Wideband Cyclostationary Spectrum Sensing and Characterization for Cognitive Radios

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Tassadaq Nawaz

Department of Electrical, Electronics, Telecommunications Engineering and Naval Architecture

University of Genova

A thesis submitted for the degree of

Doctor of Philosophy

Genova, April 2018

Abstract

Motivated by the spectrum scarcity problem, Cognitive Radios (CRs) have been proposed as a solution to opportunistically communicate over unused spectrum licensed to Primary users (PUs). In this context, the unlicensed Secondary users (SUs) sense the spectrum to detect the presence or absence of PUs, and use the unoccupied bands without causing interference to PUs. CRs are equipped with capabilities such as, learning, adaptability, and reconfigurability, and are spectrum aware. Spectrum awareness comes from spectrum sensing, and it can be performed using different techniques. Most popular techniques include matched filters, energy detectors, and cyclostationary feature detector (CFD). Among these, CFD is used for spectrum sensing since matched filtering yields a high complexity architecture, and energy detection is sensitive to noise and fails to differentiate among signals. CFD utilize the cyclostationarity of the signals by detecting the spectral peaks in spectral correltion function (SCF), which is sparse in both angular an cyclic frequency domain. Moreover, CFD can differentiate among different signals, interfering signals and noise by using the cyclostationary spectral correlation features.

Wide-band spectrum sensing is a key enabling functionality for CRs, since sensing multiple channels simultaneously increases the probability of finding spectrum holes and hence increase the throughput of the system. Due to prioritized spectrum sharing between CRs and PUs, it is not only sufficient to detect occupancy but also distinguish among different users in order to manage interference and jamming situations in CR networks. For, this purpose CFD is proposed as a means of extracting the cyclic features of the detected signals in each frequency sub-band. Once the signal features are extracted, a previously trained Artificial Neural Network (ANN) is applied to determine the types of the signals (licit or illicit).

When the CRs are operating on a wide-band (from few hundred MHz to several GHz), the spectrum sensing task becomes more complex and could

impose a large overhead to the sensing system due to high sampling rate analog-to-digital (A/D) converters, and heavy memory overhead. Compressive sensing is adopted as a solution to reduce the overhead of A/D conversion and allow us to estimate wide-band with sub-Nyquist rate sampling. After, the Nyquist rate signal has been recovered, spectral correlation function (SCF) is applied to extract the cyclic features of wide-band signal. An ANN is trained for sub-Nyquist rate samples to classify each signal as a legitimate or jamming signal.

Finally, a large dataset is created which consists of real-data generated by spectrum measurements. The main purpose for which the dataset has been created is research in the field of PHY-layer security and CR. A Software Defined Radio (SDR) platform has been used to generate modulated signals in a specified band which are stored for off-line applications. Further, the cyclic intelligent algorithm is validated on this real dataset.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation and Objectives

Cognitive radios have been proposed as a promising solution for the future spectrum scarcity problem. The term cognitive radio has been used to intelligent radio devices that are capable of learning and adapting to their radio frequency environment. Cognitive radios are built upon software defined radios, in which most of the signal processing tasks are being handled by general-purpose processors, instead of specific-purpose hardware as in legacy radio systems.

In order for cognitive radio to work, spectrum sensing is the primary task needed to be performed by a cognitive radio terminal. Many sensing techniques have been proposed over the last decade based on matched filter, energy detection and cyclostationary detection. The matched filter detector can detect the primary signals with very high accuracy, but the comprehensive prior knowledge for primary user's signal is needed. Moreover, if the environment changes, the detector's performance degrades. Energy detector is easy to implement but it fails at low signal to noise ratios. Moreover, it is unable to differentiate among different types of signals. On the other hand, cyclostationary feature detector, due to its good performance at low signal to noise ratios, has gained much attention from the research community. Furthermore, cyclostationary feature detector is able to accurately characterize or classify the spectrum, which is a key aspect for certain cognitive radio application areas, and is an essential intermediate step between detection and demodulation. Specifically in communication electronic warfare, a cognitive radio system may be required to classify different types of signals in wide-band spectrum to avoid any potentially harmful interferes / jammers.

Radio frequency jamming is the process of illegitimate radio frequency transmission on one or more channels with the aim of disrupting the communication of the

targeted system. Jamming attacks can noticeably affect the performance of wireless communication systems and can lead to significant overload in terms of data re-transmission and increased power consumption. This thesis is not only focused on detection of jamming attacks, but also to classify legitimate wave forms (modulation scheme) in wide-band radios. It is anticipated that studies presented in this thesis will create an impact on future tactical battlefield solutions. Furthermore, it is expected that outcome of the presented research will be helpful in increasing the throughput of the commercial communication systems, by allowing multiple signals to coexist within the same band.

1.2 Thesis Contributions

The main research contributions of this thesis can be summarized as follows:

- Designed a new algorithm for wide-band spectrum characterization using spectral correlation and artificial neural network.
- Designed a new algorithm for wide-band spectrum characterization using compressed sensing for sub-Nyquist rate spectrum estimation.
- Designed an robust and energy efficient algorithm for signal classification in wide-band radios using compressed sensing and artificial neural network.
- Performances of the above designed algorithms are evaluated for various jamming attacks. For example, tone, modulated and stealthy (reactive and adaptive) jamming attacks.
- A large dataset is created consisting of real-data generated by spectrum measurements. The main purpose of the dataset is to use it for research in the field of PHY-layer security and cognitive radios. A military Software Defined Radio (SDR) platform has been used to generate modulated signals in a specified band, which are stored for off-line applications.
- Practically implemented, designed spectrum characterization algorithm on the created dataset.

1.3 Thesis Organization

The thesis consist of eight chapters in total which are based on various peer-reviewed journal and conference papers. Each of the chapters serve as a self-contained text, which introduce all the relevant concepts that are required to comprehend the topic they discuss. The thesis is organized as follows:

- Chapter 2 gives background on cognitive radio technology, spectrum sensing, signal classification and other important topics relevant to this thesis. Various spectrum sensing and signal classification techniques are briefly discussed. The motivation for wide-band spectrum sensing is elaborated and compressed sensing is reviewed in context of wide-band spectrum estimation and characterization. Moreover, various existing implementations of the cognitive radio test-beds and platforms are discussed briefly in the end.

- Merely, identification of white spaces is not sufficient in cognitive radios. The spectrum may contain jamming/interfering entities that can target the ongoing licit transmission. Therefore, for secure communication, it is important to classify the sensed spectrum into friendly and jamming waveforms. In this context, a new jammer detection algorithm is proposed in Chapter 3, using spectral correlation and artificial neural network. The proposed approach assumes a Wide-band spectrum occupied by various narrow-band signals, which can be either legitimate or jamming signals. The second order statistics, namely, the spectral correlation function and artificial neural network are used to classify each narrow band signal as a legitimate or jamming signal. The algorithm performance is shown with the help of simulations.

- Chapter 4 presents a new physical layer approach for stealthy jammer detection in wide-band cognitive radio networks. Stealthy jammer is an adaptive reactive jammer with same capabilities as a cognitive radio user. These type of jammers only transmit when a legitimate transmission is detected and stop transmitting when the legitimate transmission stops. Therefore, the jamming activities of such jammers are hard to detect by the popular sensing approaches such as energy detection at physical layer . Hence, we presented in this chapter a novel cyclostationary feature detector based approach to detect such types of jammers at physical layer. The proposed algorithm considers a wide-band consisted of multiple narrow-band sub-bands, which can be occupied by licit or stealthy jamming signals . The cyclostationary spectral analysis is performed on this

wide-band spectrum to compute spectral correlation function. The alpha profile is extracted from the spectral correlation function and used as input features to artificial neural network, which classify each signal as a licit signal or a stealthy jamming signal. In the end, the performance of the proposed approach is shown with the help of Monte-Carlo simulations under different empirical setups.

- When the radios are operating on a wide-band, the sensing task becomes more complex due to high-rate sampling, analog-to-digital (A/D) converter requirements. In chapter 5, a novel algorithm is proposed for jammer detection in wide-band cognitive radios using compressed sensing and cyclic spectral analysis. First, the received wideband signal is recovered from sub-Nyquist rate samples using compressed sensing. Compressed sensing is used to alleviate Nyquist rate sampling requirements at the receiver A/D converter. After the Nyquist rate signal has been recovered, a cyclostationary spectral analysis is performed on this estimated WB signal, to compute spectral correlation function. The alpha profile is then extracted from spectral correlation function and used to classify each narrow band signal as a licit signal or illicit signal. This algorithm is applied to detect three different types of jammers, namely; tone, modulated and stealthy jammers. The performance is shown with the help of simulations as jammer detection rate versus the compression rate.

- Chapter 6 presents a cyclostationary-based jammer detection algorithm for wide-band radios using compressed sensing and artificial neural network. The proposed approach considers a wide-band spectrum, which is occupied by several narrow-band signals. These narrow-band signals can be legitimate signals or jamming signals. Compressed sensing is used to reduce the overhead of the analog-to-digital (A/D) conversion and allows one to estimate a wide-band spectrum with sub-Nyquist rate sampling. Therefore, proposed algorithm is able to recover the received wide-band signal from sub-Nyquist rate samples using compressed sensing. After the Nyquist rate signal has been recovered, the second order statistics, namely spectral correlation function, is computed to extract the cyclic features of wide-band signal. Finally, a pre-trained artificial neural network is able to characterize each narrow-band signal as a legitimate or jamming signal. In end, the performance of proposed algorithm is evaluated for various compression ratios and SNRs to observe the effect of various parameters on the classification performance.

- Chapter 7 is focused on the creation of a large dataset consisting of experimental data generated by spectrum measurements. A software defined radio platform is used to generate modulated signals in a specified band which are stored for off-line applications. Further, newly developed cyclic intelligent algorithm is validated on real dataset for radio frequency interference mitigation. The experimental results are shown in form of confusion matrices for various system configurations.

- Chapter 8 presents some of the major conclusions drawn from the presented research and details a few future directions that would be taken to further enhance the presented work.

Chapter 2

Background and related work

2.1 Spectrum Scarcity

The Radio Frequency (RF) spectrum is a precious natural resource whose allocation is governed by various government bodies around the world. Due to fixed assignment policies, most portions of the usable RF spectrum are already allocated to different services and systems as shown in Fig. 2.1. On the other hand, transition from voice-only to multimedia communications is further amplified the need for higher data rate applications. This fixed assignment of the frequencies and the growing demands for radio spectrum due to emergence of new technologies has caused spectrum scarcity [36]. Without addressing spectrum scarcity issue, the development of radio technologies become unsustainable.

In order to address this problem, innovative techniques must be developed with the goal of providing new and more efficient methods of utilizing the usable spectrum. In several spectrum measurement surveys, it has been shown that vast portions of the licensed spectrum are highly under utilized in various geographical locations at various times [36, 34, 12]. This is situation is shown in Figures 2.2, 2.3 and 2.4.

2.2 Cognitive Radio

The Cognitive Radio (CR) concept was first introduced by Mitola as " a radio or a system that senses and is aware of its operational RF environment and can dynamically and autonomously adjust its radio operating parameters accordingly" [67, 68]. Therefore, a CR is distinguished from legacy communication device by two main aspects: the cognition capability and reconfigurability. In order to make CRs flexible, the burden has been shifted from the analog to the digital domain. After a decade of extensive research, CRs have gained a lot of interest have shown much promise. The

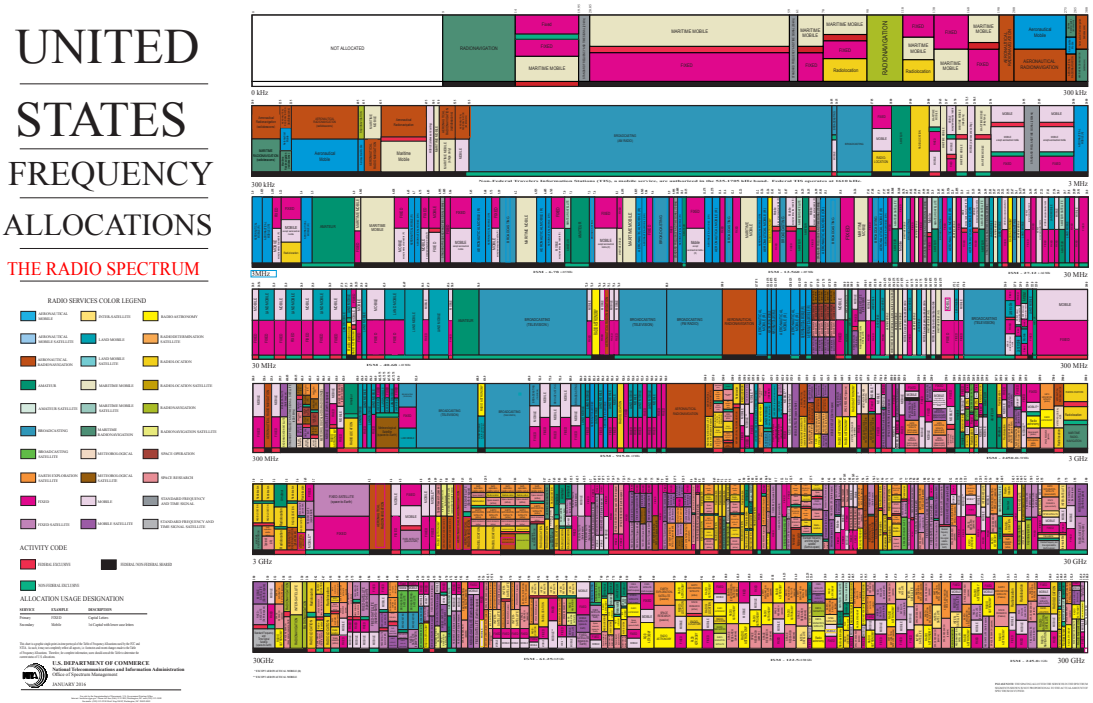
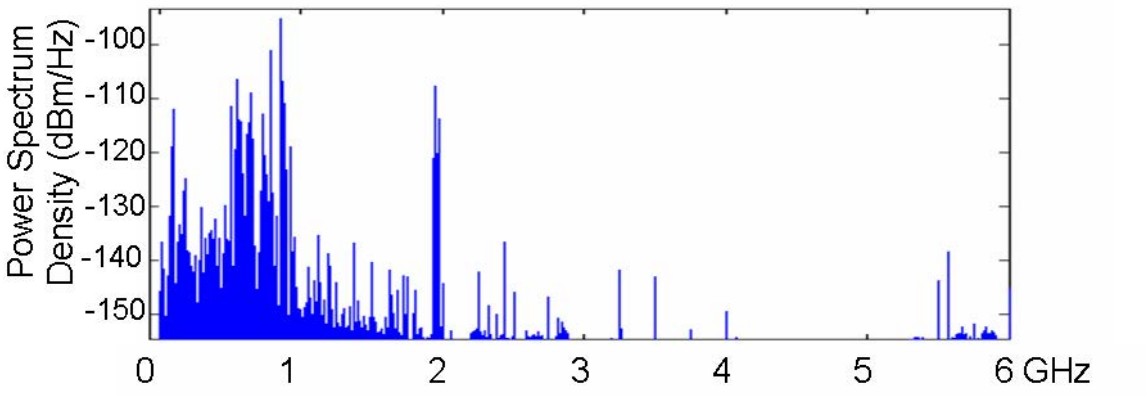


Figure 2.1: The *NTIA*'s frequency allocation chart [34]



Freq (GHz)	0~1	1~2	2~3	3~4	4~5	5~6
Utilization(%)	54.4	35.1	7.6	0.25	0.128	4.6

Figure 2.2: Measured spectrum utilization for $0-6$ GHz in downtown Berkeley [12]

fundamental idea behind a CR is the exploitation of exiting white spaces, which are licensed frequency bands that are not used by the Primary User (PU) at a given time and geographical location [82, 51, 27]. These white spaces / spectrum holes are opportunities for a secondary user (SU), and can be used either temporally, spectrally,

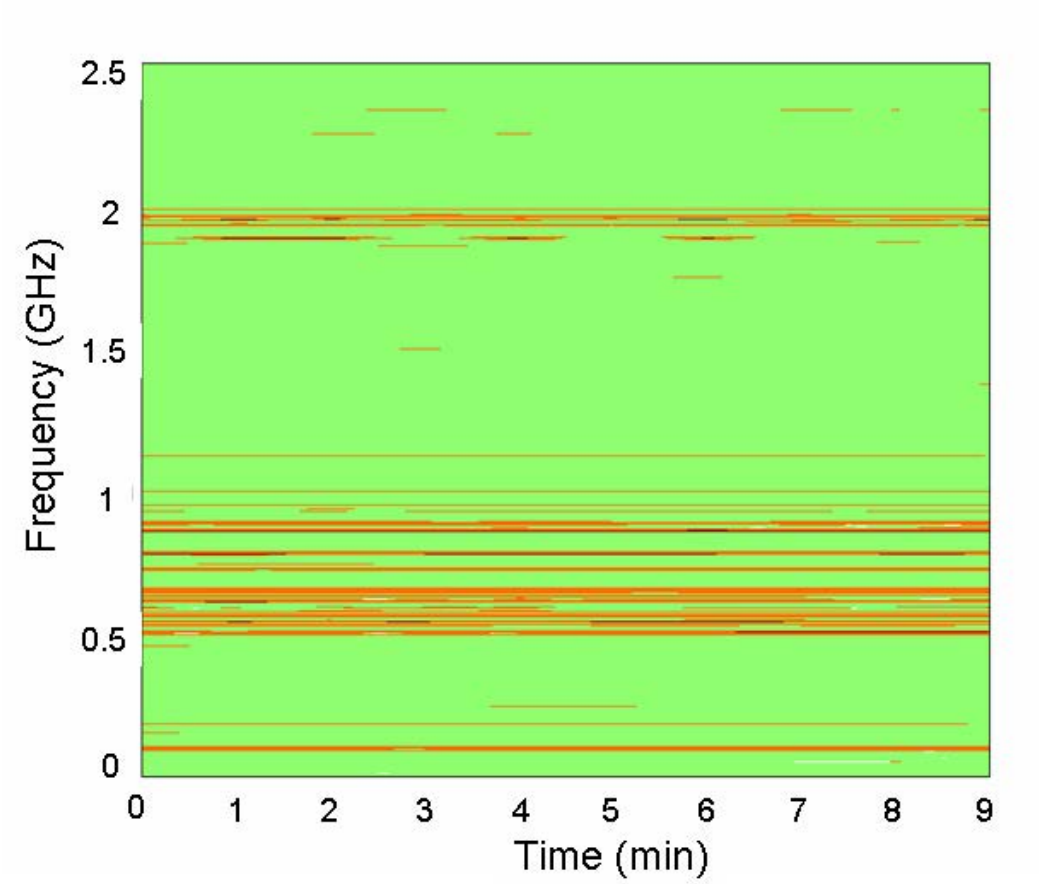


Figure 2.3: Spectrum utilization with temporal variations for $0-2.5$ GHz in downtown Berkeley [12]. Licensed user inactivity is shown as green color.

or spatially. Through CRs, the goal is to greatly increase the spectrum utilization and possibly eliminate the *false* spectrum scarcity problem caused by static spectrum allocation.

Figure 2.5 presents a cognitive cycle which shows how unique features of a CR conceptually interact with the environment. Namely, *Sensing* functionality requires contentiously monitoring the RF spectrum. *Analysis* is the characterization / classification of the spectrum. *Reasoning* needs to find the best response strategy based on the *Analysis* and *Adaption* is the transition of the device or system to new operating parameters.

One of the key aspects for a CR terminal is to avoid imposing any harmful interference to the PU while sharing the licensed spectrum. CRs are divided into three broad categories on bases of their ability to handle this problem. These catagories are overlay, underlay and spectrum-sensing (interweave) CRs. In overlay CRs, PUs share their signal information with SUs such that SUs may enhance and aid the li-

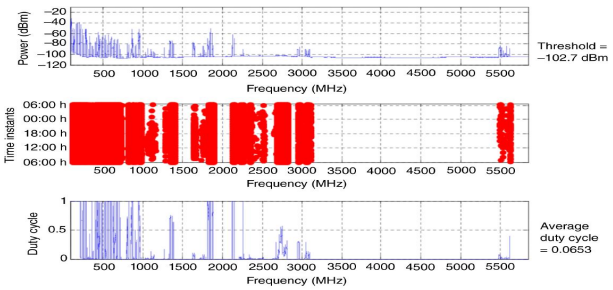


Figure 2.4: Spectrum utilization from 30 MHz to 6 GHz in Singapore [52].

censed transmission rather than competing for spectrum. In underlay approach, SUs transmissions are allowed with PUs as long as the interference level at PU remain below a tolerance threshold [57]. In spectrum sensing, SUs continuously monitor the radio environment to sense the spectrum holes and consequently use them for their transmissions. Therefore, the interweave mode allow SUs to efficiently utilize the unused white spaces , while avoiding, or limiting, collisions with PU transmissions. This dissertation is focused on interweave cognitive radios and its application, therefore, spectrum sensing will be the focus of the dissertation. Throughout this thesis, interweave CR is simply referred to as CR.

2.3 Spectrum Sensing and Signal Classification Overview

2.3.1 Spectrum Sensing

To perform its tasks properly, a CR should be aware of surrounding environment and identify all types of on going RF activities. Thus, spectrum sensing is the primary task needed to be performed by CR terminal, therefore it was identified as a major part in CRs [97, 59, 65, 14, 64, 95]. Spectrum sensing is known as the ability of a CR terminal to measure the spectrum activities due to ongoing transmissions over different frequency bands and to capture the related parameters.

