADC needs to sample the signals at much higher speeds than what current ADCs are capable of. To give an example, if we seek a signal in the ISM band with a central frequency of 2.4GHz, we will need to sample it with a sampling frequency of at least 5GHz. Many techniques were developed to solve this sampling frequency problem in cognitive radios. One of these solutions is the sub-sampling or “baseband sampling theorem” technique [80], [79]. This theory states that if a band pass waveform has a spectrum over the frequency band:

$$f_l < |f| < f_h \tag{19}$$

and occupied bandwidth of

$$B_T = f_{h-}f_l \qquad (20)$$

the signal may be reproduced from sample values if the sampling rate is

$$f_s =\geq 2B_T \qquad (21)$$

Thus, instead of requiring an ADC with a sampling frequency at the Nyquist rate of at least $2f_h$, baseband sampling allows an ADC with a much lower sampling rate to do the same job. This leads to much lower signal processing.

After sampling the signal, measurements for detection of the primary user will be carried out [71]. We can safely say that one of the succession factors for the cognitive radio will be the RF front end quality and flexibility to scan wideband in accurate and sensitive manners [46]. In the proposed algorithm, the band of interest will be selected, down converted to the baseband, and sampled through the wideband antennas with the help of adjustable band pass filters and the down converters. Signals can be found anywhere in the spectrum band of interest, which raises the need for adjustable filters and local oscillators for the down conversion [78]. The dynamic range of the signal is an important factor in the cognitive radio RF front end to have suitable sensitivity for the low SNR signals. This is where the role of the A/D converter comes in, as it should be adaptive enough to cover a wide range of dynamic ranges.

The output of the filter is sampled at Nyquist rate and N-point FFT is applied to obtain the frequency domain samples which can be modeled as:

$$Y(n)=\begin{cases} W(k) & H_0 \\ X(k)+W(k) & H_1 \end{cases} \qquad k=1,\dots,N \qquad (22)$$

where X(n) the transmitted signal at the output of the FFT is W(n) is the white noise samples, and N is the used FFT size. Many studies dealing with the RF front end design and issues have been conducted [46], [71]-[73]. However, because it is not our focus in this study, we will not consider them.

2.4.2 The Energy Detector

In this research we propose an energy detector as first stage sensing to help detect the presence of the signals before we process the sampled data and extract its features. This way we reduce the computational complexity of the whole process. After successfully receiving and sampling the band of interest, the blind signal detection process will begin in a form of energy detector to initially decide if there is a signal or just noise. The energy detector will also help in the decision process of whether the width of the band pass filter is sufficient enough to capture the whole signal without losing any frequency domain information. Fine tuning to the correct central frequency and bandwidth of the presented signal will help in achieving some coherency in the detection. Furthermore, detecting the bandwidth of the signal will help to sample the filtered band at Nyquist rate.

The energy detection is performed in the frequency domain. The magnitude square of the fast Fourier transforms (FFT) of the signal is calculated, and the output is compared to a predefined threshold γ to make the first judgment if a signal exists or not. The processing gain in this method will be proportional to FFT size N and the averaging time T. Increase in the size of FFT improves the frequency resolution, which is helpful in detecting narrow band signals. Furthermore, if we reduce the averaging time, it improves the SNR by reducing the noise power [44]. The energy estimation in the frequency domain can be described as:

$$E(Y) = \sum_{k} |Y(k)|^2 \qquad (23)$$

where $Y(k)$ represents the FFT output of the sampled spectrum and

$$Y(k) = \begin{cases} W(k) & H_0 \\ S(k) + W(k) & H_1 \end{cases} \qquad k = 1, \dots, N \qquad (24)$$

So the detection criteria will depend on the test equation, along with a predefined threshold γ, where $H_1 = E > \gamma$ represents the presence of the signal, and $H_0 = E < \gamma$ represents the absence of the signal.

The impact of choosing the threshold γ on the detection performance was explained in Section 2.2. Figure 2.5 demonstrates the proposed energy detector design.

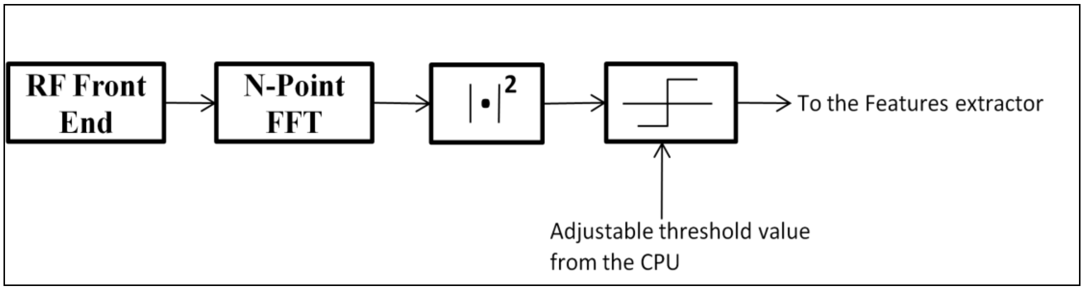

RF Front End
N-Point FFT
$|\bullet|^2$
To the Features extractor
Adjustable threshold value from the CPU

Fig 2.5 Frequency domain energy detector

2.4.3 The Feature Extraction

When detecting energy in the band of interest which may indicate the presence of a signal, the sampled signal will be passed to the features extractor to detect the main features that are present, especially the bandwidth and central frequency so as to fine-tune the RF front end. Also in this stage, detailed identification will be carried out based on the detecting features present in the signal. This process will thoroughly be explained in Chapter 4 where we illustrate the features extraction methods and the cyclostationarity detection method.

2.4.4 The Central Processing Unit (CPU)

This unit is responsible for the decision making process that is based on the parameters coming from the rest of the sensing and feature detection units. Also, the CPU controls the rest of the engine units to optimize the spectrum awareness engine. This stage will be explained in Chapter 5 where we describe the decision making algorithm.

2.4.5 Adaptive Transmitter

After identifying white spaces in the spectrum, detecting if there are any active signal(s), and revealing its properties, the spectrum awareness engine should use the proper configuration for the transmitter that provides the best spectrum utilization and interference robustness. Some of these configurations will use modulation schemes, duty cycle, hopping sequence, band of operation, bandwidth, etc. By the spectrum awareness engine doing this and by cooperating with the rest of the cognitive radio engines, the best performance outcome is achieved.

2.5 Conclusion

In this chapter, we examined the concept of the cognitive radio, and briefly described its history and previous work in cognitive radio research. The cognitive radio is built on the principal of opportunity to efficiently utilize the frequency spectrum. A creative model of cognitive radio architecture with location and environment awareness cycles [43] was described. The importance of the spectrum awareness and spectrum sensing of the model was addressed and a brief analysis of the various spectrum sensing was conducted. In this chapter we proposed a novel design for spectrum awareness engine and spectrum sensing algorithm that will be integrated with the cognitive radio architecture [43]. The RF front end and the energy detector unit design were also described.

Chapter 3

The ISM Band

In this chapter we will discuss the ISM band features and the FCC regulations for this band. We will discuss the main features of the active wireless standards in the ISM band.

3.1 Introduction

In the US, the FCC defines the ISM and unlicensed-NII (U-NII) bands as shown in Figure 3.1. The ISM bands are scattered in three different frequency bands, namely 900MHz, 2.4GHz, and 5.7GHz. U-NII bands are mainly located in the 5GHz segment of the frequency spectrum.

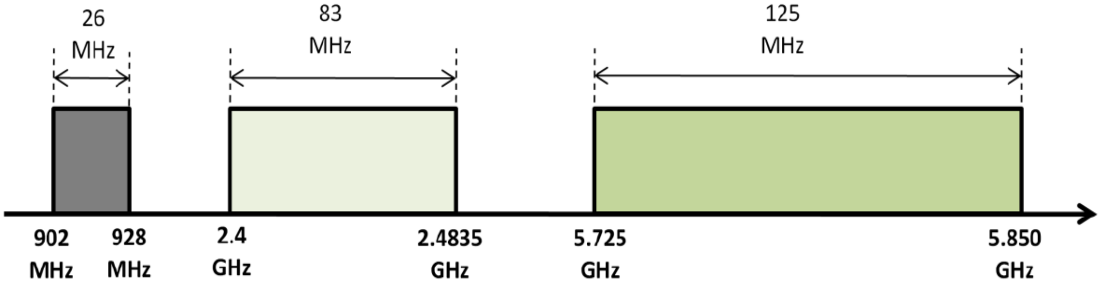


Fig 3.1 The ISM and U-NII bands [7]

Those bands are license-free, where manufacturers that build wireless devices operating in these bands are not required to buy the spectrum from FCC. However, there are some regulations concerning these bands and these are outlined in [1]. Each band has its own regulation, and regulations may change from one to another.

The 2.4GHz band provides an attractive medium for many applications using the wireless technology that currently exists or may come up in the future. Different from other frequency bands where interference is avoided between wireless devices through separation of operating frequencies, the ISM is a shared band which allows unlicensed wireless activities. Therefore, coexistence between wireless devices is important to ensure performance. Operating in the 2.4GHz segment of the spectrum, the ISM band provides the convenience of the license-free band with worldwide availability. Many wireless standards have been deployed to operate on the ISM band, such as wireless local area networks (WLAN), which is considered to be the largest wireless standard active in the ISM band. Also operating on the ISM band are the Bluetooth and Zigbee networks, some cordless phones, along with non-standard wireless devices like microwave ovens.

Coexistence between various wireless devices in the ISM band was and still is the focus of much study and research. To give an example about its importance, consider a wireless access point in a university library which provides the campus population with wireless access to the Internet and the university database. In the same library there are students using laptops and PDAs to access the Internet, others using cellulars, with some using Bluetooth headsets. All these devices are using the same medium access; specifically, the 2.4GHz ISM band. Many possible scenarios of interference between the wireless devices can be envisioned in this specific example.

Before we go further with this study, it is reasonable to first identify the standards and wireless technologies that are active in the ISM band, so that we can study each separate standard and identify its key features. It is worth mentioning that our main concern will be the ISM 2.4GHz band; therefore, we will study the standards that are available in this band only.

We presume (as many other studies in the literature do) that the major players in the ISM band can be broken down to the following:

a. WiFi IEEE 802.11 standard
b. Bluetooth IEEE 802.15 standard
c. Cordless phones
d. Zigbee networks IEEE 802.15.4
e. Microwave
f. Unknown signals (prospective standards or potential secondary users)

Before we explain the main features, properties, and differences of each standard, we will first explain some important modulation techniques that will play a major role in both the content of the standards, and the path of blind detection that we adopt in this research.

The main works of this chapter are to:

a. Analyze the main modulation schemes that are used in the ISM band.
b. Study the ISM band wireless standards and active wireless devices extensively.

c. Identify the physical layer features in each wireless standard which can be used in the process of blind identifications.

3.2 The Wireless Communication Systems

Since the beginning of the wireless communication area, engineers competed to develop the best techniques to utilize spectrum usage and enhance spectrum management, in order to increase network capacity and achieve the highest bit rate performance, besides many other motivations like the security, quality of service, etc. Communication systems evolved over the decades from simple analog modulation like the AM, FM and PM to digital modulation like MSK, FSK, and PSK. With advances in integrated circuits and the development of the microprocessor, even more developed and complicated forms of modulations and wireless communication concepts began to appear, all to support the overall performance of current communication systems, and to accommodate modern service demands and the rapidly increasing number of users.

3.2.1 Spread Spectrum

Spread spectrum is one of the popular digital communication schemes because of its various properties that makes it suitable for secure, multiple access communication networks. The fact that it is hard to intercept or detect is one reason why it was first used by the military [14]. Spreading spectrum may be defined as:

> “…a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information. The band spread is accomplished by means of a code which is independent of the data, and

> synchronized reception with the code at the receiver is used for de-spreading, and subsequently data recovery" [8].

This means that the occupied bandwidth of certain data is spread to a wider bandwidth, which will extend its power over a wider range at the same time. As shown in Figure 3.2, this is achieved by multiplying the signal with a higher frequency code sequence. The operation will spread the power spectrum density of the signal, reducing the effect of narrow band interference (both intentional and unintentional), which is one of the main features of the spread spectrum, as shown in Figure 3.3.

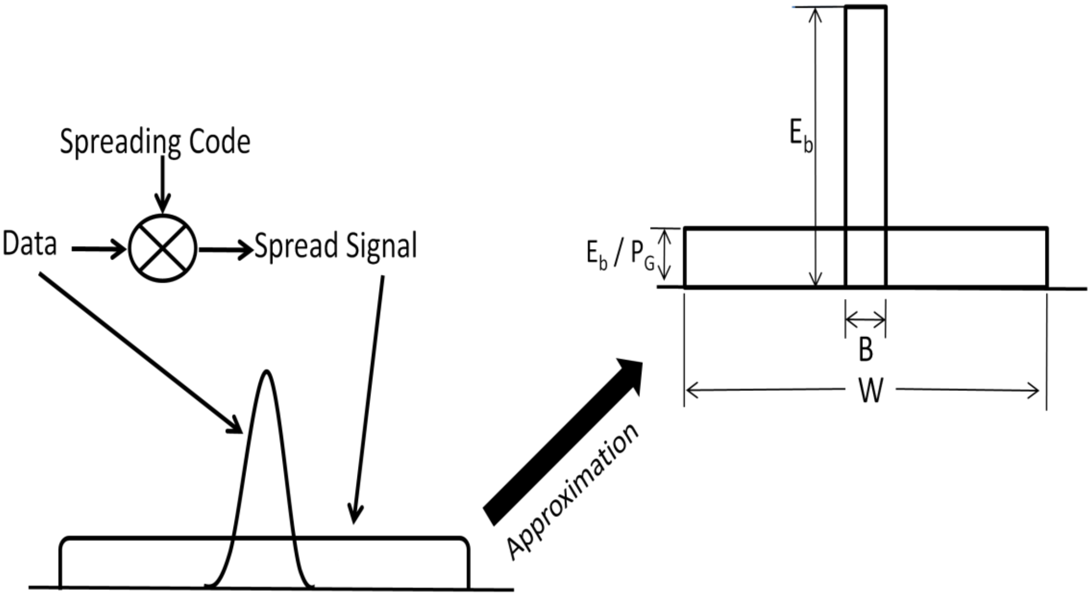


Fig 3.2 The process of spreading the information spectrum

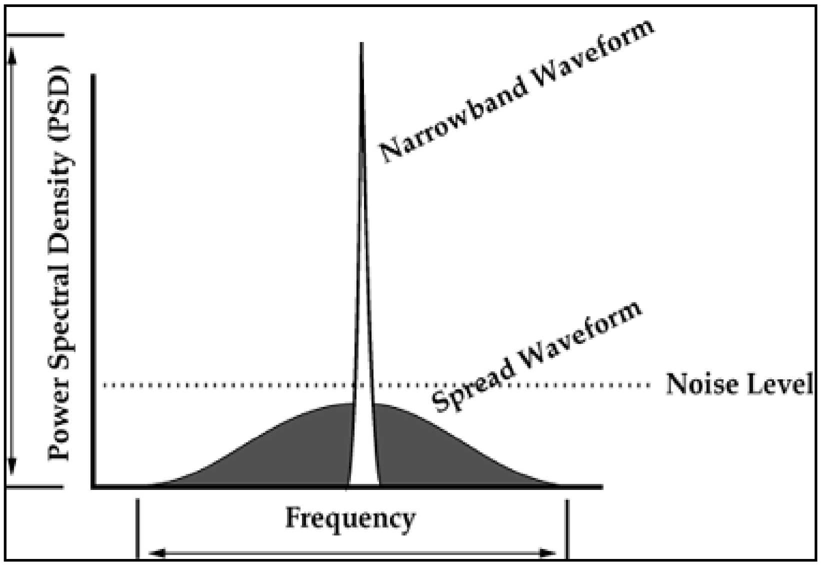


Fig 3.3 Illustration showing the DSSS immunity to narrow band interference

Other good properties of the spread spectrum are summarized below.

a. It has good tolerance towards narrow band interference and jammers.

b. It has high security due to the use of random codes which are known only to the transmitter and receiver.

c. It is suitable for multiple accessing, where more than one user shares the same bandwidth at the same time, such as has been deployed in the CDMA systems.

Spread spectrum can be classified into two main categories: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spectrum (FHSS). The DSSS scheme uses a pseudo-random sequence of positive and negative pulses at a very high repetition rate (chip rate) to spread the data bandwidth signal. The data signal is multiplied by the spreading code in the baseband stage, and then up-converts the signal to the required carrier frequency. The form of the spread signal at the output is given by:

$$s(t) = a(t)d(t)\cos(wct + \theta) \tag{25}$$

where *a(t)* is a sequence of pulses used to spread the data, and *d(t)* is the digital data. At the receiver, the spread signal is recovered by applying a “de-spreading” code that is identical to the spreading signal applied at the transmitter. Figure 3.4 shows a basic system for a DSSS scheme. The spreading signal is called Pseudo Noise code (PN code). The PN sequences are high bit rate binary sequences, which exhibit randomness properties just like noise. The PN code rate is called the chipping rate (to distinguish it from the information rate), so-called because the code sequence applied to each bit results in chipping the original bit into smaller bits. The most important property of the PN sequence is its correlation properties. PN sequence should show noise-like correlation properties to the outsider, but the sequence is known to the two devices that are using it. The definition of randomness was studied by Golomb and requires three properties, which are described in [9]. Examples of the PN sequence are the M-sequences, Gold codes and Kasami sequences.

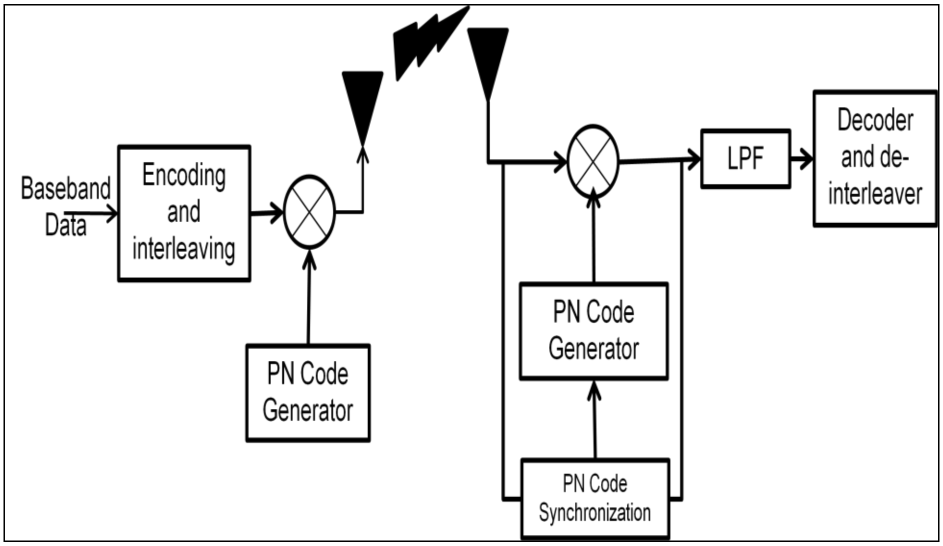


Fig 3.4 Basic DSSS communication system

On the other hand, in FHSS transmission, the random or PN sequence is used to change the carrier frequency in a random manner. This will cause spreading the data signal over a wide range of frequencies, yet no change to the original bandwidth of the data will occur. Instead, various portions of the data will be modulated and transmitted over different carrier frequencies. The order and sequence of the carrier frequencies depends on the used PN sequence. The simplest frequency hopping form is given by:

$$S_m = A\mathrm{b_m}\cos(2\pi \mathrm{f_m t})\mathrm{P_{T_b}}(\mathrm{t} - \mathrm{mT_b}) \qquad (26)$$

where b_m is the information sequence, f_m is part of N frequencies chosen to be the random frequency sequence; so the data signals hop to a new frequency every number of bits, as shown in Figure 3.5. This way the information data is spread through frequency hopping. The time duration over which the data signal spends in each frequency is called the dwell time T_b. Figure 3.6 illustrates a simple frequency hopping communication system.

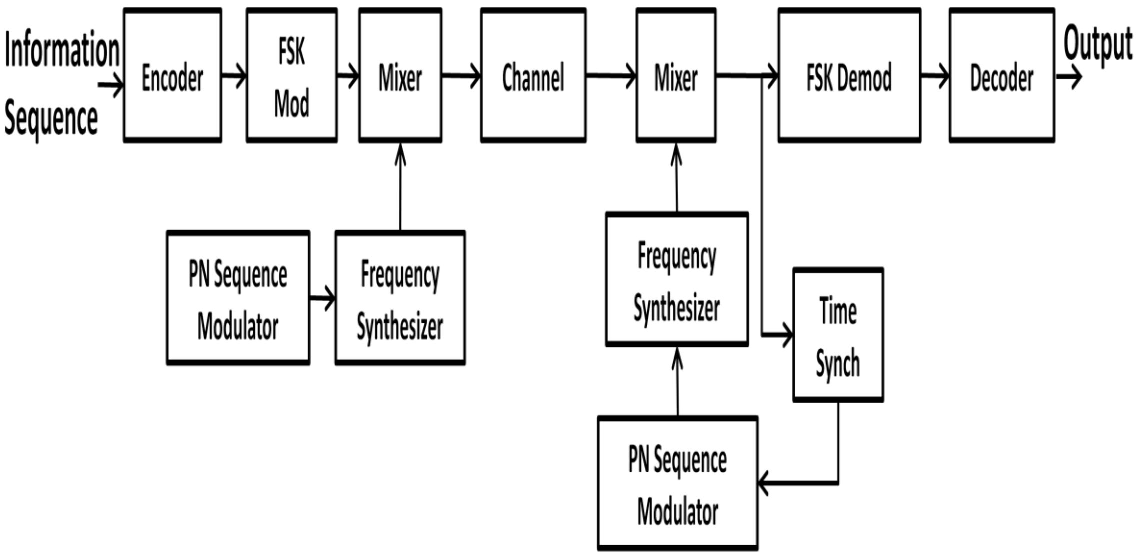


Fig 3.5 Frequency hopping spread spectrum basic transceiver

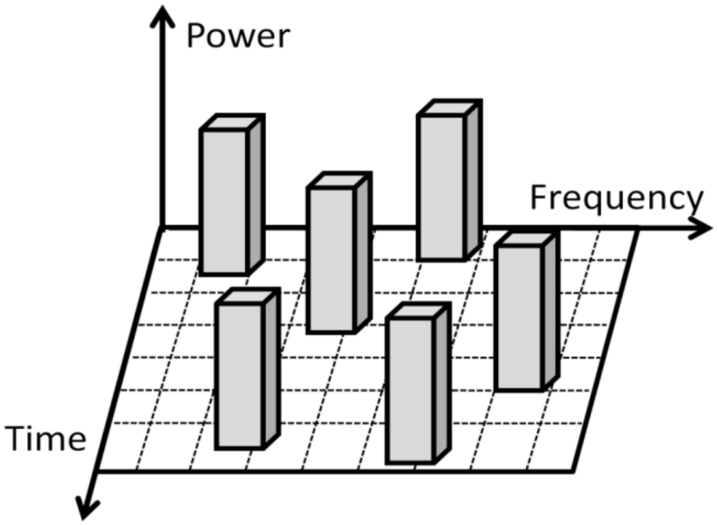


Fig 3.6 Spectrum of hopping signal

3.2.2 Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency Division Multiplexing (OFDM) is a multicarrier modulation scheme that provides efficient bandwidth utilization. OFDM is a mixture of special form of multicarrier modulation and special case of frequency division multiplexing (FDM) at the same time. Where the bandwidth itself is divided into independent subcarriers, each subcarrier is modulated by a portion of the data after dividing the data in to parallel parts and then re-multiplexed to create the OFDM carrier. At each subcarrier the data is modulated at a relatively low rate. This gives immunity against the delay spread of the channel. Ideally each subcarrier is narrow enough to face a flat fading channel.

One way to intuitively look at the way OFDM works is to use the analogy of making a shipment via truck. We have two options: we can either hire a big truck or four smaller trucks. Both methods carry the same amount of material (data). But in case of accident (interference), only 1/4th the amount of material (data) in the entire shipment will suffer. This is exactly how the OFDM shows tolerance towards interference; in the case of interference, only some subcarriers will get affected while the rest will not [10].

The main difference between the FDM and OFDM system is that OFDM does not use guard band to separate its subcarrier. On the contrary, OFDM allows some overlapping between the subcarrier without corrupting the data, through the orthogonality of the subcarriers, which is the main concept of the OFDM. The subcarriers are chosen in such a way that there is no influence of other carriers in the detection of the information in a particular carrier when the orthogonality is maintained. Since the carriers are all sinusoidal waves, we know that the area under one full period of sinusoidal wave should equal zero. In the same way, if we multiply sinusoidal waves with different frequencies, the area under the product is zero if the sinusoidal were orthogonal to each other, as shown in Figure 3.7.