Various spectrum sensing techniques have been proposed over the last decade, such as matched filtering, cyclostationay feature detection and energy detection [118, 120, 58, 63, 121, 54, 7, 62]. Matched filtering detectors are known be the best due

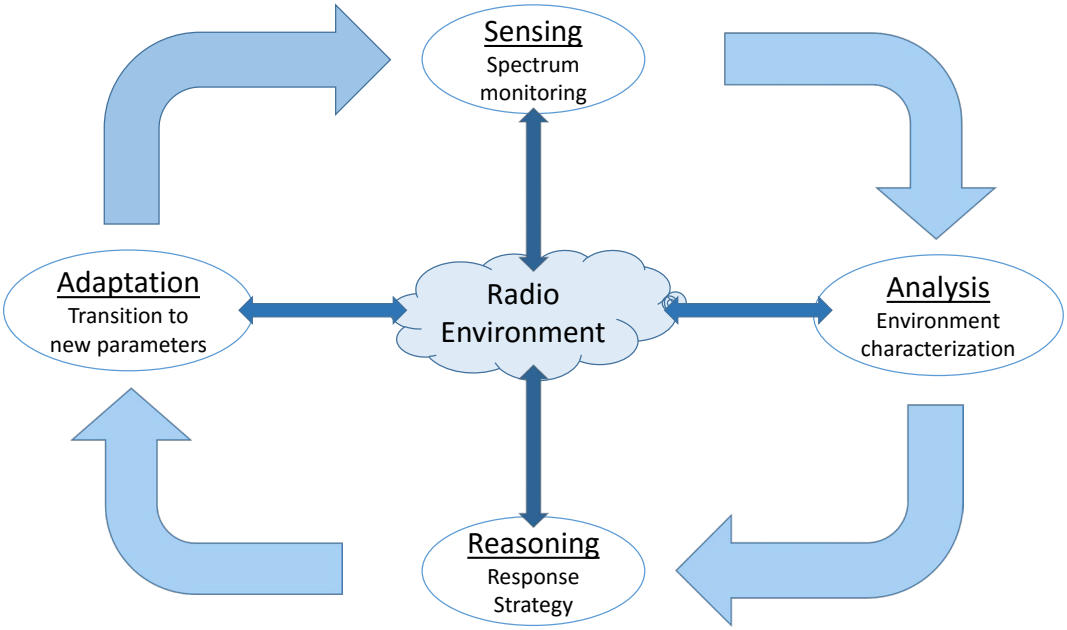


Figure 2.5: Cognitive cycle

to their detection performance even at very low SNRs but require a dedicated receiver structure for each type of signal, which may not be possible in practical CR environment. Energy detectors are blind and simplest to use but perform poorly at low SNRs. On the other hand, cyclostationary feature detectors [45, 26] use the inherent cyclic properties of the received signals. Cyclostationary feature detectors do not suffers from the noise uncertainty as they are able separate signal from noise by exploiting cyclic features of the modulated signals. Therefore, this detector is more robust than the energy detectors in this regard. The choice of detector to be considered in a CR depends on the required performance versus complexity matrix. In addition, cooperative spectrum sensing was introduced as a means of increasing the sensing accuracy by addressing the hidden terminal problems faced by wireless networks in [39, 40, 58, 121, 38, 105, 19]. In the following subsection, these spectrum sensing methods are briefly discussed.

2.3.1.1 Energy Detection

Energy detection, also known as radiometry or priodogram, is the most popular technique to detect signals due to its lowest computational cast and simplest implementation. Energy detector is used when the amplitudes of the received PU's signals

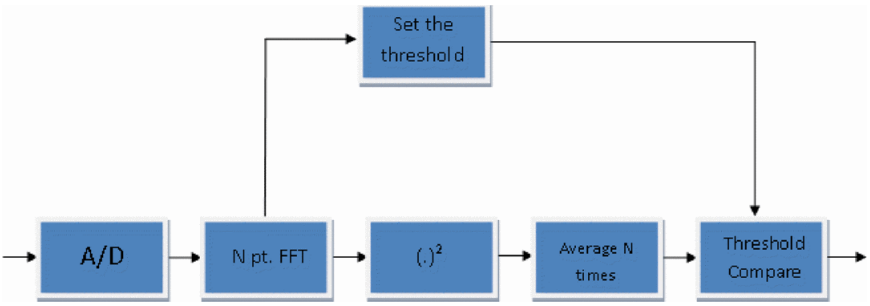


Figure 2.6: Energy detection block diagram

are unknown. The implementation steps of the energy detector is depicted in Fig. 2.6. First, the received signal is passed through a noise pre-filter and after that, it is squared and integrated to measure the energy contents. Then measured energy is compared against a predefined threshold to take the decision about the presence of the signal in particular band. The problem of the energy detection of unknown deterministic signals was explored in [4] by Urkowitz. Detailed mathematical analysis of the energy detector was presented in [4] to evaluate the probability of detection and probability of false alarm for noisy signals.Few years later, Kostylev [55] revisited the problem of energy detection and presented the analyses for noisy signals effected by different kinds of fading, such as Ricean, Rayleigh and Nakagami. The disadvantage of this spectrum sensing technique is it cannot distinguish between different types of signals, therefore, it can not be used for spectrum characterization. Moreover, energy detectors have poor performance under low SNR and can not detect the weak signals.

2.3.1.2 Matched Filtering Detection

The matched filter detector is the optimal method to detect any signal [87, 46, 53, 122, 106] because it maximizes the received SNR at receiver. Matched filter requires to demodulate the PU's signal in a CR network which would require for a CR to have prior signal information of the PU's at both PHY and MAC layers [11]. This information may include, such as modulation technique, pilots, spreading codes, preambles and packet format. The matched filter based sensing is performed by correlating the observed signal with the known sample to detect the presence of the PU. The main advantage of this detection technique is, it requires less time and few samples of the received PU's signal. However, this technique requires a dedicated receiver structure for PU which may not be possible in a CR networks. The matched filter based detection technique is depicted in Fig. 2.7.

Figure 2.7: Matched filter detection block diagram

2.3.1.3 Cyclostationary Feature Detection

Communication signals usually imposed on carrier sine waves, spreading code or hoping sequences which causes built-in periodicity. Such signals are known as *cyclostationary*, because their mean and autocorrelation exhibits periodicity [41, 42, 44]. Cyclostationary feature detection used this periodicity to detect and differentiate the modulated signals in noise and interference. The cyclostationary based detection algorithms utilize the cyclostationary of the modulated signals by detecting spectral peaks in spectral correlation function [44]. Unlike energy detectors which relay on power spectral density, a real valued, one dimensional transform, the spectral correlation function is two dimensional transform which is complex valued. Cyclostationary detector block diagram is depicted in Fig. 2.8.

Figure 2.8: Cyclostationary feature detection block diagram

The received signal is passed first through a noise pre-filter than an N-point discrete Fourier transform (DFT) is performed to decompose time domain signal into its frequency contents. After DFT, spectral correlation is taken and averaged over the symbol time T to spectral correlation function. Finally, features are extracted from spectral correlation function in order to detect and classify different type of signals. Cyclostationary feature detectors have been used by several researchers in context of CR due to their good performance at low SNRs, such as, [98, 62, 28] to name a few important ones. In [98], authors used cyclostaionary signatures for detection, network identification and rendezvous in the context of dynamic spectrum access and CR. Authors in [62], proposed an energy efficient collaborative cyclostationary spectrum sensing technique for CR systems. In [28], a fast and simple implementation scheme is introduced using single-cycle cyclostationary spectrum sensing. Furthermore, cooperation and coordination among SUs was studied to improve the detection and classification performance of the proposed detector.

2.3.2 Signal Classification

After detection and features extraction of active signals, a CR can construct an RF mapping of the on-going activities in order to learn certain characteristics about its RF domain. This RF mapping is considered to accumulate the obtained knowledge about the RF environment over time, which may assist a CR terminal in its future decision-making. Such RF mapping is based on the feature vectors that are extracted from the sensed signals. By using the suitable probabilistic models, the extracted features can be used to infer certain properties about the RF environment. For example, if the features are considered to be obtained from a mixture model, then classification methods can be used to identify the RF signals belong to certain wireless communication system. On the basis of a properly designed signal classification process, the CR terminal can identify whether a detected signal belongs to a known system (legitimate signals) or to an interferer of jammer (illegitimate signals) [110, 94, 124], which is also the objective of this thesis. This knowledge can used by a CR to decide whether to access or avoid a certain spectral band or channel. Moreover, this information can be used for designing an anti-jamming system in electronic warfare systems.

Signal classification algorithms can be divided into two categories. The Maximum likelihood (ML) algorithms [108, 86, 50, 8] are the optimal classifiers in Bayesian sense. They need the distribution of the incoming samples, and minimize the probability of false classification given a finite number of samples. However, the classification performance of the ML algorithms depend on uncertainties in the received signal. Further, ML classifiers are complex to implement, because they require to store multi-dimensional probability distribution functions. On the other hand, feature-based (FB) [99, 75, 114] classification algorithms exploit the statistical features of the incoming signal instead of relaying on the complete probability distribution function. FB based algorithms are less sensitive to uncertainties in the received signal model, are less complex to implement, but they are sub-optimal classifiers. However, the loss in classification performance is usually compensated by increasing the sample set.

Designing a FB algorithm, to differentiate the communication signals, relies on the choice of the features selected for classification. In particular, FB classifiers form a higher dimensional space in which signals of distinct features can be separated by a hyperplane. One example of such classifiers is the cumulants classifier [99] where a hierarchical tree is presented to distinguish between one or more types at each stage of classification. Another FB based classifier is Goodness of Fit (GoF) classifiers which use the probability distribution function of a given feature of the received samples.

Such classifiers depend on the knowledge of the distribution of the received signal under the different hypotheses. However, these type of classifiers are more robust to modeling imperfections than ML based classifiers. Other famous FB classifiers are cyclostationary-based classifiers which exploits the cyclic features of the received signals for classification. In this thesis cyclostationary-based classifiers are considered. The cyclic features are extracted for different types of signals, are then fed to pre-trained artificial neural network, to classify each signal as legitimate or jamming signal.

2.4 Motivation for Wideband Spectrum Sensing and Compressed Sensing

Wideband spectrum sensing has been addressed in recent CR applications [9, 10, 60, 109, 101] and has many benefits when it comes to dynamic spectrum allocation (DSA). First, sensing wideband spectrum would entail oppertunistically occupying unused spectrum from multiple frequency bands, i.e. ISMB band, TV band, etc. Moreover, wideband sensing increases the probability of finding spectrum holes, and therefore increases the CR throughput.

Wideband spectrum sensing and characterization can be performed either using narrowband or wideband RF front-end. Narrowband RF front-ends permits the sensing CR to tune to a single spectral subband at a time. In this approach, sensing would need tuning of the local oscillator used for downconversion, and only a single subband can be sensed at a time. In wideband RF front-end approach, RF front-ends downconvert a wide range of frequencies to baseband, where filtering is performed in digital domain. In this kind of receivers, sensing multiple channels would only require changing the filtering performed in DSP while keeping the RF front-end fixed. In this thesis, we focus on deployment of the wideband RF front-ends as sensing multiple channels can be performed in a fixable manner through digital processing.

When the cognitive radios are operating on a wide-band (from few hundred MHz to several GHz), the sensing task becomes more complex and imposes a large overhead to the spectrum sensing system due to the high-rate sampling, analog-to-digital (A/D) converter, and heavy memory usage. However, high sampling rate A/D converters consume high power and are hard to design. In order to reduce sampling rate requirements, compressed sensing [30] is an appealing solution that samples wideband signals below the Nyquist rate, given that the received wideband spectrum is sparse in a given domain. Due to low spectrum occupancy by PUs, the spectrum in CR

networks are typically sparse in frequency domain.Signal recovery using compressed sensing needs, intense, nonlinear optimization to find the sparset solution. One solution to this problem is provided by Convex Programming as in Basis Pursuit [16]. The other solution in literature, is to use Greedy Algorithms, such as Matching Pursuit [31] and Orthogonal Matching Pursuit [104].

Compressed sensing is used in many application areas, such as, image processing, radar signal processing video processing and other wireless services. In CR domain, some of the contributions are [32, 76, 90, 102, 85]. Authors, in [32] used traditional filter-bank based approach for wideband spectrum sensing in a multi-carrier communication environment. It has been shown that this approach has higher spectral dynamic range than traditional power spectrum estimation approaches. Another filter-based approch can be found in [76], where the filter output has been considered for channel energy vector recovery via compressed sensing. A new approach was proposed in [90] for multiband joint detection in order to detect the active PUs over multiple frequency bands. In this work, authors have claimed this scheme outperforms the traditional approaches in practical conditions. In [102] a compressed sampling followed by a wavelet based approach was used to detect and classify the wide-band RF signals. The authors in [85] proposed a compressed sensing based scheme to estimate wideband spectrum in CR networks. In essence, authors in [85] introduced the autocorrelation of compressed signal to estimate the spectrum of the sparse wideband signal.

2.5 Cognitive Radio Test-beds

Apart from large theoretical contributions, there has been various practical implementation too in CR domain. A brief overview of the hardware and software characteristics and the developed functionalities for some state-of-the-art CR test-bed and platforms architecture is given as follows. A CR platform was developed at Berkeley Wireless Research Center and it was based on the Berkeley Emulation Engine (BEE2) [13] and the reconfigurable 2.4 GHz radio frequency (RF) front ends. The fiber links were used for inter-communication. BEE2 consisted of five Xilinx Vertex-2 field programmable gate arrays (FPGAs) with support of up to 18 RF-chains, enabling experiments multiple input multiple output (MIMO) communication systems. In this platform, RF front ends support for 25 MHz bandwidth in a 85 MHz frequency range and all DSP is carried out directly on this platform. The software architecture was built on Matlab Simulink and Xilinx System Generator library to support interfaces

with A/D converters and memory. The main research focus was placed on spectrum sensing implementation. The practical performances and constraints of the well known spectrum sensing techniques, i.e. energy detectors and cylostationary detectors were shown in imperfect channel conditions. Researchers at the Kansas University, developed a agile radio, which was named as KUAR citeoz36, was a low cast SDR based platform which used 1.4 GHz general purpose processor (GPP), Xilinx Vertex-2 FPGA and a RF front-end with 30 MHz spectral bandwidth. It was developed to work in 5-6 GHz spectrum band. The most of DSP was delegated to FPGA which was targeted using the software libraries running Linus operating system. KUAR control library was consisted of a set of Application Programming Interfaces (APIs) and was core of KUAR's software architecture. The main research topics of interest included radio spectrum survey, agile transmission techniques, and channel sounding techniques. Maynooth Adaptable Radio System (MARS) [33] was another famous SDR/ CR experimental test-bed consisting of an RF front end interconnected with personal computer (PC). All the DSP was performed on the PC's GPP. This test-bed was able to operate in the 1.75-2.45 GHz range and The direct conversion architecture was implemented on both transmitter and receiver sides. The software architecture called IRiS, was highly reconfigurable, and compatible with both Linus and Windows operating systems. Research studies and implementation included spectrum sensing, image and video transmissions and interoperability with other SDR platforms.

Chapter 3

Exploiting the Cyclic Features for Spectrum Characterization in Wide-band Radios

3.1 Introduction

Cognitive radio (CR) is a promising technology for future wireless spectrum allocation to improve the use of licensed bands. However, security challenges faced by cognitive radio technology are still a hot research topic. One of prevailing challenges is the radio frequency jamming attack, where adversaries are able to exploit on-the-fly reconfigurability potentials and learning mechanism of cognitive radios in order to devise and deploy advanced jamming tactics. Jamming attacks can significantly impact the performance of wireless communication systems and lead to significant overheads in terms of retransmission and increment of power consumption. In this chapter, a novel jammer detection algorithm is proposed using cyclic spectral analysis and artificial neural networks (ANN) for wide-band (WB) cognitive radios. The proposed approach assumes a WB spectrum occupied by various narrow-band (NB) signals, which can be either legitimate or jamming signals. The second order statistics, namely, the spectral correlation function (SCF) and ANN are used to classify each NB signal as a legitimate or jamming signal. The algorithm performance is shown with the help of simulations. The rest of the chapter is organized as follows. Section 3.2 explains some background related to this work. Section 3.3 describes the system model and problem formulation. Section 3.4 presents the proposed algorithm, Section 3.5 covers the simulation results and discussion and finally the chapter is concluded in section 3.6.

3.2 Background

Over the years, cognitive radio (CR) has attained great attention from the communication society due to its ability of allowing dynamic / opportunistic spectrum access in a spectrum sparse environment [68], [47]. A CR dynamically interacts with the environment and updates the operating parameters with mission of exploiting the spectrum holes without affecting primary (licensed) user activity. To gain the knowledge of spectrum holes, spectrum sensing is the primary task needed to be performed by a CR terminal [116].

In literature, various spectrum sensing techniques have been proposed for CRs, such as, energy detection, cyclostationary feature detection (CFD) and matched filtering detection [113]. Among these methods, the CFD [113] is capable of detecting the primary signal from the interference and noise even in very low signal-to-noise ratio (SNR) regions. This performance is achieved at the cost of increased implementation complexity. The Federal Communications Commission (FCC) of the United States has suggested CFD as an alternative to improve the detection sensitivity in CR networks. Generally, energy detector fails at low SNRs while matched filtering detector requires a dedicated receiver structure which may not be possible in a practical cognitive radio terminal. CFD exploits the cyclostationarity of modulated signals by detecting spectral peaks in spectral correlation function (SCF) or spectral coherence function (SOF) [45, 93, 96], which are sparse in both angular (f) and cyclic (α) frequency domain. Major advantage of CFD based detector lies on its abilities to perform better than energy detector at low SNR values and to distinguish different modulated signals. Furthermore, the cyclic spectral analysis has been used as a robust tool for signal classification when the carrier frequency and bandwidth information is unavailable [111], [61]. A comparison among the most common sensing methods in terms of complexity and accuracy is made by [118]. In Fig. 3.2, those methods are mapped into a plane that allows to compare them easily.

Radio frequency (RF) jamming refers to the process of illegitimate RF transmission on one or more RF channels with the objective of causing maximum distortion to the communication of the targeted system. The RF jamming and anti-jamming concepts are classical in radio communication itself, but recent progresses in CR technology has enabled devising and deploying of more advanced, self-reconfigurable jamming [22] and anti-jamming [23] solutions. Spectrum sensing information plays a key role in anti-jamming systems. This information may be used to detect potential jamming entities [72], [73] and to take proactive measures to ensure communication

continuity [70] and security [21]. Moreover, a history of observations can be maintained and used to devise more effective anti-jamming tactics. For example, when a frequency hopping spread spectrum (FHSS) based system is considered, CR may modify its hopping sequence to avoid the channels which are occupied by potential jamming entities [91]. In order to design the proper anti-jamming system, there is a need for a reliable jammer detection algorithm. This chapter introduces a new algorithm for jammmer detection for WB CRs. A WB spectrum is assumed to be consisting of multiple sub-bands, each occupied by a narrow-band (NB) signal. These NB signals can be legitimate or jammers. The cyclic frequency profile (α-profile) and angular frequency profile (f-profile) of the cyclic spectral analysis are used as input features for an artificial neural network (ANN). Based on the ANN classifier, each of the NB signal is classified either as a licit or a jamming signal. Finally, the proposed algorithm performance is evaluated for various SNRs to observe the effects of diverse parameters on the classification.

3.3 System Model and Problem Formulation

We considered a received WB spectrum of Δ Hz. This WB spectrum can be occupied by various NB signals $n \in \{1, 2, 3.....N\}$, with different carrier frequencies and modulation types that we want to identify. The received WB signal is an aggregated time-domain signal which can be presented as:

$$r(t) = \sum_{n=1}^{N} h_n(t) * S_n(t) + w(t) \tag{3.1}$$

Where $S_n(t)$ denotes the $n\text{-}th$ transmitted signal, $h_n(t)$ is the channel coefficient between $n\text{-}th$ transmitter and receiver, * denotes the convolution operation and $w(t)$ is the additive white Gaussian noise (AWGN) with zero mean and power spectral density σ_w^2 . We assume that NB signals can be generated by different types of modulation schemes, such as, binary frequency shift keying (BFSK), binary phase shift keying (BPSK), quadrature amplitude modulation (QAM), quadrature phase shift keying (QPSK), or any other modulation scheme as shown in Fig. 3.1(a). The WB is divided into multiple equal bandwidth SBs and each of these SBs can be occupied by NB signals with no spill over energy into neighboring SBs.

For our proposed system, a single tone is considered as a jamming signal. The jammer is considered to be a cognitive jammer, which has the knowledge of carrier frequencies of legitimate signals. This jammer can jam any of SBs, if it has higher

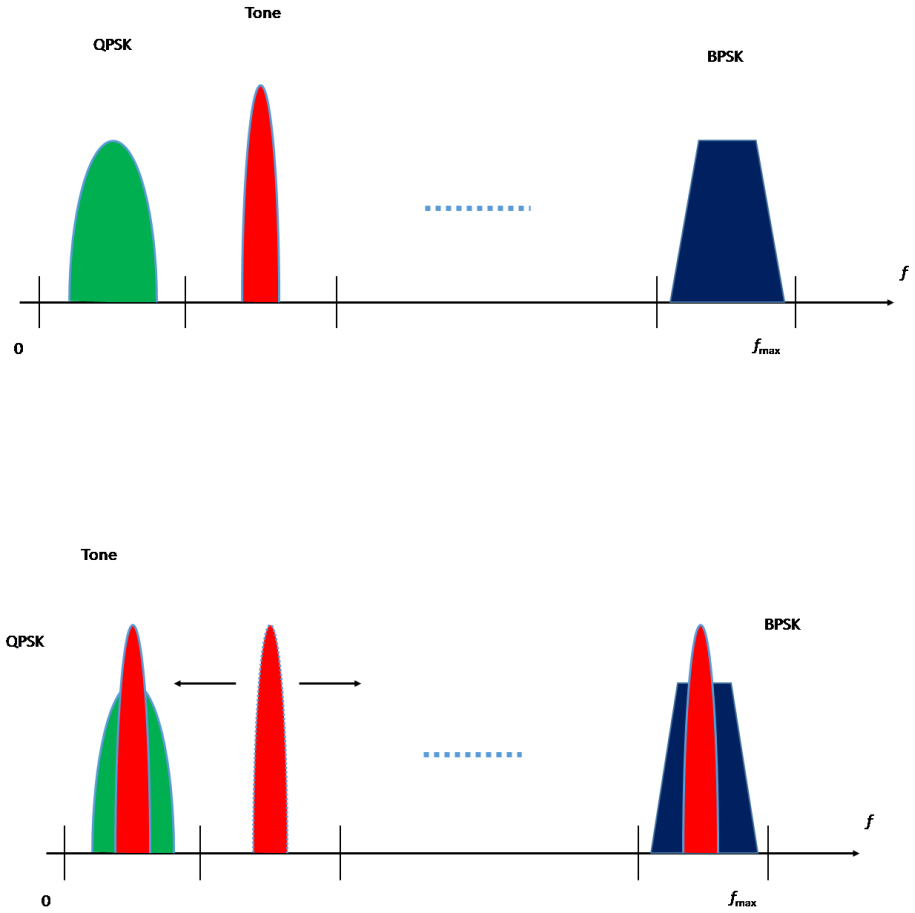


Figure 3.1: (a) Wide-band spectrum divided into multiple sub-bands (SB) and each SB is occupied by a narrow-band signal. (b) Narrow-band jammer (Tone) jumps to the neighboring SB to jam licit (BPSK or QPSK) signal.

power than the legitimate signal as depicted in Fig. 3.1(b). The tone jammer is very successful against NB signals, due to the fact that it allows to concentrate all power on a single data channel. The tone jamming is often considered as the best strategy for jammers with limited transmission power. Let us assume that the targeted signal is QPSK-modulated and uncoded, and that targeted system uses the coherent detection. Then, the error probability (p_e) to either jam the in-phase component (I) or quadrature component (Q) of the targeted signal can be given as:

Where P_r is the received power of targeted signal, P_n is thermal noise power, P_j is the jamming signal received power, θ^j is the phase of jamming signal, and

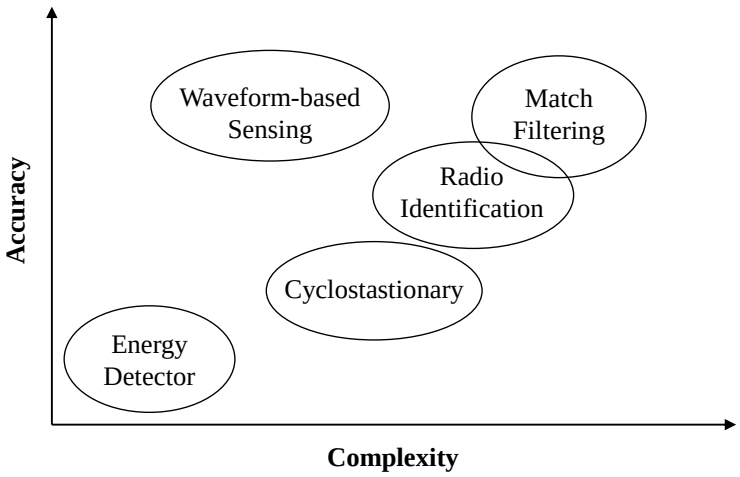


Figure 3.2: A comparison of common sensing methods

Q is the Gaussian Q-function. For our system model we consider that $P_j >> P_r$, therefore $p_e \approx 100\%$ whenever jammer transmits on the same channel as the targeted transmitter-receiver pair.

$$p_e^{\mathrm{I}} = Q(\sqrt{\frac{P_r}{P_n}}(1 - \sqrt{\frac{2P_j}{P_r}}Sin(\theta^j)) \tag{3.2}$$

$$p_e^{\mathrm{Q}} = Q(\sqrt{\frac{P_r}{P_n}}(1 + \sqrt{\frac{2P_j}{P_r}}Cos(\theta^j)) \tag{3.3}$$

3.4 Proposed Algorithm

In this section we will first introduce SCF, then neural networks and at the end we will present our newly proposed algorithm.

3.4.1 Cyclostationary Spectral Analysis

A process $x(t)$ is said to be wide-sense cyclostationary with period T_0 if its mean $E[x(t)] = \mu_x(t)$ and autocorrelation $E[x(t)x(t+\tau)] = R_x(t,\tau)$ are both periodic with period T_0, in such case, they can be defined respectively as:

$$M_x(t+T_0) = M_x(t) \quad ; \quad R_s(t+T_0,\tau) = R_x(t,\tau) \tag{3.4}$$

The autocorrelation function of a wide-sense cyclostationary process can be expressed in terms of its Fourier series components.

$$R_x(t,\tau) = E[x(t+\tau/2)x^*(t+\tau/2)] \tag{3.5}$$

$$R_x(t,\tau) = \sum_{\alpha} R_x^{\alpha} e^{j2\pi\alpha t} \tag{3.6}$$

Where, $\alpha = \frac{a}{T_0}$ and a is an integer. $E[.]$ is the expectation operator, α is the set of Fourier components, and $R_x^{\alpha}(\tau)$ represents the cyclic autocorrelation function (CAF) and gives Fourier components. CAF is given by:

$$R_x(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} R_x(t,\tau) e^{-j2\pi\alpha t} dt \tag{3.7}$$

When $R_x(t,\tau)$ is periodic in t with period T_0, (7) can be expressed as:

$$R_x^{\alpha}(\tau) = \frac{1}{T_0} \int_{\frac{-T_0}{2}}^{\frac{T_0}{2}} R_x(t,\tau) e^{-j2\pi\alpha t} dt \tag{3.8}$$

The Fourier Transform of the CAF is known as SCF and is given by:

$$S_x^{\alpha}(f) = \int_{-\infty}^{\infty} R_x^{\alpha}(\tau) e^{-j2\pi f\tau} d\tau \tag{3.9}$$

Where α is cyclic frequency and f is the angular frequency. The major benefit of spectral correlation is its insensitivity to background noises. Since the temporal correlation of different spectral components are measured; and the spectral components of noise are completely uncorrelated in time due to the fact that noise is wide-sense stationary process, such noise does not play significant factor in the SCF. This fact allows the spectral correlation of a signal to be accurately calculated even at low SNRs. Furthermore, different types of modulated signals (BPSK, AM, FSK, MSK, QAM, PAM) with overlapping power spectral densities have highly distinct SCFs. Our simulations are restricted to the BPSK and QPSK modulation schemes due to the fact that higher order QAM and higher order PSK do not exhibit second order periodicity or exhibits the same features as QPSK. Therefore, these signals can be distinguished by higher order spectral analysis [43]. An example of the SCF of WB signal is depicted in Fig. 3.3

SCF computation requires large amount of data, which makes it unreasonable for a classifier to operate on it in real time. We used here both cycle frequency profile (α-profile) and angular frequency profile (f-profile) as features for classification given in (10) and (11). The α-profile of SCF for WB signal is shown in Fig. 3.4.

$$I(\alpha) = max_f[S_X^{\alpha}] \tag{3.10}$$

$$I(f) = max_{\alpha}[S_X^{\alpha}] \tag{3.11}$$

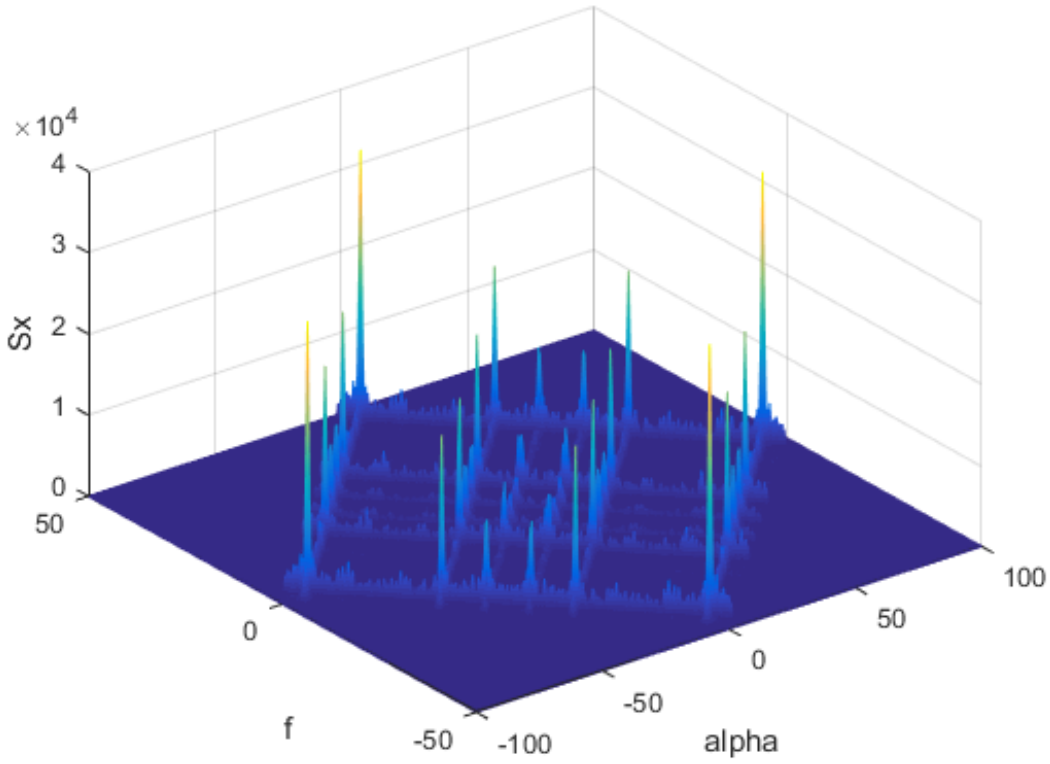


Figure 3.3: SCF of a wide-band spectrum hosting BPSK and QPSK modulated signals and a non-modulated tone signal.

3.4.2 Detection

The crest factor is used for signal detection and is equal to the peak amplitude of a waveform divided by its root mean square value. The crest factor is a dimensionless quantity. For detection, the threshold C_{TH} is first calculated when no signal is present, i.e., when $r(t) = w(t)$ in (3.1).

$$C_{TH} = \frac{max(I(\alpha))}{\sqrt{\frac{(\sum_{\alpha=0}^{N} I^2(\alpha))}{N}}} \tag{3.12}$$

Because $w(t)$ is AWGN, therefore, C_{TH} is a random value. The probability density function (PDF) of C_{TH} is estimated to obtain false alarm rate. The estimated PDF of C_{TH} can be evaluated by plotting the histogram of C_{TH}. To test the signal presence in each SB binary hypothesis testing is performed as follows:

$$\begin{aligned} H_0 &: r(t) = w(t) \\ H_1 &: r(t) = S(t) + w(t) \end{aligned} \tag{3.13}$$

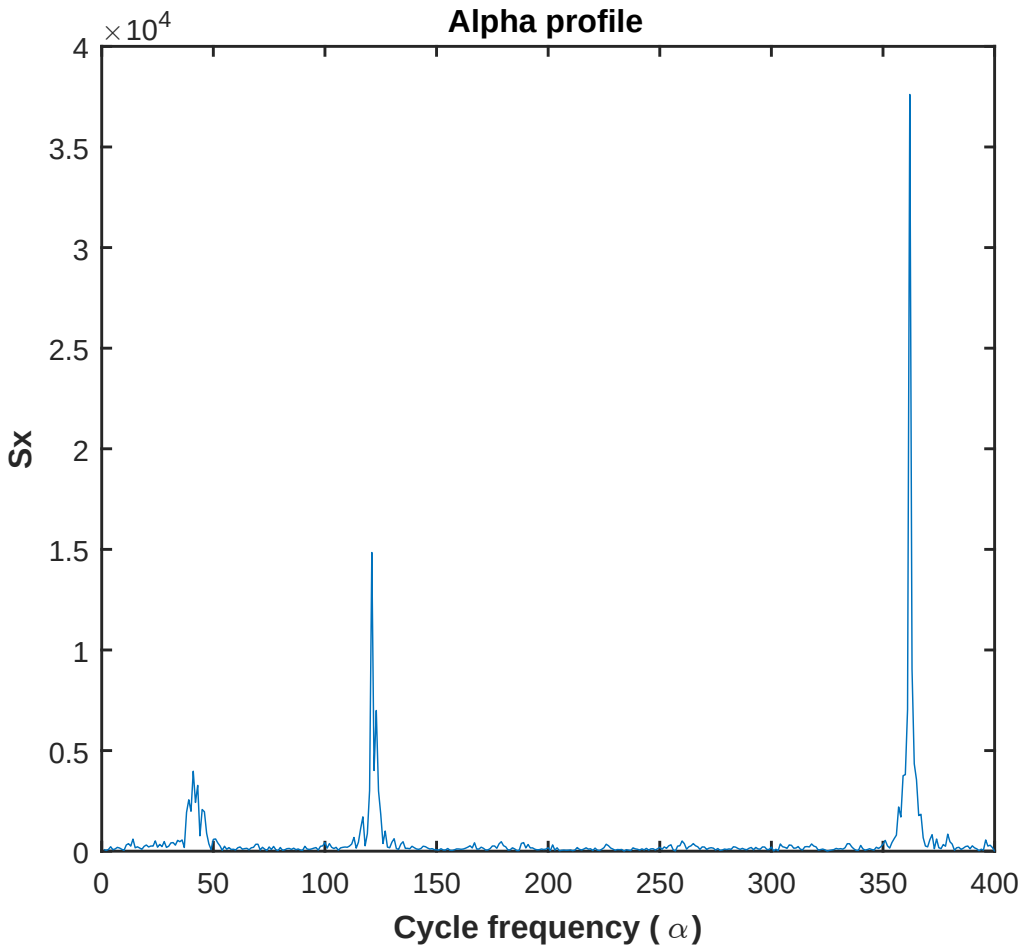


Figure 3.4: α-profile of a wide-band spectrum hosting BPSK, QPSK and a tone signal at different cyclic frequencies.

And the signal test can be performed as follows:

$$\begin{aligned} C_I \leq C_{TH} &: Declare H_0 \\ C_I > C_{TH} &: Declare H_1 \end{aligned} \tag{3.14}$$

3.4.3 Artificial Neural Network Classifier

Our proposed system uses an Artificial Neural Network (ANN) as classifier due to its ease of implementation and potential to generalize any carrier frequency, symbol rate and phase offset. The system was designed to classify signals as BPSK, QPSK, Jammer (single tone), BPSK plus Jammer and QPSK plus Jammer. We trained the ANN to identify the above five classes of signals. The SCF of WB produces a large amount of data, which makes impossible for a classifier to work on it in real time.

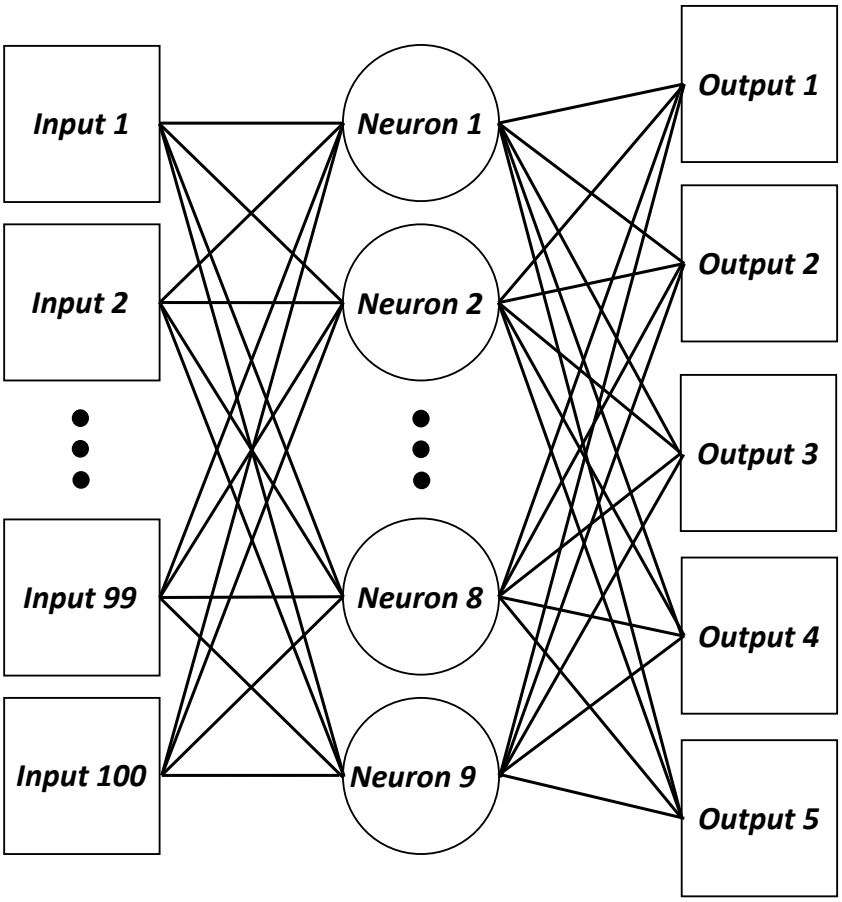


Figure 3.5: Proposed Neural Network

In order to reduce the amount of data for a classification stage, we used α and f profiles as input features for an ANN. Accordingly, the proposed ANN is composed by 100 inputs related to the concatenation of α and f profiles, a single hidden layer whose neurons use the hyperbolic tangent sigmoid as neural transfer function; and an output layer of five neurons related to each type of signal taken into account in this work. Each output value is in the range $(0, 1)$. Accordingly, the output class with the highest value between $(0, 1)$ is considered as the signal class. An ANN training based on the scale conjugate gradient propagation [69] is considered.

The selection of a single hidden layer is proposed due to the classification process simplicity of this particular problem, it was found that with a single layer results over the 90% of true positive classification were obtained for the 5 types of signal classes considered in this work. Such results indicate that considering more hidden layers would increment the training time and overall results would not be significantly

improved. According to this, in order to choose an appropriate number of neurons such that does not compromise notably the training time and guarantees robustness at repeating the training process for new ANNs, it is proposed to train multiple times 10 different architectures in which the number of neurons in the single layer is varied from 1 to 10.

A total of 100 trains are executed for each ANN architecture. For each run, weights are initialized randomly and a dataset composed by 20,000 signals is used in order to train (70%), validate (15%) and test (15%) each architecture. In order to evaluate and compare the overall performance of each architecture, the expression of equation (3.15) was taken into consideration.

$$\Psi_m = W_e(ANN_{err}^m)(std_{err}^m) + W_t(ANN_t^m)(std_t^m) \tag{3.15}$$

Where m is an indicator of the ANN architecture. ANN_{err}^m represents the normalized average error of the 100 trained ANNs for the particular architecture m. ANN_t^m is the normalized average time that an architecture m took in the training phase. std_{err}^m and std_t^m are the standard deviations of the normalized error and training time respectively for a particular ANN architecture m. W_e and W_t are global weights which indicate the impact that errors and training times have respectively in the performance expression. Both parameters are related in the following way: $W_e + W_t = 1$. Based on that, Fig. 3.6 shows the overall performance of each architecture m for high values of W_e and therefore low values of W_t. This constrain is considered in the present work in order to give more relevance to the error optimization instead of the consumed training time.

From Fig. 3.6, it is possible to observe that the architecture of 9 neurons in the hidden layer presents the best overall performance in terms of error and training time minimization. According to this, the ANN architecture of 9 neurons that presented the highest performance among the 100 trains was used for classification purposes and its results are discussed in section 3.5. The final ANN architecture used in this work is shown in Fig. 3.5.

The proposed algorithm can be summarized as follows: The receiver observes a WB signal and then computes its SCF. The α and f profiles of SCF are subsequently extracted. The WB is then divided into multiple equal length SBs. The detection is performed at every SB and a decision is made about the presence of the signal. After that, detected signals go through the classification process. The α and f profiles of detected signals are concatenated and fed to a previously trained ANN. The ANN

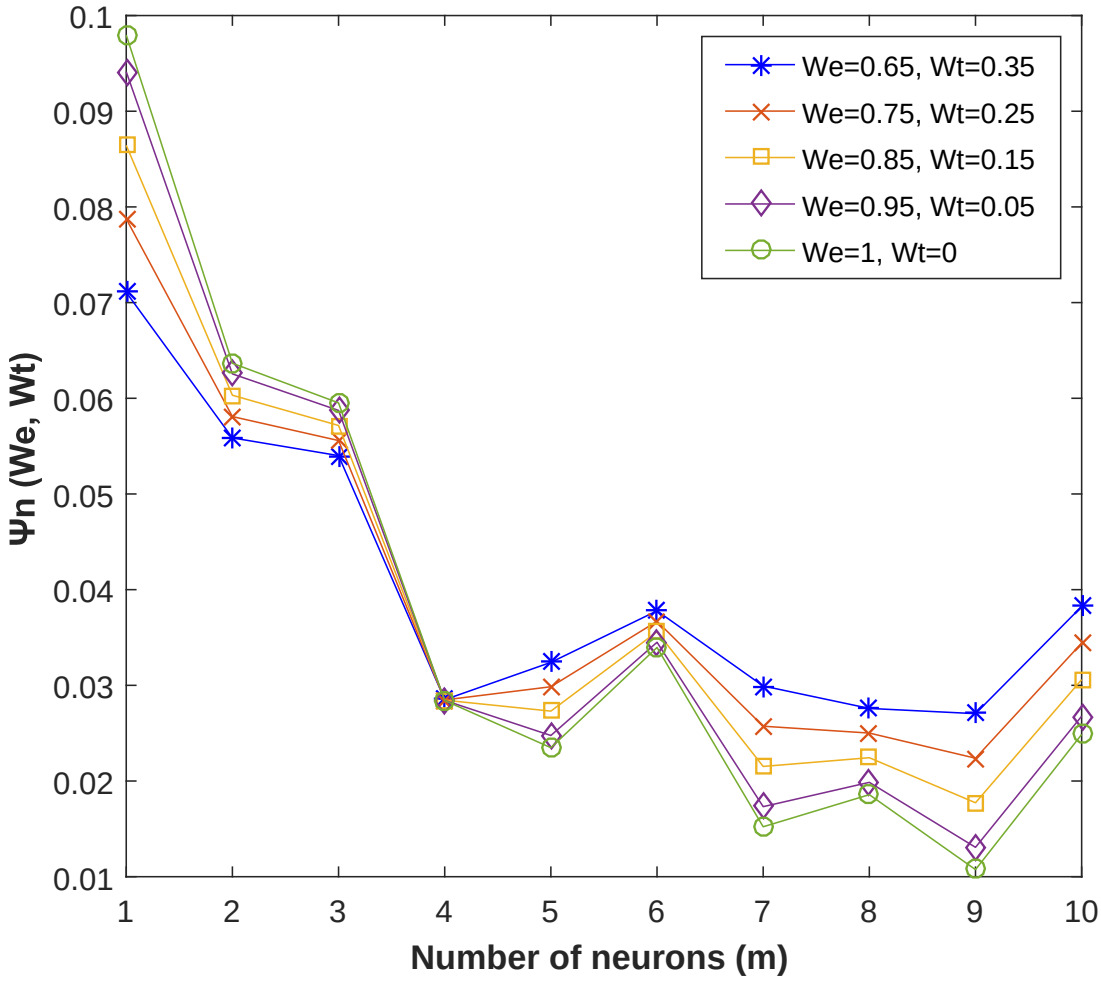


Figure 3.6: Neural Network performance for different number of neurons

classifies the received NB signal in each SB as a licit user or a jammer. The pseudo-code of the proposed algorithm is outlined in Algorithm 1.