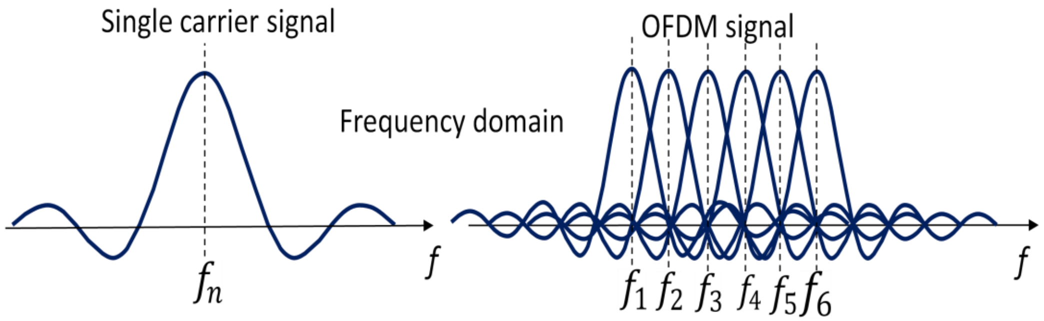


Fig 3.7 OFDM signal of six subcarriers

Although OFDM is relatively new concept, it has gained a great deal of attention during the last decade as it overcame many challenges, especially the ones associated with high bit rate communication, the main problems being frequency selectivity and time dispersion. OFDM is used by many applications nowadays, including WLAN systems, Digital Audio Broadcasting (DAB) [11] and Terrestrial Digital Video Broadcasting (DVB-T) [12] in Europe, and in Asymmetric Digital Subscriber Line (ADSL) [13]. With all these powerful properties of the OFDM, it has its weak points, such as sensitivity to frequency offsets caused by the mismatch between the transmitter and receiver oscillator. This is a problem to the OFDM because it causes loss of orthogonality. Another unprofitable problem is the large Peak-to-Average Power Ratio (PAPR) of the OFDM signal, which requires high quality power amplifiers with large linear ranges. Other problems include phase distortion, time-varying channel and time synchronization, which are not our main concerns in this research. To show the importance of the OFDM modulation and because it has a large role in the ISM band wireless standards, we will describe in more detail the OFDM system and features in the following sections.

3.2.2.1 OFDM System Model

The Discrete Fourier transform (DFT) of the discrete sequence $\mathrm{y(k)}$with a length of N, $\mathrm{Y(k)}$ is defined as [13]

$$\mathrm{Y(k)} = \sum_{\mathrm{k=0}}^{\mathrm{N-1}} \mathrm{y(k)} \mathrm{e}^{-\mathrm{j}\frac{2\pi \mathrm{kn}}{\mathrm{N}}} \tag{27}$$

and the Inverse Discrete Fourier transform (IDFT) is represented as

$$\mathrm{y(n)} = \frac{1}{\mathrm{N}} \sum_{\mathrm{k=0}}^{\mathrm{N-1}} \mathrm{Y(k)} \mathrm{e}^{\mathrm{j}\frac{2\pi \mathrm{kn}}{\mathrm{N}}} \tag{28}$$

As stated earlier, the OFDM system converts the data stream from serial form to parallel blocks, each block with size of N. By using IDFT we obtain the OFDM signal. The time domain samples can be described as

$$x(n) = IDFT\{X(k)\} \tag{29}$$

$$x(n) = \frac{1}{N}\sum_{k=0}^{N-1} X(k)e^{j\frac{2\pi kn}{N}} \qquad n = 0, \dots , N-1 \tag{30}$$

where X(k) is the symbol transmitted on the kth subcarrier and N is the number of subcarriers. The symbols are obtained from the data bits after being digitally modulated using one of the modulation schemes like Phase Shift Keying (PSK), Quadrature Amplitude Modulation (QAM), etc. The symbols X(k) are considered a frequency domain signal and the samples x(n) are considered the time domain of the signal.

We have already stated that the most important fact about the OFDM is the orthogonality of the subcarriers. Only if we achieve orthogonality will we have no effects from the other subcarriers in the detection of information at a particular subcarrier at the receiver. Otherwise loss of the orthogonality will cause inter-carrier interference (ICI). Therefore, to maintain the orthogonality of the OFDM symbol the following should be achieved:

$$\frac{1}{Ts} = \Delta f \tag{31}$$

Δf is the subcarrier spacing, and Ts is the useful symbol duration. So if N-point IDFT is used, the total bandwidth of the OFDM signal will be

$$\mathrm{W} = \mathrm{N}\Delta\mathrm{f} \tag{32}$$

The time domain signal is then extended to avoid the inter-symbol interference (ISI) between symbols. A typical OFDM system is shown in Figure 3.8.

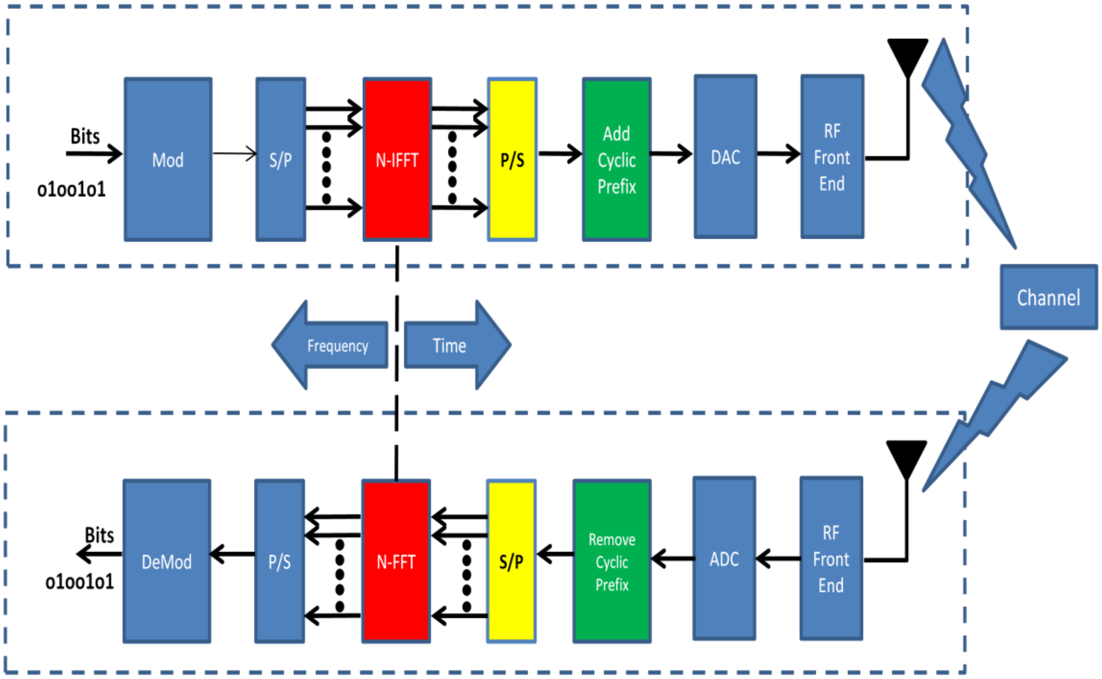


Fig 3.8 Typical OFDM system

3.2.2.2 Cyclic Prefix in OFDM Symbol

Passing signals through a time dispersive channel may cause ISI and frequency selectivity if the delay spread of the channel is greater than the symbol duration. Having ISI in the OFDM system can cause loss of orthogonality which may lead to an ICI problem. To overcome this problem, a method introduced by Peled and Ruiz [15] proposed to cyclically extend the OFDM time signal by copying the last part of the OFDM time signal, called the cyclic prefix (CP), and replicating it at the front of the symbol during the transmission. This is then removed at the receiver side before demodulating the signal. One issue to be considered is that the CP length should be more than the delay spread to assure that the multipath components of the symbols will not interfere with the useful symbol to avoid the ISI, as shown in Figure 3.9. This way the CP will have three benefits:

a. It serves like a guard to protect the symbols from ISI.

b. It can be used for synchronization and blind signal identification.

c. It will prevent the ICI because CP will convert the liner convolution with the channel impulse response in time, which causes a scalar multiplication in the frequency domain, resulting in preservation of the orthogonality.

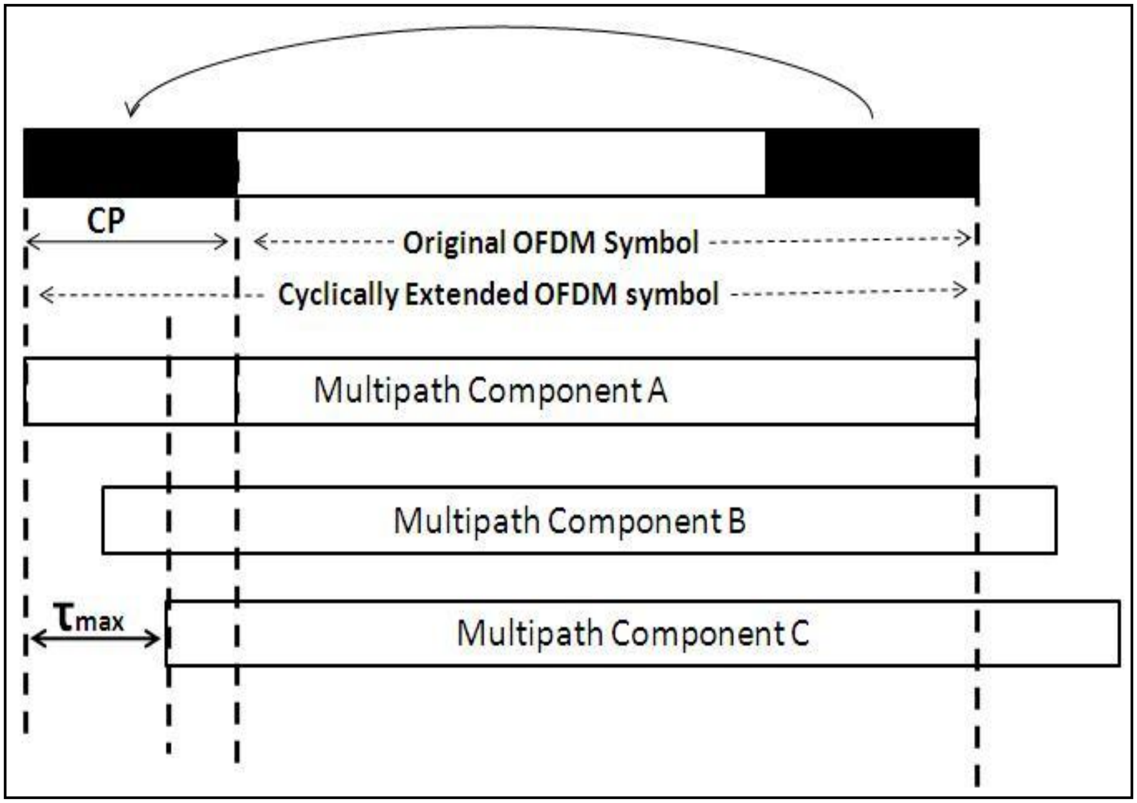


Fig 3.9 Illustration of cyclic prefix extension

The main features and basics of the OFDM system can be summarized by the following:

a. OFDM can achieve high bit rate with high delay spread tolerance.

b. OFDM system divides the data into lower bit rate parallel bit streams, and each parallel bit stream is modulated on an individual subcarrier out of N total number of subcarriers.

c. OFDM uses CP technique to avoid ISI and ICI.

3.3 WiFi IEEE 802.11 Standards

The wireless local area networks (WLAN) technologies appeared in the markets and began to quickly increase the number of shipped equipment and the number of users thanks to rapid internet growth, businesses data networks, and low-cost integrated wireless radio designs. The first widely deployed wireless LAN solutions used the 2.4GHz band since in the beginning this band was assigned for spread spectrum technologies [4]. Individual and large businesses widely adopted IEEE 802.11 wireless network access points and client devices.

IEEE 802.11 standard has three main branches:

a. IEEE 802.11a, which works in the 5GHz band.

b. IEEE 802.11b, which works in the 2.4GHz band.

c. IEEE 802.11g, which works in the 2.4GHz band.

Table 3.1 gives a quick glance at the three standards' histories and main features.

Table 3.1 The three main branches of the IEEE 802.11 standard

Protocol	Release Date	Operation Feq.	Data Rate (max)	Modulation Technique	Range (Radius Indoor)	Range (Radius Outdoor)
802.11a	1999	5 GHz	54 Mbit/s	OFDM	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	11 Mbit/s	DSSS	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	54 Mbit/s	OFDM	~35 Meters	~140 Meters

Since our only concern is the blind detection in the 2.4GHz band, we will not deal with the IEEE 802.11a standard, not to mention that this standard has a lot of similarities with the IEEE 802.11b standard except in the band of operation. Also worth mentioning is that we will only focus on the physical layer features and properties that concern us in our detecting algorithm.

3.3.1 WiFi IEEE 802.11b

The IEEE 802.11b operates in the 2.4GHz band. The FCC assigns 11 channels in the ISM band, as shown in Table 3.2. For this standard, each channel is 22MHz bandwidth [21].

Table 3.2 The 11 channels assigned by the FCC to the ISM band

Channel	Lower Frequency	Center Frequency	Upper Frequency
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.451	2.457	2.468
11	2.451	2.462	2.473

Only three of these channels are none overlapping: 1, 6, and 11. This standard uses the DSSS modulation scheme and has different data rate modes, which are 1Mbps, 2Mbps, 5.5Mbps and 11Mbps. The used spreading codes in this standard are the Barker code sequences in the low data rate mode (1, 2 Mbps) and the Complementary Code Keying (CCK) in the high data rate mode.

The rest of the main features are shown in Table 3.3. These spreading codes are used because they have low autocorrelation properties, as explained earlier in this chapter.

Table 3.3 IEEE 802.11b data rate specifications

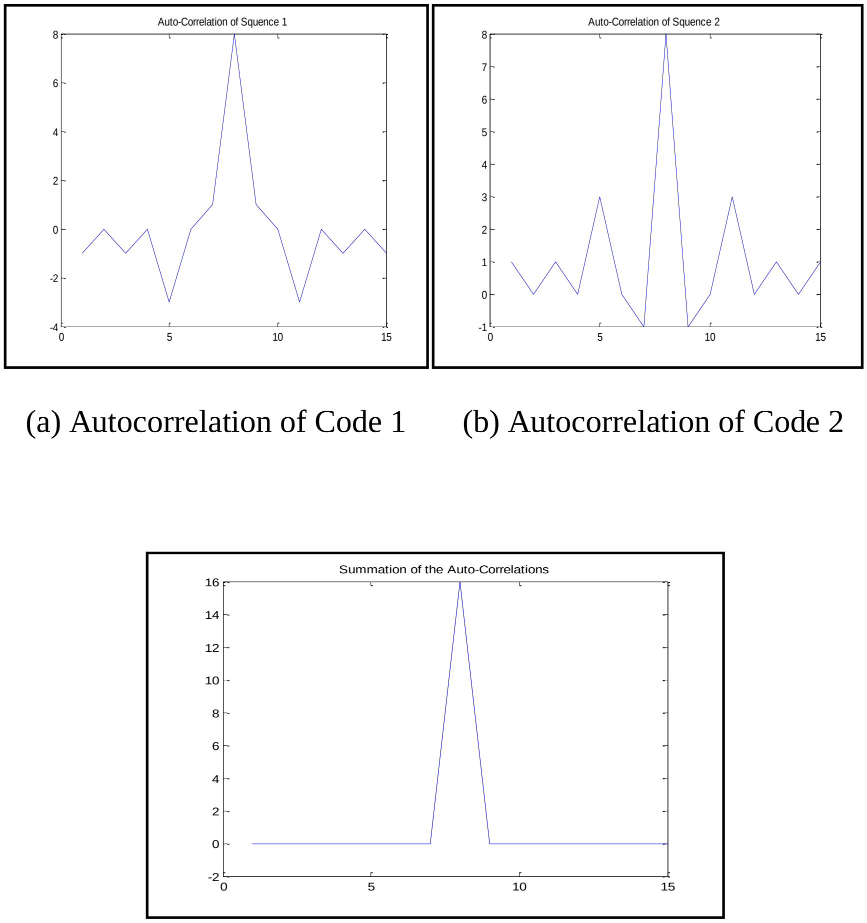
Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Code)	BPSK	1 MSps	1
2 Mbps	11 (Barker Code)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Barker sequences codes consist of sequences of +1s and -1s. The Barker code lengths that are used in the DSSS modulation are 11 and 13. Table 3.4 shows the possible Barker codes.

Table 3.4 Possible Barker codes

Length	Codes	
2	+1 -1	+1 +1
3	+1 +1 -1	
4	+1 -1 +1 +1	+1 -1 -1 -1
5	+1 +1 +1 -1 +1	
7	+1 +1 +1 -1 -1 +1 -1	
11	+1 +1 +1 -1 -1 -1 +1 -1 -1 +1 -1	
13	+1 +1 +1 +1 +1 -1 -1 +1 +1 -1 +1 -1 +1	

On the other hand, CCK code was first proposed by Golay [19]. Binary complementary codes are a subset of CCKs. These codes are pairs of finite code sequences with the same length. The condition for two codes to be considered as complementary of each other is that the summation of the auto correlation functions of each code should yield zero, except for zero lag, as shown in Figure 3.10. It must be mentioned that the codes used in 802.11b are not real but complex (i.e. poly-phase).



(a) Autocorrelation of Code 1 (b) Autocorrelation of Code 2

(c) Summation of the two autocorrelation

Fig 3.10 Illustration of the condition for two codes to be complementary to each other

In 802.11b, CCK codes are generated using the formula:

$$C = (C0, \dots, C7)$$
$$= (e^{j\,(\emptyset 1+\emptyset 2+\emptyset 3+\emptyset 4)}, e^{j\,(\emptyset 1+\emptyset 3+\emptyset 4)}, e^{j\,(\emptyset 1+\emptyset 2+\emptyset 4)}, -e^{j\,(\emptyset 1+\emptyset 4)}, e^{j\,(\emptyset 1+\emptyset 2+\emptyset 3)}, e^{j\,(\emptyset 1+\emptyset 3)},$$
$$-e^{j\,(\emptyset 1+\emptyset 2)}, e^{j\,\emptyset 1}) \qquad (33)$$

In 11Mbps and 5.5Mbps data rate modes, data bits are split into chips, each having 8 and 4 bits respectively. Those chips are used to generate the spreading CCK code. In the case of 11Mbps, 6 out of 8 bits are used to determine the phase values and the remaining two are used to modulate the signal in QPSK by exploiting the common phase term in each code element. While in 5.5Mbps mode, 2 out of 4 bits are used for code generation and the remaining two are used for QPSK modulation. Therefore, the possible number of CCK codes for 11Mbps is (2^6), whereas it is (2^2) for 5.5Mbps.

Depending on the data bits, the phases $\emptyset 1, \dots, \emptyset 4$ are mapped in Table 3.5.

Table 3.5 The generation of the CCK codes depending on the data bits

DIBIT(d_{i+1},d_i)	Phase
00	0
01	π
10	π/2
11	- π/2

It is only reasonable to have a correlation based receiver to detect the IEEE 802.11b standard, and this is what happens in reality. At the receiver the signal is correlated with every possible codeword. Figure 3.11 demonstrates a typical diagram for a IEEE 802.11b receiver [20].

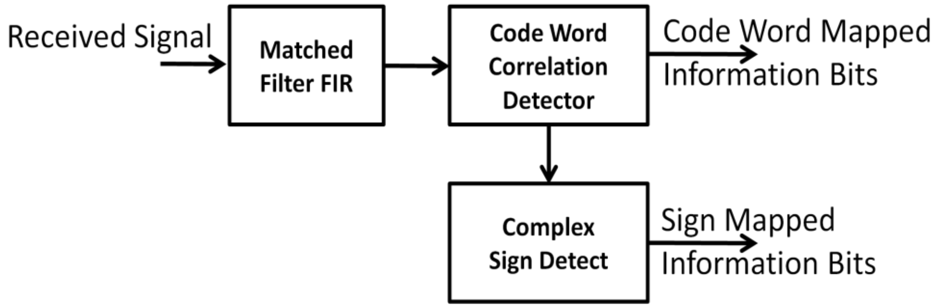

Received Signal
Matched Filter FIR
Code Word Correlation Detector
Code Word Mapped Information Bits
Complex Sign Detect
Sign Mapped Information Bits

Fig 3.11 A typical IEEE 802.11b receiver

To sum up the properties of the IEEE 802.11b standard:

a. It operates in the 2.4 GHz frequency range.

b. It has 11 channels assigned to it in the US, occupying a bandwidth of 22MHz.

c. Bit rate modes are 1Mbps, 2Mbps, 5.5Mbps and 11Mbps.

d. It employs Direct-Sequence Spectrum Spreading (DSSS).

e. The lower data rates use Barker sequences, whereas the high data rates use Complementary Code Keying (CCK).

3.3.2 WiFi IEEE 802.11g

The IEEE 802.11g operates in the 2.4GHz band. The FCC assigns 11 channels to it in the ISM band, and each channel is 22MHz bandwidth [21]. The used channels are shown in Table 3.2. Only three of these channels are none overlapping: 1, 6, and 11. Data rate modes and modulation order are shown in Table 3.6.

Table 3.6 Data rate modes and modulation for the IEEE 802.11g standard

Data Rate (Mb/s)	Modulation	Coding rate	Coded bits/ subcarrier	Coded bits/Symbol	Data Bits/Symbol
6	BPSK	1/2	1	48	24
9	BPSK	3 / 4	1	48	36
12	QPSK	1/2	2	69	48
18	QPSK	3 / 4	2	69	72
24	16 QAM	1/2	4	192	96
36	16 QAM	3 / 4	4	192	144
48	64 QAM	2/3	6	288	192
54	64 QAM	3/4	6	288	216

This standard uses the OFDM modulation which makes it more effective in a multipath environment than the IEEE 802.11b standard. The number of subcarriers is 64, out of which 11 subcarriers at the end of both sides of the spectrum are set to zero for spectrum shaping reasons and to suppress the sideloops at the end of the OFDM spectrum to minimize the ICI. These shut off subcarriers will work as a guard bands at both ends of the spectrum. One subcarrier at zero frequency is set to zero as well, to help the D/A and A/D converters and to get rid of the DC offset. Leaving 52 active subcarriers, four of these subcarriers are BPSK modulated pilot tones used for channel estimation. The subcarrier spacing is 312.5 KHz. The total OFDM symbol is 4µs; the useful symbol duration is 3.2µs, and the CP rate in this standard is 1/4. Due to the total symbol duration, the symbol rate of this standard is 250 KHz. Due to the use of OFDM system, the PAPR is usually high, and it is vulnerable to Doppler spread.

One interesting feature in the IEEE 802.11g standard is that it supports higher data rates using the OFDM, and the low rates using CCK/Barker as well, to ensure backward compatibility with existing IEEE 802.11b equipment.

To sum up the main features of the IEEE 802.11g standard:

a. It operates in the 2.4 GHz frequency range.

b. It has 11 channels assigned to it in the US, occupying a bandwidth of 22MHz.

c. It has high bit rate modes.

d. It uses OFDM modulation.

e. It has a useful symbol duration of 3.2 µs, and a whole symbol duration of 4µs.

f. It has subcarriers numbering 64, and a subcarrier spacing of 312.5KHz.

g. It is spectrally efficient.

h. It is more effective in a multi-path environment (ISI).

i. It is capable when narrow band interference is present.

j. It has a high PAPR.

3.4 IEEE 801.15.1/2 Bluetooth

Bluetooth technology was first developed by Ericsson in 1994. This standard operates on the 2.4GHz bandwidth. It is considered a short range (up to 10 meters) wireless personal area network (WPAN). It became very popular from the beginning of its development for its various applications and the services that can be provided through it, from cellphone headsets to laptop applications, and many others.

Bluetooth standard uses a mixture of Time Division Duplex (TDD) and FHSS transmission mode over 79 channels with 1MHz spacing within the range of 2.400 – 2.4835GHz assigned to this standard by the FCC. The central frequencies are chosen from the following equation [22]:

$$Fc = 2402 + K\ MHz\ , k = 0, \ldots ,78 \qquad (34)$$

There are two data rate modes: the basic data rate with symbol rate of 1Mbps and the enhanced data rate with symbol rate of 2Mbps/3Mbps. The signal hops from one channel to another with a rate of 1600 times per second. The hopping sequence is derived using a pseudo-random sequence determined by the master device in the network and broadcasted to the slave devices. Transmission time is divided in to 625µs time slots. One packet of transmission can take from one up to five time slots [23]. Two hopping modes in the Bluetooth are available. The basic is where the device uses a fixed hopping list regardless of the channel status. And the adaptive frequency hopping (AFH) incorporates interference identification to update the hopping list and exclude any channel that contains interference source. There are three defined power categories for the Bluetooth transmission, listed below and illustrated in Table 3.7.

Table 3.7 Three defined power categories for Bluetooth transmission

Power Class	Max. Output Power	Nominal Output Power	Min. Output Power	Distance
1	100 mW (20 dBm)	N/A	1mW (0 dBm)	100m
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	20m
3	1 mW (0 dBm)	N/A	N/A	10,

To sum up the main features of the Bluetooth:

a. It operates in the 2.4GHz frequency range.

b. It has 79 channels with 1MHz separation, occupying a bandwidth of 1MHz.

c. It has two bit rate modes.

d. It uses FHSS and TDD.

e. Its time slot length is 625µs, and the transmission can use up to five time slots.

f. It has resistance to interference, especially with the AFH mode.

g. It has three power transmission modes.

3.5 IEEE 802.15.4 Zigbee Networks

Zigbee is part of the WPAN family that operates in ISM band and has the features of being small, low maintenance, and low power. It is used for communication applications that require low data rate, a secure network, and low power consumption. This standard covers a transmission range up to 75 meters [26]. In the 2.4GHz ISM band, Zigbee has 16 defined channels with 5MHz bandwidth each. The central frequency of each channel is calculated as:

$$Fc = 2405 + 5 * (k - 11)MHz \;\; k = 11,12, \ldots ,26 \tag{35}$$

The bit rate offered is 250Kbps, with a symbol rate of 62.5Ksps. The modulation scheme used in this standard is the DSSS with a chip rate of 2000Kcps [25]. According to the standard specifications [24], the transmitter power is 0.5mW (-3dBm). One of the main advantages of the Zigbee is the low duty cycle communication with less than 10ppm duty cycle. Lowering the duty cycle minimizes the power consumption, thus increasing battery life. Transmission intervals may range as follows [27]:

$$15.36ms * 2^n, 0 \leq n \leq 14 \tag{36}$$

To sum up the main features of the Zigbee that are useful for our purposes:

a. It operates in the 2.4GHz frequency range.

b. It has 16 channels with 1MHz separation, occupying a bandwidth of 5MHz.

c. Its bit rate is 250Kbps.

d. It uses DSSS, with chip rate 2000Kcps.

e. Its time slot length can be between 15.36ms up to 251.65824 seconds.

f. It has a low duty cycle (<50%).

g. It has low transmission power$\cong$ -3dBm.

h. Its range is up to 75m

3.6 Microwave Ovens

Microwave ovens (MWO) are the perfect example of non-intentional interference of transmitters in the 2.4GHz ISM band. Although microwave ovens were not meant to transmit electromagnetic waves, they usually leak these waves during operation in scattered power all over the ISM band. This phenomenon causes a non-intentional interference and disturbs the other devices operating in the same band. Many studies have addressed the microwave signal model and its interference effects [29], [30], [31]. Using these studies as reference as well as examining a real microwave recorded signal, we noticed that the spectrum in microwave ovens has a distinguished shape (see Figure 2.12) and an occupied bandwidth of 20MHz, where most of the energy is concentrated in 15MHz bandwidth. The time domain signal is transmitted as bursts during the positive cycle of the standard electric power lines frequency [29]. When the positive cycle voltage exceeds some threshold, two bursts appear (these bursts are referred to in the literature as the transient parts). One starts at the beginning of the ON cycle, and the other one at the end of the ON cycle of the microwave. The width of each transient part is $\sim 1ms$. The microwave signal in the ON mode is somehow similar to frequency modulation (FM) signals. The frequency sweep of the FM signal in the microwave has a duration close to half of the time period duration of the electricity power line, so in the US it is between 5- 7ms. There are changing power levels during the frequency sweep of the ON period. These changes in the power level are expressed as an Amplitude

Modulated (AM). So, the frequency sweeping part of the microwave signal is modeled as a combined AM-FM signal waveform [31]. Figure 3.13 shows a time domain microwave signal with the two bursts that represent the transient parts of the ON period marked as A and B.

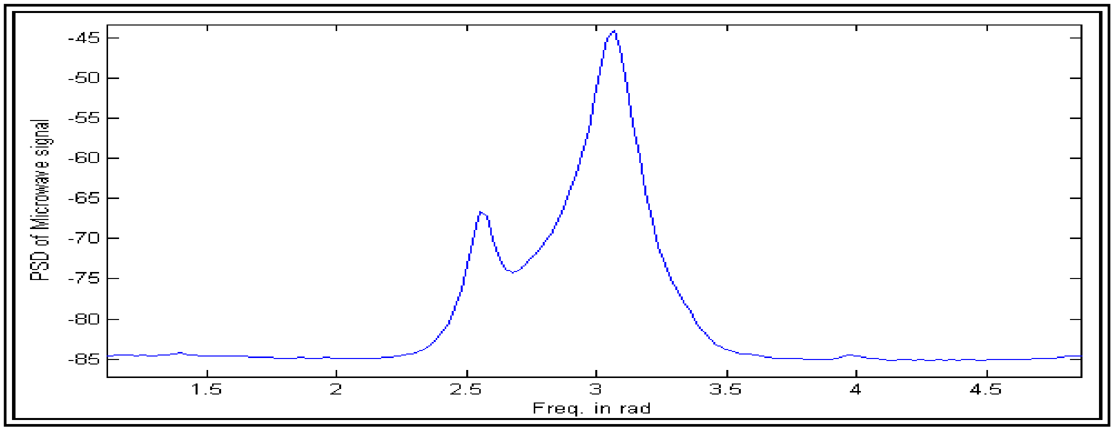


Fig 3.12 The spectrum of a microwave oven signal

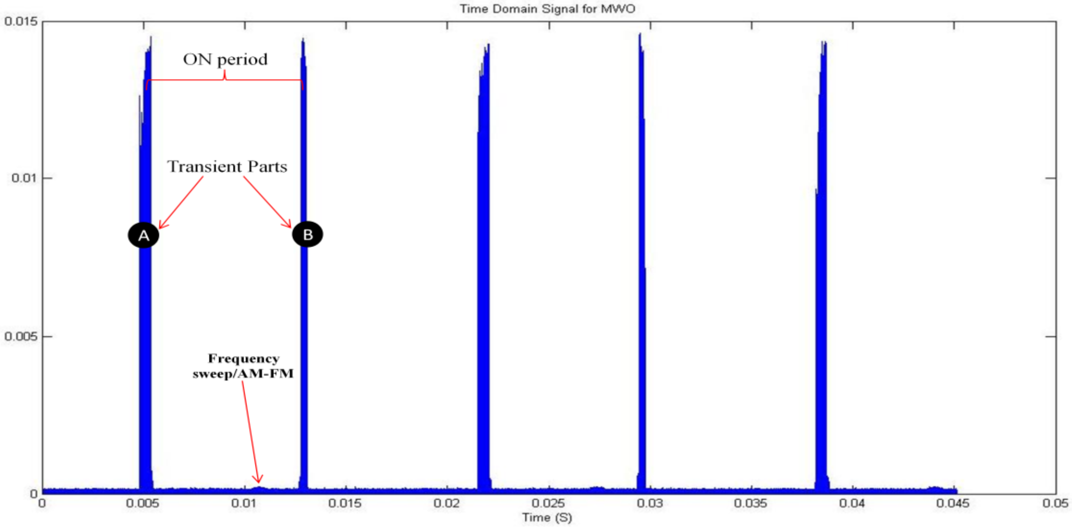


Fig 3.13 Microwave oven time domain signal

Studies have shown that a microwave signal can be best modeled by the following mathematical formula [30]:

$$s(t) = Ax(t)\cos(2\pi f_c t + \beta \sin(2\pi f_{ac} t)) \, , |t| < 0.5Ts \tag{37}$$

where $(t) = cos(2\pi f_{ac} t)$, and Ts is the sweep time.

To sum up the main features of the microwave oven standard that are useful for our present study:

a. It is in the 2.4GHz band.

b. It has no predefined channels or central frequencies.

c. It has periodic transmission, occupying a bandwidth of 20MHz.

d. It transmits in bursts (transient parts) synchronized to electric power lines cycle.

e. It has a distinguished power spectrum shape.

f. Its signal is modeled as an AM and FM signal.

g. Its transient part width $\sim 1ms$, the AM-FM part duration is 5- 7ms.

h. Its duty cycle is close to 50%.

3.7 Cordless Phones

Cordless telephones have been one of the most popular technologies in the telecommunication market for a while now. Currently, there are many types of cordless phones, depending on the band of operation. Since we are concerned with the ISM band, we will focus only on the types that operate on the 2.4GHz range. The first noticeable feature is that cordless phones do not follow a specific protocol or standard. Each manufacturer defines its own devices' features and RF front end specifications. Most cordless phones that work in the 2.4GHz range use FHSS or DSSS. The devices that use DSSS have 8 -16 channels of a bandwidth between 5MHz or 10MHz, compared to the Bluetooth with its 1MHz bandwidth 79 channels. The bit rates for cordless phones are less than 100kbps.

3.8 Unknown Signals

ISM band technology would not be an area of innovation without expecting to have unknown signals every now and then, such as new prospective standards, cognitive radio secondary users, and new unintentional interference. This class is random and uncertain, yet it has to follow the FCC regulation in the ISM band. This fact can help us to form some ideas about what we may face. Therefore, we add unknown signals to our study as well to be prepared for any future situation.

3.9 Conclusion

The ISM band is a license-free band, where wireless activities share the same spectrum with very limited regulations. Due to this fact, it is now one of the attractive bands for manufacturers, and many wireless standards are operating in this band. We have described the variety of wireless technologies that are working in this band, and we demonstrated how important coexistence is for all these wireless activities to operate safely in this part of the spectrum.

In this chapter we looked closely at the modulation schemes and communication systems that can exist in the ISM band, and demonstrated how each system tries to utilize the spectrum and how they handle interference. We also thoroughly examined each of the wireless standards and activities that may operate in the ISM band, and we identified the main physical layer features and properties of each wireless standard. Different wireless standards can utilize the same features or modulation techniques.

Chapter 4

Features Extraction

In this chapter we describe the features extractions stage and explain the algorithms used to extract each feature. A comprehensive list of features that can be used to detect the presence of the ISM band technologies is discussed and analyzed.

4.1 Introduction

As we explained in Chapter 2, the cognitive radio should have the capability to blindly identify interference and try to mitigate its effects. This capability will be executed in the spectrum awareness engine. In Chapter 2, a novel design for the spectrum awareness engine was proposed. Descriptions of the RF front end and the energy detection components were given. Studies show that energy detection alone is not sufficient to have an accurate idea about the available spectrum or the interference [74], [44], [81], [82]. Therefore we propose a feature detector stage to deeply explore the captured signal's features to try to identify them.

Many studies in the literature examined the various features of the wireless signals. Some even proposed methods to extract these features. Some examples include:

a. In [50], the bandwidth is estimated through the use of FFT operation.

b. In [84], 4th order cumulants test is used to extract the used carrier systems.

c. In [102], moments test is applied to reveal the carrier system.
d. In [103], a cosine modulated bank filter is used to blindly identify the multicarrier modulation
e. In [108], autocorrelation function is used to estimate the OFDM time parameters
f. In [110], cyclostationarity is deployed to estimate the OFDM frequency domain parameters

As it is shown, different approaches are proposed to extract different types of features. In this research we define the possible features that can be targeted and propose a comprehensive algorithms to extract each one of these features with the appropriate approach.

The main works in this chapter are to:

a. Identify the possible PHY layer features that can help in the detection process.
b. Study the cyclostationarity theory and the cyclostationarity detector.
c. Build algorithms to detect each of the proposed features.
d. Propose a feature detector design that consists of handful of algorithms to detect the various features.

4.2 Feature Detector

After applying the energy detection and making the first decision about signal presence, we try to extract as much information as possible from the captured signal. These signal features can be detected using a single approach or multiple approaches such as autocorrelation based test, cyclostationarity based parameters extraction, and joint time frequency analysis. These algorithms can be used together for extracting the different features that may present in the signal. Figure 4.1 illustrates the proposed design.

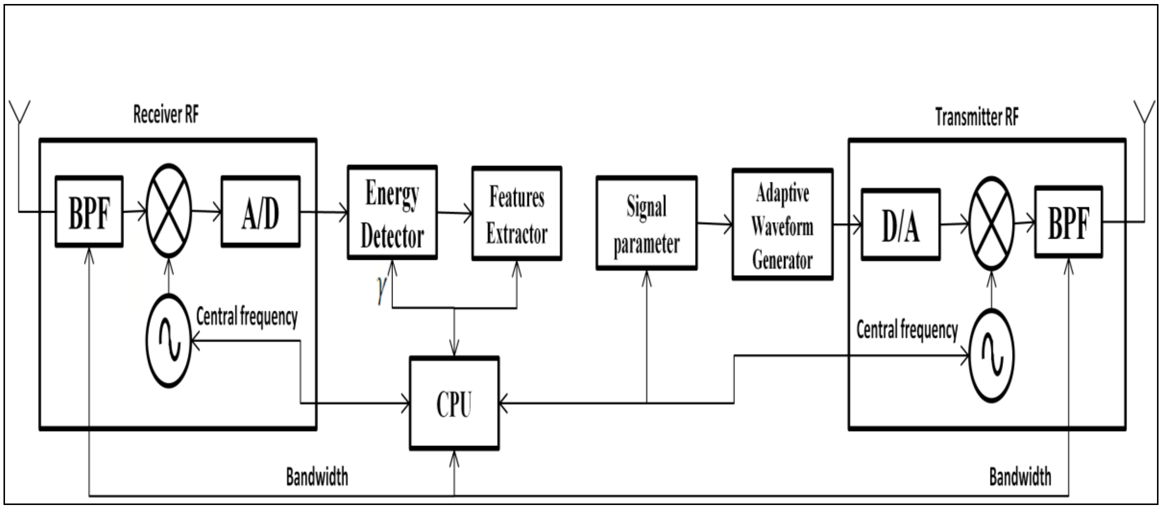


Fig 4.1 The proposed model

First we define the physical layer features and characteristics that can be used to identify signals and interferences as below:

a. Power related: SNR, Peak to Average Power Ratio (PAPR)

b. Time of occurrence (statistical observation over a period of time)

c. Frequency domain related features: central frequency, bandwidth (OBW, 3dB BW)

d. Duty cycle

e. Statistical characteristics: mean, variance, CCDF, moments (2nd, 3rd …, etc.), autocorrelation function properties

f. Cyclostationary feature

g. Distinguishing between single carrier or multicarrier

h. Single carrier: digital modulation, DSSS, FHSS

i. Multicarrier parameters: time (symbol duration, CP duration) and frequency (subcarrier spacing, number of subcarriers)

j. Modulation type and order

k. Chip rates

l. Symbol rates

m. Hopping sequence

n. FCC regulation

A comprehensive algorithm is proposed to extract each one these features. One thing to point out is that we took in consideration the computational complexity in the design of each algorithm.

4.3 Bandwidth and Central Frequency Estimation

The wireless standards usually utilize predefined bandwidths (depending on the data rate). The bandwidth of a detected signal is estimated, and the bandwidth value is used in the process of identification [50], [93]. The same applies to the central frequency of operation, as different wireless standards use different predefined central frequencies. Even in frequency hopping spread spectrum, there are certain predefined central frequencies the devices will operate on, as we observed in the Bluetooth case.

There are some proposed ways in the literature for bandwidth and central frequency estimation. For instance, in [94], wavelets decomposition is used to calculate the bandwidth of the signal. In [95] the author uses the Welch periodogram to calculate the average power spectrum and find out its length, then detects the two endpoints of the signal spectrum, calculates the distance between these points, and finds the bandwidth. In [50], FFT is applied on the time domain signal, and a threshold is defined to decide which frequency bins are occupied to calculate the start and the end of the signal bandwidth.

In our proposed algorithm, right after the energy detection stage, we need to check if there is one signal or more than one signal in the spectrum, and to make sure that we captured all of the signals. For this purpose we calculate the power spectrum density of the signal (PSD), and pass the PSD to an edge detector algorithm to make sure that we have only one signal in the sampled spectrum. To estimate the bandwidth and central frequency, we use the time frequency Heisenberg-Gabor inequality concept.

4.3.1 Heisenberg-Gabor Principle

In many cases, the time-frequency resolution of a signal is restricted to the Heisenberg-Gabor inequality. Signals can be characterized in both time and frequency domains at the same time by considering their mean localization and dispersions in each of the mentioned domains.

If we have:

$$|x(t)|^2 \tag{38}$$

and

$$|X(f)|^2 \tag{39}$$

representing the probability distribution of the signal in both time and frequency domain respectively, we can calculate the mean and the standard deviation as:

$$t_m = \frac{1}{Ex}\int_{-\infty}^{\infty} t\,|x(t)|^2\,dt \qquad \textit{average time} \tag{40}$$

$$f_m = \frac{1}{Ex}\int_{-\infty}^{\infty} f\,|X(f)|^2\,df \qquad \textit{average frequency} \tag{41}$$

$$T^2 = \frac{4\pi}{Ex}\int_{-\infty}^{\infty} (t - t_m)^2\,|x(t)|^2 dt \qquad \textit{time spreading} \tag{42}$$

$$B^2 = \frac{4\pi}{Ex}\int_{-\infty}^{\infty} (f - f_m)^2\,|X(f)|^2 df \qquad \textit{frequency spreading} \tag{43}$$

Ex is the energy of the signal and assumed to be finite:

$$Ex = \int_{-\infty}^{\infty} |x(t)|^2\,dt < \infty \tag{44}$$

Since we can calculate the power spectrum density of the signal $X(f)$, we define the following:

$$f_m = \frac{1}{Ex}\int_{-\infty}^{\infty} f\,|X(f)|^2\,df \tag{45}$$

$$B = 2\sqrt{\frac{\pi}{Ex}\int_{-\infty}^{\infty}(f - f_m)^2\,|X(f)|^2 df} \tag{46}$$

where f_m is the central point of the power distribution, hence the central frequency and B is the frequency spreading around the center point, hence the bandwidth. Then the Heisenberg-Gabor inequality is:

$$\mathrm{BT} \geq 1 \tag{47}$$

The main feature of this method of estimation is the simplicity of computation. The power spectrum density of sampled signals is easily calculated thanks to the simplicity of the current FFT circuitry, allowing just two equations to give us a good estimate for the bandwidth and the central frequency. Also this method is independent of the SNR value, which means that we do not need an SNR estimator. Figure 4.2 illustrates the performance of the proposed bandwidth estimation algorithm against various SNR values. As we can see, the algorithm gives relatively low error rate in low SNR values. The signal used in this evaluation is OFDM signal, 10 symbols, FFT size 512, CP 1/8.

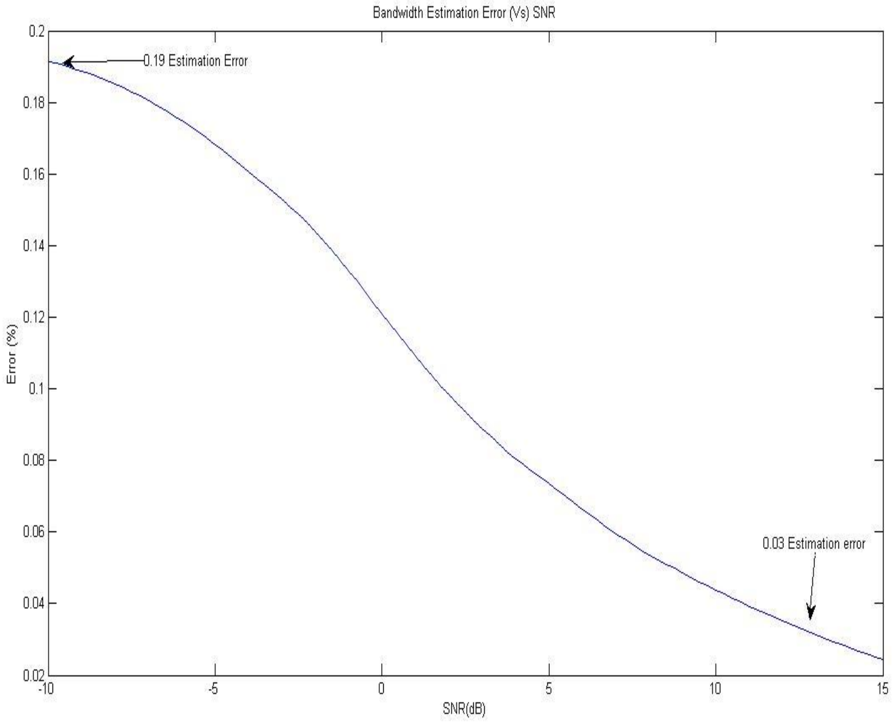


Fig 4.2 Bandwidth estimation error with SNR values

It is worth mentioning that in the case of real recorded data, we neglect some samples at the beginning and at the end of the signal spectrum to take the roll off factor of the filter into consideration and compensate for the drop in magnitude at both ends due to the receiver's front end filter.

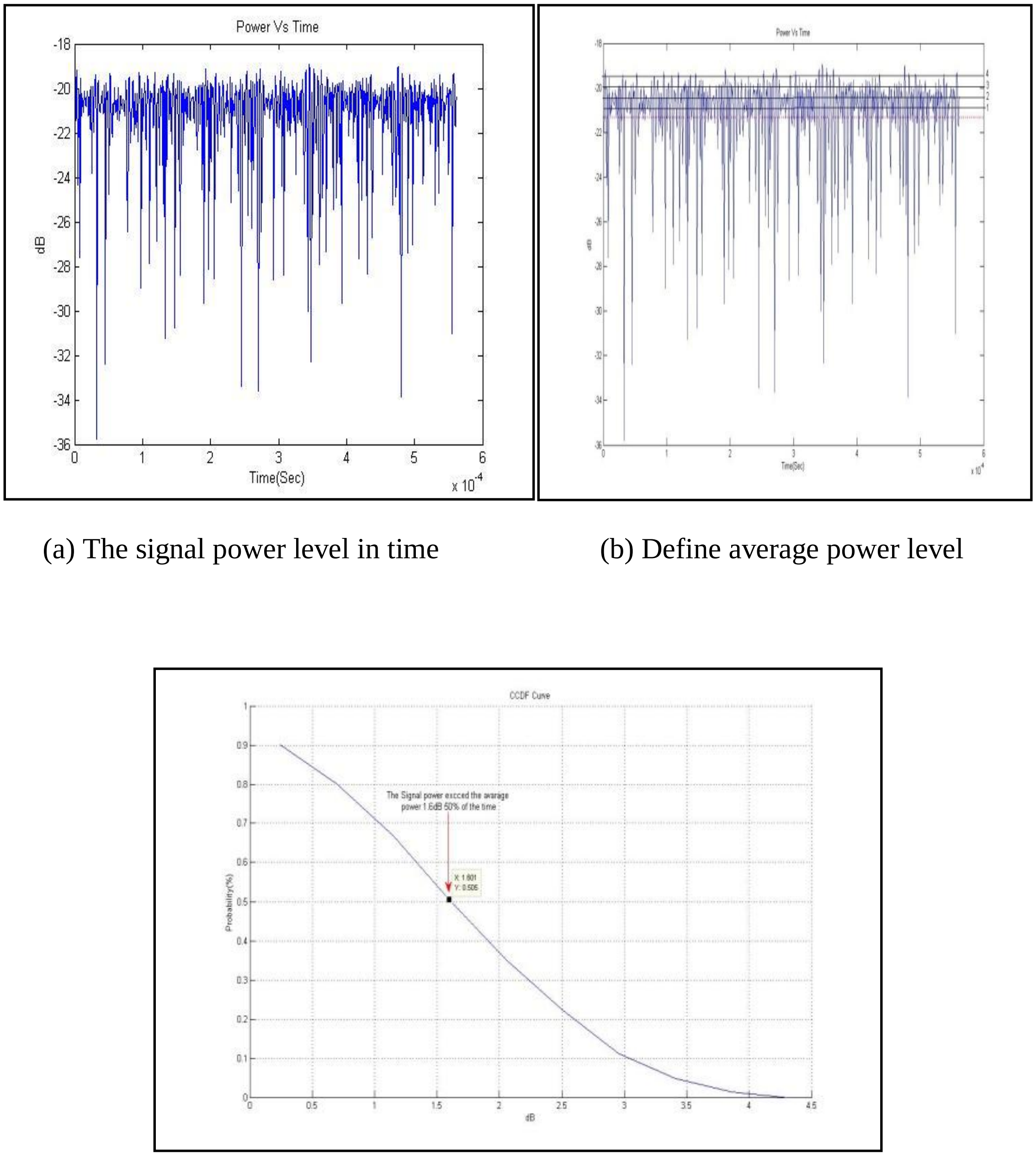
4.4 Power Related Metrics

The signal power and the SNR of the received signal can be a useful tool to provide an idea about the identity of the signal. For example, in Zigbee networks the power transmission is low according to the Zigbee networks specifications (≅-3dBm). In Bluetooth there are three power transmission modes, and each power mode has a specific transmission distance; meaning that in the case of Bluetooth technology, the transmission power can indicate the effective distance of the device. And that is why power metrics are calculated in the proposed algorithm and feed into the decision making part of the algorithm.

4.4.1 CCDF

The move to 3G systems and the adoption of OFDM modulations is pushing signals to have higher peak-to-average power ratios. Current OFDM based communication systems combine subcarriers, resulting in a peak-to-average. This signal characteristic can be an identifying feature for the OFDM based systems, especially if we have prior knowledge about the primary signal statistics [97]. Here the Power Complementary Cumulative Distribution Function (CCDF) curves come into the picture as they provide critical information about the peak-to-average power behavior of the signal. The CCDF plot describes how much time the signal spends at or above a given power level [96].

To explain how to construct the CCDF curves, let us consider a signal power level with time representation, as in Figure 4.3a. The signal in the mentioned form is difficult to quantify due to its randomness. In order to get some useful power information from the signal, we can statistically describe the power levels with respect to the average power in the signal. Figure 4.3b represents a specific power level above the average. We calculate the percentage of the time the signal spends at or above each power level, which represents the probability for that particular power level, as in Figure4.3c. Then the CCDF can be defined as the power levels with respect to the average versus their probability. With the prior knowledge of the expected signal statistics and the channel, CCDF can help with the blind identification of the signals, especially the multicarrier based ones.