3.5 Experimental Results and Discussion

A 50 ΔHz WB spectrum is assumed to be under observation by a CR terminal. This WB is divided into 5 SBs. These SBs can be either free or occupied by a NB signal. For testing the proposed system, we assume BPSK and QPSK signals as legitimate signals and sine wave is treated as a jamming signal. The received signals are considered to be affected by AWGN. The detection threshold C_{TH} is computed

Algorithm 1 Pseudo-code for proposed algorithm

```
function JAMMER DETECTOR
    Initialize all SB states to "free"
    Receive the WB signal
    Estimate the SCF of WB signal
    Extract the α-profile and f-profile
    Divide WB into i SBs
    for i = 1 to I, do
        Compute test statistic (C_I)
        Compute threshold (C_TH) based on desired P_f
        Compare C_TH with C_I
        Decision ← H_0 or H_1
    end for
    if H_1 then
        Concatenate α-profile and f-profile and feed to previously trained Neural Network
        Decision ← Licit or Jammer
    end if
end function
```

by fixing the false alarm rate of $P_f = 10\%$. Monte-carlo simulations are run for 1000 iterations for each signal and at each SNR.

We configure our system in three different ways: (a) we placed the BPSK signal in SB-1, QPSK in SB-5 and jamming signal in SB-2; (b) QPSK signal is in SB-5 while jamming signal jumps to SB-1 to jam the BPSK signal; and (c) BPSK signal is in SB-1 while jamming signal jumps to SB-5 to jam the QPSK signal. The sampling rate is set at Nyquist rate of 100 ΔHz. First, the α profile based detector is used to detect the signal in each sub-band. If it declares that a signal exists, then this signal goes through the signal classification stage. The detection performance is shown in Fig. 3.7.

The ANN selected based on the process described in 3.4.3, as mentioned previously, the system is trained with 20,000 signals at various SNRs and carrier frequencies so that the system performance does not depend on the knowledge of SNR and carrier frequencies. The proposed system correctly classifies all signals with a total classification rate of 0.985. In order to examine only the α-profile impact, another ANN whose inputs only depend on α-profile information was trained and tested with the same parameters explained before. The total classification rate for this case is 0.93.

The performance of both the systems is further evaluated for independent testing signals, with different carrier frequencies and SNRs (-9 dB to 9 dB) from training signals. The curves for classification accuracy vs SNR level for different signals are

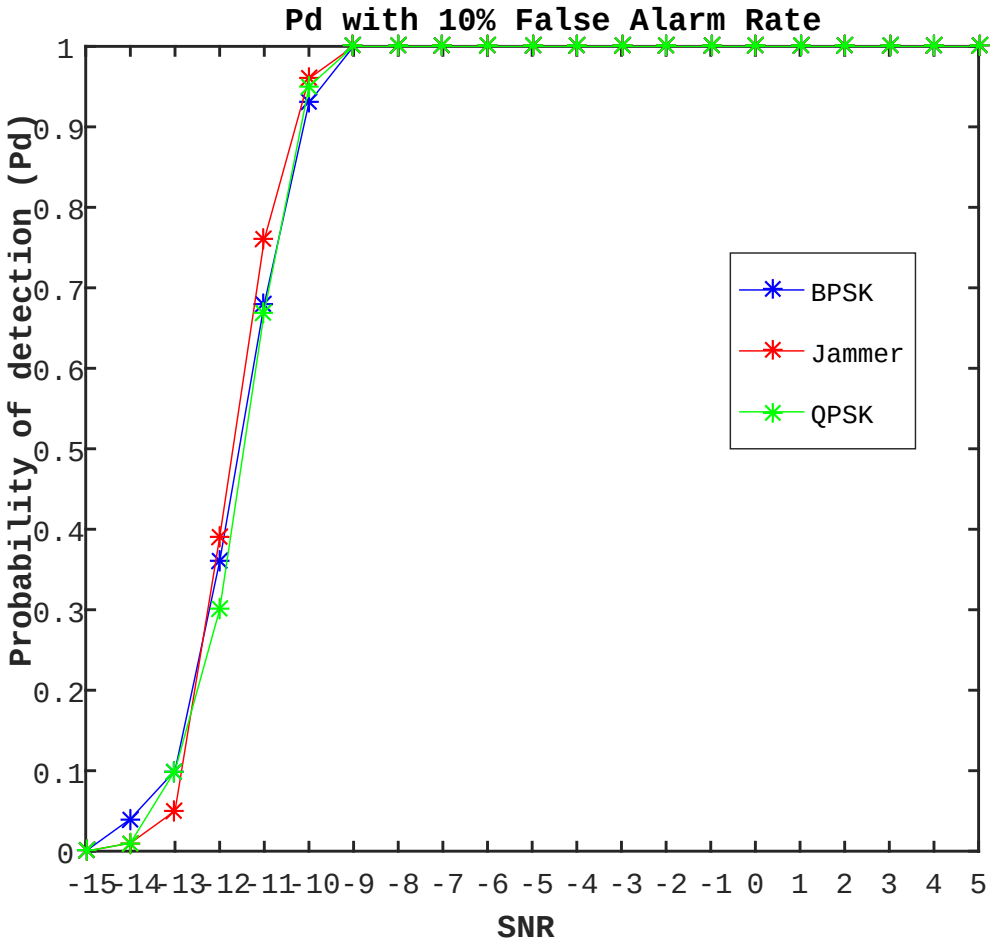


Figure 3.7: Detection probability vs. SNR with 10% false alarm rate

plotted in Fig. 3.8, where curves marked with star represent the system with α-profile as input and curves marked with circles represents the system with concatenated α and f-profiles as input features. It is possible to infer from Fig. 3.8 that by using both, the α-profile and f-profile the signal classification rate is significantly increased as compared to using only the f-profile for classification.

The overall classification accuracy for both systems is shown in Fig. 3.9. The plot shows there are approximately no errors observed above 0 dB SNR ($\alpha - f$ profiles), which shows a significant performance gain compare to common methods of signal classifications, which need 10 dB to 20 dB for comparable classification rates [71].

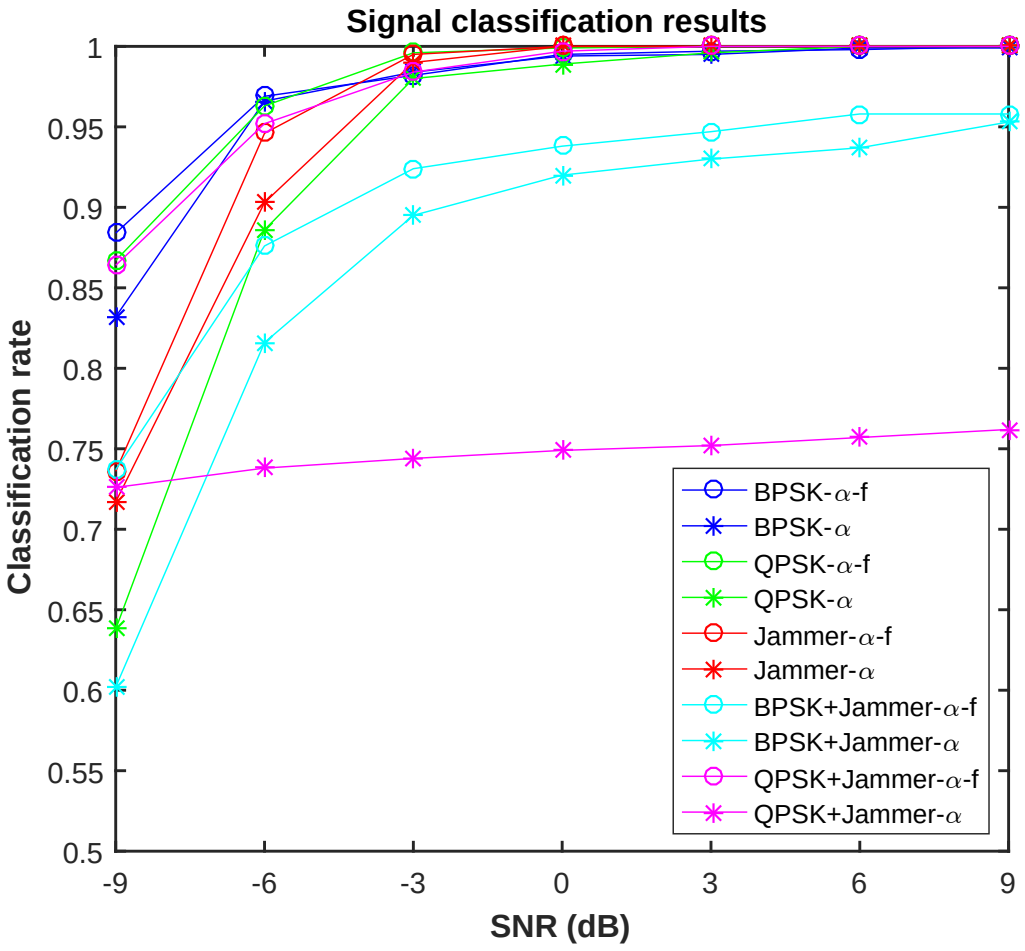


Figure 3.8: Classification results for different types of signals

3.6 Conclusion

In this chapter, we proposed a cyclic spectral analysis based on a jammer detection algorithm for WB CR networks. The WB was considered to be occupied by several NB signals with unknown carrier frequencies. These signals were assumed to be either licit signals or jamming signals. The received WB was fed to the CFD to estimate the SCF of the signal. The α and f profiles were extracted and for true positive detection of the signal, the α and f-profiles were fed to ANN which was previously trained. In the end, the classification performance for each detected signal was evaluated at different SNR values. The proposed algorithm appears to perform well at various SNR values down to -3 dB. Since the spectral correlation function of different signals are highly different, it appears to be a very effective parameter to use in classification.

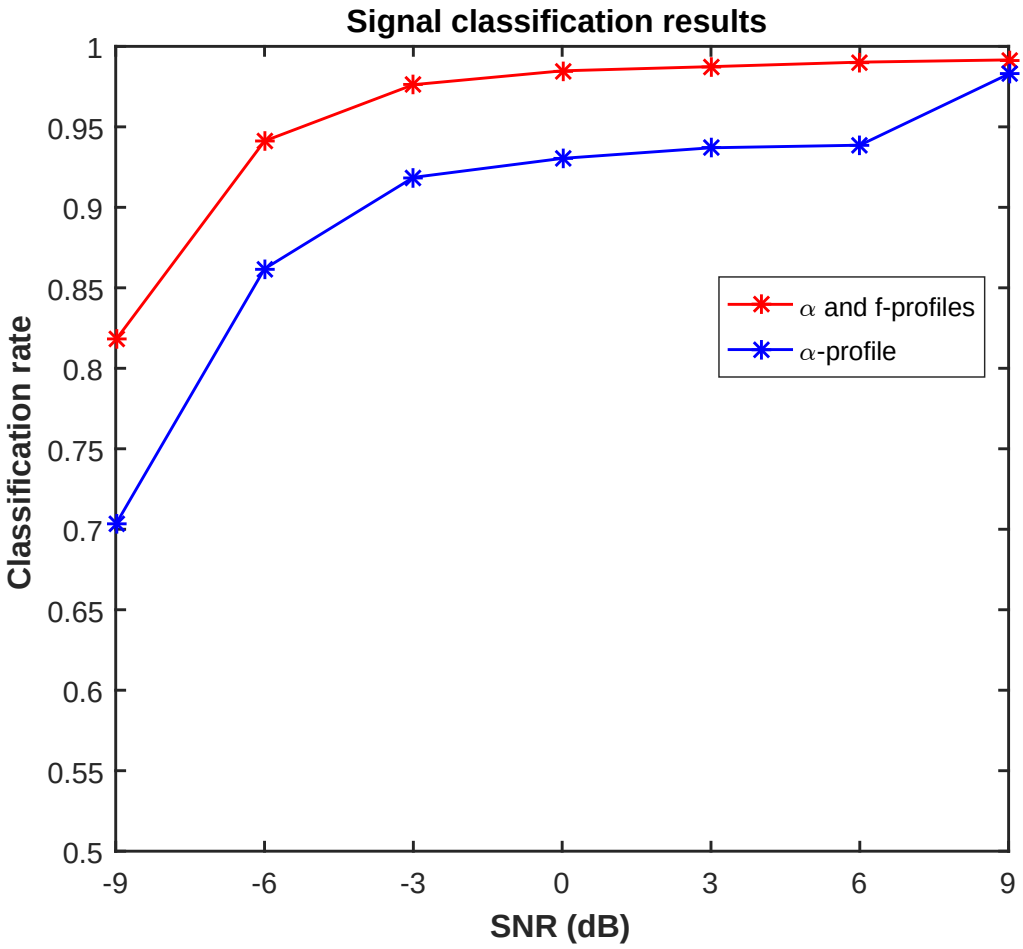


Figure 3.9: Overall classification results

The ability of CR to accurately and reliably identify different types of signals (legitimate or illegitimate) can significantly increase the anti-jamming performance of the system. The knowledge about band occupied by jammer and its type (modulated or tone) can be used to avoid the bands frequently jammed and to design an efficient anti-jamming system against such attacks.

Chapter 4

Spectrum characterization for Stealthy Jamming Attacks in Wideband Radios

4.1 Introduction

This chapter presents a new physical layer approach for stealthy jammer detection in wide-band (WB) cognitive radio networks. Stealthy jammer is an adaptive reactive jammer with same capabilities as a CR user. These type of jammers only transmit when a legitimate transmission is detected and stop transmitting when the legitimate transmission stops. Therefore, the jamming activities of such jammers are hard to detect by the popular sensing approaches such as ED at physical layer . Hence, we presented in this chapter a novel cyclostationary feature detector based approach to detect such types of jammers at physical layer. The proposed algorithm consider a WB consists of multiple narrow-band sub-bands (SB), which can be occupied by licit or jamming signals . The cyclostationary spectral analysis is performed on this WB signal to compute spectral correlation function (SCF). The alpha profile is extracted from the SCF and used as input features to artificial neural network (ANN), which classify each NB signal as a licit signal or a jamming signal. In the end, the performance of the proposed approach is shown with the help of Monte-Carlo simulations under different empirical setups.

The rest of the chapter is organized as follows. Section 4.2 presents the background in detailed, Section 4.3 describes the system model and problem formulation, Section 4.4 presents the proposed algorithm. Experimental results are discussed in section 4.5. In Section 4.6, chapter is concluded.

4.2 Background

Cognitive radio (CR) is known as a promising technology to solve the problems of scarcity and inefficient utilization of radio spectrum, due to its ability of allowing dynamic/opportunistic spectrum access in spectrum sparse environment [68], [47]. A CR dynamically interacts with its environment and adjust its driving parameters in order to exploit the white spaces without affecting the primary user activity. In order to obtain the information about spectrum holes, CR needs to perform Spectrum sensing and different spectrum sensing techniques such as energy detection (ED), cyclostationary feature detection (CFD) and matched filtering (MF) [116] have been largely under investigation. Among these, CFD has the ability to detect primary signals from interference and noise even in low signal to noise ratios (SNRs) conditions, on the other hand MF needs a dedicated receiver structure which may not be possible in a practical CR terminal while ED fails at low SNRs. CFD exploits the cyclostationarity features of the communication signals by detecting spectral peaks in spectral correlation function (SCF) or spectral coherence function (SOF) [45, 96]. Furthermore, the cyclic spectral analysis has been used as a robust mechanism for signal classification when the carrier frequency and bandwidth information is not available [35, 61].

While CR technology is introduced as a solution for dynamic spectrum access (DSA), it has brought serious threats to network security due to its ability of sensing and exploring a wide range frequencies and opportunistic usage. Due to these capabilities, it is easier for the attackers to launch sophisticated attacks in such networks. For example, the malicious user may claim to be a primary user, and carry out the primary user emulation (PUE) attacks [15]. The attackers can also examine the spectrum themselves, and conduct smart jamming [107, 83]. A common property of these jamming attacks is that they cause anomalous spectrum usage and disrupt the dynamic spectrum access, thus known as Anomalous Spectrum Usage Attacks (ASUAs) in the context of cognitive radio networks [88] .

PUE attacks have been studied extensively [15], we assume anomalous spectrum users attack such as stealthy jamming attacks. Stealthy jammer is considered as an adaptive reactive jammer with same capabilities as CR user, due to its stealthy nature it only starts jamming after a legitimate transmission is detected, and will stop jamming as soon as the legitimate transmission stops. As a result, the jamming activities of such jammers are hard to detect by the popular spectrum sensing approaches such as ED at physical layer. In [88], a cross layer approach is considered

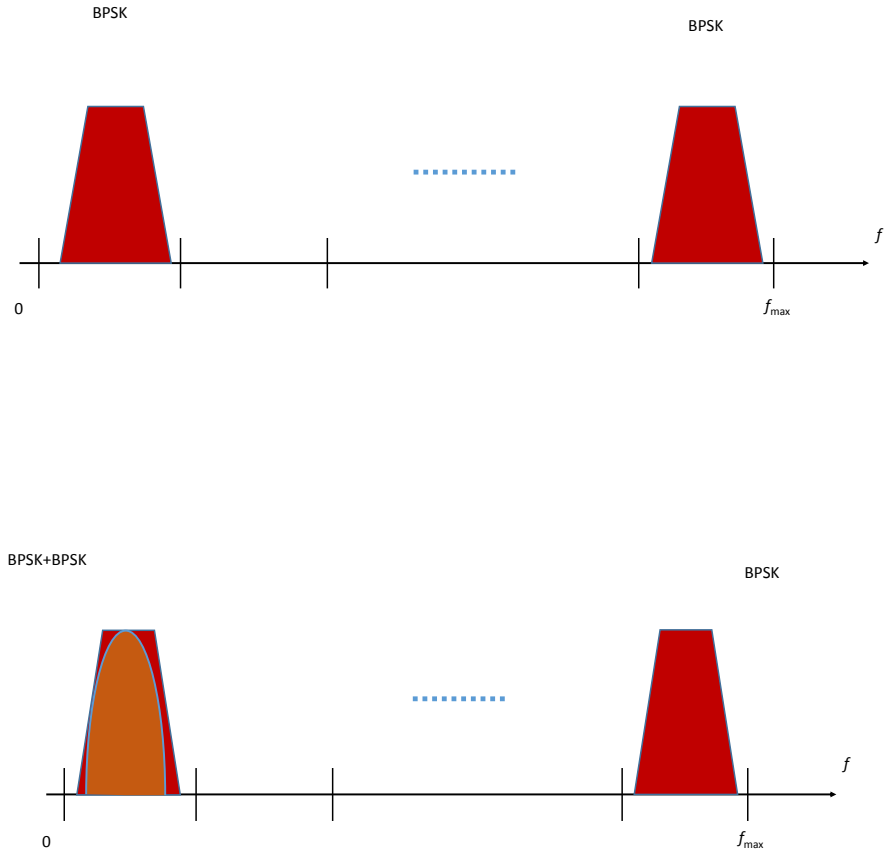


Figure 4.1: (a)Wide-band spectrum divided into multiple sub-bands (SB) and each SB is occupied by a narrow-band signal or free (b) Narrow-band stealthy jammer (BPSK) jumps to the SB1 to jam licit (BPSK) signal

to detect the stealthy jammer. In most of the previous work, that assumed physical layer jamming attacks assume either additive white Gaussian noise (AWGN) jamming [84] or tone jamming . In [2] and [3], the authors explore modulation based jamming attacks and have shown that these modulated jamming tactics can lead to optimum jamming in power constrained environment. In our work, we consider an adaptive stealthy jammer, which can adapt to different modulation schemes in order to exploit optimum jamming strategy against victim signal. Therefore, in order to design the proper anti-jamming system against these stealthy jamming attacks, there is a need for a reliable jammer detection algorithm.