(a) The signal power level in time

(b) Define average power level

(c) CCDF Curve

Fig 4.3 CCDF implementation

Figure 4.4 illustrates the algorithm results for different types of modulations.

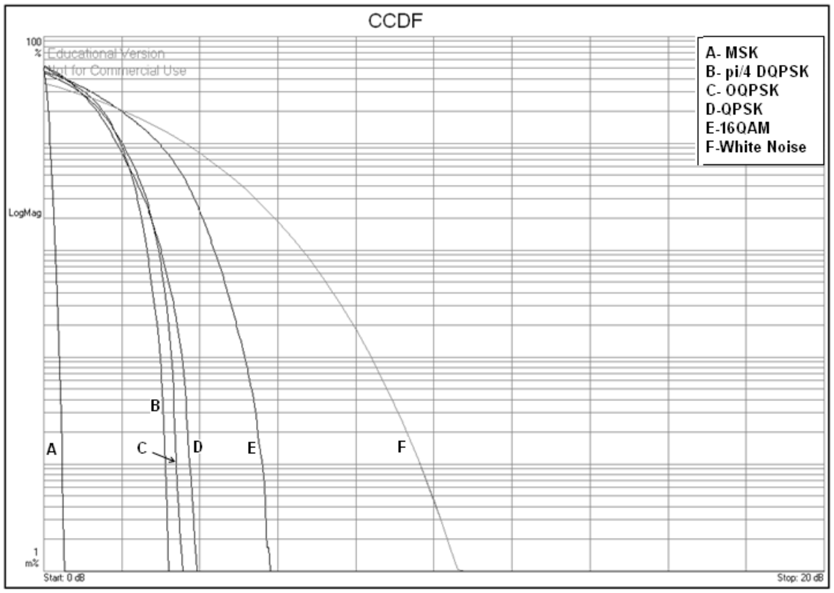


Fig 4.4 CCDF curves for different modulation schemes

4.5 Single Carrier versus Multicarrier

ISM band contains different types of wireless standards, as explained in Chapter 3. Some standards adopt the multicarrier approach like the OFDM based WLAN, and some take the single carrier approach, like cordless phones. Knowing this, we identify the importance of detecting the signal's carrier system, not only to participate in the process of the decision making of the blind detection but also to reduce the computational complexity of the decision making. There are two methods in the literature to discriminate the single carrier and multicarrier systems. Those are the 4th order cumulants test and the moments test.

In the cumulant based test, since OFDM signals has Gaussian distribution or close to Gaussian, a time domain statistical test for Gaussianity is applied on the signals [98], to detect if the signals are using multicarrier transmission. This approach was used for the first time by Akmouche in 1999 [84]. According to the cumulants test, cumulants of order k > 3, which are generalizations of autocorrelation function, can be used to quantify departures from Gaussianity [98]. So if the data in hand (sampled signal) has a Gaussian distribution, the kth order cumulants C_{kx} disappear for k > 3, where the cumulants C_{kx} is defined as [98]:

$$C_{kx}(i1, \dots, i_{k-1}) = \sum_{i=-\infty}^{\infty} x(i)x(i+i_1) \dots x(i+i_{k-1}) \tag{48}$$

Some weak points were noticed in this method of multicarrier test. For instance, the test was SNR-dependent, and the accuracy of the results heavily affected in dispersive channels. For those reasons we chose not to use the cumulants based test.

4.5.1 Moments Based Test

Moments test was first used as a modulation type and order identifier for single carrier systems by evaluating the summation results of power-law elements [101]. Later on, the test proposed to be used for the multicarrier signal identifications [100], [102]. To explain the moments test algorithm let us consider the baseband sampled signal model as:

$$y(n) = x(n) + n(n) \tag{49}$$

where $y(n)$ is the received signal, $x(n)$ is the transmitted signal, and $n(n)$ is the white Gaussian noise. The mixed moments of the received signal will be:

$$M_{p+q,q}(y) = E\{y(n)^p \times (y(n)^*)^q\} \tag{50}$$

where the denoted * refers to the conjugation. Therefore we can form:

$$M_{2,1}(y) = E(y(n) \times y(n)^*) \; = E(|y(n)|^2) \tag{51}$$

$$M_{4,2}(y) = E(y(n)^2 \times (y(n)^*)^2) \; = E(|y(n)|^4) \tag{52}$$

$$M_{6,3}(y) = E(y(n)^3 \times (y(n)^*)^3) = E(|y(n)|^6) \tag{53}$$

Furthermore, we define two parameters:

$$k_{20} \; = M_{4,2}(y)/M^2{}_{2,1}(y) \tag{54}$$

$$k_{30} \; = M_{6,3}(y)/M^3{}_{2,1}(y) \tag{55}$$

The ideal values for k_{20} and k_{30} are shown in Table 4.1.

Table 4.1 Ideal values for k_{20} and k_{30}

	k_{20}	k_{30}
64 QAM	1.378	2.21
32 QAM	1.306	1.88
16 QAM	1.312	1.93
MPSK	1	1
MFSK	1	1
OFDM	2	6

Since $y(n) = x(n) + n(n)$, then:

$$P = E\{|y|^2\} = E\{|x|^2\} + \{|w|^2\} = S + N \tag{56}$$

The moments will be:

$$M_{2,1}(y) = E(y(n) \times y(n)^*) \ = S + N \tag{57}$$

$$M_{4,2}(y) = E(y(n)^2 \times (y(n)^*)^2) \ = k_2 S^2 + 4NS + 2N^2 \tag{58}$$

$$M_{6,3}(y) = E(y(n)^3 \times (y(n)^*)^3) = k_3 S^3 + 9k_2 S^2 N + 18N^2 + 6N^3 \tag{59}$$

So the new parameters for $y(n)$ are:

$$v_{20} = \frac{M_{4,2}(y)}{M^{2}{}_{2,1}(y)} = \frac{E(|y(n)|^4)}{E^2(|y(n)|^4)} = \frac{m_{20}(S/N)^2 + 4S/N + 2}{(S/N)^2 + 2S/N + 1} \qquad (60)$$

and:

$$v_{30} = \frac{M_{6,3}(y)}{M^{3}{}_{2,1}(y)} = \frac{E(|y(n)|^6)}{E^3(|y(n)|^2)} = \frac{m_{30}(S/N)^3 + 9m_{20}(S/N)^2 + 18S/N + 6}{(S/N)^3 + 3(S/N)^2 + 3S/N + 1} \qquad (61)$$

where m_{20} m_{30} are the parameters k_{20} and k_{20} scaled by 2, and 6 respectively [102] and can be chosen from the Table 4.2.

Table 4.2 Ideal values for m_{20} and m_{30}

	m_{20}	m_{30}
64 QAM	1.378×2	2.21×6
32 QAM	1.306×2	1.88×6
16 QAM	1.312×2	1.93×6
MPSK	1×2	1×6
MFSK	1×2	1×6
OFDM	2×2	6×6

Let us remember that

$$SNR = 10log_{10}(S/N) \tag{62}$$

From equation (60) we can derive the SNR equation:

$$SNR = \frac{v_{20} - 2 \pm \sqrt{4 + m_{20}v_{20} - 2m_{20} - 2v_{20}}}{v_{20} - m_{20}} \tag{63}$$

Up to this point we need m_{20} or the modulation type in order to estimate the SNR. The algorithm proposes to use the SNR estimation and modulation characterization in [104] jointly to detect the multicarrier signals as follows:

a. Calculate the moments $M_{2,1}(y)$, $M_{4,2}(y), and\ M_{6,3}(y)$ of the sampled signal.

b. Calculate v_{20}, and v_{30}.

c. Assume that the modulations that can be detected are A=B+C, either single carrier modulations, B={$MFSK_{M=2,4,8}, MPSK_{M=2,4,8}, MQAM_{M=16,32,64}$}, or multicarrier modulation, C={OFDM}.

d. Assume a particular modulation $\theta \in A$ is received in the sampled signal, the corresponding $m^{(\theta)}{}_{20}$ and $m^{(\theta)}{}_{30}$ can be obtained from Table 4.2.

e. Estimate the $SNR^{(\theta)}$ through the estimation equation (63), using m_{20}^{θ}, and v_{20}^{θ} values.

f. Calculate the estimation value of v_{30} we call it $\widetilde{v_{30}^{\theta}}$, using the $SNR^{(\theta)}, m_{20}^{\theta}, m_{30}^{\theta}$ values in (61) equation.

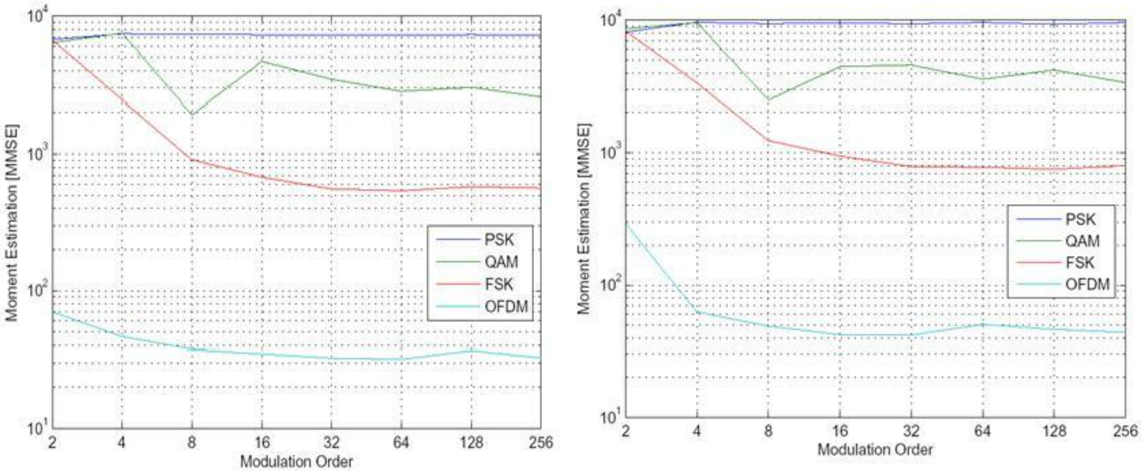
g. Repeat steps 4-6 and calculate the $\widetilde{v_{30}^{\theta}}$ for all possible modulations in $\{A\}$.

h. Calculate the estimation error $\left|\widetilde{v_{30}^{\theta}} - v_{30}\right|$ for each modulation in $\{A\}$.

i. Finally, select the modulation used in the received signal based on the minimum mean squared error(MMSE) criterion:

$$\theta = arg_{\theta}^{min}\left(E\left(\left|\widetilde{v_{30}^{\theta}} - v_{30}\right|^{2}\right)\right) \tag{64}$$

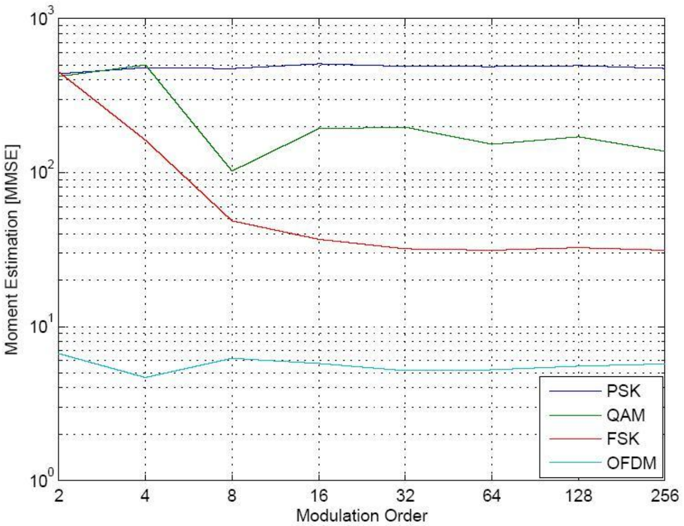
The algorithm is tested for different SNR values, and through 10 sample-spaced uniformly distributed channel taps channel, to evaluate the performance. Figure 4.5 illustrates the outcome of the algorithm for different modulation schemes, when the $m^{(\theta)}{}_{20}$, and $m^{(\theta)}{}_{30}$ parameters are set to be OFDM signal [100]. We can clearly see that we have the minimum (MMSE) values when the signal is OFDM based, which indicates that the tested signal was OFDM.



(a) 10 tabs channel, SNR=10

(b) 10 tabs channel, SNR=15

Fig 4.5 Moments test performance with different SNR values



(c) 10 tabs channel, SNR= 0

Fig 4.5 (Continued)

4.6 Modulation Order and Type of Single Carrier Signals

The same algorithm that is described in 4.5.1 is used to identify the digital modulation order. The same (MMSE) argument will hold when the algorithm is applied with different modulations parameters and the values that reflect the least MMSE value in (64) will represent the modulation used in the received signal.

Despite the simplicity of the moments test, it has been proven that it can be misleading when used to identify the digital modulation orders [105], especially when the received signal has FSK modulation. Figure 4.6 illustrates the results of the moments test algorithm when the transmitted signal is FSK, showing that the test gives inconsistent results. We explain how to overcome this problem by using our fuzzy logic-like decision making process in Chapter 5.

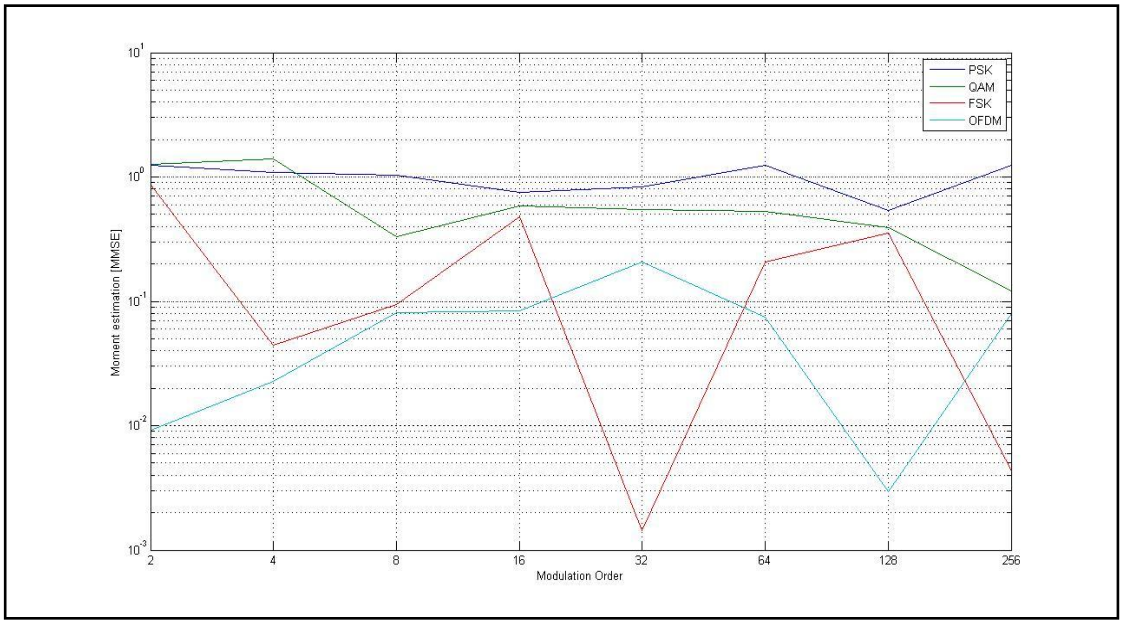


Fig 4.6 Moments test for FSK signals with different orders in 10 tabs channel, SNR=0

4.7 OFDM Signals Parameters Estimation

There are many proposed algorithms to blindly estimate the OFDM parameters in both time domain and frequency domain [107], [108], [109], [110]. In [108], autocorrelation is performed and the total symbol duration is estimated through the distance between the correlation peaks. The cyclic prefix (CP) length is estimated through joint time frequency transform. In [109] the useful symbol duration is calculated through autocorrelation based algorithm, while the total symbol duration is calculated by finding the distance between consecutive peaks in cross correlation based algorithm. In [110], different approaches were taken, where the author estimates the sampling frequency using the cyclostationarity introduced by the signal oversampling, uses the result of the cyclostationarity to estimate the number of subcarriers, and finally estimates the CP length and the symbol duration through cyclostationarity based algorithm.

After a detailed search in the literature and testing the proposed methods on both simulated and real captured signals, we narrowed down our approaches to the following. The OFDM symbol duration will be calculated through an autocorrelation based algorithm. The total symbol duration will be calculated through a slicing cross correlation algorithm with fixed window length. CP duration will be calculated based on the total symbol duration and the useful symbol duration results. The subcarrier spacing is calculated from the useful symbol results, which will eventually lead to the calculation of the number of subcarriers.

4.7.1 OFDM Time Parameters Estimation

Let us recall the OFDM signal model and symbol component that we explained in Chapter 3.

OFDM system converts the serial data stream into parallel parts of size N and modulates these parts into different subcarriers through the inverse discrete Fourier transform (IDFT).The time domain signal can be described as:

$$x(n) = \mathrm{IDFT}\{X(k)\} = \frac{1}{N}\sum_{k=0}^{N-1} X(k)e^{j\frac{2\pi kn}{N}} \qquad n = 0, \dots, N-1 \qquad (65)$$

where $X(k)$ is the symbol transmitted on the kth subcarrier and N is the number of subcarriers. The OFDM time signal is cyclically extended by copying the last part of the OFDM symbol, and replicating it at the front of the symbol during the transmission. Figure 4.7 illustrates OFDM symbol structure.

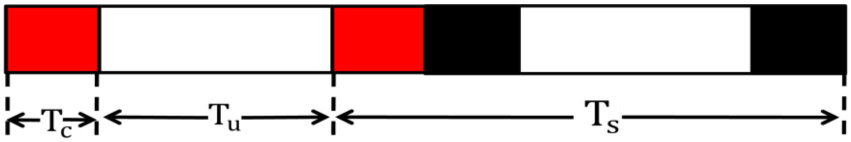


Fig 4.7 The structure of the OFDM symbols

where T_s is the total symbol duration, T_c is the cyclic prefix duration, and T_u is the useful symbol duration.

Let us also assume that the baseband received signal over multipath channel is:

$$r(t)= \sum_{l=0}^{l-1} h_l(t)s(t-\tau_l)+w(t) \qquad (66)$$

where $s(t)$ is the OFDM signal, $w(t)$ is the white Gaussian noise, $h_l(t)$ is the path complex gain representation, with the path delay τ_1 and 1 is the sample-spaced channel taps. As shown, OFDM symbol will have cyclic reception, which should cause correlation properties to exist between them in the OFDM symbol. We use this fact to develop algorithms to estimate the time parameters of the OFDM symbol.

4.7.1.1 Useful Symbol Duration

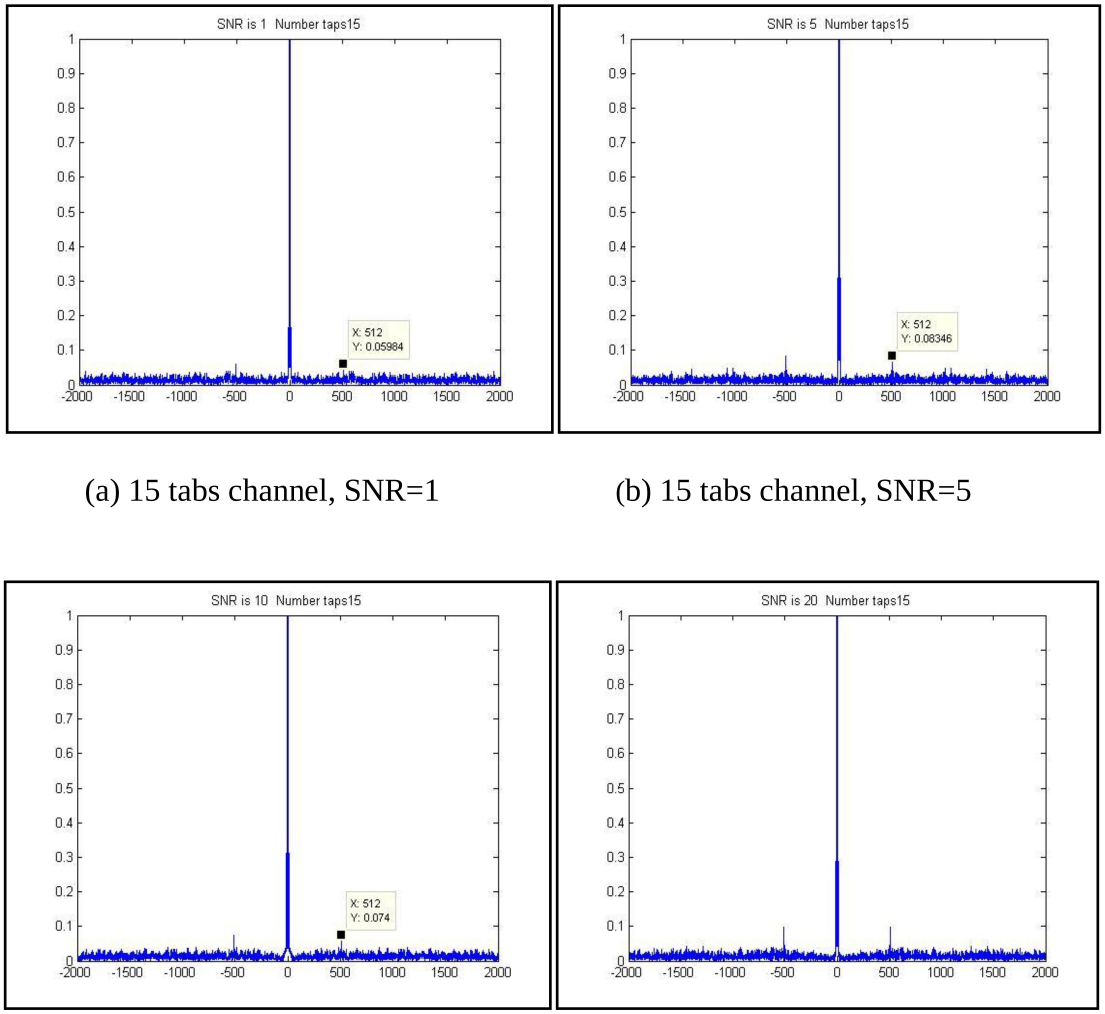
After estimating the central frequency and the occupied bandwidth, the signal can be down converted and sampled. And the autocorrelation function of the received signal $r(t)$ can be defined as [109]:

$$E\{r(n)r^{*}(n+\Delta)\} = \begin{cases} \sigma_s^2+\sigma_w^2 & \Delta= 0 \\ \sigma_s^2 e^{-j2\pi\varepsilon} & \Delta= N_u \\ 0 & \text{other} \end{cases} \quad (67)$$

N_u represents the useful symbol duration. Then the useful symbol duration will be:

$$\widetilde{N_u} = arg_{\Delta}^{max}\left\{\frac{\left|R_{Use\,(\Delta)}\right|}{en_{Use}\,(\Delta)}\right\} \qquad \Delta= 1,2,\ldots,N \quad (68)$$

Where N is the number of samples acquired during the observation time, $R_{Use(n)}$ is the correlation function of the received signal with different correlation lags, and en_{Use} (n) is the power of data in each correlation window to normalize the correlation results. So the peak site $\widetilde{N_u}$ is the length of useful symbol in samples. This algorithm is robust against the frequency offset and phase offset [111], [112]. The performance of the algorithm is tested over different values of SNR and number taps multipath fading channel. Figure 4.8 illustrates the acquired peak through the algorithm in different SNR values with a 15 sample-spaced uniformly distributed multipath channel taps. The reason that the multipath does not overcome the useful symbol duration peak is that at the lag equal to the useful symbol duration, the CP of all symbols will correlate at the same time, which creates a relatively high correlation power compared to the multipath components peaks.



(a) 15 tabs channel, SNR=1

(b) 15 tabs channel, SNR=5

(c) 15 tabs channel, SNR=10

(d) 15 tabs channel, SNR=20

Fig 4.8 Useful symbol duration estimation algorithm results over different SNR values for 10 OFDM symbols with useful symbol duration of 512 samples

4.7.1.2 Total Symbol Duration

The total symbol duration is estimated through the periodicity feature the OFDM symbol has due to the CP [112]. An algorithm has been designed to search for the CP periodicity by using a sliding correlation window with fixed window length equal to the possible CP lengths and fixed correlation length equal to the estimated useful symbol duration. To reduce the computational complexity we use our knowledge about the possible CP sizes in the wireless system standards, which are 1/4, 1/8, 1/16, and 1/32. Figure 4.9 illustrates the mechanism of our algorithm.

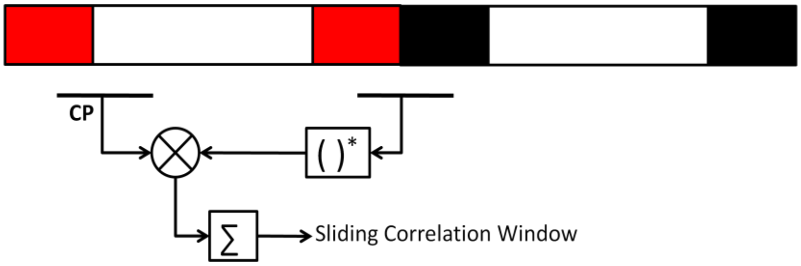


Fig 4.9 The sliding window technique for estimating the total symbol duration

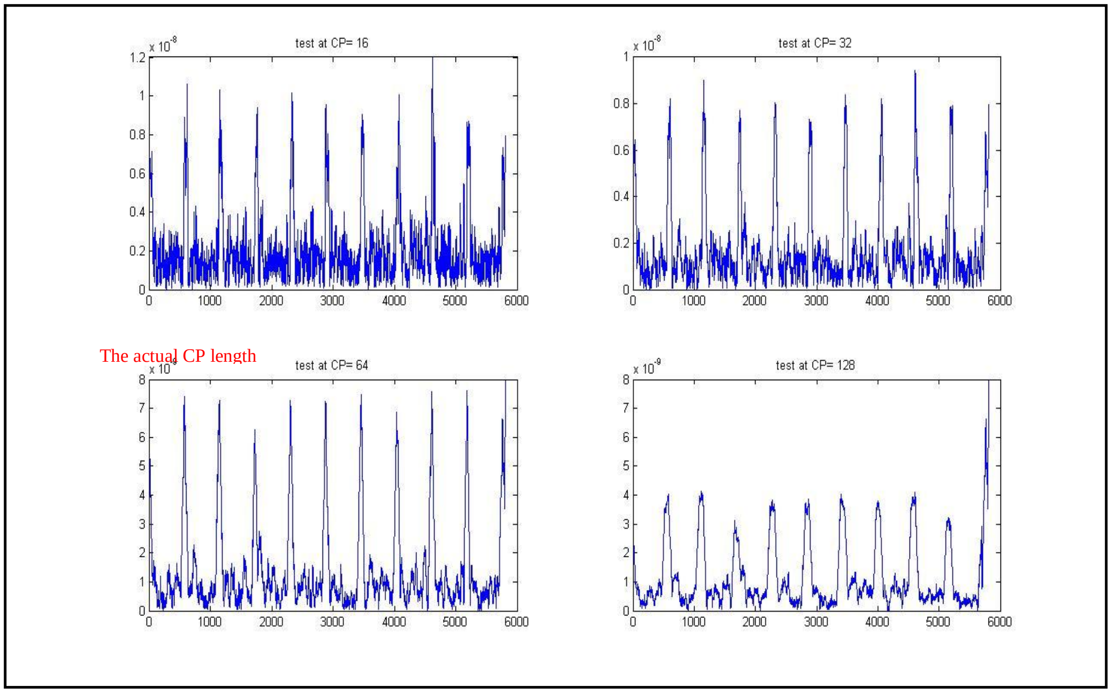
When using this method, consecutive peaks will be obtained. As we go closer to the actual CP length, we notice that the consecutive peaks become smoother. However this is not sufficient to be detected using MATLAB. It was observed that the distance between neighboring consecutive peaks equals the total symbol duration (symbol duration + CP duration); therefore we measure the distances between the midpoints of each two consecutive peaks and use a histogram to detect the most repeated value. This value will be equal to the total symbol duration, therefore:

$$L_{21} < L_{22} < L_{23} < \cdots \qquad (69)$$

$$H(p) = Hist\lfloor L_{2(j+1)} - L_{2j} \rfloor \quad j = 1,2,3,\ldots \qquad (70)$$

$$N_s = Max\ H(p) \qquad (71)$$

where L_{21} L_{22} L_{23} ... is the midpoint of each consecutive peak in the correct sequence in which they appear, $H(p)$ is the histogram function of the distance between each two neighboring peaks, and N_s is the total symbol duration estimation. Figure 4.10 illustrates the consecutive peaks due to the sliding window algorithm with different values of CP.


test at CP= 16

test at CP= 32

The actual CP length

test at CP= 64

test at CP= 128

Fig 4.10 The result of the sliding window correlation based algorithm when tested on the same OFDM symbols for different CP lengths

4.7.1.3 Cyclic Prefix Duration

After estimating the useful symbol duration and the total symbol duration, the cyclic prefix will simply be the result of subtracting them both:

$$N_c = N_s - N_u \tag{72}$$

Up to this point all the time parameters are estimated and detected, and what is left are the frequency domain parameters. Figure 4.11 shows the success rate of our algorithm for different SNR values.

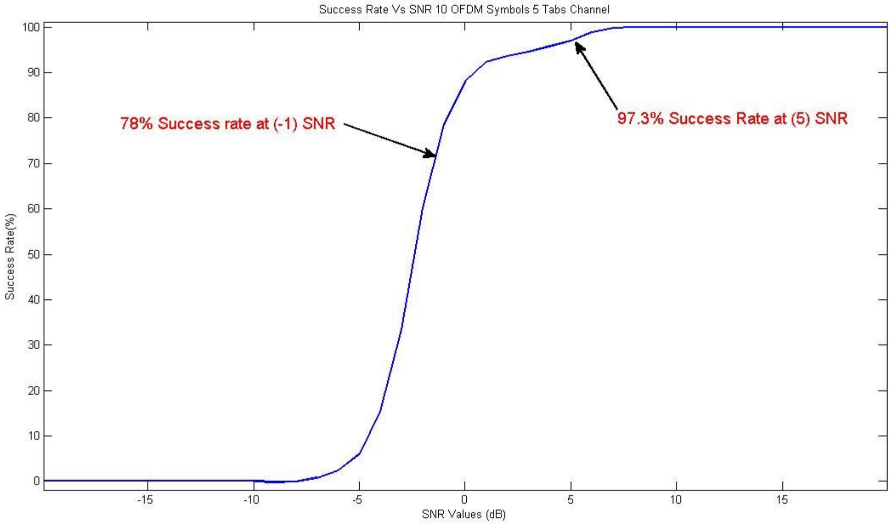


Fig 4.11 The success rate of the time parameters estimation

4.7.2 OFDM Frequency Domain Parameters

It was shown in Chapter 3 that it is important for the OFDM symbol to sustain the subcarrier orthogonality. In order to do that, this condition should apply:

$$\frac{1}{T_u} = \Delta f \tag{73}$$

where Δf is the subcarrier spacing. Thus, if N-point IDFT is used, the total bandwidth of the OFDM signal will be:

$$W = N\Delta f \tag{74}$$

where W is the total bandwidth of the OFDM signal and N is the FFT size. Assuming that the received OFDM signal sustains its orthogonality and since the useful symbol duration is known at this stage, we simply calculate the subcarrier spacing through equation (72).

Furthermore, since the total bandwidth is known, the number of subcarrier can be calculated as well:

$$N = \frac{W}{\Delta f} \tag{75}$$

As it has been illustrated, no prior information is required in all the proposed estimation algorithm, and no synchronization is needed.

4.8 Cyclostationarity Features

Cyclostationarity feature detection is one of the most popular methods for blind signal detection and identification [46], [65]-[70], [126]. Many researchers look at the cyclostationarity as the answer to many blind identification and spectrum sensing problems. In this section we try to explain the cyclostationarity and its features so that we may incorporate it into our signal identification algorithms. Much of the next section is part of the unfinished work of Dr. Arthur Snider [115].

4.8.1 Introduction to Cyclostationarity

The cyclostationary theory was first introduced by Gardner [54] in his paper series about the exploitation of the cyclostationary features in random processes [54]-[63]. In [115] the cyclostationary process is described as a stationary random process (signal) that has been engineered and modified by a periodic operation, such as amplitude modulating (AM) the signal, frequency shifting the signal, sampling the signal, or filtering the signal. For the purpose of illustration, let us look at some examples of cyclostationary processes.

Assuming $Q(t)$ is the stationary random signal, then:

$$E\{Q(t)\} = \mu_Q \tag{76}$$

and

$$E\left\{Q(t_1)\overline{Q(t_2)}\right\}= R_Q(|t_1 - t_2|) \tag{77}$$

If we multiply $Q(t)$ with a periodic function like:

a. Frequency shifting, then: $X(t) = Q(t)e^{j\omega t}$
b. AM, then: $X(t) = Q(t)\cos(wt + \theta)$
c. Sampling, then: $X(t) = Q(t)\sum_{n=-\infty}^{\infty} \delta(t - nT_s)$

All these operations will result in a cyclostationary signal $X(t)$ and will introduce frequencies that were not in the original stationary process. The cyclostationary analysis in [54] is a method to detect these artificial frequencies that was introduced to the stationary process for engineering purpose; the goal being to design a tool that will detect the hidden frequencies and ignore the original frequencies in the signal:

$$D_{\omega_{det}}\,[\,X(t)] = \begin{cases} 0 & if\ \omega_{det}\ \neq \text{Hidden frequencies} \\ 0 & if\ \omega_{det}\ = \text{Hidden frequencies} \end{cases} \tag{78}$$

where $D_{\omega}[\,]$ is the proposed detector. In [54],and later in [115], this detector was developed in a form of a mathematical tool, that is:

$$E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2} X(t)e^{-j\,\omega_{det}\,t}dt\right\} \tag{79}$$
[1]

To examine the effect of this tool, we apply it on the three examples of the cyclo-stationary processes we mentioned earlier:

a. Frequency shifting a stationary signal:

$$X(t) = Q(t)e^{j\omega t} \tag{80}$$

$$E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2} X(t)e^{-j\,\omega_{det}\,t}dt\right\} = E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2} Q(t)e^{j\omega t}\ \ e^{-j\,\omega_{det}\,t}dt\right\} \tag{81}$$

[1] The formula shown was developed by [115], which is slightly different than Gardner's mathematical representation for the cyclostationary detector [54].

$$D_{\omega_{det}} = \begin{cases} \mu_Q & \omega_{det} = \omega \\ 0 & otherwise \end{cases} \tag{82}$$

The detector picks up the ω of the carrier frequency shifter.

b. AM:

$$X(t) = Q(t)\cos(\omega t + \theta) = Q(t)\frac{e^{j(\omega t+\theta)} + e^{-j(\omega t+\theta)}}{2} \tag{83}$$

$$E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2} X(t)e^{-j\omega_{det}t}dt\right\} = E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2} Q(t)\left[\frac{e^{j(\omega t+\theta)}}{2} + \frac{e^{-j(\omega t+\theta)}}{2}\right] e^{-j\omega_{det}t}dt\right\}$$

$$= \begin{cases} \frac{\mu_Q}{2} & \omega_{det} = \omega \\ \frac{\mu_Q}{2} & \omega_{det} = -\omega \\ 0 & otherwise \end{cases} \tag{84}$$

The detector picks up the frequencies of the amplitude modulator.

c. Sampling:

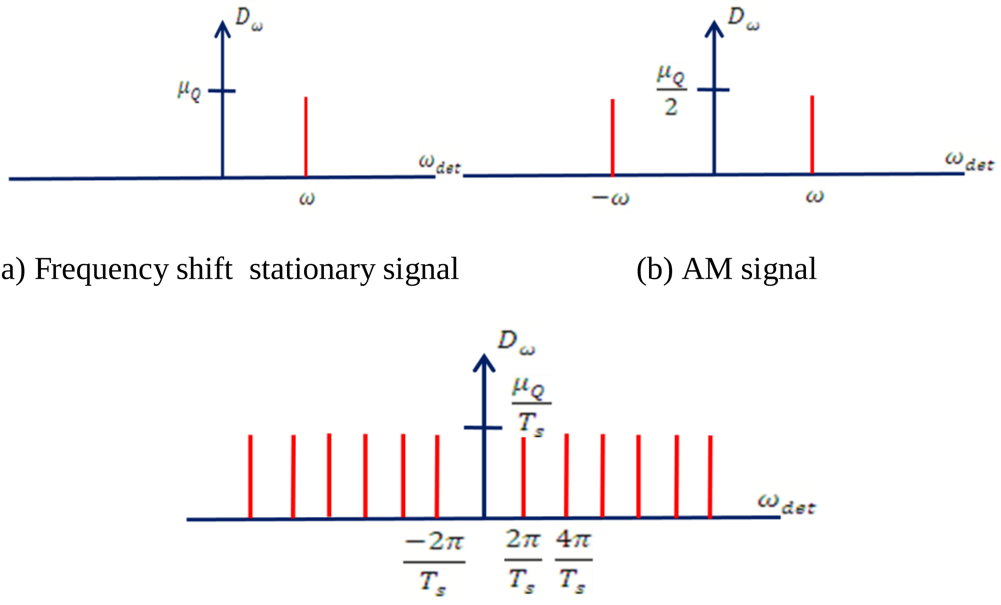
$$X(t) = Q(t)\sum_{n=-\infty}^{\infty}\delta(t - nT_s) = Q(t)\sum_{n=-\infty}^{\infty}\frac{1}{T_s}e^{j2\pi n\frac{t}{T_s}} \tag{85}$$

$$E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2} X(t)e^{-j\omega_{det}t}dt\right\} = E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2}\left[Q(t)\sum_{n=-\infty}^{\infty}\frac{1}{T_s}e^{j2\pi n\frac{t}{T_s}}\right]e^{-j\omega_{det}t}dt\right\}$$

$$D_{\omega_{det}} = \begin{cases} \frac{\mu_Q}{T_s} & \omega_{det} = \frac{2\pi n}{T_s} \\ 0 & otherwise \end{cases} \tag{86}$$

So the detector will pick up the harmonics of the sampling frequency.

Figure 4.12 illustrates the different cyclostationary detector results for the cyclostationary processes examples.



(a) Frequency shift stationary signal

(b) AM signal

(c) Sampled signal

Fig 4.12 The cyclostationary detector results for three different cyclostationary signals

One drawback the detector has occurs when the stationary process (signal) has zero means.

In this case:

$$E\{Q(t)\} = 0 \tag{87}$$

The detector will not work as planned. To overcome this problem we pass the signal through the nonlinear operation like a quadratic to force the signal mean to be nonzero. For instance, passing a zero mean stationary signal through a square law operation will change its mean to nonzero.

In [54] the author proposes to multiply the signal with a conjugated shifted version of itself as a nonlinear operation to avoid the zero mean signal case. So if:

$$X(t) = Q(t) \tag{88}$$

then

$$y(t) = Q\left(t+\frac{\tau}{2}\right)\overline{Q\left(t-\frac{\tau}{2}\right)} \tag{89}$$

and the detector will be:

$$E\left\{\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2}\underbrace{Q\left(t+\frac{\tau}{2}\right)\overline{Q\left(t-\frac{\tau}{2}\right)}}_{R_Q(\tau)\;if\;\omega_{det}=0}e^{-j\omega_{det}t}dt\right\} \tag{90}$$

where $\omega_{det} = 2\pi\alpha$ in Gardner's notation. This final form of the detector is called the cyclic autocorrelation function (CAF). For a signal with finite samples to represent it, the cyclic autocorrelation will be estimated by:

$$R_Q^{\alpha}(\tau) = \sum_{n} \left[Q(n+\tau)\overline{Q(n-\tau)}e^{-j2\pi\alpha n}\right] \tag{91}$$

In the process, a spectral correlation function (SCF) is defined to simplify the detector function in some cases. The SCF for a sampled signal will be:

$$S(f,\alpha) = \sum_{\tau=-\infty}^{\infty} R_Q^{\alpha}\,(\tau)e^{-j2\pi f\tau} \tag{92}$$

Using these tools we can examine the cyclostationarity features of signals. It is shown that all modulated signals contain cyclostationary features [54], [61], [88], [90], [107]. So it is only reasonable to examine the possible features in the received signal and to try to map the detected features to the possible standards.

4.8.2 Cyclostationarity for Signal Detection

As stated earlier, the cyclostationary approach is one of the most common methods for blind detection and spectrum sensing. In our algorithm we use the cyclostationarity features to detect two main hidden periodicities in signals. Those are the symbol rate of the single carrier based signals and the chip rate of the direct spread spectrum (DSSS) signals.

4.8.2.1 Symbol Rate Detection

Assume that $a(t)$ is a zero mean stationary random process, then:

$$E\{a(t)\} = 0 \tag{93}$$

and

$$E\{a(t)a(t-\tau)\}= R_a(\tau) \tag{94}$$

a(t) has defined autocorrelation and power spectrum density (PSD) where:

$$S_a(f) = F(R_a(\tau)) \tag{95}$$

Let $x(t)$ be the amplitude modulation of $a(t)$ at f_0 carrier frequency:

$$x(t) = a(t)\cos(2\pi f_0 t) \tag{96}$$

then the power spectrum density of $x(t)$ is:

$$S_x(f) = \frac{1}{4}S_a(f+f_0) + \frac{1}{4}S_a(f-f_0) \tag{97}$$

Figure 4.13 illustrates the PSD of both signals.

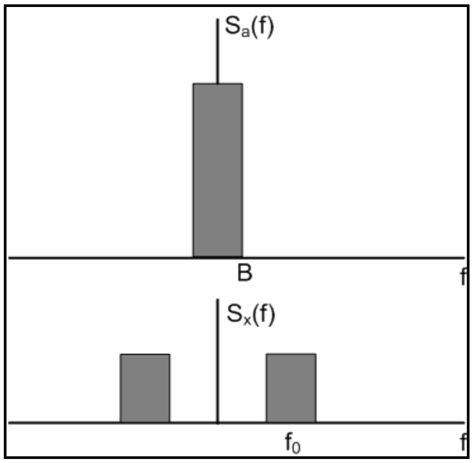


Fig 4.13 PSD of $a(t)$ and $x(t)$

The carrier frequency f_0 in the AM signal is hidden periodicity due to the modulation operation. If we pass the signal though a quadratic operation like square law operation, as suggested by [54], the result will be:

$$y(t) = x(t)^2 = a(t)^2 \cos(2\pi f_0 t)^2 \tag{98}$$

$$y(t) = \frac{1}{2}[b(t) + b(t)\cos(2\pi(2f_0)t)] \tag{99}$$

where:

$$b(t) = a(t)^2 = \mathrm{K} + \mathrm{c(t)} \tag{100}$$

$$K = E\{a(t)^2\} > 0 \tag{101}$$

Since $b(t)$ has nonzero mean, this will result in spectral line in the PSD at the zero frequency and two spectral lines components in the PSD of $y(t)$ as shown in Figure 4.14.

$$S_y(f) = \frac{1}{4}\Big[K\delta(f) + S_c(f) + \ K\delta(f+2f_0) + K\delta(f-2f_0) + \frac{1}{4}S_c(f+2f_0) + \frac{1}{4}S_c(f-2f_0)\Big] \qquad (102)$$

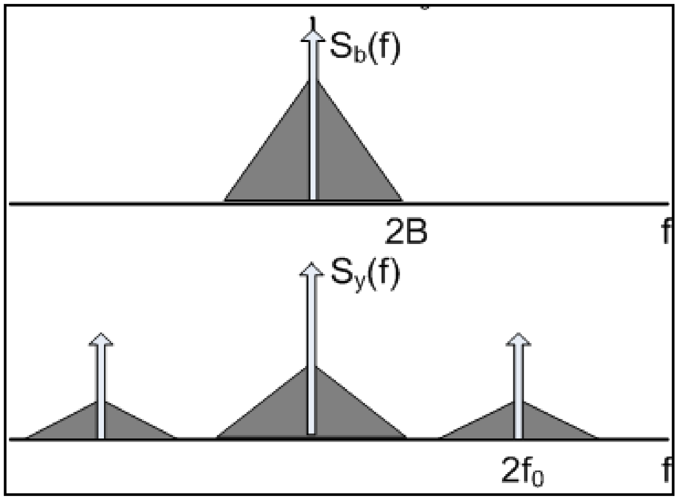


Fig 4.14 PSD of $b(t)$ and $y(t)$

Therefore, the quadratic operation reveals the hidden periodicity of the AM signal. In digital communication systems $a(t)$ is sampled and the pulses (if pulse-shaped) are transmitted through a pulse-shaped filter to prepare the signal and make it more suitable to be transmitted through the channel, as illustrated in Figure 4.15.

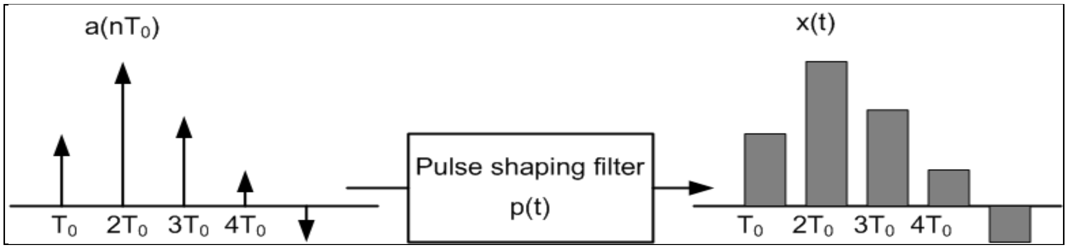


Fig 4.15 The pulse-shaping process

To examine the effect of the pulse-shaping let us assume that:

$$x(t) = \sum_{n} a(nT_s)p(t - nT_s) \tag{103}$$

where $a(nT_s)$ is zero mean data, $p(t)$ is the pulse shaping filter and T_s is the symbol rate.

Then the PSD of $x(t)$ will be:

$$S_x(f) = \frac{1}{T_s}|P(f)|^2 \sum_{m} S_a\left(f - \frac{m}{T_s}\right) \tag{104}$$

Figure 4.16 Illustrates the PSD mentioned above.

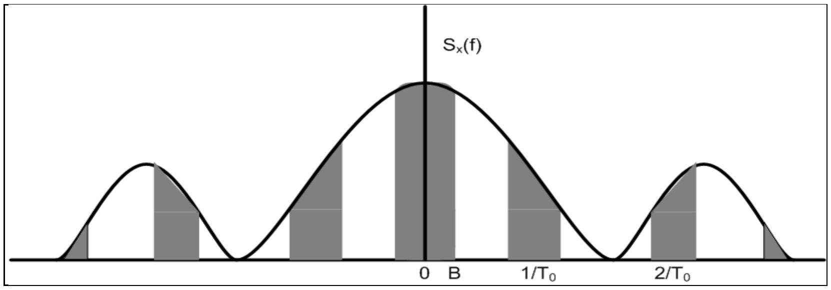


Fig 4.16 PSD of the pulse-shaped signal $x(t)$

Again, there are no spectral lines in the PSD, but the symbol period will cause a built-in periodicity in the signal that we can look for.

If we pass the signal through quadratic transformation of the square law, we have:

$$y(t) = x(t)^2 = \sum_n b(nT_s)q(t - nT_s) \tag{105}$$

where

$$b(nT_s) = a(nT_s)^2 = \mathrm{K} + \mathrm{c}(T_s) \tag{106}$$

$$q(t) = p(t)^2 \tag{107}$$

$$K = E\{a(nT_s)^2\} > 0 \tag{108}$$

Now the squared signal $y(t)$ has a positive mean, so its PSD will have spectral line components at each $\frac{m}{T_s}$. As illustrated in Figure 4.17, the PSD representation will be:

$$S_y(f) = \frac{1}{T_s}|Q(f)|^2 \sum_m \left[K\delta\left(f - \frac{m}{T_s}\right) + S_c\left(f - \frac{m}{T_s}\right)\right] \tag{109}$$

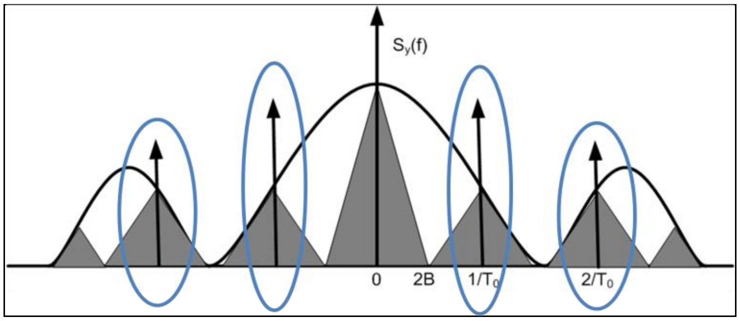


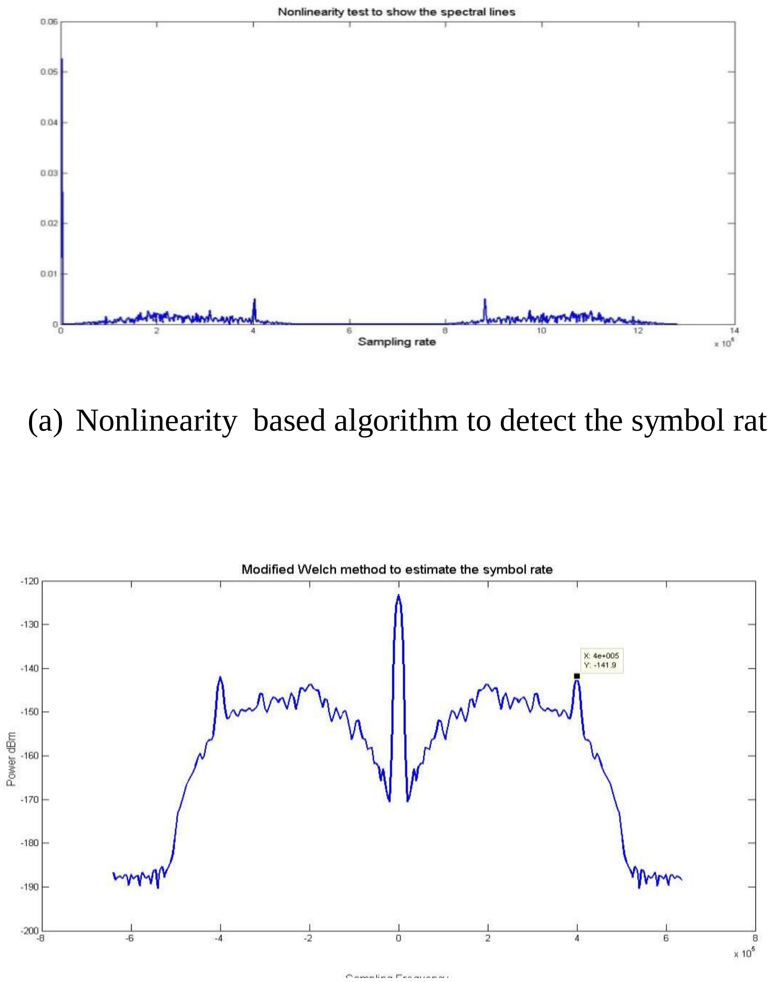
Fig 4.17 PSD of $y(t)$

As we show that spectral lines will appear at each period of the symbol rate, we use this feature and apply it on our received signal to detect the symbols rates as follows. We use the effect of nonlinear operations on the pulse-shaped signal to detect the symbol rate, pass the received signal through a square law operation, and calculate the power spectrum representation:

$$y(t) = x(t)^2 \tag{110}$$

$$S_y(f) = FFT(x(t)^2) \tag{111}$$

If we apply this operation on received signals to test the cyclostationary features, we are able to detect a peak that corresponds to the symbol rate of the digitally modulated signals, as shown in Figure 4.18a. Furthermore, [114] and [116] recommend to detect the symbol rate feature using the Welch periodogram [117]. A cyclostationarity detector is developed using Welch periodogram to detect the symbol rate of the digital modulation type signals. The result of the algorithm is shown in Figure 4.18b.