In this chapter, a new physical layer based algorithm is proposed to detect stealthy

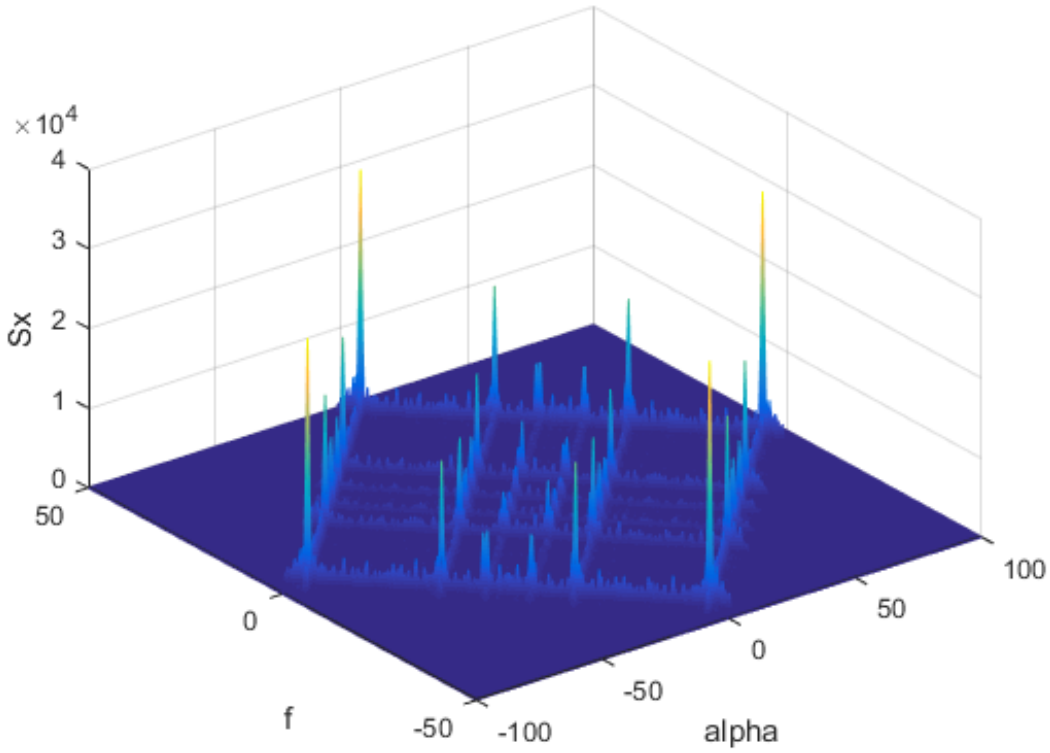


Figure 4.2: SCF of a wide-band spectrum hosting a BPSK and a QPSK modulated signals.

jamming attacks in WB CRs. A WB spectrum is considered to be composed of multiple sub-bands, each one of which can be occupied by narrow-band (NB) signal or free. These NB signals can be licit or stealthy jamming signal. The first step of the algorithm is to compute the SCF of the WB spectrum. Then the cyclic frequency profile (α-profile) is extracted from SCF and used as input features for an artificial neural network (ANN) based classifier. Based on an ANN classifier, each of the NB signal is classified either as a licit signal of stealthy jamming signal. Finally, the performance of the algorithm is evaluated for various SNRs to observe the effects on classification performance.

4.3 System Model and Problem Formulation

We consider that a Δ Hz of WB spectrum in the frequency range $\{0, f_{max}\}$ is under the observation of CR terminal. The WB spectrum can be occupied by various NB signals $S_l(t)$, $l \in \{1, 2, 3.....N\}$, with different carrier frequencies and modulation

Table 4.1: Optimal jamming signals in a coherent scenario

Victim Signal	Modulation scheme of pulsed jamming signal
BPSK	BPSK
QPSK	QPSK
4-PAM	BPSK
16-QAM	QPSK

types. The received WB signal is an aggregated time-domain signal which can be presented as:

$$y(t) = \sum_{l=1}^{N} h_l(t) * S_l(t) + w(t) \tag{4.1}$$

here $S_l(t)$ denotes the *l-th* transmitted signal, $h_l(t)$ is the channel response between *l-th* transmitter and receiver, * denotes the convolution operation and $w(t)$ is the additive white Gaussian noise (AWGN) with zero mean and power spectral density σ_w^2 . These NB signals can be generated by different types of modulation schemes, such as, binary phase shift keying (BPSK), quadrature amplitude modulation (QAM), quadrature phase shift keying (QPSK), binary frequency shift keying (BFSK), binary phase shift keying (BPSK), quadrature amplitude modulation (QAM), or any other modulation scheme as shown in Fig. 4.1. Moreover, we assume that the transmitter can change its modulation schemes. The received WB at CR terminal is divided into multiple equal bandwidth SBs and each of these SBs can be occupied by NB signals with no spill over energy into neighboring SBs.

For our system, we consider a stealthy jammer with the same capabilities as a CR user. This jammer is equipped with CFD and can adapt to different modulation schemes in order to use optimal jamming tactic against target signal. The modulated jamming attacks are very successful for power constrained jamming in order to maximize the error probability of digital modulated legitimate signals. The optimal jamming signals against targeted digital amplitude-phase modulated signals is in Tab. 4.1 [3].

4.4 Proposed Algorithm

This section illustrates the proposed algorithm as a solution to the problem described in Section 4.3. We first introduce cyclostationary spectral analysis, then neural networks and eventually we will present our newly proposed algorithm.

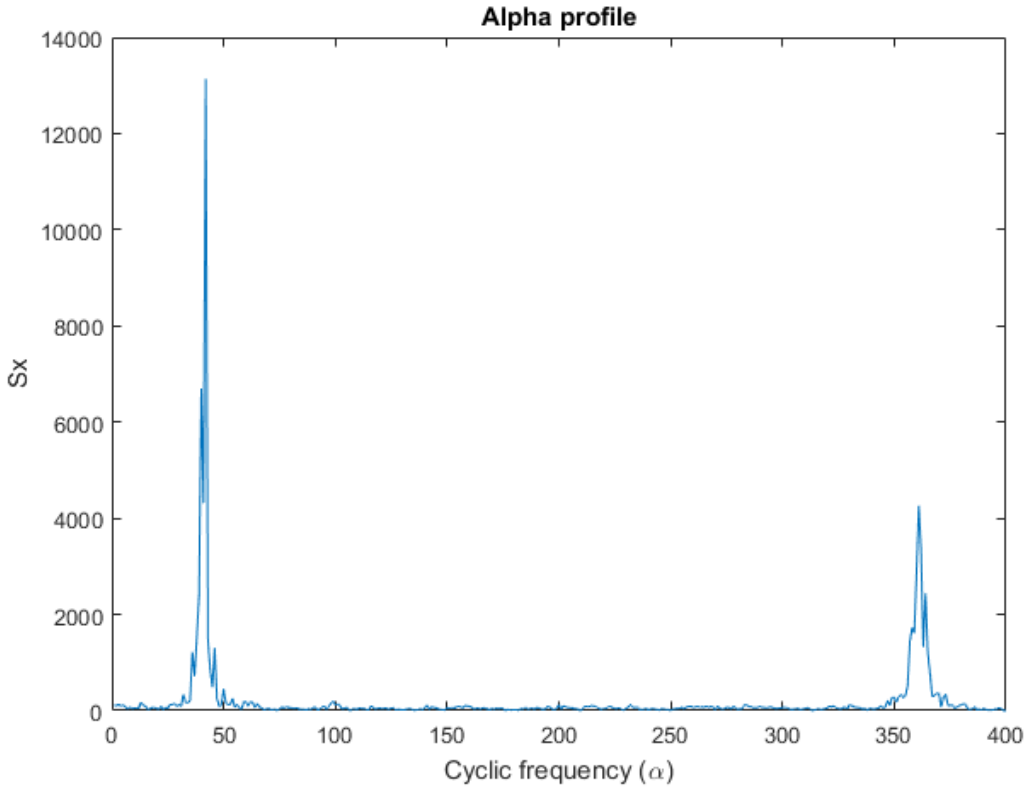


Figure 4.3: α-profile of a wide-band spectrum hosting a BPSK and a QPSK modulated signal at different cyclic frequencies.

4.4.1 Cyclostationary Spectral Analysis

A process $x(t)$ is said to be wide-sense cyclostationary with period T_0 if its mean $E[x(t)] = \mu_x(t)$ and autocorrelation $E[x(t)x(t+\tau)] = R_x(t,\tau)$ are both periodic with period T_0, in such case, they can be defined respectively as:

$$M_x(t+T_0) = M_x(t) \quad ; \quad R_s(t+T_0,\tau) = R_x(t,\tau) \tag{4.2}$$

The cyclic autocorrelation function (CAF) of a wide-sense cyclostationary process can be given as follow:

$$R_x^{\alpha}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} R_x(t,\tau) e^{-j2\pi\alpha t} dt \tag{4.3}$$

The cyclic Wiener relation states that spectral correlation function (SCF) can be obtained from the Fourier transform of the cyclic autocorrelation function in (3) is known as SCF and is given by:

$$S_x^{\alpha}(f) = \int_{-\infty}^{\infty} R_x^{\alpha}(\tau) e^{-j2\pi f\tau} d\tau \tag{4.4}$$

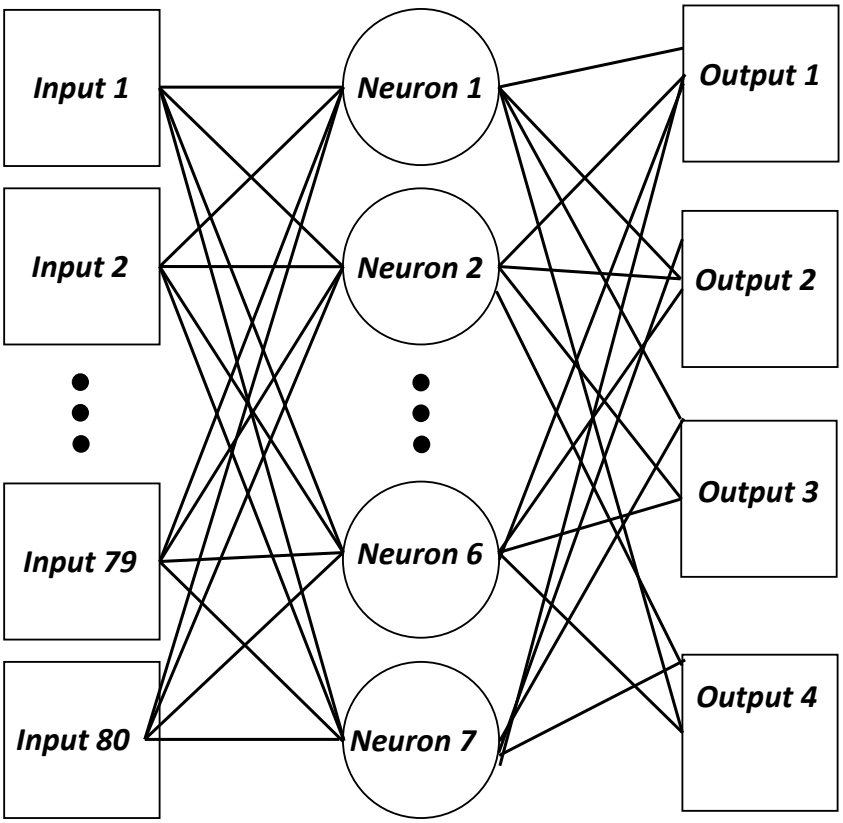


Figure 4.4: Proposed Neural Network

Where α is cyclic frequency and f is the angular frequency. The major benefit of spectral correlation is its insensitivity to background noises, since the spectral components of noise are completely uncorrelated in time due to the fact that noise is wide-sense stationary process, such noise does not play significant role in the SCF. The SCF of the WB signal is shown in Fig. 4.2. The, α profile is extracted from SCF, which is given by (4.5) and depicted in Fig. 4.3.

$$I(\alpha) = max_f[S_X^\alpha] \tag{4.5}$$

4.4.2 Artificial Neural Network Classifier

Our considered system uses an Artificial Neural Network (ANN) as a classifier due to its success for pattern recognition applications. The system is designed to identify the four signal classes BPSK, QPSK, BPSK plus BPSK, QPSK plus QPSK. We trained the ANN to classify the above four classes of signals. The SCF of WB spectrum produces a large amount of data, therefore, α profile is extracted from the SCF and used as input features for an ANN. Accordingly, the considered ANN is composed by 80 inputs related to α profile, a single hidden layer whose neurons use the hyperbolic tangent sigmoid as neural transfer function; and an output layer of four neurons related to each class of signal taken into account in this work. The output value is in range (0,1). Accordingly, the output class with highest value between (0,1) is considered as the signal type. An ANN training based on the scale conjugate gradient propagation [69] is considered in this work.

A single hidden layer is proposed due to the simplicity of the classification process for this particular problem, it was found that with single hidden layer results over 90% of true positive classification were obtained for the four types of signal classes considered in this work. These results show that considering more hidden layers would increase the training time and overall results would not be significantly improved. In order to choose an appropriate number of neurons such that does not compromise training timing and guarantees robustness for ANN, it is proposed to train multiple times 10 different architectures in which the number of neurons in single hidden layer is varied from 1 to 10.

For each ANN architecture, a total of 100 trains are executed and for each run, weights are initialized randomly. A dataset composed by 36,000 signals is used in order to train (70%), validate (15%) and test (15%) each architecture. The performance of each architecture is evaluated using equation (4.6).

$$\Psi_n = W_e(ANN_{er}^n)(std_{er}^n) + W_t(ANN_t^n)(std_t^n) \tag{4.6}$$

Here n is an indicator of the ANN architecture. W_e and W_t are global weights which represent the impact that errors and training times have respectively. These two parameters are related in the following way: $W_e + W_t = 1$. ANN_{er}^n and ANN_t^n represent the normalized average error and normalized average training time for the particular architecture n consecutively. std_{error}^n and std_{time}^n are the standard deviations of the normalized error and training time respectively for a particular ANN architecture n. In (4.6) high weight is given to W_e as compare to W_t to optimize error rather the

consumed training time. According, to this, the ANN architecture of 7 neurons that presented the highest performance among 100 trains was used for classification. The final ANN architecture used in this work is shown in Fig. 4.4.

Algorithm 2 Pseudo-code for proposed algorithm

```
function STEALTHY JAMMER DETECTOR
    Initialise all SB states to "free"
    Receive the WB signal
    Estimate the SCF of the WB signal
    Extract the α profile from SCF
    Divide WB into i SBs
    for i = 1 to I, do
        Feed the corresponding α profile to previously trained Neural Network
        Decision ← Licit or Stealthy Jammer
    end for
end function
```

The proposed algorithm can be summarized as follows: A WB spectrum is received at CR terminal. The SCF of WB is computed and the α profile is then extracted from SCF. The WB is divided into multiple equal length SBs. The α of the corresponding SB is fed to a previously trained ANN. The ANN classifies the received NB signal in each SB as legitimate user or a stealthy jammer. The pseudo-code of the proposed algorithm is outlined in Algorithm 2.

4.5 Experimental Results and Discussion

We assumed a 500 ΔHz WB spectrum received by CR terminal. Th WB is consisted of 5 SBs. Each of the SBs can be either free or occupied by NB signal. We consider BPSK and QPSK as licit signals. The transmitter can choose either modulation scheme with probability of 0.5. Similarly, the jammer can choose optimum jamming strategy against legitimate waveform from Tab. 4.1, i-e BPSK against BPSK and QPSK against QPSK. However, the jammer can jam one band at a time. The received signals are considered to be affected by AWGN. We configure the system in such a way that SB-1 and SB-4 are occupied by BPSK signals.The sampling rate is set at Nyquist rate of 1000 ΔHz.

In this work, the system is trained with 36,000 signals at various SNRs so that performance does not depend on the knowledge of SNR. The proposed ANN based classifier correctly classifies all signals with a total classification rate of 0.99.

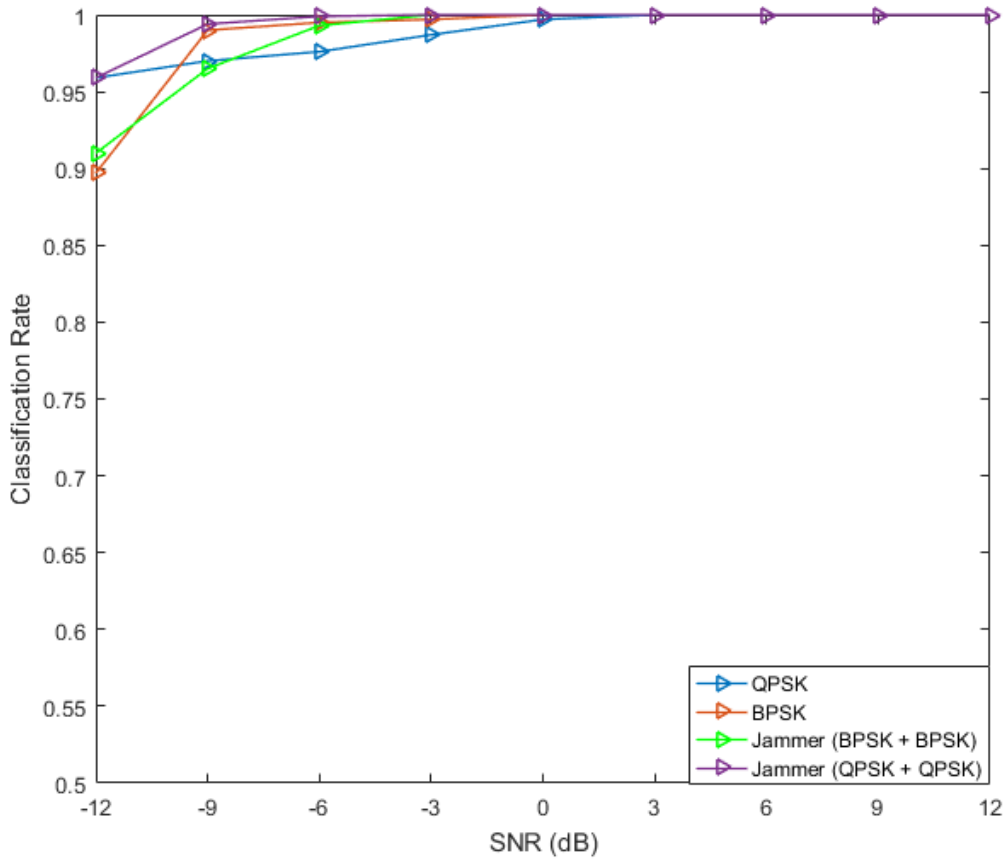


Figure 4.5: Classification results for different types of signals .

The performance of the proposed system is further evaluated for independent testing signals, with different SNRs (-12 dB to 12 dB) from training signals. The Fig. 4.5 shows the classification rate vs SNR level for different types of signals. It is easy to infer from Fig. 4.5 that the proposed algorithm not only correctly classifies both jamming classes but also successfully classifies legitimate signals. The overall classification accuracy for proposed system is shown in Fig. 4.6. The figure shows there are approximately no errors observed above -6 dB. The proposed algorithm shows a significant performance gain compare to common techniques, which need 10 dB to 20 dB for comparable classification rates [71].

4.6 Conclusion

In this work, we presented a novel physical layer based approach for stealthy jammer detection in WB cognitive radios. The WB was consisted of multiple SBs, which

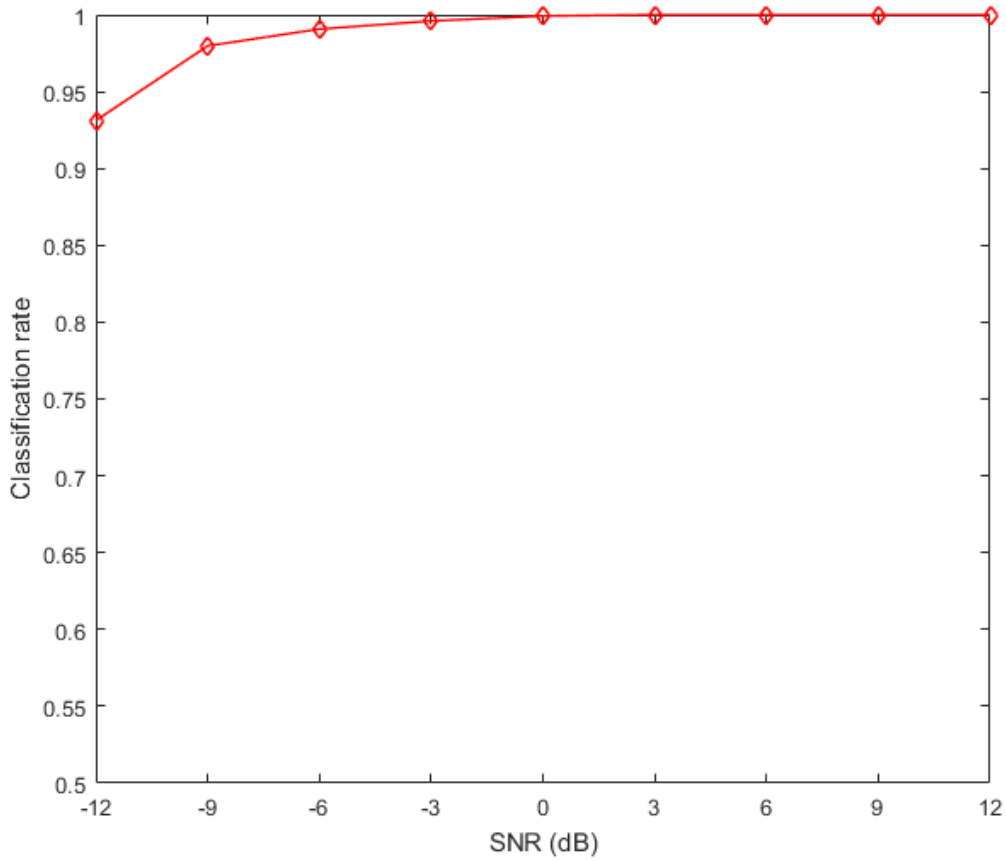


Figure 4.6: Overall classification results .

were occupied by several NB signals with known carrier frequencies and symbol time. The NB signals were assumed to legitimate or jamming signals. The receive WB spectrum was fed to the CFD to estimate the SCF of the signal. The α profile was extracted from SCF and fed to previously trained ANN. The ANN classify the signals to be legitimate or jamming. In the end, the performance of proposed algorithm was evaluated at different SNR values. The algorithm appears to perform well at various SNR values down to -12 dB.

Chapter 5

Spectrum Characterization using Compressed Sensing for Wide-band Radios

A new algorithm for interference / jammer detection is proposed in this chapter for wide-band (WB) cognitive radio (CR) networks. First, the scanned WB spectrum, which is comprised of multiple narrow-band (NB) signals, is recovered from sub-Nyquist rate samples using compressed sensing. Compressed sensing allows us to alleviate Nyquist rate sampling requirements at the receiver analog-to-digital converter (ADC). After the Nyquist rate signal has been recovered, a cyclostationary feature detector is employed on this estimated signal to compute the cyclic features. Finally, the proposed algorithm uses the second order statistics, namely, the spectral correlation function (SCF), to classify each NB signal as a legitimate signal or an interfering / jamming signal. In the end, performance of the proposed algorithm is shown with the help of Monte-Carlo simulations under different empirical setups.