(a) Nonlinearity based algorithm to detect the symbol rate

(b) Welch based algorithm to detect the symbol rate

Fig 4.18 Symbol rate estimation without and with using Welch periodogram

We notice that there is a dominant peak when the detector frequency is equal to the symbol rate. Furthermore, there is another peak at frequency zero. To isolate the zero frequency peak, we designed the algorithm to search between $0.25BW - BW$ to make sure that we will pick up only the peak corresponding to $\frac{1}{T_s}$. We picked up this range based on the following analysis.

In pulse-shaped signal cases, the filter bandwidth and roll-off factor impact the occupied bandwidth of the signal as follows:

$$BW \propto \frac{1}{2} R_s (1+\alpha) \tag{112}$$

where α is the roll-off factor of the pulse shaping filter, R_s is the symbol rate, and BW is the signal bandwidth. Knowing that $\alpha < 1$, it is obvious that the bandwidth of the signal is larger than the symbol rate. Figure 4.19 illustrates the symbol estimation performance with respect to the SNR in 5 Tabs AWGN channel.

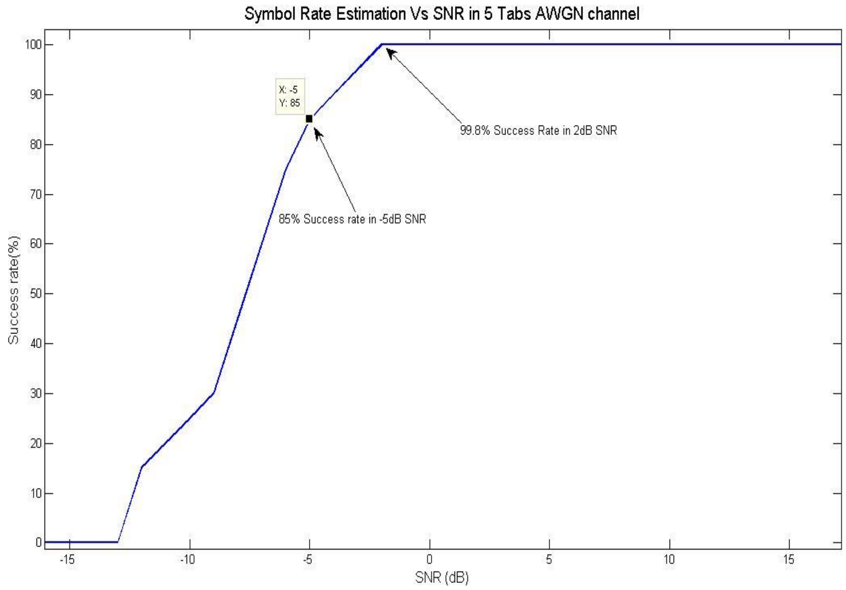


Fig 4.19 Symbol rate estimation algorithm performances with respect to SNR

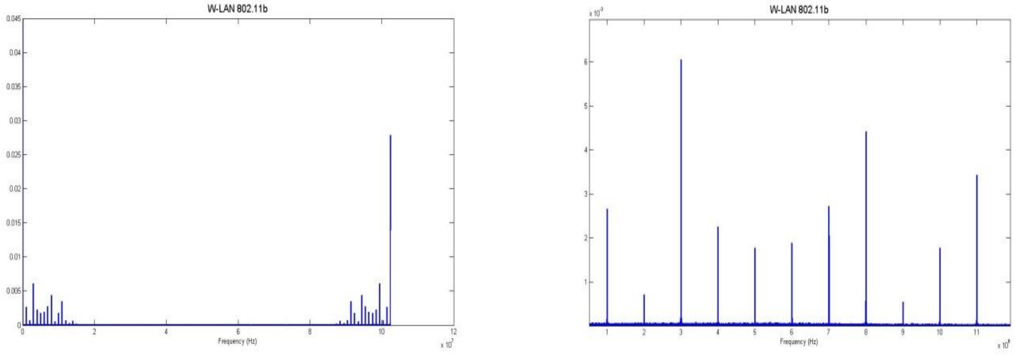
4.8.2.2 Chip Rate Estimation

Applying the same algorithm described in the previous section on the DSSS signals will result in revealing the chip rate features.

As we explained in Chapter 3, each bit of duration T is spread into a sequence of N chips. Therefore:

$$T_c = \frac{T}{N} \tag{113}$$

where T_c is the chip duration and N is the spreading sequence length. The algorithm reveals the chip rate as well as the symbol rate of the original data before spreading. As illustrated in Figure 4.20, the used signal is WLAN signal IEEE 802.11b. The chip rate of this signal is 11Mcps, and the symbol rate is 1Mbps. We observe discrete spectrum lines with symbol rate intervals, as well as a peak at 11MHz that corresponds to the chip rate of the system. Figure 4.21 illustrates a typical WLAN 802.11b transmitter.



(a) Full spectrum of the algorithm output (b) Zoomed spectrum

Fig 4.20 WLAN IEEE 802.11b DSSS signal when tested using the nonlinear algorithm

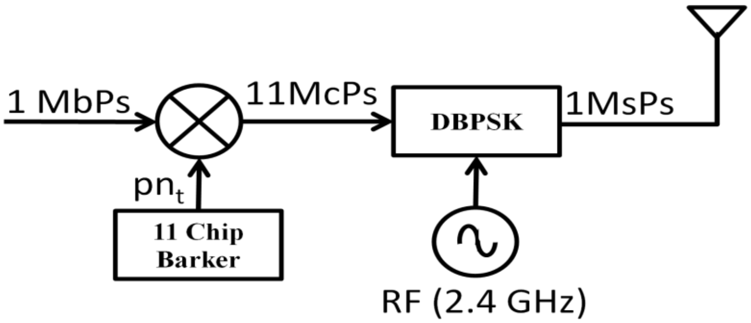


Fig 4.21 Typical WLAN DSSS transmitter

These discrete spectral lines can help with the detection of DSSS signals by searching for their existence. Also, we estimate the symbol period and the chip width by calculating the space of the discrete spectrum lines at the same time. A similar approach is used in [118] and those results matched our algorithm results.

4.9 Hopping Sequence

In frequency hopping spread spectrum (FHSS), a hopping sequence is deployed to spread the signal over a wide range of frequencies to avoid interference. The data stream is divided and transmitted over different central frequencies after modulating each part with Gaussian frequency shift keying (GFSK). The knowledge of the used hopping sequence is crucial to demodulate the received signal at the receiver. In this research we propose a method to detect the hopping sequence as a unique feature of each FHSS standard.

4.9.1 Joint Time Frequency Analysis

The main benefits of the joint time frequency (JTF) are to give us the temporal spectrum components of the signal. Using JTF analysis will help us reveal the behavior of the signal in both time and frequency at the same time. This information is particularly important in case of frequency hopping signals, where both time information and frequency information will be needed to analyze the hopping sequence. There are a handful of studies and approaches about the JTF analysis in the literature [119], [120]. Some use the short time Fourier transform (STFT), others use wavelets transform approach, while Gabor expansion is deployed by other researchers. In this research we adapted the STFT approach to conduct our JTF analysis. In STFT we simply divide the signal to short periods of time through a sliding windowing technique, and the Fourier transom of each windowed part of the signal is calculated, resulting in a two dimensional characterization of the signal. The STFT representation of a given signal is:

$$STFT(\tau, w) = \int_{-\infty}^{\infty} x(t)w(t-\tau)e^{-jw\tau}\,dt \tag{114}$$

where $x(t)$ is the signal to be analyzed, and $w(t)$ is the window function. As it is shown in the equation, the result is a complex function that describes the phase and magnitude of the signal in both time and frequency domain. One thing that should be emphasized is that the tradeoff between time domain and frequency domain resolution is associated with the window selection [113]. Decreasing the window size will result in a better resolution in the time domain information because the length of the signal will be shorter, but the frequency domain resolution wills decrease. In general practices, the window is chosen to be either Gaussian or Hanning windows.

4.9.2 Spectrogram

The spectrogram is one of the common applications of the STFT. The horizontal axis represents time domain, while the vertical axis represents the frequency domain. A third dimension is expressed in the spectrogram using color coding to describe the magnitude of the signal at a certain frequency and time point. The spectrogram is calculated through the STFT, and the representation of the spectrogram is:

$$Spectogram(t,w) = |STFT(t,w)|^2 \tag{115}$$

In the digital world we get the spectrogram for a sampled signal through breaking the signal samples into overlapped chunks. Then each chunk is passed through a Fourier transform operation to get the signal frequency representation and the spectrum magnitude. A measurement of magnitude versus frequency for each time instant is performed, and the time plot is put side to side to construct the three dimensional image. Figure 4.22 illustrates the designed spectrogram.

A spectrogram algorithm is performed on the received FHSS signal to reveal the time and frequency information. The three dimensional matrix is then analyzed to find the central frequency of each hop with the time of occurrence. This way the hopping sequence will be detected.

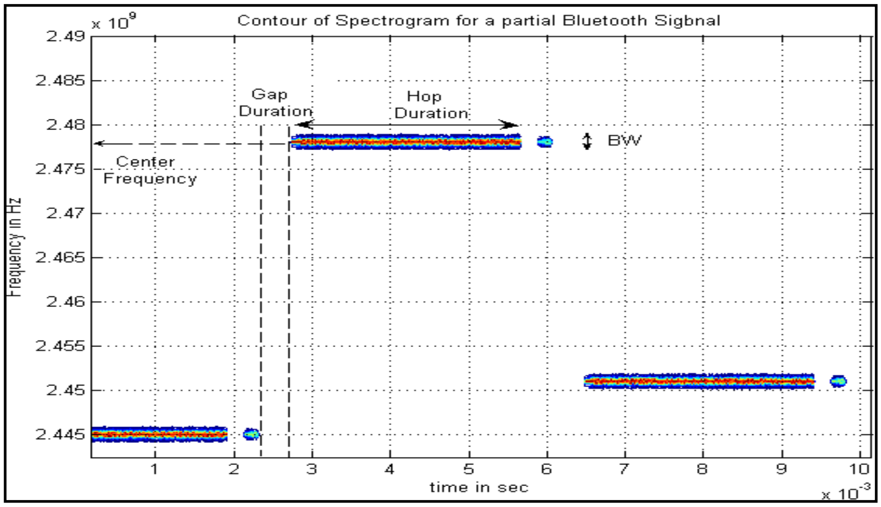


Fig 4.22 Spectrogram representation of a Bluetooth signal

There are many features that may be obvious or hidden in wireless communication signals. Identifying these features will be the success factor for any blind detection algorithm. In this chapter we defined the possible physical layer features that can participate in the process of identifying an unknown signal. Bandwidth and central frequency is estimated through a novel approach algorithm. Power related measurements of the signal are calculated. Moments test based algorithm is designed to detect multicarrier signals. A comprehensive OFDM parameter estimation has been proposed to estimate both time and frequency parameters. An introduction to the cyclostationarity is given, and an illustration of the cyclostationarity features detector was described. Symbol rate estimation is done through the nonlinearity Welch periodogram approach, as well as the DSSS chiprate and symbol rate estimation. An introduction to the joint time frequency analysis is given, along with a comprehensive JTF based algorithm that is proposed to detect the FHSS and the used hopping sequence.

4.10 Conclusion

There are many features that may be obvious or hidden in wireless communication signals. Identifying these features will be the success factor for any blind detection algorithm. In this chapter we defined the possible physical layer features that can participate in the process of identifying an unknown signal. Bandwidth and central frequency is estimated through a novel approach algorithm. Power related measurements of the signal are calculated. Moments test based algorithm is designed to detect multicarrier signals. A comprehensive OFDM parameter estimation is proposed to estimate both time and frequency parameters. An introduction to the cyclostationarity is given, and illustration to the cyclostationarity features detector was described. Symbol rate estimation is done through the nonlinearity Welch periodogram approach, as well as the DSSS chiprate and symbol rate estimation. An introduction to the joint time frequency analysis is given, along with a comprehensive JTF based algorithm that is proposed to detect the FHSS and the used hopping sequence.

Chapter 5

Decision Making Algorithm

In this chapter we describe the decision making process that follows the features extraction stage. We propose novel ISM band blind signal identification algorithms which utilize all of the possible detected features before making a final judgment.

5.1 Introduction

Many algorithms were proposed for blind signal identification, but many of these studies target a specific type of signal or one wireless standard. For instance in [50], the proposed algorithm focuses only on the energy detection, bandwidth, and central frequency to make the judgment. In [83] a threshold for the short time Fourier transform is set to identify the DSSS signals. In [85] bandwidth and energy level of the signal is used to identify the signal type. In [46], [65]-[70] [86]-[90], cyclostationarity is used to classify the signals. In [84] 4th order cumulants test is used to identify multicarrier systems, as well as many other algorithms that can be found where only a certain number of features are incorporated for the purpose of identification. This way may be sufficient enough to use for the band of interest where only certain licensed operators may be present. In the ISM band, on the other hand, there are many standards that operate at the same time, with no license needed. This makes signal detection and identification more complicated, and the uncertainties are larger. Therefore, to build up reliable blind signal identification in the ISM band, we need to make sure that as many eventualities as possible are covered. This is mainly because in the ISM band many known and unknown prospective wireless standards can appear due to the license-free quality of the ISM band. In this research we are trying to integrate all the possible features detection methods, and collect as much knowledge as possible about the signal. Only then will we use the data we have collected about the received signal to make the judgment.

The main works in this chapter are to:

a. Propose a framework for the central processing unit in the spectrum awareness engine.
b. Integrate the entire feature extraction algorithms in one controlled unit.
c. Utilize the detected features in a novel fuzzy logic-like decision making mechanism.
d. Analyze the FCC regulation for the ISM and integrate the features rule into the proposed algorithm.

5.2 The Proposed Framework

The final piece in our spectrum awareness engine will be the control and logic unit that will regulate the rest of the component’s work and utilize the incoming and outgoing information. Let us examine the proposed spectrum awareness engine flow chart that is illustrated in Figure 5.1. The band of interest will be chosen by the transmission upon request. The RF front end will sample the band of interest and pass the sampled data to the energy detection unit. The energy detector will identify the occupancy of the channel. If the channel is occupied, the sampled signal will be passed to the feature detector to extract the features and information. After searching for all the possible features, a comprehensive control and decision unit will utilize all the information and make the proper decision about the signal's nature, will either initiate the proper transmitter configuration to overcome the interference or mark the band of interest as occupied, and request a change of band.

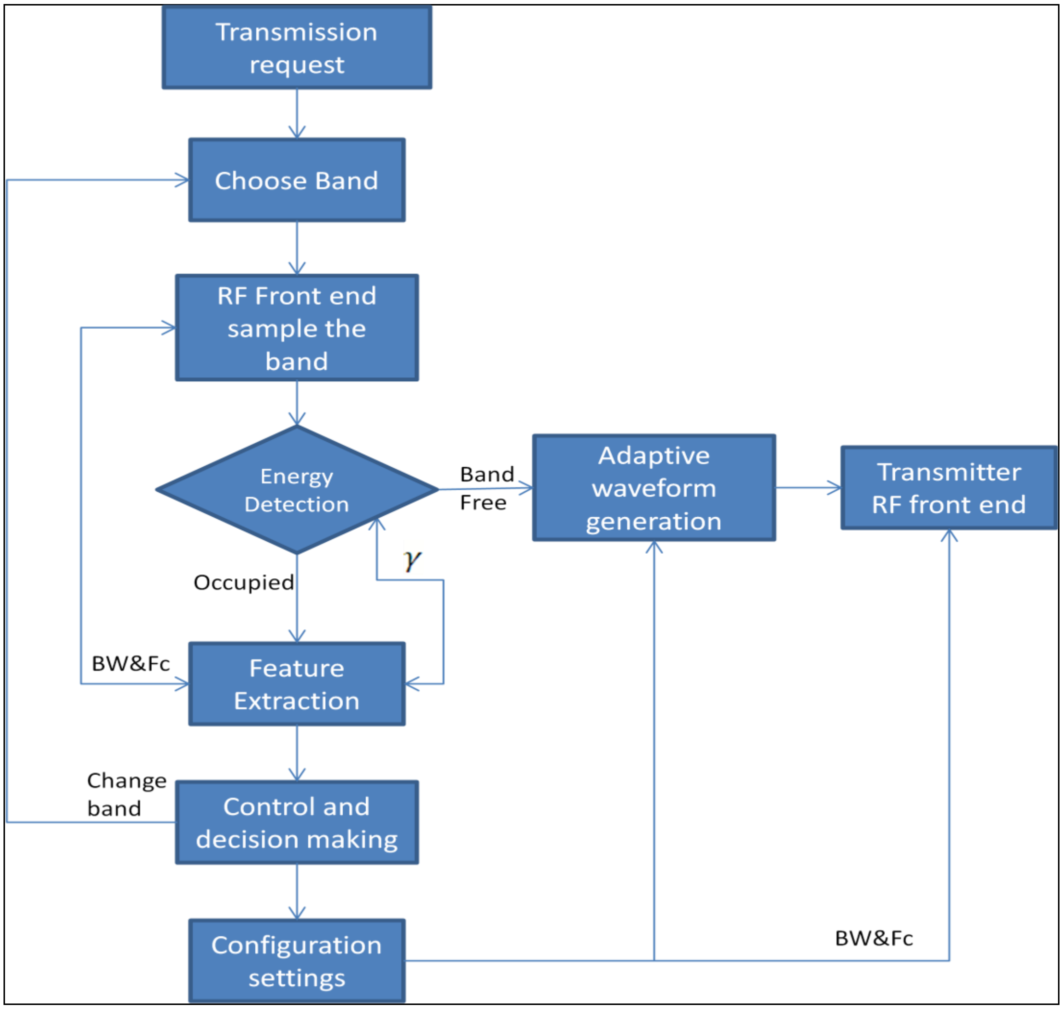


Fig 5.1 The spectrum awareness engine flow chart

The performance of the controlling and decision algorithm will define the overall effectiveness of our cognitive radio performance. This is what makes it a very important part of our spectrum awareness engine. The following sections describe the decision making flow based on the detected features.

5.3 The Decision Making

By now we can safely say that wireless standards have overlapping features and techniques. This means that although each wireless standard is unique, there exist common physical layer features which can be found between different wireless standards. Therefore, making a decision about a detected signal is not as straightforward as it may appear, especially if we keep in mind that the ISM band can be the band of operation for many wireless standards. From this point of understanding, we propose a novel approach to utilize the detected features while making the final judgment.

In Chapter 3 we thoroughly investigated each possible technology that may appear in the ISM band, and we analyzed their main features and characteristics. Using what we learned, an identification table was proposed. We cross linked each standard with the features that may identify it. Table 5.1 described the mapping of the defined features with each wireless standard.

Table 5.1 The identifying features for each wireless standard

Standard Features	W-lan IEEE 802.11g	W-lan IEEE 802.11b	BT IEEE 802.15 V.1	BT IEEE 802.15V.2	Cordless phones. (DSSS)	Cordless phones (FHSS)	Zigbee 802.15.4 DSSS	W-USB OFDM UWB	MW signals
PAPR	☞							☞	
CCDF	☞	☞			☞		☞	☞	
Time Of occurrence			☞	☞		☞			☞
Central Frequency	☞	☞	☞	☞	☞	☞	☞	☞	
BW(OBW, 3dB)	☞	☞	☞	☞	☞	☞	☞	☞	
Duty cycle									☞
Statistical infromations	☞	☞	☞	☞	☞	☞	☞	☞	☞
Single carrier		☞	☞	☞	☞	☞	☞		
Multicarrier	☞							☞	
Symbol Rate		☞			☞		☞		
DSSS		☞			☞		☞		
DSSS Chip rate.		☞			☞		☞		
FHSS			☞	☞		☞			
Hopping Sequence			☞	☞		☞			
Modulation Type and order									
OFDM Time parameters	☞							☞	
OFDM Frequency parameters	☞							☞	
FCC ISM Regulation	☞	☞	☞	☞	☞	☞	☞	☞	

☞ **Represent a potential identifying feature**

As demonstrated in Table 5.1, some features can be present in more than one wireless standard. This means that there is no precise answer; rather, approximations are more appropriate and hence, fuzzy logic reasoning is well-suited to the situation. For this reason, we adapt a fuzzy logic-like approach and soft decision making.

5.3.1 FCC Regulations for the ISM Band

Before we continue describing the proposed decision making algorithm, we need to describe one last piece of the puzzle, the FCC regulations for the ISM band. We mentioned before that the ISM is a license-free band, and any wireless device can be active in it. Although the band is license-free, it is not regulation free. The FCC regulates the usage of the ISM band, and these regulations should be followed by any wireless device operating in it. For our spectrum awareness engine, this is one of the best reference features. Because they are mandatory regulations, no one can bypass them. Thus, it is important to study the FCC regulations in the ISM band and to try to understand them and use these regulations for the benefit of our blind identifications.

In Part 15 Section 15.247 of Title 47 of the Code of Federal Regulations (CFR) [1], [121], the FCC put up rules for the frequency hopping systems that operate in the ISM band, more precisely the 2.4G ISM band. We summarize the points that deal with the 2.4GHz band that we also deem to be useful to our algorithms as [2]:

a. Frequency hopping systems should have hopping channels frequencies with a minimum separation of 25KHz or the 20dB bandwidth of the hopping channel, whichever is greater.

b. The system shall hop to channel frequencies that are selected at the system hopping rate from a pseudorandomly ordered list of hopping frequencies.

c. Each frequency must be used equally on the average by each transmitter.

[2] These regulations are located in Part 15 of the FCC rules (47 CFR 15.247).

d. Frequency hopping systems shall use at least 15 hopping frequencies.

e. The maximum 20dB bandwidth of the hopping channel is 1MHz.

f. The average time of occupancy on any frequency shall not be greater than 0.4 seconds within a 30 second period.

We believe that the most important rules are the fifth and sixth, as they state that any hopping sequence should have a bandwidth of no more than 1MHz. This allows us to decrease the computational complexity in our algorithm because it means that we do not need to check if the signal is frequency hopping if its bandwidth is more than 1MHz. Also, it indicates that to check a frequency hopping sequence, we need to observe the signal for at least 0.4 seconds.

5.3.2 Control and Execution

The process begins by first estimating the bandwidth and the central frequency of the signal. If the bandwidth is less than 2MHz, we can safely assume that the signal might be a FHSS. In this case the signal will be passed to the joint time frequency analysis unit to check if the signal is FHSS and to extract the hopping sequence. If the signal bandwidth is larger than 2MHz, we can safely assume that the signal is not FHSS; therefore, we can overcome the joint time frequency analysis.

Power related measurements are conducted, as well as the duty cycle information by passing the signal through a burst detector. The signal will be tested for single carrier or multicarrier schemes. If the carrier test indicates that the signal is multicarrier, the

OFDM parameter estimation will be applied to extract the time and frequency parameters of the signal. Otherwise, the moments test and the nonlinearity based algorithm is executed to determine the modulation scheme. The outcome will be the modulation type and order identification or the confirmation that DSSS exists in the signal. In case of a DSSS signal, we extract the chip rate of the signal through the nonlinearity and cyclostationarity test.   The symbol rate is estimated through the nonlinearity test for all the single carrier signals and is reported to the decision unit as well. At the end of this flow, we have the features parameters that we described in Chapter 4, and these are fed into our decision unit. Figure 5.2 illustrates the feature detector and the decision making unit work flow.

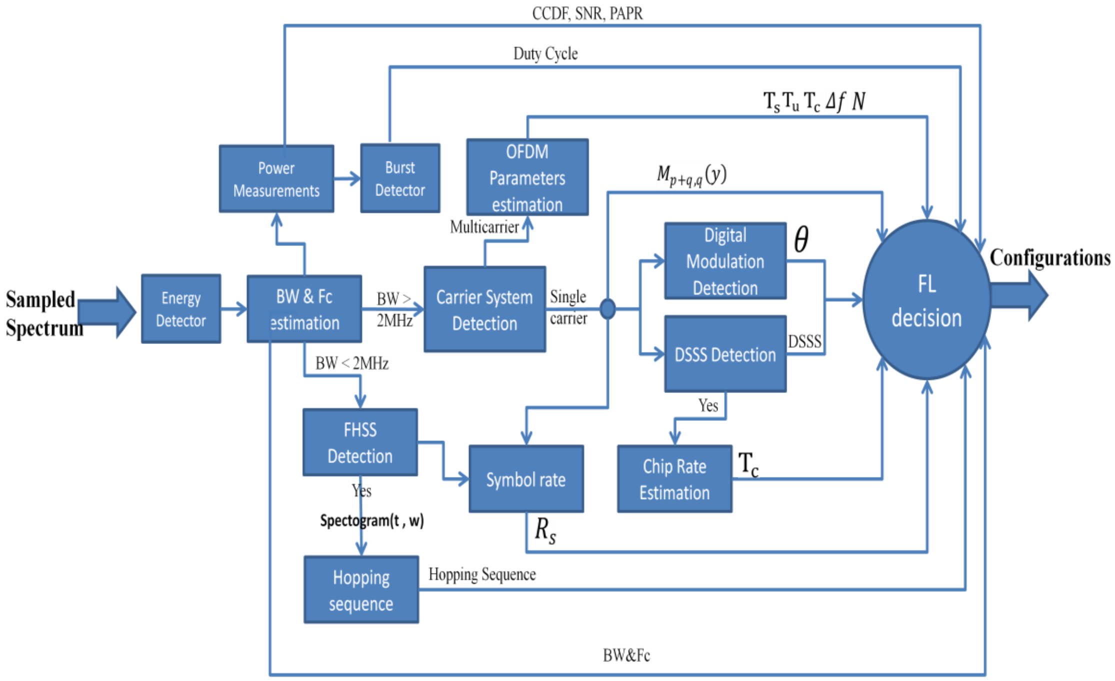


Fig 5.2 Feature detection and decision making flow chart

5.3.3 Fuzzy Logic and Soft Decision Algorithm

The concept of fuzzy logic was introduced by Lofti Zadeh, a professor at the University of California-Berkeley [92]. The author presented the concept not as a control method but as a technique of utilizing data by allowing partial set membership rather than crisp set membership or non-membership. Zadeh reasoned that people do not require precise numerical information input, and yet they are capable of highly adaptive control. We adapt the same approach in the proposed algorithm. Instead of taking the path of hard decision and precise answer in the cognitive radio, we believe that it is more reasonable to report a soft decision and probabilities about the present signal. Therefore, we propose the following method to make the decision.

A weight is given to each detected feature, and then according to the developed Table 5.1, the weight of the detected feature is transferred to the prospective wireless standards that match the feature within its standard characterization (we discussed this characterization in Chapter 3). By the end of mapping all the detected features to the possible wireless technologies, the algorithm will calculate the total weight of each wireless technology, and a probability of the presence of each wireless standard will be reported as a soft decision of the current detected signal. This way we will take into consideration all the features present instead of dropping some features when making the decision. The biggest benefit of this is seen in the case of unknown signals or new standards, where all the detected signal characteristics will be taken into account when setting up the transceiver configurations. For more illustrations, let us take the following examples. In Example 1, a WLAN standard IEEE 802.11g signal is passed to the features extraction and decision units. After extracting the features, we have the following outputs:

a. Bandwidth= 20MHz

b. Fc = 2.417GHz

c. No FHSS analysis is required, since the bandwidth is >2

d. Carrier test indicates multicarrier based signal

e. OFDM time parameters estimation results: T_s~4 µs T_c~0.8 µs T_u~3.2 µs

f. OFDM frequency parameters estimation results: Δf~ 312.5 KHz N~64

g. CCDF curves indicate high PAPR

The algorithm response is illustrated in Figure 5.3

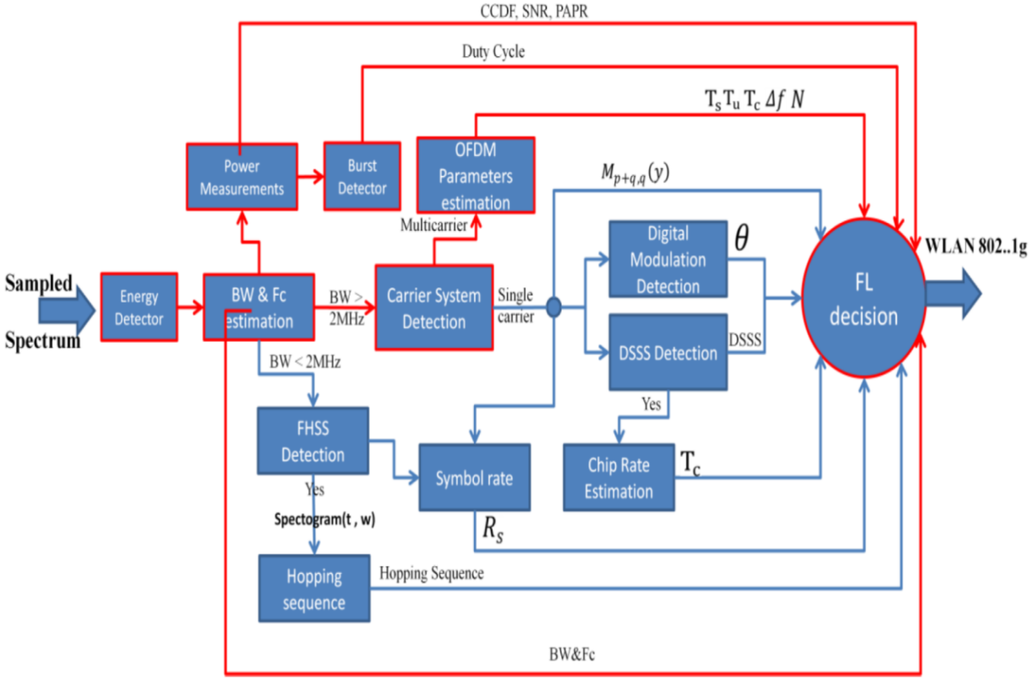
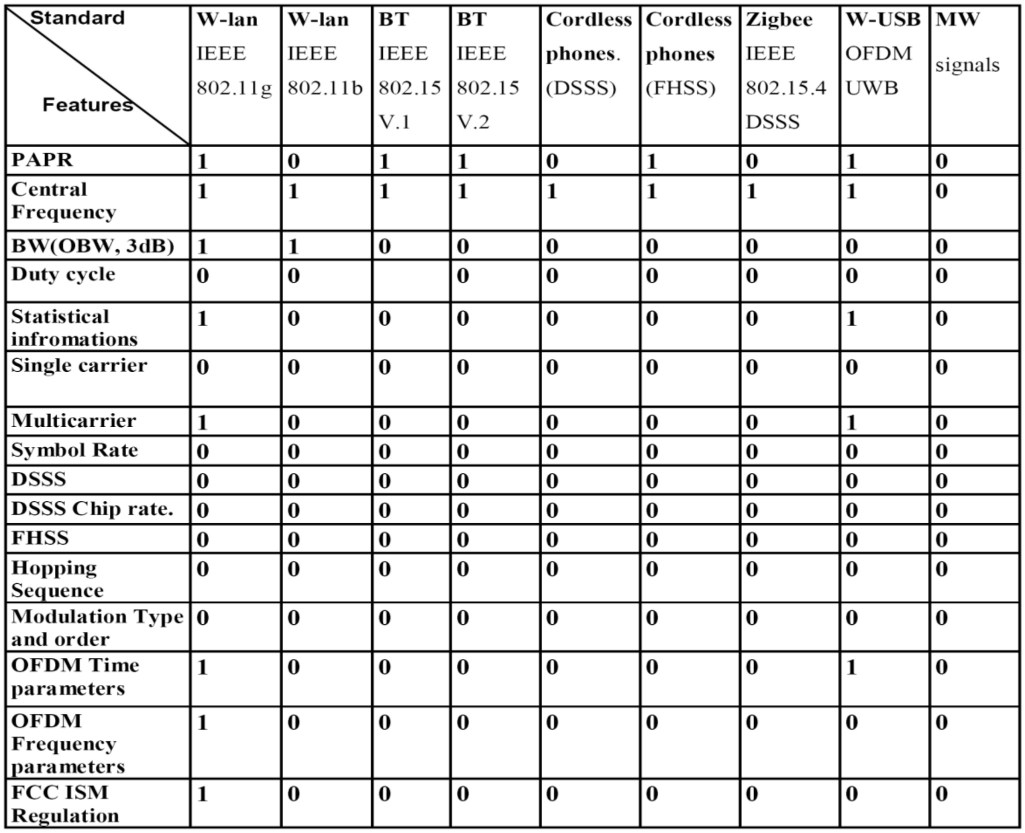


Fig 5.3 The algorithm response for a WLAN 802.11g input signal

The decision tree that will be created in the FL decision unit is illustrated in Table 5.2.

Table 5.2 The FL decision tree of Example 1



Standard Features	W-lan IEEE 802.11g	W-lan IEEE 802.11b	BT IEEE 802.15 V.1	BT IEEE 802.15 V.2	Cordless phones. (DSSS)	Cordless phones (FHSS)	Zigbee IEEE 802.15.4 DSSS	W-USB OFDM UWB	MW signals
PAPR	1	0	1	1	0	1	0	1	0
Central Frequency	1	1	1	1	1	1	1	1	0
BW(OBW, 3dB)	1	1	0	0	0	0	0	0	0
Duty cycle	0	0		0	0	0	0	0	0
Statistical infromations	1	0	0	0	0	0	0	1	0
Single carrier	0	0	0	0	0	0	0	0	0
Multicarrier	1	0	0	0	0	0	0	1	0
Symbol Rate	0	0	0	0	0	0	0	0	0
DSSS	0	0	0	0	0	0	0	0	0
DSSS Chip rate.	0	0	0	0	0	0	0	0	0
FHSS	0	0	0	0	0	0	0	0	0
Hopping Sequence	0	0	0	0	0	0	0	0	0
Modulation Type and order	0	0	0	0	0	0	0	0	0
OFDM Time parameters	1	0	0	0	0	0	0	1	0
OFDM Frequency parameters	1	0	0	0	0	0	0	0	0
FCC ISM Regulation	1	0	0	0	0	0	0	0	0

The final decision indicates that the biggest possibility is that the detected signal is wireless LAN IEEE 802.11g.

Another example is as follows. Example 2 represents a Bluetooth signal that is passed to the features extraction and the decision units. After extracting the features we have the following outputs:

a. Bandwidth ~ 1MHz

b. Fc = 2.406GHz

c. FHSS analysis is required, since the bandwidth is < 2

d. FHSS test positive

e. Hopping sequence

The algorithm response is illustrated in Figure 5.4.

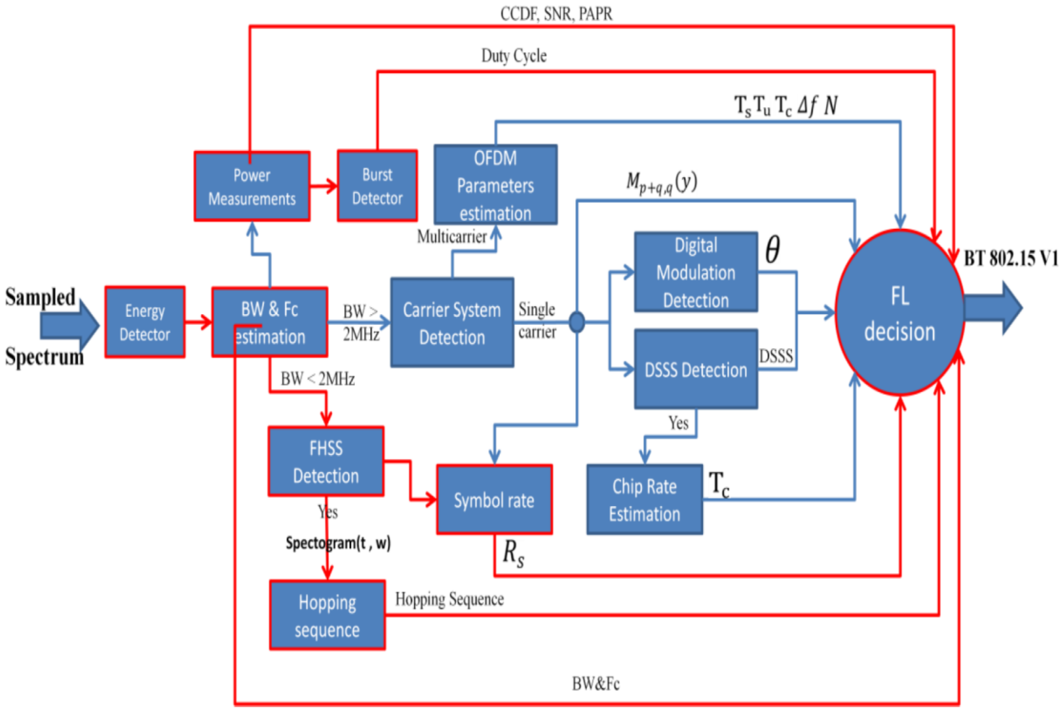
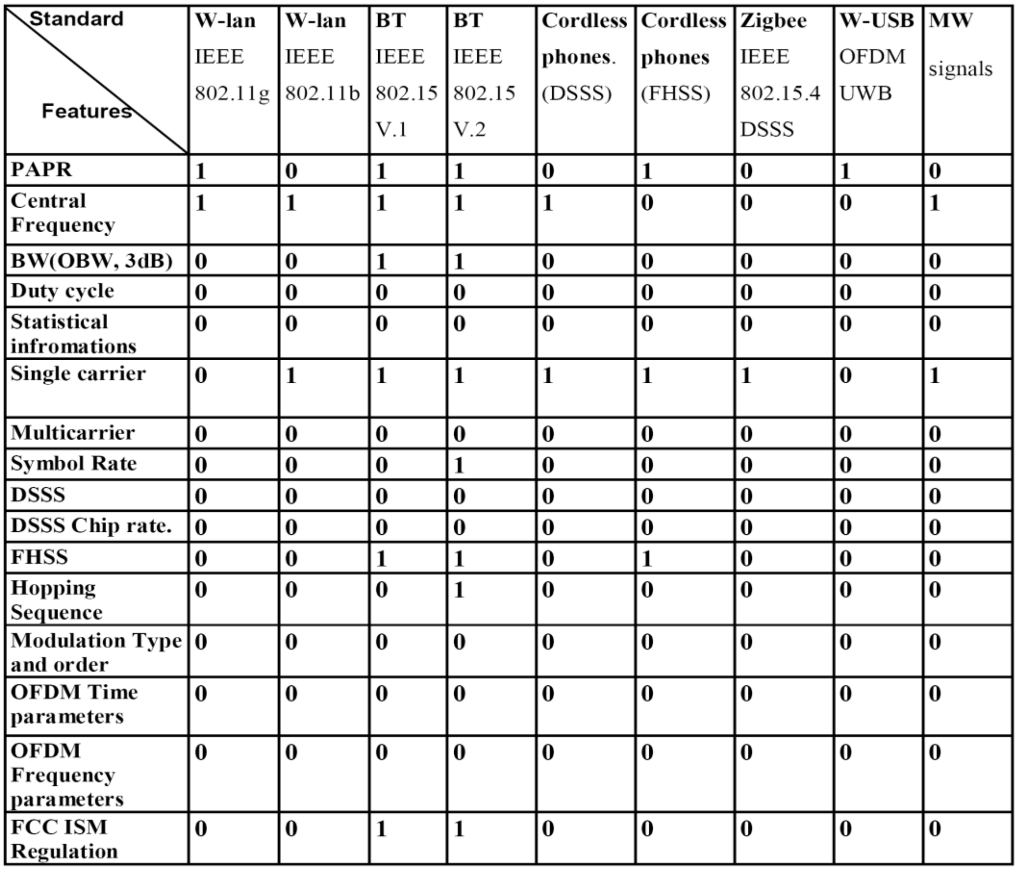


Fig 5.4 The algorithm response for a Bluetooth input signal

The decision tree that will be created in the FL decision unit is illustrated in Table 5.3.

Table 5.3 The FL decision tree of Example 2



Standard Features	W-lan IEEE 802.11g	W-lan IEEE 802.11b	BT IEEE 802.15 V.1	BT IEEE 802.15 V.2	Cordless phones. (DSSS)	Cordless phones (FHSS)	Zigbee IEEE 802.15.4 DSSS	W-USB OFDM UWB	MW signals
PAPR	1	0	1	1	0	1	0	1	0
Central Frequency	1	1	1	1	1	0	0	0	1
BW(OBW, 3dB)	0	0	1	1	0	0	0	0	0
Duty cycle	0	0	0	0	0	0	0	0	0
Statistical infromations	0	0	0	0	0	0	0	0	0
Single carrier	0	1	1	1	1	1	1	0	1
Multicarrier	0	0	0	0	0	0	0	0	0
Symbol Rate	0	0	0	1	0	0	0	0	0
DSSS	0	0	0	0	0	0	0	0	0
DSSS Chip rate.	0	0	0	0	0	0	0	0	0
FHSS	0	0	1	1	0	1	0	0	0
Hopping Sequence	0	0	0	1	0	0	0	0	0
Modulation Type and order	0	0	0	0	0	0	0	0	0
OFDM Time parameters	0	0	0	0	0	0	0	0	0
OFDM Frequency parameters	0	0	0	0	0	0	0	0	0
FCC ISM Regulation	0	0	1	1	0	0	0	0	0

The results indicate highest probability for the Bluetooth standard. Moreover, the Bluetooth version 2 has slightly higher probability due to its match with the detected hopping sequence.

As we see, the more we know about the features and statistics of the prospective standards that we may encounter, the better our algorithm performance will be.
Recall that the FSK problem we encountered in Chapter 4 is an example of the effect of the prior knowledge of standard specifications. The algorithm in the test for carrier system shows some inconsistence when tested for the FSK modulation. At some points,

the algorithm gave a result of OFDM signal while the signal was FSK. If we were making our judgment only based on the result of the carrier system test, we may reach the wrong conclusion and think that the signal is OFDM. But using all the features to make the judgment, we see that even though the algorithm gives a positive answer for the OFDM, the bandwidth does not support this decision since it indicates an FHSS signal with a hopping sequence. So the final result will have larger probability to back it up that the signal is FHSS.

The algorithm performance for different wireless standard is calculated. Table 5.4 illustrates the success rate of the algorithm blind detection in different SNR environments.

Table 5.4 The algorithm performance results of success rate detection

Standard SNR	Wlan 802.11g	Wlan 802.11b	Bluetooth	Cordless Phone	MWO
0	89%	87%	79%		
5	90%	88%	84%		
10	95%	93%	87%		
15	97%	96%	88%		
20	97%	96%	90%	93%	91%

5.4 Location and Time of Occurrence

Some additional features we can use for information are the location and time of occurrence. It was shown in [39], [40], [82], [122], and [123] that the location information can serve in cognitive cycle improvement. Furthermore in [40], [123]-[125], it was explained how Bayesian theory can be used to incorporate the past experience in the future decision making. Since the cognitive radio will monitor the spectrum continuously, the history of the decision making and the spectrum usage information over time is valuable to the learning ability of the cognitive radio. We did not implement an algorithm for this particular purpose, but we will describe the general outlines for such algorithm for the sake of consistency in the aim of this research.

The Bayesian theory states that a relationship can be established between an event and the prior knowledge about it. This means that it relates the conditional probability of an event given a certain observation. This theorem is considered as a model of learning, which makes it a perfect fit in the cognitive radio application. The Bayesian theorem is expressed as:

$$P(H|E) = \frac{P(E|H)P(H)}{P(E)} \tag{116}$$

where H represents a specific hypothesis, $P(H)$ is the prior probability of H that was inferred before new evidence, E, $P(E|H)$ is the conditional probability of seeing the evidence E if the hypothesis H happens is true, $P(E)$ is the marginal probability of E (the a priori probability of witnessing the new evidence E under all possible hypotheses), and

$P(H|E)$ is the posterior probability of H given E. It is shown in the described formula how the prior information (the history) is incorporated to decide the current probability.

5.5 Conclusion

In this chapter a novel framework for the central processing unit was developed. We demonstrated full utilization of all the extracted features before making the decision. We briefly explained fuzzy logic and integrated it into our algorithm. We explained how the FCC rules are a common ground for the entire possible wireless standard in the ISM band and that every device in the band should follow these rules. These rules were explained and analyzed. We pointed out that some of the rules can be used as features to indicate standards, so we integrated those rules into the proposed algorithm to minimize the computational complexity. Some examples were given to demonstrate how the algorithm behaves in different situations. And finally, we briefly explained the importance of the time of occurrence and the history of occurrence in the learning process of the cognitive radio.

Chapter 6

Summary and Conclusions

6.1 Summary of Works and Contributions

This research deals with the cognitive radio implementations issues in the 2.4GHz ISM band and the possibility of coexistence between cognitive radios and the pre-existing wireless standards that are active in the band. In this thesis, we proposed a new and realistic design to the spectrum awareness engine to be integrated with the model proposed in [43]. Furthermore, we designed the spectrum awareness engine to be compatible with the ISM band.

The contributions and implementations of this thesis can be summarized as follows:

a. Cognitive radio concepts and proposed models

   We defined and analyzed cognitive radio and its functionalities. We demonstrate the importance of the spectrum awareness and the continued sensing abilities in the cognitive radio performance. We identified the proposed models for cognitive radios and explained the common cognition cycle. We proposed a novel design for the spectrum awareness engine which is both realistic and can be implemented with the current circuitry capabilities, with the help of the software defined radio. We described the weaknesses and problems associated with the two common choices for spectrum sensing: the energy detector and matched filter detector.

Finally we proposed to use the energy detector only as a pre-stage in order to avoid its weaknesses.

b. The industrial scientific and medical band

We studied the ISM band characteristics and regulations extensively. We analyzed the wireless standards that may operate in the ISM band. We identified the main features of the wireless standards, especially the physical layer features that can be used in the process of blind identifications.

c. Spectrum awareness engine

We showed that there are many features which can be used to indicate wireless standards that are not utilized. We proposed a list of features to be used in our blind identification design. Since each feature requires a special way of processing to extract it, we proposed appropriate algorithms to detect the features. We attempted to increase the performance and accuracy of each algorithm, taking into consideration the computational complexity in the process of the design. We proposed an ISM band feature detector design and integrated the implemented algorithms for each individual feature into one feature detector.

d. Decision making and process controlling

We demonstrated how some features can exist in more than one standard and how this may cause confusion in the process of decision making. We developed a work flow for the central controlling unit, to help organize the work of all the units together to give the highest performance. We proposed a proper decision making method to utilize all the possible detected features and observations in order to avoid conflict, which may be due to the detection of common features or the outside impairments that the signal can suffer from and that may distort some features.

6.2 Conclusions

The ISM band is one of the most popular destinations for wireless standards for many reasons, one of which is the fact that it is a license-free band and opens to any wireless device. Although it is a free-to-use kind of band, there are regulations and rules to be followed, and in the US those rules are designed by the FCC to ensure fairness and innovation by the wireless devices. Peaceful coexistence between the wireless standards is important in the ISM band, and recently, an increasing concern has been given to this issue due to the fact that the numbers of users in the ISM band are increasing rapidly, which leads to many interference issues. A certainty is that characterizing the signals will help overcome their interference effects, with the cognitive radio as the ultimate solution.

The cognitive radio is one very promising technology. Day by day with the increasing developments in microprocessors and the software designed radio, the cognitive radio is getting more attention and raises hopes. Many models and work flows have been proposed for the cognitive radio, and more attempts should be done toward converting these models to realistic circuitry based models. The most important capability of the cognitive radio is the spectrum awareness performance since the spectrum is the most valuable wireless resource.

Wireless standards have many features, some common and some different. In this thesis, a novel design has been proposed to utilize all these features to blindly identify the signals in order to evaluate how to overcome their effects. The decision making method will have a big impact on the spectrum awareness performance of the cognitive radio, especially in a band like the ISM where every device can operate. Fuzzy logic and a soft decision approach should be considered in the cognitive radio functionalities since flexibility should be one of the cognitive radio's main characteristics.

6.3 Future Work

The ISM band has become very popular and the sanctuary of many wireless standards. We expect that this rapid growth will continue, which mean only one thing-- more congestion and more interference. That is why we believe that more research about the ISM band cognitive radio should take place.

In this research we study the identifications of the wireless signals assuming that there is no interference, and only the signal of interest is present. For this reason, the next step in this research will be to study the effect of interferences on the identification process and develop methods to isolate the interfering signals during the identification process. Since there are some indications that the ISM band will have fewer regulations, another future work can be the study of the features extraction in a total regulation free ISM band. Another possible open research area is to study the effect of channel impairments that the signal may suffer from and the effect of these impairments on the detection performance and features clearance. Furthermore, methods can be developed to overcome the channel effect during the detection and identification process.

References

[1] Federal Communications Commission, “Title 47-Telecommunication, Chapter I, Part15-Radio Frequency Devices” US Government Printing Office, 2007 CFR Title 47, Volume 1, 2007. [Online]. Available: http://www.access.gpo.gov/nara/cfr/waisidx_07/47cfr15_07.html [Accessed April 1, 2009].