The rest of the chapter is organized as follows. Section 5.1 introduces the different state-of-the-art used in this chapter. Section 5.2 describes the system model and problem formulation. Section 5.3 outlines the spectral correlation function (SCF) overview and proposed algorithm. Experimental results for different types of jamming attacks are discussed in section 5.4, 5.5 and 5.6. Finally, the chapter is concluded in Section 5.7 along with some future directions.

5.1 Introduction

Over the last few years, cognitive radios [68], [47] have plucked much attention from wireless communication community due to its applications for Dynamic / Oppor-

tunistic spectrum access (DSA / OSA). Cognitive radio is an intelligent device which is aware of its spectrum environment and changes its parameters accordingly for the purpose of DSA / OSA. In order to attain spectrum awareness, reliable spectrum sensing is an important primary task for the cognitive radios and methods such as energy detection (ED), cyclostationary feature detection (CFD) and matched filtering (MF) [1] have been largely under investigation.

Among these methods, CFD [41], [42] exhibits good performance with acceptable implementation complexity at medium to low signal-to-noise ratios (SNR). Specifically speaking, ED fails at low SNRs while MF requires dedicated receiver structure which may not be possible in a practical cognitive radio terminal. CFDs utilize the cyclostationarity of the modulated signals by detecting spectral peaks in the spectral correlation function (SCF) [44], which is sparse in both angular and cyclic frequency domain. Furthermore, CFD can differentiate among different modulated signals, interfering signals and noise by using the cyclostationary spectral correlation features.

When the radios are operating on a wide-band (WB), the task of signal estimation becomes complex due to high rate ADC requirements. Compressed sensing [30] is an appealing solution to alleviate requirements of high sampling rates provided that the signal is sparse in some given transform domain. Then, CFD requires to estimate the SCF of the received WB spectrum from sub-Nyquist samples. One approach, which appeared in [18], is to first recover the Nyquist samples from sub-Nyquist samples, then estimate the SCF and perform feature detection. For Nyquist samples recovery, [18] used the modulated wideband converter (MWC) [66]. On the other hand, in the very first papers [100, 103], authors performed the SCF estimation directly from sub-Nyquist samples by exploiting the sparsity structure in two-dimensional SCF domain.

Radio frequency (RF) jamming is a conventional method of disrupting the communication of the targeted system. Recent advances in cognitive radio technology enabled devising self-reconfigurable and advanced jamming and anti-jamming solutions [22, 23]. An anti-jamming system based on the cognitive radio technology may use the spectrum sensing information to detect potential interfering or jamming entities [72], and take proactive measures to ensure communication continuity. Furthermore, it may collect a history of the observations, and use it to devise anti-jamming tactics with even higher probability of success. For example, in case of a frequency hopping system, the cognitive radio may modify its hopping pattern to avoid the channels which are frequently occupied by the potential interfering / jamming entities [91]. In order to do so, there is a need for a reliable interference / jammer detection algorithm.

In this work, we introduce a new interference / jammer detection algorithm which exploits the cyclic features of the modulated narrow-band (NB) signals in a WB spectrum. The first step of the algorithm is to recover the Nyquist rate WB spectrum, which is assumed to be occupied by various NB signals, from sub-Nyquist samples using compressed sensing. To achieve this, we use the conventional basis pursuit (BP) technique [16]. The recovered signal is then fed to the CFD to estimate the SCF of the recovered signal. The peaks in the SCF are then compared with the corresponding values of the legitimate signals' SCF, which are stored in a database. Based on this comparison, each of the detected signals is classified either as a licit signal or a jamming signal. Main advantage of using CFD based detector lies in its well known ability to perform better than ED at low SNR values. Finally, performance of the proposed algorithm is evaluated for various compression ratios at low SNR to observe the effects of various parameters on classification performance. To the best of our knowledge, this kind of jammer detection algorithm has not been introduced so far in the open literature.

5.2 System Model and Problem Formulation

In the context of cognitive radio, we focus on the processing of a received WB spectrum of Δ Hz. We assume that this WB signal can be occupied by various NB signals $s_m(t)$, $m \in \{1, 2, ..., M\}$, with known carrier frequencies, symbol periods and modulation types that we want to identify. The receiver observes an aggregated time-domain signal which can be expressed as

$$r(t) = \sum_{m=1}^{M} h_m(t) * s_m(t) + w(t) \tag{5.1}$$

where $h_m(t)$ is the channel coefficient between m-th transmitter and receiver, $*$ denotes the convolution operation and $w(t)$ is the AWGN with zero mean and power spectral density σ_w^2. We consider that these NB signals can have different modulation schemes, such as, binary phase shift keying (BPSK), binary frequency shift keying (BFSK), quadrature phase shift keying (QPSK), or any other modulation as shown in Fig. 5.1 (a). The WB is sliced into multiple SBs of equal bandwidths and each of these NB signals can occupy one SB with no spill-over energy into the neighboring SBs.

For our system, we consider three different types of jammers, namely; tone [78], modulated [80], and stealthy jammers [79] . The former two jammers can jam any of

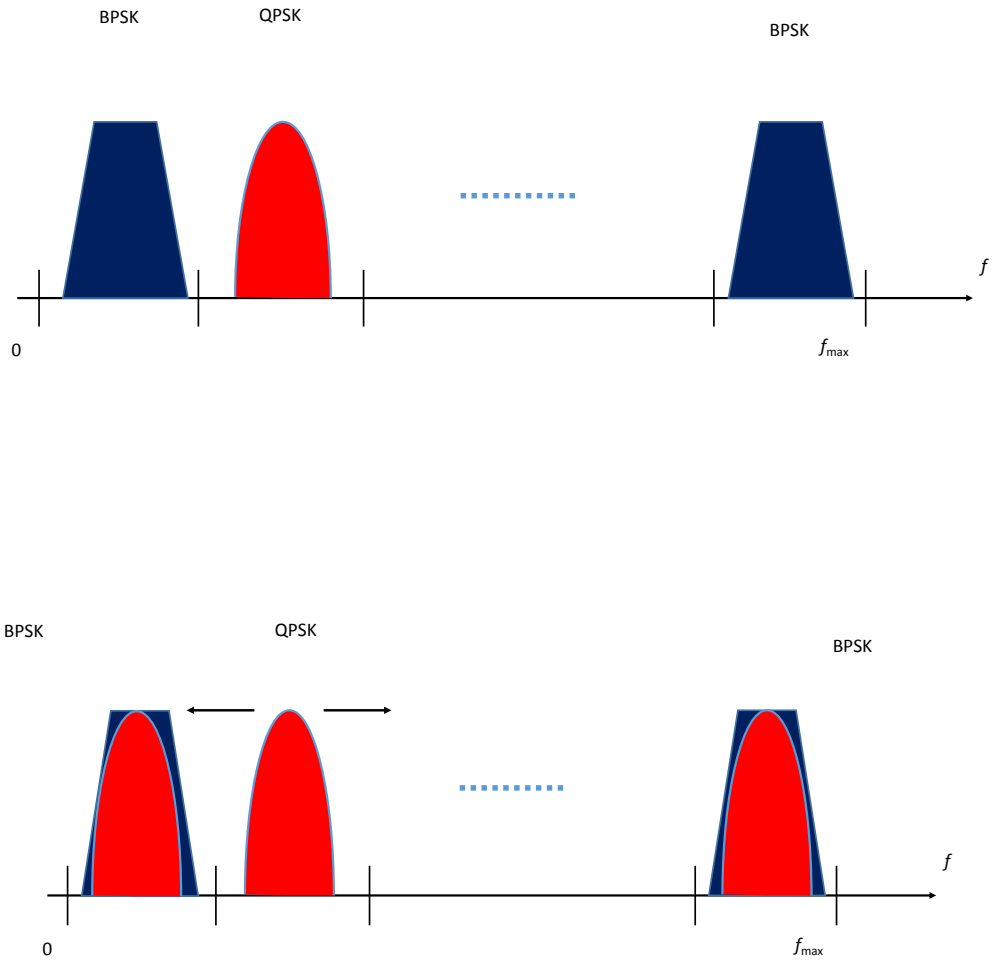


Figure 5.1: (a) Wide-band spectrum divided into multiple sub-bands (SB) and each SB is occupied by a narrow-band signal. (b) Narrow-band jammer (QPSK) jumps to the neighboring SB to jam licit (BPSK) signal.

the SBs, either free or occupied, if it has higher power than the legitimate signal as shown in Fig. 5.1 (b). However, the later stealthy jammer is a reactive and adaptive jammer. This type of jammers only transmit when there is ongoing transmission on channel [79]. When the modulated jammer is in free SB, it can be considered as a primary user emulation (PUE) attack. Let us assume that the targeted signals are uncoded BPSK and QPSK and the targeted receiver implements coherent detection, the error probability P_e to jam BPSK or to either jam the in-phase component (I)

or quadrature component (Q) of the targeted QPSK signal can be calculated as [20]:

$$\begin{aligned} \mathrm{P_e}^{I} &= Q\left(\sqrt{2\frac{\sigma_R}{\sigma_N}}\left(1-\sqrt{\frac{2\sigma_J}{\sigma_R}sin(\theta^J)}\right)\right) \\ \mathrm{P_e}^{Q} &= Q\left(\sqrt{2\frac{\sigma_R}{\sigma_N}}\left(1+\sqrt{\frac{2\sigma_J}{\sigma_R}cos(\theta^J)}\right)\right) \end{aligned} \tag{5.2}$$

where σ_R is the received power of the targeted signal, σ_N is the thermal noise power, σ_J is the received power of the jamming signal, θ^J is the phase of the jamming signal, and Q represents the Gaussian Q-function. For simplicity of analysis, we assume that $\sigma_J >> \sigma_R$, resulting in $\mathrm{P_e} \approx 100\%$ whenever the jammer transmits on the same channel as the targeted transmitter-receiver pair.

5.3 Proposed Algorithm

In this section, we first introduce some background on the SCF. After that, we explain the preliminaries of compressed sensing conforming to [119, 74] and present our proposed algorithm.

5.3.1 Spectral Correlation Function Overview

A random process $s(t)$ is said to be wide sense cyclostationary with period T_0 if its mean $E[s(t)] = \mu_s(t)$ and autocorrelation $E[s(t)s(t+\tau)] = R_s(t,\tau)$ are both periodic with the period T_0, i.e.,

$$\mu_s(t+T_0) = \mu_s(t), \qquad R_s(t+T_0,\tau) = R_s(t,\tau). \tag{5.3}$$

The autocorrelation of a wide-sense cyclostationary random process can be expanded in a Fourier series as follows:

$$R_s(t,\tau) = \sum_{\alpha} R_s^{\alpha}(\tau)e^{j2\pi\alpha t}, \tag{5.4}$$

where $\alpha = a/T_0$ and a is an integer. The Fourier coefficients, i.e., the cyclic autocorrelation functions are given as

$$R_s^{\alpha}(\tau) = \frac{1}{T}\int_{-\infty}^{\infty} R_s(t,\tau)e^{-j2\pi\alpha t}dt. \tag{5.5}$$

Taking the Fourier transform of above, the SCF is obtained as follows:

$$S_s(f,\alpha) = \int_{-\infty}^{\infty} R_s^{\alpha}(\tau)e^{-j2\pi f\tau}d\tau, \tag{5.6}$$

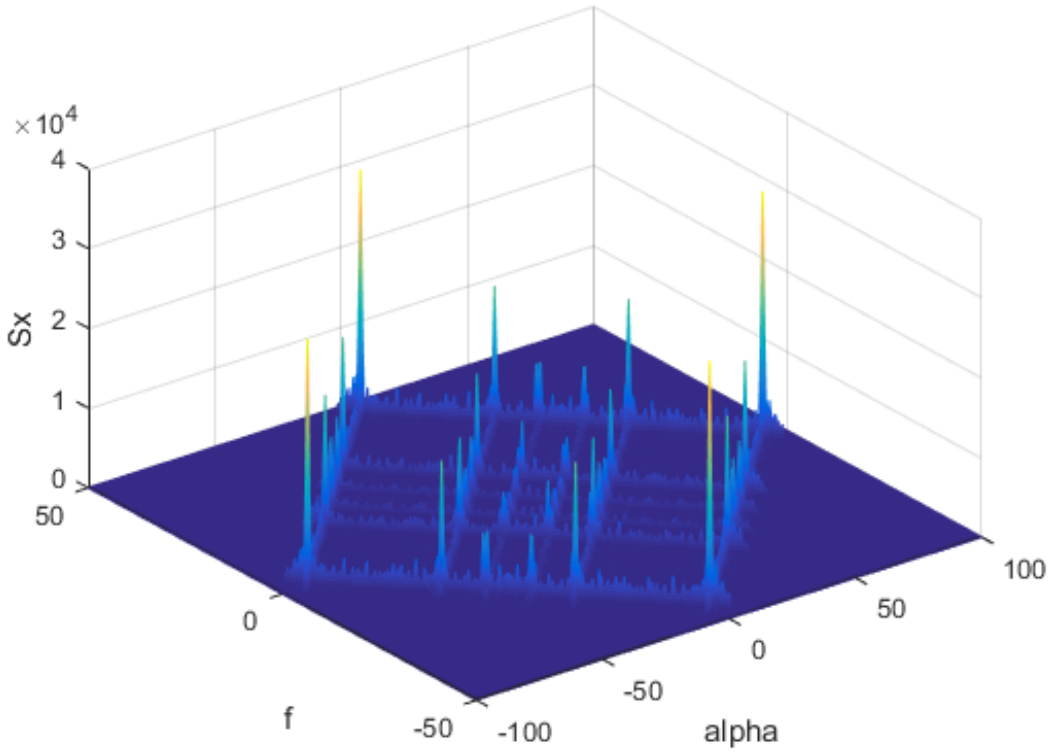


Figure 5.2: SCF of a wide-band spectrum hosting two BPSK signals and a QPSK modulated jamming signal.

where α is the cyclic frequency and f is the angular frequency. It is worth noting that AWGN is a widesense stationary process and has no cyclic correlations. Thus the SCF of noise has no spectral features at $\alpha \neq 0$. The SCF produces large amount of data which makes it hard to classify the signals in near real time. Therefore, α profile is extracted from SCF, which is given by (5.7) and depicted in Fig. 5.3.

$$I(\alpha) = max_f[S_X^\alpha] \tag{5.7}$$

5.3.2 Compressed Sensing and Proposed Algorithm

The frequency response of the received WB signal shown in (5.1) can be observed by taking an N-point discrete fourier transform (DFT) on $r(t)$, as follows:

$$\mathbf{r}_f = \sum_{m=1}^{M} \mathbf{D}_h^{(m)} \mathbf{s}_f^{(m)} + \mathbf{w}_f \tag{5.8}$$

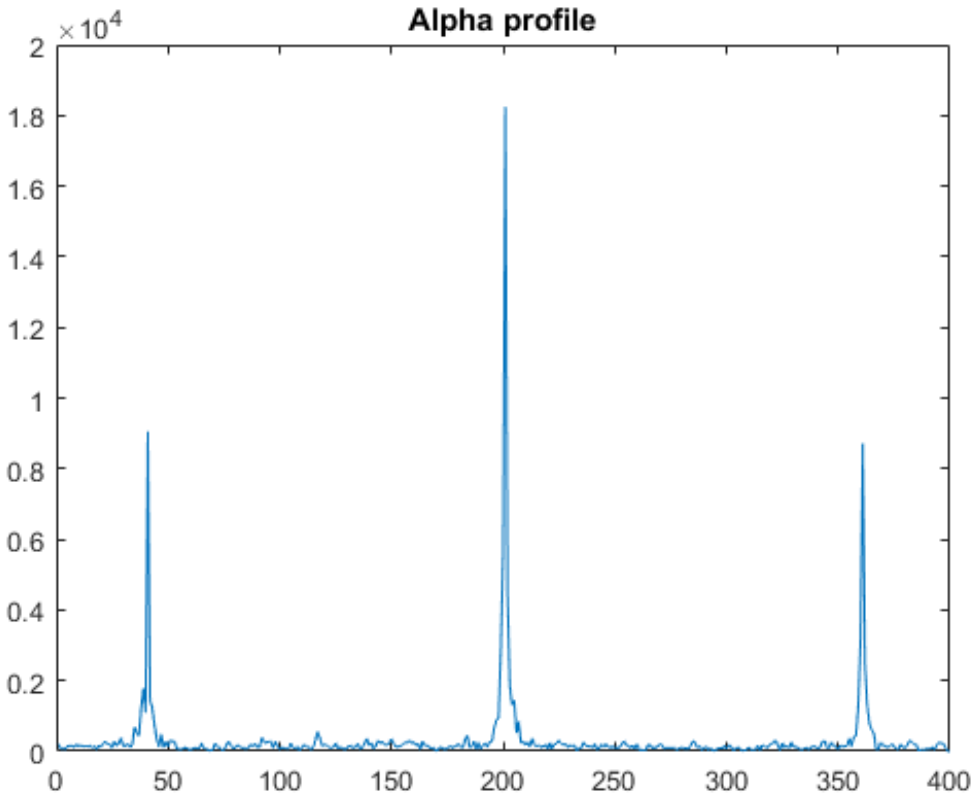


Figure 5.3: α-profile of a wide-band spectrum hosting two BPSK signals and a QPSK modulated jamming signal at different cyclic frequencies.

where r_f is a $N \times 1$ vector of frequency-domain samples, $\mathbf{D}_h^{(m)} = diag\left(\mathbf{h}_f^{(m)}\right)$ is an $N \times N$ diagonal channel matrix, and $\mathbf{h}_f^{(m)}$, $\mathbf{s}_f^{(m)}$ and $\mathbf{w}_f$ are the discrete frequency-domain samples of $h_m(t)$, $s_m(t)$ and $w(t)$, respectively. Adopting $\overline{\mathbf{s}}_f = [(\mathbf{s}_f^{(1)})^T, ..., (\mathbf{s}_f^{(M)})^T]^T$ to denote the signal spectrum of the transmitted signals, $\mathbf{H}_f = [\mathbf{D}_h^{(1)}, ..., \mathbf{D}_h^{(M)}]$ to denote the corresponding channel matrix for the receiver, this signal model can be generalized as follows:

$$\mathbf{r}_f = \mathbf{H}_f \overline{\mathbf{s}}_f + \mathbf{w}_f. \tag{5.9}$$

From the above expression, we can observe that the spectrum sensing task requires to estimate $\overline{\mathbf{s}}_f$ in (5.9) provided we have $\mathbf{H}_f$ and $r(t)$. To alleviate Nyquist rate sampling requirements at the receiver ADC, we can take advantage of the advances in signal recovery algorithms to recover Nyquist rate signal from sub-Nyquist samples. Various computationally feasible algorithms, such as, BP [16] or Orthogonal Matching Pursuit (OMP) [104], were developed to reliably estimate the received signal sampled at sub-Nyquist rate sampling.

The compressed time-domain samples are needed to be collected at the receiver. For this, a compressed sensing matrix $\mathbf{S}_c$ is constructed to collect a $K \times 1$ sample vector $\mathbf{x}_t$ from $r(t)$ as follows:

$$\mathbf{x}_t = \mathbf{S}_c \mathbf{r}_t \tag{5.10}$$

where $\mathbf{r}_t$ is the $N \times 1$ vector of discrete-time representations of $r(t)$ at the Nyquist rate and $\mathbf{S}_c$ is the $K \times N$ projection matrix with $K \leq N$. There are various designs introduced in literature for compressive sampler such as non-uniform sampler [41] and random sampler [42].

Noting that $\mathbf{r}_t = \mathbf{F}_N^{-1}\mathbf{r}_f$, and given K compressed measurements, the frequency response $\overline{\mathbf{s}}_f$ can now be estimated in (5.9), as follows:

$$\mathbf{x}_t = \mathbf{S}_c^T \mathbf{F}_N^{-1} \mathbf{H}_f \overline{\mathbf{s}}_f + \tilde{\mathbf{w}}_f \tag{5.11}$$

where $\tilde{\mathbf{w}}_f = \mathbf{S}_c^T \mathbf{F}_N^{-1} \mathbf{w}_f$ is the noise sample vector which is white Gaussian. In the context of cognitive radio networks, i.e., low spectrum occupancy by the licensed users, the signal vector $\mathbf{s}_f$ is sparse in frequency domain. The sparsity is measured by p-norm $||\overline{\mathbf{s}}_f||_p$, $p \in [0, 2)$, where $p = 0$ indicates exact sparsity.

Therefore, equation (5.11) is a linear regression problem with signal $\overline{\mathbf{s}}_f$ being sparse. This signal $\overline{\mathbf{s}}_f$ can be estimated by solving the following linear convex optimization problem:

$$\hat{\mathbf{s}}_f = \arg\min_{\overline{\mathbf{s}}_f} ||\overline{\mathbf{s}}_f||_1, \quad s.t. \quad \mathbf{x}_t = \mathbf{S}_c^T \mathbf{F}_N^{-1} \mathbf{H}_f \overline{\mathbf{s}}_f \tag{5.12}$$

This optimization problem can be solved by various different methods, for example, by means of Convex Programming as in BP [16] method or by usage of Greedy Algorithms such as OMP [104].

After the reconstructed Nyquist rate WB signal have been obtained from sub-Nyquist samples, it can be fed to CFD to estimate the SCF of the reconstructed signal. The procedures involved in the computation of SCF are outlined in previous subsection. Obviously, the estimated SCF in this case depends on how well the WB signal was estimated from compressed sensing, which in turn depends on the sparsity of the signal and the compression rate. We assume that the algorithm has access to a database containing pre-defined SCF values of the legitimate NB signals. The algorithm then compares the estimated SCF values with those in the database, eventually classifying each signal as "legitimate" or "jamming" signal. The pseudo-code of the proposed algorithm is outlined in Algorithm 3 and a generic block diagram summarizing the proposed algorithm is shown in Fig. 5.4.

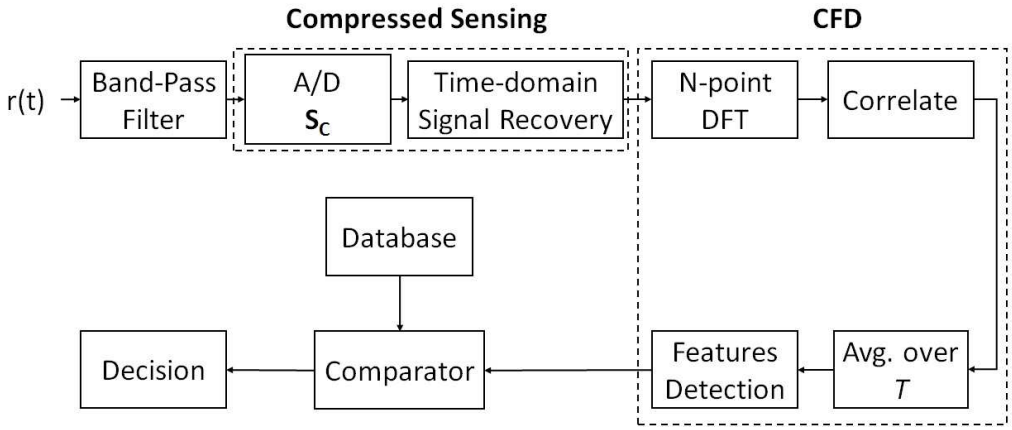


Figure 5.4: A generic block diagram of the implementation of proposed algorithm.

The proposed algorithm is computationally inexpensive but posses some limitations, such as;
(i) Simple classification using licit waveform parameters stored in a database, and
(ii) Requirements to maintain databases with licit waveform parameters.
Alternatively, more advanced classification techniques such as a neural network based approach or support vector machine (SVM) methods could be use to train the algorithm with licit waveform parameters. This may not only improve the classification performance of the algorithm but also relieve the requirements to maintain databases. Furthermore, this kind of jammer detection algorithm could be used in formulating intelligent game-theoretic based anti-jamming schemes as in [22]. The pseudo-code of the proposed algorithm is outlined in Algorithm 3.

5.4 Empirical Results and Discussion for Tone Jamming

For the experiments, we assume a WB spectrum of 50 ΔHz is under observation. This WB is sliced into 5 SBs of equal bandwidths. Each of this SB is assumed to be either free or occupied by a NB signal. For testing, we assume the BPSK and QPSK signals to be our legitimate signals while a sine wave is treated as a jamming signal. Out of various recovery algorithms, we use BP algorithm for signal recovery through compressed sensing. The SNR is set at 0 dB and compression ratios are varied from $K/N = 0.25$ to $K/N = 1.0$. Two different setups are considered: (a) BPSK signal is using SB-1, QPSK signal is using SB-5 and jamming signal is jamming empty SB-3;

Algorithm 3 Pseudo-code for proposed algorithm

```
function JAMMER DETECTOR
    Initialise all SB states to "free"
    Receive the WB signal
    Set compression rate  K/N
    Construct the measurement matrix  Sc
    Estimate the WB from compressed samples using BP
    Compute the SCF of estimated WB signal
    Extract the α profile from SCF
    Divide WB into i SBs
    for i = 1 to I, do
        Access the database
        Compare parameters with the database waveforms
        Decision ← Licit or Jammer
    end for
end function
```

(b) BPSK signal is in SB-1 while jamming signal jumps to SB-5 to jam the QPSK signal. The Nyquist sampling rate is $f_s = 100$ ΔHz and the frequency resolution is $f_s/N = 5/2$. Note that we keep a large frequency resolution for demonstration but it should take appropriate smaller value in practice. Having known the carrier frequencies of the licit signals, classification is performed at $\alpha \neq 0$, where AWGN exhibits no spectral features. The simulations are run for 1000 Monte-Carlo iterations. The results are shown in graphical form instead of confusion matrices to counter space limitations.

Fig. 5.5 shows the jammer detection rate versus the compression rate for occupied SBs. It is observable that the jammer detection rate in SB-3 is about 0.99 at $K/N = 1.0$ while that of SB-1 and SB-5 its around 0.08. Meaning that both in SB-1 and SB-5, the algorithm correctly classified the legitimate signals (BPSK as BPSK and QPSK as QPSK) with 92% accuracy while for 8%, algorithm wrongly classified the legitimate signals as jammer. With the decrease in K/N, the jammer detection rate for SB-3 decreases while that for SB-1 and SB-5 increases. It is because will less samples available for recovery, the recovered signal is less accurate. As a consequence, the estimated SCF by the CFD is also different from what is stored in the database and therefore, wrong classifications are increased. For example, at $K/N = 0.55$, the jammer detection rate in SB-3 is 0.61 while wrong classification of jammer as BPSK is 0.11 and that of jammer as QPSK is 0.28. Likewise, the jammer detection rate in SB-1 and SB-5 is around 0.15 and wrong classification of BPSK as QPSK is 0.05 and that of QPSK as BPSK is 0.08.

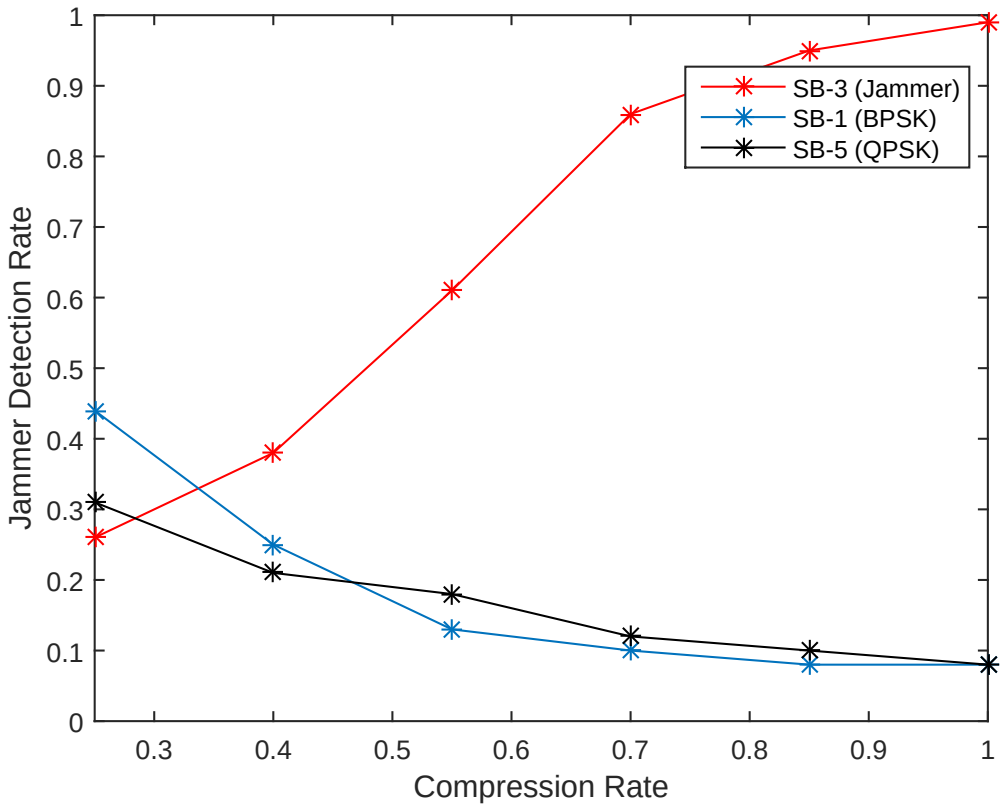


Figure 5.5: Performance of Jammer Detection Algorithm over various compression ratios and SNR = 0 dB. SB-1 is used by BPSK, SB-5 is occupied by QPSK and SB-3 is occupied by jammer.

Jammer detection rate versus the compression rate is plotted in Fig. 5.6 for second test configuration where the jammer is now jumped into SB-5 to jam the licit QPSK signals. As can be seen the jammer detection rate falls to 0.61 in SB-5 as compared to 0.99 in SB-3 from previous test scenario. It is because the algorithm is now classifying a mixture of QPSK and Jammer in SB-5 as QPSK with a rate of 0.39 but ideally it should have classified SB-5 to be jammed. Once again the jammer detection rate falls as the compression rate is decreased due to poor recovery of the WB signal at low compression rates. For instance, at $K/N = 0.40$ the jammer detection rate is approximately 0.51 in SB-5 with wrong classifications as QPSK to be 0.12 and as BPSK to be 0.37. The jammer detection rate in SB-1 is approximately the same as before.

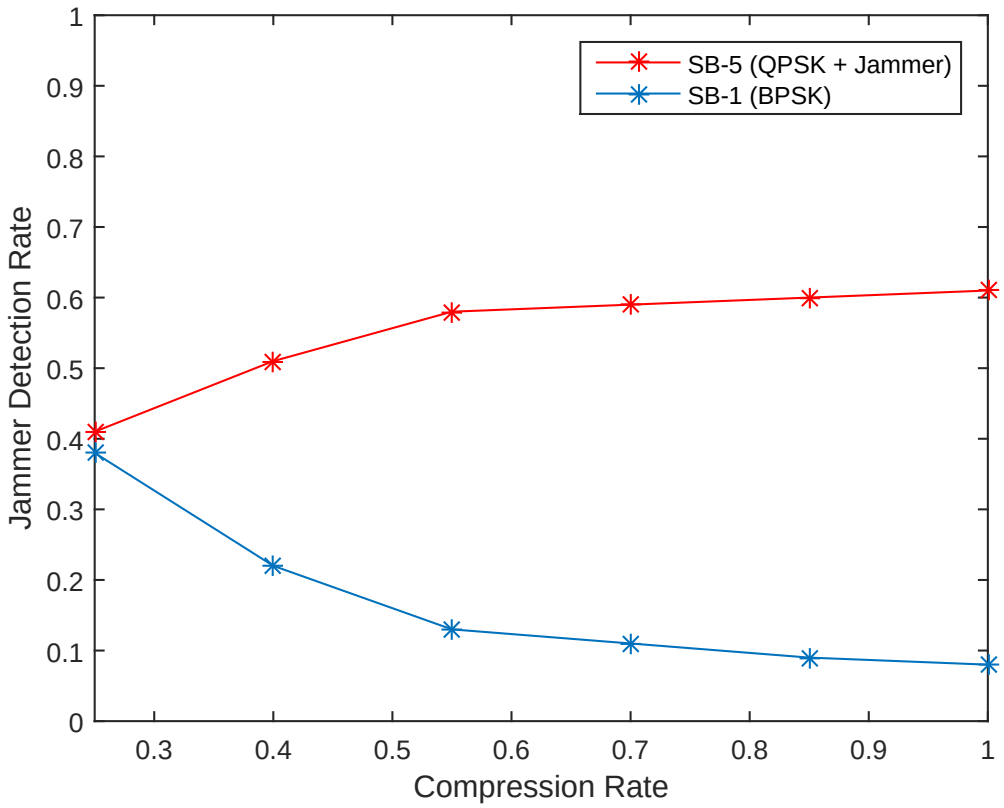


Figure 5.6: Performance of Jammer Detection Algorithm over various compression ratios and SNR = 0 dB. SB-1 is occupied by BPSK signal while jammer has jumped from SB-3 to SB-5 to jam QPSK signal.

5.5 Empirical Results and Discussion for Modulated Jamming

A 50 ΔHz WB spectrum is assumed to be under observation by a CR terminal. This WB is divided into 5 SBs. These SBs can be either free or occupied by a NB signal. For testing the proposed system, we assume BPSK as legitimate signals and QPSK is treated as a jamming signal. The received signals are considered to be affected by AWGN. The BP algorithm is used for signal recovery through compressive sensing. The sampling rate is set at Nyquist rate of 100 ΔHz. We set SNR at 0 dB and compression rate (K/N) are varied from 0 to 1. We configure our system in two different ways: (a) we placed the BPSK signals in SB-1 and SB-5 and jamming signal in SB-3; (b) BPSK signal is in SB-5 while jamming signal jumps to SB-1 to jam the licit BPSK signal. It is assumed that carrier frequencies of legitimate users are known. The classification of the signals is performed at $\alpha \neq 0$, where AWGN exibits no spectral

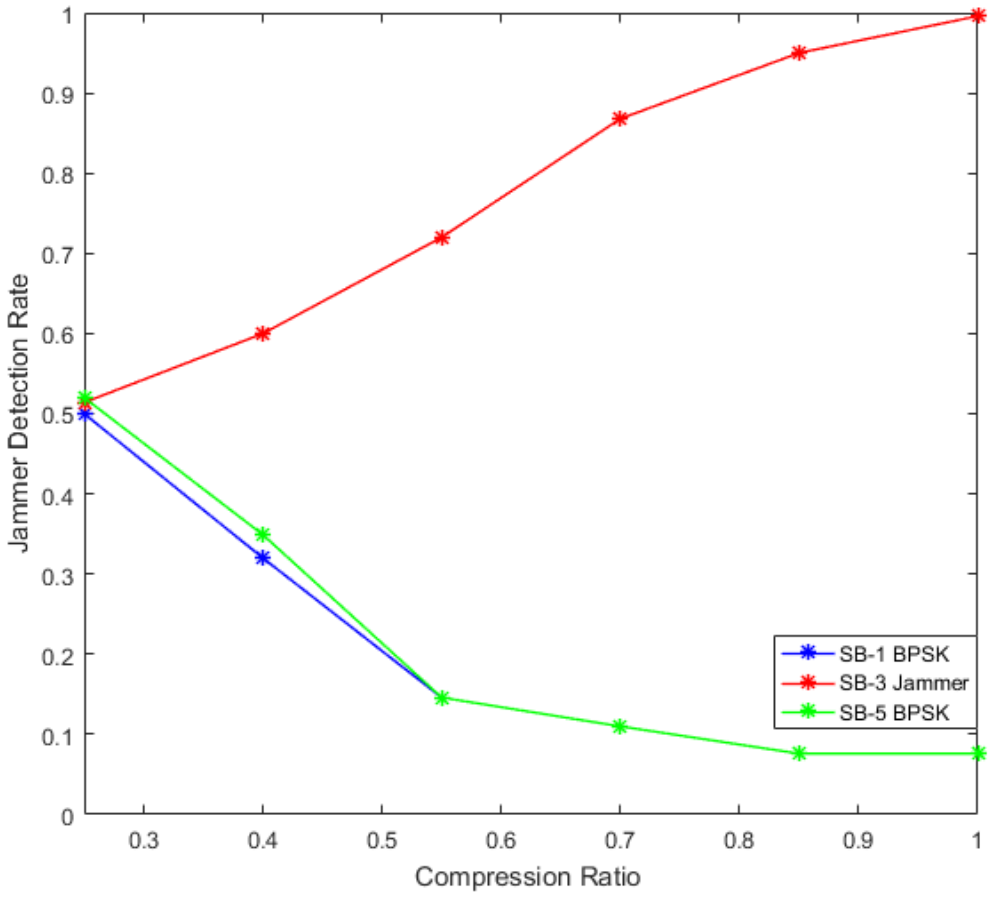


Figure 5.7: Performance of Jammer Detection Algorithm over various compression ratios and 0 dB SNR. SB-1 and SB-5 are used by BPSK signals and SB-3 is occupied by modulated jammer .

features. The Monte-carlo simulations are run for 1000 iterations for each K/N. The results are shown in the forms of graphs. For first system configuration, the jammer detection rate versus compression ratio is plotted in Fig. 5.7. It can be seen from this figure that the jammer detection rate is approximately 1 in SB-3 at $K/N = 1$. Due to false classification (false positive), the jammer detection in SB-1 and SB-5 is 0.076, which intern means that algorithm correctly classified the legitimate signals with 92% accuracy while for 8% algorithm wrongly classified the legitimate signals as jammer. When K/N is decreased, the jammer detection rate for SB-3 decreases while that for SB-1 and SB-5 increases. It is due to the reason that less samples are now available for WB signal recovery, hence recovered signal is less accurate. Therefore, the computed SCF is also different from what is stored in the database, which leads

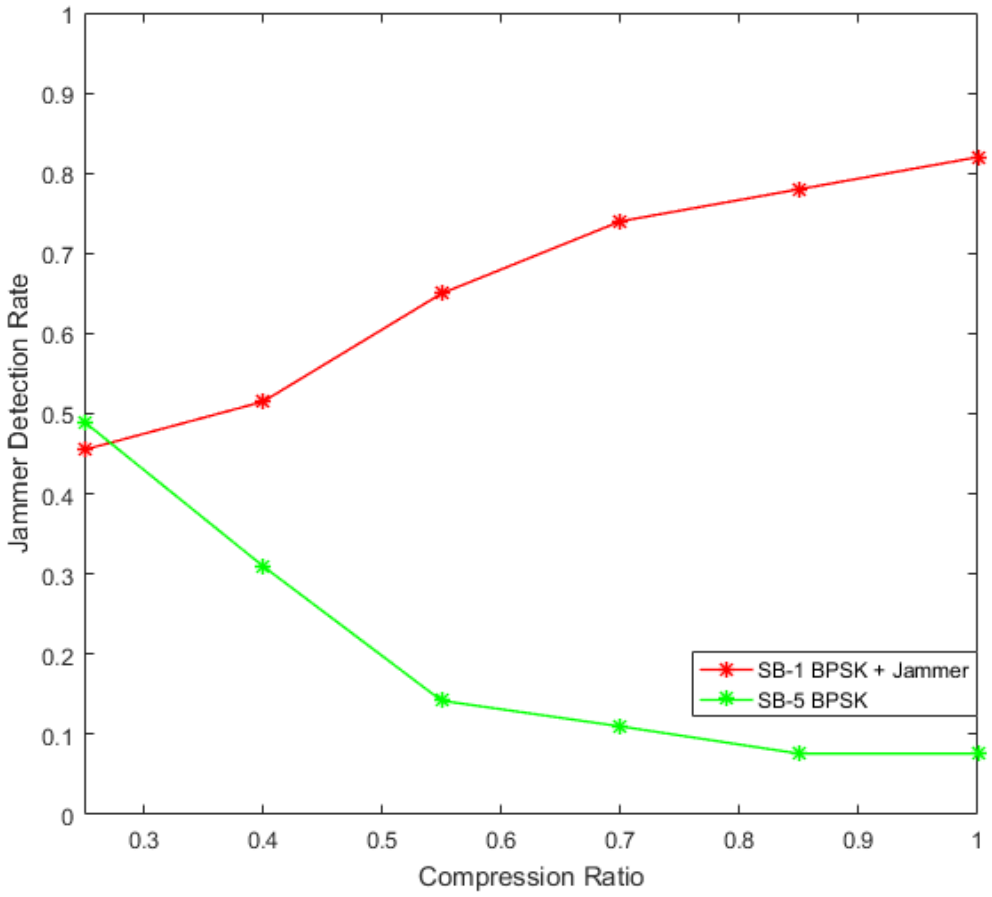


Figure 5.8: Performance of Jammer Detection Algorithm over various compression ratios and 0 dB SNR. SB-5 is occupied by BPSK signal while modulated jammer has jumped from SB-3 to SB-1 to jam BPSK signal.

to wrong classification. For example, at $K/N = 0.70$, the jammer detection rate in SB-3 is 0.868 while wrong classification of jammer as BPSK is 0.132. similarly, the jammer detection rate in SB-1 and SB-5 is 0.11. Fig. 5.8 shows the jammer detection rate versus compression ratio for second system configuration, where the jammer is now jumped to SB-1 to jam licit BPSK signals. It can be observed that jammer detection rate decrease to 0.82 in SB-1 as compared to 1 in SB-3 from previous case. It is because the algorithm is now classifying a mixture of BPSK and Jammer in SB-1 as it also classify BPSK with classification rate of 0.18. The jammer detection rate is also fallen for this system configuration as the compression ratio is decreased due to poor recovery of the WB spectrum at low compression rates. For instance, at $K/N = 0.55$ the jammer detection rate is approximately 0.65 in SB-1 with wrong

classifications as BPSK to be 0.35.

5.6 Empirical Results and Discussion for Stealthy Jamming

We consider a 500 ΔHz WB spectrum under the observation of a CR terminal. This WB is consisted of 5 SBs and each of these SB can either be free or occupied by a NB signal. For experiments, we assume BPSK and QPSK as legitimate signals. The transmitter can alter its modulation scheme over the time and the probability of selecting either BPSK or QPSK is 0.5. Similarly, the jammer can choose optimum jamming strategy against legitimate waveform, i-e BPSK against BPSK and QPSK against QPSK. However, the jammer can jam one band at a time. The received signals are considered to be affected by AWGN. The BP algorithm is used for signal recovery through compressive sensing. The sampling rate is set at Nyquist rate of 1000 ΔHz. The SNR is set to 0 dB and compression ratio (K/N) is varied from 0 to 1. We configure our system in such a way that we placed the BPSK signals in SB-1 and SB-4. It is assumed that carrier frequencies of legitimate users are known. The classification of the signals is performed at $\alpha \neq 0$, where AWGN exhibits no spectral features. The Monte-carlo simulations are run for 1000 iterations for each K/N and results are shown in the form of graphs.