[2] J. Mitola and G. Q. Maguire, “Cognitive radio: Making software radios more personal,” IEEE Personal Commun. Mag., vol. 6, no. 4, pp. 13-18, August 1999.

[3] Farpoint Group “Evaluating Interference in Wireless LANs: Recommended Practice”, Technical Note Document FPG 2006-307.2 January 2008. [Online] Available: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns736/net_implementation_white_paper0900aecd80554f8b.pdf. [Accessed April 1, 2009]

[4] Atheros Communication, “Worldwide Regulatory Progress for Wireless LANs,” 2003. [Online] Available: http://www.super-g.com/collateral/Atheros_Regulatory_whitepaper.pdf. [Accessed January 11, 2009].

[5] Farpoint Group, “The Effects of Interference on General WLAN Traffic” Document FPG 2006-328.3 January 2008. [Online] Available: http://www.cisco.com/en/US/solutions/collaterall/ns340/ns394/ns348/ns736/net_implementation_white_paper0900aecd805eb8a5.pdf. [Accessed April 2009]

[6] Cisco, “Spectrum Expert,” Cisco, 2009. [Online]. Available: http://www.cisco.com/en/US/ products/ps9393/ index.html. [Accessed April 2009].

[7] Morrow, Robert, Wireless Network Coexistence. McGraw-Hill Professional, 2004

[8] R. Pickholtz, D. Schilling, L. Milstein, “Theory of Spread-Spectrum Communications--A Tutorial,” IEEE Transactions on Communications, vol. 30, no. 5, pp. 855-884, May 1982

[9] A.J. Viterbi, CDMA: Principles of Spread Spectrum Communication. Addison-Wesley, 1995.

[10] Langton, Charan. “Orthogonal Frequency Division Multiplex Tutorial”, pp. 1-22, 2002. [Online]. Available: http://www.complextoreal.com/chapters/ofdm2.pdf. [Accessed April 2009].

[11] Radio broadcasting systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers, ETSI - European Telecommunications Standards Institute Std. EN 300 401, Rev. 1.3.3, May 2001.

[12] Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television, ETSI-European Telecommunications Standards Institute Std. EN 300 744, Rev. 1.4.1, Jan. 2001.

[13] Asymmetric Digital Subscriber Line (ADSL), ANSI - American National Standards Institute Std. T1.413, 1995.

[14] A. M. Wik, A. L. Lindblad, “Novel LPI concept using filtered spreading codes,” IEEE Military Communications Conference, McLean, Oct. 1996, vol. 1, pp. 90-94.

[15] A. Peled, A. Ruiz, "Frequency domain data transmission using reduced computational complexity algorithms," IEEE International Conference on Acoustics, Speech and Signal Processing, vol. 5, pp. 964-967, Apr 1980

[16] Wikipedia, "Guglielmo Marconi," 2002. [Online] Available: http://en.wikipedia.org/wiki/ Guglielmo _ Marconi#cite_note-12. [Accessed March 12, 2009].

[17] Wikipedia, "IEEE 802.11" 2002. [Online]. Available: http://en.wikipedia.org/wiki/802.11 #cite_note-0. [Accessed March 12, 2009].

[18] Terr, David and Weisstein, Eric W. "Barker Code," Mathworld—A Wolfram Web Resource, 2009. [Online]. Available: http://mathworld.wolfram.com/BarkerCode.html [Accessed March 12, 2009]

[19] M. Golay, "Complementary series," IEEE Transactions on Information Theory, vol. 7, no. 2, pp. 82-87, April 1961

[20] Pearson B., "Complementary Code Keying Made Simple", Application Note, May 2000. [Online]. Available: http://www.eetasia.com/ARTICLES/2001MAY/2001MAY25_NTEK_DSP_AN.PDF. [Accessed February 12, 2009].

[21] IEEE Standards Association, "IEEE 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE, March 3, 2008. [Online]. Available: http://standards.ieee.org/getieee802/802.11.html. [Accessed March 11, 2009].

[22] Bluetooth Special Interest Group, “Bluetooth Core Specification V1.2”, 2009. [Online]. Available: [http://www.bluetooth.org/foundry/adopters/document/Bluetooth_Core_Specification_v1.2. [Accessed March 11, 2009]

[23] Bluetooth Special Interest Group , “Specification of the Bluetooth System”, Bluetooth.org, 2009. [Online]. Available: http://bluetooth.com/Bluetooth/Technology/Works/Core_Specification_v21__EDR.htm. [Accessed March 15, 2009].

[24] J. T. Adams, “An introduction to IEEE STD 802.15.4,” IEEE Aerospace Conference, Jul. 2007, pp. 8.

[25] S.C. Ergen ZigBee/IEEE 802.15.4 Summary, September 2004. [Online] Available: http://www.sinemergen.com/zigbee.pdf [Accessed March 11, 2009].

[26] Wikipedia, “Zigbee,” 2002. [Online] Available: http://en.wikipedia.org/wiki/ZigBee. [Accessed February 11, 2009].

[27] Y. Yamao, S. Takagishi, “Time Shift Grouping Access in IEEE 802.15.4 MAC Beacon Mode for Layered-Tree Networks,” IEEE Consumer Communications and Networking Conference, pp. 338-342, Jan. 2008.

[28] T. M. Taher, M. J. Misurac, J. L. LoCicero, D. R. Ucci, “Microwave Oven Signal Interference Mitigation For Wi-Fi Communication Systems,” IEEE Consumer Communications and Networking Conference, pp. 67-68, Jan. 2008.

[29] A. Kamerman, N. Erkocevic, “Microwave Interference on Wireless LAN’s Operating in the 2.4 GHz ISM Band,” in Proc. of IEEE PIMRC, vol. 3, 1997, pp. 1221-1227.

[30] T.M. Taher, A. Z. Al-Banna, J.L. LoCicero, and D.R. Ucci, “Characteristics of an Unintentional Wi-Fi Interference Device – The Residential Microwave Oven,” in Proc. IEEE Military Communications Conference, Oct. 2006, pp. 1-7.

[31] T. M. Taher, M. J. Misurac, J. L. LoCicero, D. R. Ucci, “Microwave Oven Signal Modelling,” IEEE Wireless Communications and Networking Conference, pp.1235-1238, April 2008.

[32] National Telecommunications and Information Administration, “United States Frequency Allocation Chart,” US Department of Commerce, 2003. [Online] Available: http://www.ntia.doc. gov/ osmhome/ Allochrt.html. [Accessed February 2009].

[33] Federal Communications Commission, “Spectrum Policy Task Force,” FCC, 2009. [Online]. Available: http://www.fcc.gov/sptf/. [Accessed February 2009].

[34] Federal Communications Commission, “ Spectrum Policy Task Force ,” Rep. ET Docket no. 02-135, Nov. 2002.

[35] J. Mitola “Cognitive radio for flexible mobile multimedia communications,” IEEE International Workshop on Mobile Multimedia Communications, pp. 3-10, Nov 1999

[36] S. Haykin, “Cognitive radio: Brain-empowered wireless communications,” IEEE Journal on Selected Areas in Communications, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[37] S. Mangold, Z. Zhong, K. Challapali, C. T. Chou, “Spectrum agile radio: radio resource measurements for opportunistic spectrum usage,” in Proc IEEE Global Telecommunications Conference, vol. 6, Dallas, TX, Dec. 2004, pp. 3467 – 3471.

[38] H. Arslan and M. E. Sahin, “Cognitive UWB-OFDM: Pushing Ultrawideband Beyond Its Limit via Opportunistic Spectrum Usage,” Journal of Communications and Networks-Special Issue on Spectrum Resource Optimization, vol. 8, no. 2, pp. 151-157, June 2006.

[39] H. Celebi and H. Arslan, “Utilization of Location Information in Cognitive Wireless Net- works,” IEEE Wireless Communications Magazine-Special issue on Cognitive Wireless Networks, vol. 14, no. 4, pp. 6-13, Aug. 2007.

[40] H. Arslan, Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems. Springer, June 2007.

[41] H. Celebi, I. Guvenc, H. Arslan, “On the Statistics of Channel Models for UWB Ranging,” IEEE Sarnoff Symposium, Princeton, NJ, March 2006.

[42] IEEE Standards Coordinating Committee 41 “Dynamic Spectrum Access Networks,” 2007. [Online]. Available: http://www.ieeep1900.org

[43] H. Celebi and H. Arslan, “Enabling location and environment awareness in cognitive radios,” Elsevier Computer Communications-Special Issue on Advanced Location-Based Services, vol. 31, no. 6, pp. 1114-1125, April 2008.

[44] A. Sahai, N. Hoven, and R. Tandra, \Some fundamental limits on cognitive radio," in Forty-Second Allerton Conference on Communication, Control and Computing, September 2004.

[45] N. A. Robert Price, “Detection theory,” IEEE Transaction Information Theory, vol. 7, pp. 135-139, July 1961.

[46] D. Cabric, S. Mishra, and R. Brodersen, “Implementation issues in spectrum sensing for cognitive radios,” in Proc. Asilomar Conference on Signals, Systems and Computers, vol. 1, Nov. 2004, pp. 772–776.

[47] Federal Communications Commission, “Notice of proposed rulemaking and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies,” ET Docket No. 03-108, Dec. 2003, [Online]. Available: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-322A1.pdf [Accessed April 1, 2009].

[48] S. M. Kay, Fundamentals of statistical signal processing: Detection theory. Prentice Hall, 1998, vol. 2.

[49] Urkowitz, H., “Energy detection of unknown deterministic signals,” in Proc. IEEE, vol.55, no.4, pp. 523-531, April 1967.

[50] T. Yucek, H. Arslan, “Spectrum Characterization for Opportunistic Cognitive Radio Systems,” IEEE Military Communications Conference, Oct. 2006, pp. 1-6.

[51] S. Shankar, C. Cordeiro, K. Challapali, “Spectrum agile radios: utilization and sensing architectures,” in proc. IEEE international Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, Maryland, USA, Nov. 2005, pp. 160–169.

[52] D. Cabric, S. Mishra, and R. Brodersen, “Implementation issues in spectrum sensing for cognitive radios,” in IEEE Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, vol. 1, Pacific Grove, California, USA, Nov. 2004, pp. 772–776.

[53] F. Digham, M. Alouini, and M. Simon, “On the energy detection of unknown signals over fading channels,” in Proc. IEEE International Conference on Communications., vol. 5, Seattle, Washington, USA, May 2003, pp. 3575–3579.

[54] W. Gardner, “Exploitation of spectral redundancy in cyclostationary signals,” IEEE Signal Processing Magazine, vol. 8, no. 2, pp. 14-36, Apr 1991.

[55] W. Gardner, “Spectral Correlation of Modulated Signals: Part I--Analog Modulation,” IEEE Transactions on Communications, vol. 35, no. 6, pp. 584-594, Jun 1987.

[56] W. Gardner, W. Brown, Chih-Kang Chen, “Spectral Correlation of Modulated Signals: Part II--Digital Modulation”, IEEE Transactions on Communications, vol. 35, no. 6, pp. 595-601, Jun 1987.

[57] W. Gardner, “Signal interception: a unifying theoretical framework for feature detection," IEEE Transactions on Communications, vol. 36, no. 8, pp. 897-906, Aug 1988.

[58] W. Gardner, “The Role of Spectral Correlation in Design and Performance Analysis of Synchronizers", IEEE Transactions on Communications, vol. 34, no. 11, pp. 1089-1095, Nov 1986.

[59] W. Gardner, C. Spooner, “Signal interception: performance advantages of cyclic-feature detectors,” IEEE Transactions on Communications, vol. 40, no. 1, pp. 149-159, Jan 1992.

[60] C. Spooner, W. Gardner, “Robust feature detection for signal interception,” IEEE Transactions on Communications, vol. 42, no. 5, pp. 2165-2173, May 1994.

[61] W. Gardner, L. Franks, "Characterization of cyclostationary random signal processes," IEEE Transactions on Information Theory, vol. 21, no. 1, pp. 4-14, Jan 1975.

[62] W. Gardner, "Representation and estimation of cyclostationary processes (Ph.D. Thesis abstr.)," IEEE Transactions on Information Theory, vol. 19, no. 3, pp. 376-376, May 1973.

[63] W. Gardner, "Measurement of spectral correlation," IEEE Transactions on Acoustics, Speech and Signal Processing, vol. 34, no. 5, pp. 1111-1123, Oct 1986.

[64] R. Roberts, W. Brown, H. Loomis, "Computationally efficient algorithms for cyclic spectral analysis," IEEE Signal Processing Magazine, IEEE, vol. 8, no. 2, pp. 38-49, Apr 1991.

[65] N. Khambekar, L. Dong, V. Chaudhary, "Utilizing OFDM guard interval for spectrum sensing," in Proc. IEEE Wireless Communication and Networking Conference, Hong Kong, Mar. 2007, pp. 38–42.

[66] M. Oner and F. Jondral, "Cyclostationarity based air interface recognition for software radio systems," in Proc. IEEE Radio and Wireless Conference, Atlanta, Georgia, USA, Sept. 2004, pp. 263–266.

[67] Ghozzi Mohamed, Marx Francois, Dohler Mischa, Palicot Jacques, "Cyclostatilonarilty-Based Test for Detection of Vacant Frequency Bands," 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications, pp. 1-5, June 2006.

[68] D. Cabric, A. Tkachenko, R. Brodersen, "Spectrum Sensing Measurements of Pilot, Energy, and Collaborative Detection," IEEE Military Communications Conference, Oct. 2006, pp.1-7.

[69] Wenjie Ma, ShiMing Yang, Wu Ren, ZhengHui Xue, WeiMing Li, ‘Spectral correlation function in low SNR environment,” Radio Science Conference, Asia-Pacific, pp. 197-200, Aug. 2004.

[70] K. Maeda, A. Benjebbour, T. Asai, T. Furuno, T. Ohya, “Recognition Among OFDM-Based Systems Utilizing Cyclostationarity-Inducing Transmission” 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, April 2007, pp.516-523

[71] S. K. Mitra, Digital Signal Processing: A Computer-Based Approach. New York USA: McGraw-Hill, 2000.

[72] Peter Kenington, RF and Baseband Techniques for Software Defined Radio. Artech House Incorporated, 2005

[73] A. Poon, R. Brodersen, D. Tse, “Degrees of freedom in spatial channels,” IEEE Transactions on Information Theory, vol. 51, Feb 2005.

[74] H. Tang, “Some physical layer issues of wide-band cognitive radio systems,” in Proc. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, Maryland, USA, Nov. 2005, pp. 151-159.

[75] M. Olivieri, G. Barnett, A. Lackpour, and A. Davis, “A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios,” in Proc. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, Maryland, USA, Nov. 2005, pp. 170-179.

[76] A. Ghasemi and E. Sousa, “Collaborative spectrum sensing for opportunistic access in fading environments,” in Proc. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, Maryland, USA, Nov. 2005, pp. 131-136.

[77] J. Lehtomaki, J. Vartiainen, M. Juntti, H. Saarnisaari, “Spectrum sensing with forward methods,” in Proc. IEEE Military Communications. Conference, Washington, D.C., USA, Oct. 2006, pp. 1-7.

[78] M. Rahman and K. Shamsaifar, “Electronically tunable LTCC based multi-layer filter for mobile handset application,” in Proc. IEEE MTT-S Inter. Microwave Symposium Digest, vol. 3, Philadelphia, Pennsylvania, USA, June 2003, pp. 1767-1770.

[79] Richard A. Killoy, “Design and Implementation of a Link Level Software Radio,”, 1997, [Online]. Available: http://www.ittc.ku.edu/RDRN/papers/thesis/killoy_thesis_slide_061999.pdf [Accessed: Jan.1.2009]

[80] R. Vaughan, N. Scott, D. White, “The theory of bandpass sampling”, IEEE Transactions on Signal Processing , vol.39, no.9, pp.1973-1984, Sep 1991

[81] A. Sonnenschein, P. Fishman, “Radiometric detection of spread-spectrum signals in noise of uncertain power,” IEEE Transactions on Aerospace and Electronic Systems, vol.28, no.3, pp.654-660, Jul 1992

[82] Yucek T. Arslan, H. “A survey of spectrum sensing algorithms for cognitive radio applications” IEEE Communications Surveys & Tutorials, vol. 11, pp. 116-130, 2009.

[83] Zhao Zhijin, Sun Zheng, Mei Fei, “A threshold detection method of DSSS signal based on STFT,” IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, vol. 2, pp. 879-882, Aug 2005.

[84] W. Akmouche, “Detection of multicarrier modulations using 4th-order cumulants,” in Proc. IEEE Military Communications Conference, vol. 1, Atlantic City, New Jersey, USA, Oct./Nov. 1999, pp. 432-436.

[85] S. Mishra, R. Brodersen, S. Brink, R. Mahadevappa, “Detect and avoid: an ultra-wideband/WiMAX coexistence mechanism [Topics in Radio Communications],” IEEE Communications Magazine vol. 45, no. 6, pp. 68-75, June 2007.

[86] Kim Kyouwoong, I Akbar, K. Bae, Urn Jung-sun, C. M. Spooner, J. H. Reed, “Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio,” 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, April. 2007, pp. 212-215.

[87] P. D. Sutton , K. E. Nolan, L. E. Doyle, “Cyclostationary Signatures for Rendezvous in OFDM-Based Dynamic Spectrum Access Networks,” 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks , April 2007, pp.220-231.

[88] A. Tkachenko, A, D. Cabric, R. W. Brodersen, “Cyclostationary Feature Detector Experiments Using Reconfigurable BEE2,” 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, April 2007, pp. 216-219.

[89] M. K. Tsatsanis, G. B. Giannakis, “Transmitter induced cyclostationarity for blind channel equalization,” IEEE Transactions on Signal Processing, vol. 45, no. 7, pp. 1785-1794, Jul 1997.

[90] Chen Hou-Shin, Gao Wen, D. G. Daut, “Spectrum Sensing Using Cyclostationary Properties and Application to IEEE 802.22 WRAN,” IEEE Global Telecommunications Conference, Nov. 2007, pp. 3133-3138.

[91] A. Gorcin, J. Mitola, H. Arslan, “Detection and Identification of Wireless Signals with a robust coarse detection technique and template matching,” submitted to Dynamic Spectrum Access (DSA) Special Issue of EURASIP Advances in Signal Processing Journal.

[92] Lotfi Asker Zadeh, Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers by Lotfi A. Zadeh. World Scientific Publishing Company, May 1996.

[93] J. Palicot and C. Roland, “A new concept for wireless reconfigurable receivers,” IEEE Communications Magazine, vol. 41, no. 7, pp. 124-132, 2003, Jul 2003.

[94] P. Liu, B. Li, Z. Lu, and F. Gong, “An OFDM bandwidth estimation scheme for spectrum monitoring,” in Proc. International Wireless Communications, Networking and Mobile Computing Conference, vol. 1, Maui, Hawaii, USA, Sept. 2005, pp. 248-251.

[95] Hai-ying Zhang, Chao-wei Yuan, “A Method for Blind Detection of OFDM Signal Based on Power Spectrum Reprocessing,” Eighth International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, vol. 2, pp.181-186, Aug. 2007.

[96] A.P. Webster, J. Paviol, Liu Jiang; H. Arslan, L.P. Dunleavy, “Measurement-based modeling of a 5 GHz WLAN transmitter,” IEEE Radio and Wireless Conference, pp. 403-406, Sept 2004.

[97] M. Carroll and T.A. Wysocki "Characterization of indoor wireless channel at 5 GHz U-NII bands," elsevier, Computers and Electrical Engineering, vol. 30, no. 5, pp. 331-345, July 2004.

[98] G. B. Giannakis, M. K. Tsatsanis "Time-domain tests for Gaussianity and time-reversibility." IEEE Transactions on signal processing, vol. 35, no. 1, pp. 18-26, Jan 1990.

[99] Xu Bin, Yang Chenyang, Mao Shiyi, "A multicarrier detection algorithm for OFDM systems without guard time", IEEE International Conference on Communications, May 2003, vol. 5, pp. 3377-3381

[100] B. Wang, L. Ge, "A novel algorithm for identification of OFDM signal," in Proc. International wireless communications, networking and mobile computing Conference, vol. 1, Sept 2005, pp. 261-264.

[101] S.S. Soliman, S. Hsue, "Signal classification using statistical moments," IEEE Transactions on Communications, vol. 40, no. 5, pp. 908-916, May 1992

[102] Wang Bin, Ge Lindong, "Blind Identification of OFDM Signal in Rayleigh Channels," Fifth International Conference on Information, Communications and Signal Processing, pp. 950-954.

[103] B. Farhang-Boroujeny, "Multicarrier modulation with blind detection capability using cosine modulated filter banks," IEEE transactions on communications, vol.51, no.12. pp. 2057-2070, Dec 2003.

[104] Wei Dai, Youzheng Wang, and Jing Wang, “Joint power estimation and modulation classification using second- and higher statistics,” in Proc. International wireless communications, networking and mobile computing Conference, vol. 1, pp. 155-158, Mar. 2002.

[105] Su Wei, J.A. Kosinski, Yu Ming, “Dual Use of Modulation Recognition techniques for Digital Communication Signals,” IEEE Systems, Applications and Technology Conference, Long Island, May 2006, pp.1-6.

[106] D. Grimaldi, S. Rapuano, and G. Truglia, “An automatic digital modulation classifier for measurement on telecommunication networks,” in Proc. IEEE Instrumentation and Measurement Technology Conference, Anchorage, AK, May 2002, pp. 957-962.

[107] H. Li, Y. Bar-Ness, A. Abdi, O. Somekh, and W. Su, “OFDM modulation classification and parameters extraction,” in Proc. IEEE International Conference Cognitive Radio Oriented Wireless Networks and Communications, Mykonos Island, Greece, June 2006, pp. 1-6.

[108] A. Walter, K. Eric, Q. Andre, “OFDM parameters estimation a time approach,” in IEEE Thirty-Fourth Asilomar Conference on Signals, Systems and Computers, vol.1, Pacific Grove, California, USA, Nov. 2000, pp.142-146.

[109] Liu Peng, Li Bing-bing, Lu Zhao-yang, Feng-kui Gong, “A blind time-parameters estimation scheme for OFDM in multi-path channel,” International Conference on Wireless Communications, Networking and Mobile Computing , vol. 1, pp. 242-247, Sept. 2005.

[110] Shi Miao, Y. Bar-Ness, Wei Su, “Blind OFDM Systems Parameters Estimation for Software Defined Radio,” 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, April 2007, pp.119-122.

[111] T. Yucek, H. Arslan, “OFDM Signal Identification and Transmission Parameter Estimation for Cognitive Radio Applications,” IEEE Global Telecommunications Conference, Nov. 2007, pp. 4056-4060.

[112] H. Ishii, G. W. Wornell, “OFDM Blind Parameter Identification in Cognitive Radios,” IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 1, pp. 700-705, Sept 2005.

[113] A. Hesham and H. Arslan, “Multidimensional Signal Analysis and Measurements for Cognitive Radio Systems,” in Proc. IEEE Radio and Wireless Symposium, pp. 639-642, Jan 2008.

[114] M. Kueckenwaitz, F. Quint, J. Reichert, “A robust baud rate estimator for noncooperative demodulation,” in Proc. 21st Century Military Communications Conference, vol. 2, Oct. 2000, pp.971-975.

[115] A. D. Snider, Introduction to Random Processes. (Manuscript in preparation)

[116] L. Mazet, P. Loubaton, “Cyclic correlation based symbol rate estimation,” in Proc. Thirty-Third Asilomar Conference on Signals, Systems, and Computers , vol.2, Oct. 1999, pp.1008-1012.

[117] P. Welch, “The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms,” IEEE Transactions on Audio and Electroacoustics , vol. 15, no. 2, pp. 70-73, Jun 1967.

[118] Zhanqi Dong, Hanying Hu, "The Detection, Symbol Period and Chip Width Estimation of DSSS Signals Based on Delay-Multiply, Correlation and Spectrum Analysis," in Proc. of the International MultiConference of Engineers and computer scientists, Honk Kong, China, March. 2007, pp. 1198-1201.

[119] D. L. Jones and R. G. Baraniuk, "An adaptive optima lkernel time-frequency representation," IEEE Transactions on Signal Processing, vol. 43, no. 10, pp. 2361-2371, Oct 1995.

[120] D. L. Jones and T. W. Parks, "A resolution comparison of several time-frequency representations," IEEE Transactions on Signal Processing, vol. 40, no. 2, pp. 413– 420, Feb 1992.

[121] Matthew, 802.11 Wireless Networks: The Definitive Guide, Second Edition. O'Reilly Media, Incorporated, April 2005

[122] S. Haykin, "Cognitive radar: a way of the future," IEEE Signal Processing Magazine, vol. 23, no. 1, pp. 30-40, Jan 2006.

[123] Rajamani Ganesh , Sastri L. Kota , Kaveh Pahlavan , Ramón Agusti, Emerging Location Aware Broadband Wireless Ad Hoc Networks. Springer, 2005

[124] A. De Maio, A. Farina, "Adaptive Radar Detection: A Bayesian Approach," International Radar Symposium, May 2006, pp.1-4.

[125] S. Haykin, Adaptive signal processing. John Wiley and Sons, 2006.

[126] P. D. Sutton, J. Lotze, K. E. Nolan, L. E. Doyle, "Cyclostationary Signature Detection in Multipath Rayleigh Fading Environments," 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Aug. 2007, pp.408-413.