In Fig. 5.9 the jammer detection rate versus compression ratio is plotted for SB-1, It can be seen from this figure that the jammer detection rate is around 0.9 at $K/N = 1$. Due to false classification (false positive), the jammer detection in SB-1 is 0.08, which means that the proposed algorithm correctly classified the BPSK with 92% accuracy while for 8% algorithm wrongly classified the legitimate signals as jammer. When K/N is decreased, the jammer detection rate for SB-1 decreases while wrong classification is increased due to the reason that now less samples are available for WB signal recovery, hence estimated signal is less accurate. Therefore, the SCF of the signal is also different from what is previously stored in the database, which leads to wrong classification. For instance, the jammer detection rate is 0.57, while false classification of BPSK as a jammer (BPSK + BPSK) is 0.35 at $K/N = 0.40$, Fig. 5.10 shows the jammer detection rate versus compression ratio for second case, when the transmitter adopt QPSK as modulation scheme and jammer also apt to its optimum jamming scheme against QPSK. It can be seen that jammer detection rate is 0.95 in SB-1 and the wrong classification of QPSK as a jammer is 0.02. The jammer detection rate is also fallen for this case as the compression ratio is decreased

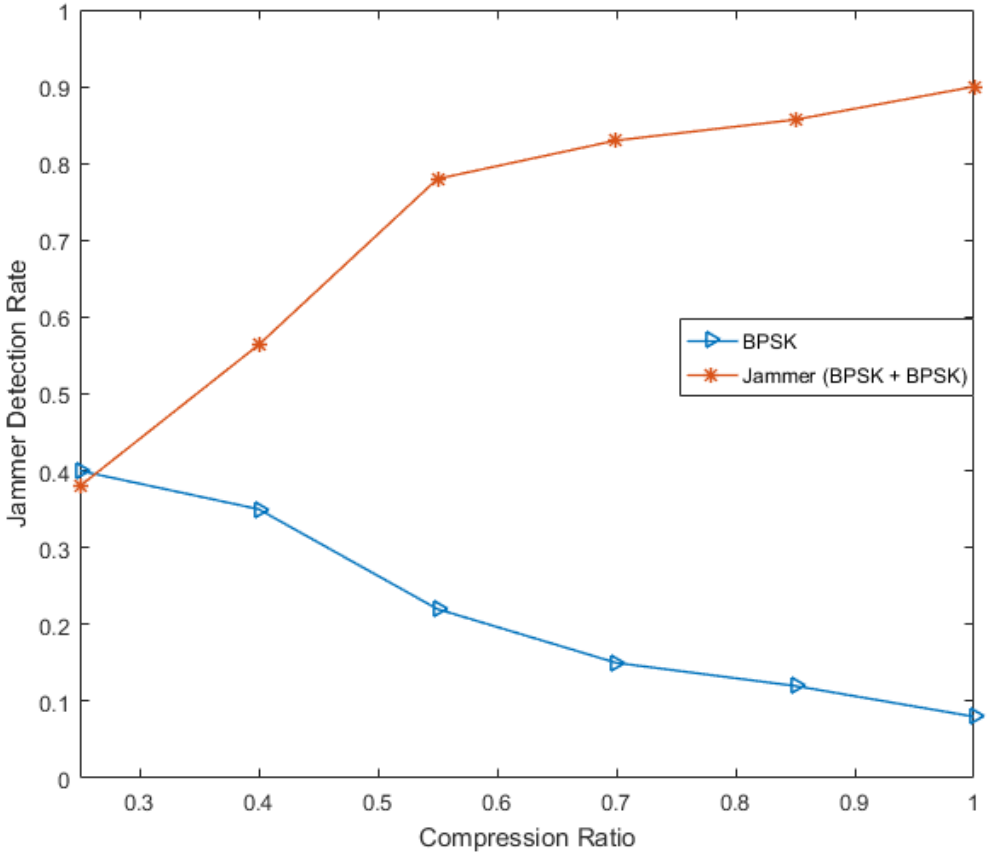


Figure 5.9: Performance of Jammer Detection Algorithm over various compression ratios and 0 dB SNR. SB-1 and SB-5 are used by BPSK signals and stealthy jammer target licit signal in SB-1 .

due to poor recovery of the WB spectrum at low compression rates. For example, at $K/N = 0.40$ the jammer detection rate is approximately 0.55 in SB-1 and wrong classifications of QPSK as a jammer is increased to 0.45. Similar, procedure is valid for all other occupied SBs.

5.7 Conclusion and Future Work

In this chapter, we proposed a cyclic feature based jammer detection algorithm for WB cognitive radio networks. The WB was considered to be comprised of several NB signals with known carrier frequencies and symbol times. To alleviate ADC complexity, compressed sensing was employed for recovering the Nyquist rate samples of the WB signal from sub-Nyquist sampling. The recovered signal was then fed to

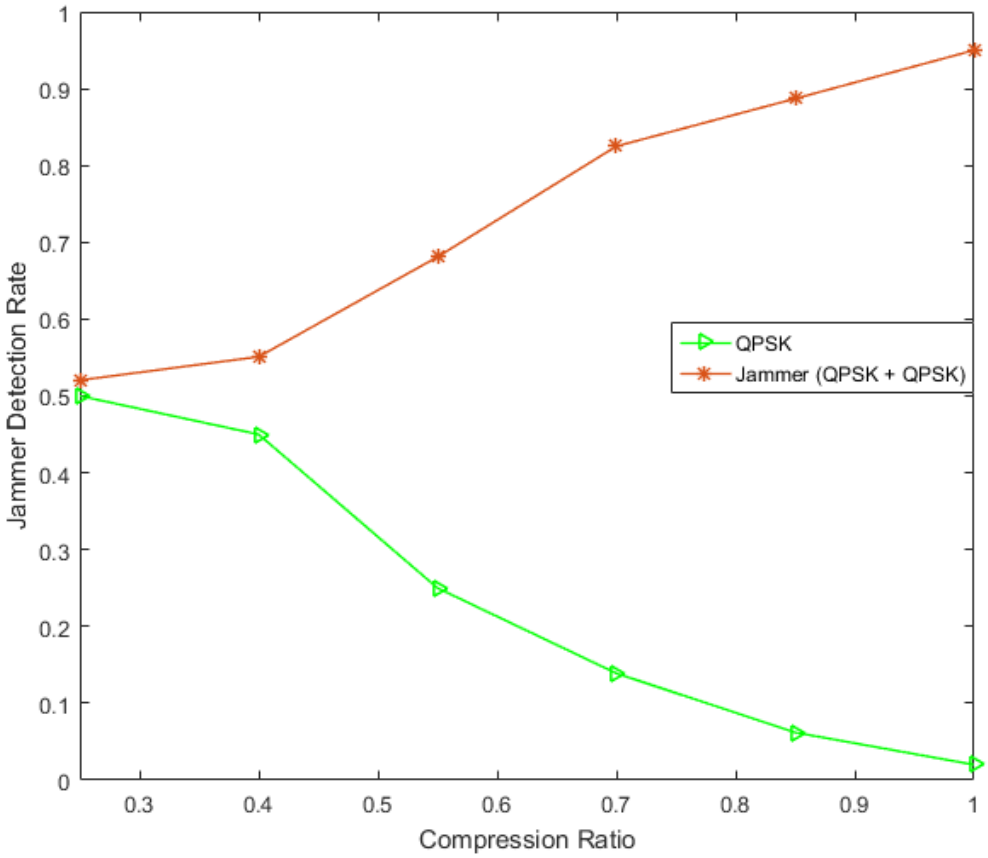


Figure 5.10: Performance of Jammer Detection Algorithm over various compression ratios and 0 dB SNR. The licit users changed modulation scheme to QPSK in SB-1 and SB-5 and stealthy jammer target licit signal in SB-1 .

the CFD to estimate the SCF of the signal. After that, estimated SCF from CFD was compared with the SCF of the licit waveforms' database to identify jamming waveforms in each SB. In the end, results were evaluated for different occupancy states of the WB spectrum over various compression rates at low SNR value, with the help of Monte-Carlo simulations.

The proposed algorithm appears to perform well within the limitations imposed for using simple classification based on plain comparison of parameters from database. Alternatively, better classification techniques such as a neural network based or support vector machine (SVM) classifier could improve the performance of the algorithm. Additionally, such a jammer detection algorithm could be helpful in formulating intelligent anti-jamming strategies for WB cognitive radio systems.

Chapter 6

Spectrum Characterization using Compressed Sensing and Artificial Neural Networks

6.1 Introduction

Jamming attacks can noticeably affect the performance of wireless communication systems and can lead to significant overhead in terms of data re-transmission and increased power consumption. In this chapter, a novel compressed sensing based jammer detection algorithm is proposed using cyclic spectral analysis and artificial neural network (ANN) for wide-band (WB) cognitive radios. The proposed approach considers a WB spectrum, which is occupied by several narrow-band (NB) signals. These NB signals can be legitimate signals or jamming signals. Compressed sensing (CS) is used to reduce the overhead of the analog-to-digital conversion (ADC) and allows one to estimate a WB spectrum with sub-Nyquist rate sampling. Therefore, proposed algorithm is able to recover the received WB signal from sub-Nyquist rate samples using CS. After the Nyquist rate signal has been recovered, spectral correlation function (SCF) is computed to extract the cyclic features of WB signal. Finally, a pre-trained ANN is able to classify each NB signal as a legitimate or jamming signal. This ANN is trained for sub-Nyquist samples, which significantly increases the signal classification rate. In the end, performance of proposed algorithm is shown with Monte-Carlo simulations under different empirical setups.

The rest of the chapter is organized as follows. Section 6.2 explains some background on the problem. Section 6.3 describes the system model and problem formulation, followed by the proposed algorithm in Section 6.4. Section 6.5 covers the simulation results and discussions and finally the chapter is concluded in section 6.6.

6.2 Background

Over the years, spectrum resources are becoming more and more expansive, for example ISM bands are clutched and busier than ever. On the other hand, the licensed spectral bands are reported under-utilized (spectrum holes) by the Primary Users (PUs). Cognitive radio is proposed to opportunistically utilize the licensed bands by Secondary Users (SUs) without interference to PUs. This is the reason cognitive radio has attained great attention from wireless communication community in recent years. A cognitive radio dynamically interacts with the environment and adopts the operating parameters accordingly for the purpose of dynamic/ opportunistic spectrum access (DSA / OSA) [68], [47]. In order to discover the spectrum holes, spectrum sensing is the primary task needed to be performed by a cognitive radio terminal [116].

In literature, various spectrum detectors have been proposed for cognitive radios, such as matched filter detector (MFD), energy detector (ED) and cyclostationary feature detector (CFD) [113]. The MFD can detect the primary signals very well, but the comprehensive prior knowledge for the PU's signal is needed. Furthermore, if the environment changes, the detector's performance degrades. The ED is easy to implement, and usually has good performance in low noise environment. ED is suggested in the IEEE 802.22 standard for spectrum sensing. However, it fails at low SNRs. In most cases, spectrum sensing is needed to detect the weak primary signals accurately. Therefore, another typical spectrum detector called CFD, has been proposed to significantly improve the detection probability of the PU signals. CFD is able to accurately detect and even classify the primary signals under low SNR condition, thanking to its cyclic frequency features, which can be extracted and recognized in different modulation signals. This performance is achieved at the cost of increased implementation complexity. CFD uses the cyclostationarity of the modulated primary signals by detecting spectral peaks in spectral correlation function (SCF) or spectral coherence function (SOF) [5, 115, 78], which are sparse in both angular (f) and cyclic (α) frequency domain. Furthermore, it has been used as a robust tool for signal classification when the carrier frequency and bandwidth information is unavailable [35, 61, 6].

When the cognitive radios are operating on a wide-band (from few hundred MHz to several GHz), the sensing task becomes more complex and imposes a large overhead to the spectrum sensing system due to the high-rate sampling, analog-to-digital (A/D) converter, and heavy memory usage. Compressive sensing (CS) [30] is an interesting

solution to alleviate requirements of high sampling rates provided that the signal is sparse in some given transform domain. Signal sparsity is the main requirement for CS to work and in the case of cognitive radio networks, it is a practical assumption because not all frequency bands are occupied all the time in all geographical locations [68]. Therefore, spectrum of the cognitive radio network is sparse in frequency domain due to low occupancy by the PUs. CS requires non-linear optimization to find the optimal solution for signal estimation and this could be achieved by means of greedy algorithms such as Matching Pursuit (MP) [31] or Orthogonal MP [104]. The other solution in literature is the use of Convex Programming as in Basis Pursuit (BP) [16]. Then, CFD needs to estimate the SCF of the received wide-band (WB) spectrum from sub-Nyquist samples. A possible approach [18] is to first recover Nyquist samples from sub-Nyquist samples, then estimate the SCF and perform feature extraction. For Nyquist samples recovery, authors in [66] used modulated wide-band converter (MWC). On the other hand, a different method is adopted in [100],[103] where authors perform the SCF estimation directly from sub-Nyquist samples by exploiting the sparsity in two dimensional SCF domain.

Radio frequency (RF) jamming is the process of transmitting illegitimate signals on one or more occupied channels with the objective of disrupting the communication of the targeted system. Jamming and anti-jamming concepts are as old as radio communications itself, but recent development in CR technology has permitted devising and deploying of more advanced, self-configurable jamming[22] and anti-jamming [23] solutions. Spectrum sensing plays a key role in designing anti-jamming systems. This spectrum sensing information can be used to detect potential jammers [73] and to take proactive measures to ensure communication continuity and security. Furthermore, an observation set can be maintained over the time and used to employ more effective anti-jamming tactics. For example, when a frequency hopping spread spectrum (FHSS) based system is used, cognitive radio can modify its hopping sequence to avoid the channels which are occupied by jamming entities [91]. In order to design an appropriate anti-jamming system, there is a need for a reliable jammer detection algorithm.

In this work, we propose a new jammer detection algorithm for WB cognitive radios. The first step is to recover the Nyquist rate WB spectrum, which consists of various NB signals, from sub-Nyquist samples using CS. For this, we use the conventional BP technique [16]. The reconstructed signal is then fed to the CFD to estimate the SCF of the WB signal. The cyclic frequency profile ($\alpha - profile$) is extracted from SCF and is used as input features for an artificial neural network (ANN) based classifier.

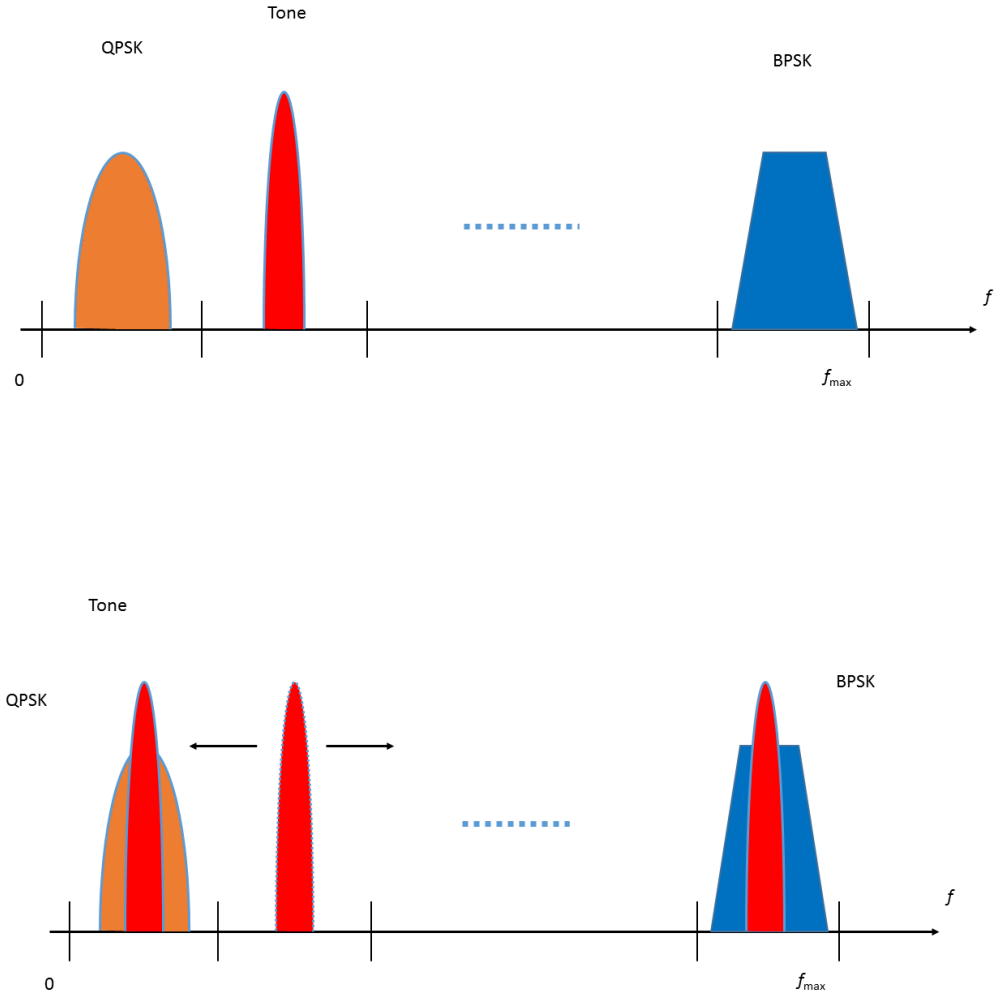


Figure 6.1: (a) Wide-band spectrum divided into multiple sub-bands (SB) and each SB is occupied by a narrow-band signal. (b) Narrow-band jammer (Tone) jumps to the neighbouring SB to jam licit (BPSK or QPSK) signal.

Two different ANN based classifiers are discussed in this work and one with higher classification performance is used for jammer detection. Based on the ANN classifier, each of NB signal is classified either as a legitimate signal or a jamming signal. Finally, the performance of proposed algorithm is evaluated for various compression ratios and SNRs to observe the effects of various parameters on the classification performances.

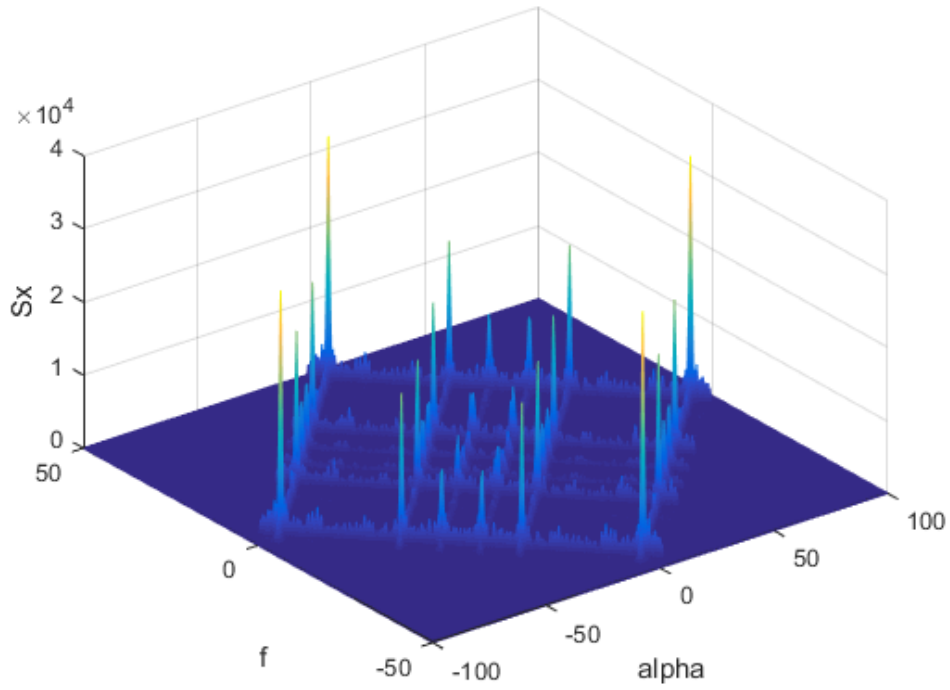


Figure 6.2: SCF of a wide-band spectrum hosting BPSK and QPSK modulated signals and a non-modulated tone signal.

6.3 System Model and Problem Formulation

We consider a received WB spectrum of Δ Hz. This WB spectrum can be occupied by various NB signals $n \in \{1, 2, 3.....N\}$, with different carrier frequencies and modulation types that we want to identify. The received WB signal is an aggregated time-domain signal which can be presented as

$$r(t) = \sum_{n=1}^{N} h_n(t) * s_n(t) + w(t) \tag{6.1}$$

where $s_n(t)$ denotes the *n-th* transmitted signal, $h_n(t)$ is the channel coefficient between *n-th* transmitter and receiver, * denotes the convolution operation and $w(t)$ is the additive white Gaussian noise (AWGN) with zero mean and power spectral density σ_w^2 . We assume that these NB signal can be generated by different types of modulation schemes, such as, binary frequency shift keying (BFSK), binary phase shift keying (BPSK), quadrature amplitude modulation (QAM), quadrature phase shift keying (QPSK), or any other modulation scheme as shown in Fig. 6.1 (a). The

WB is divided into multiple equal bandwidth SBs and each of these SBs can be occupied by NB signals with no spill over energy into neighbouring SBs.

For our proposed system, a single tone is considered as a jamming signal. The jammer is considered to be a cognitive jammer, which has the knowledge of carrier frequencies of legitimate signals. This jammer can jam any of SBs, if it has higher power than the legitimate signal as depicted in Fig. 6.1(b). The tone jammer is very successful against NB signals, due to the fact that it allows to concentrate all power on a single data channel. The tone jamming is often considered as the best strategy for jammers with limited transmission power [20]. Let us assume that the targeted signal is QPSK-modulated and uncoded, and that targeted system uses the coherent detection. Then, the error probability (p_e) to either jam the in-phase component (I) or quadrature component (Q) of the targeted signal can be given as follow [73],[20]

$$p_e^{\mathrm{I}} = Q(\sqrt{\frac{P_r}{P_n}}(1 - \sqrt{\frac{2P_j}{P_r}}\mathrm{Sin}(\theta^j)) \tag{6.2}$$

$$p_e^{\mathrm{Q}} = Q(\sqrt{\frac{P_r}{P_n}}(1 + \sqrt{\frac{2P_j}{P_r}}\mathrm{Cos}(\theta^j)) \tag{6.3}$$

here, P_r is the received power of targeted signal, P_n is thermal noise power, P_j is the jamming signal received power, θ^j is the phase of jamming signal, and Q is the Gaussian Q-function. For our system model we considered that $P_j >> P_r$, therefore $p_e \approx 100\%$ whenever jammer transmits on the same channel as the targeted transmitter-receiver pair.

6.4 Proposed Algorithm

In this section we first introduce SCF, CS and ANN, and at the end newly proposed algorithm is presented.

6.4.1 Cyclostationary Spectral Analysis

A process $r(t)$ is said to be wide-sense cyclostationary with period T_0 if its mean $E[r(t)] = \mu_r(t)$ and autocorrelation $E[r(t)r(t+\tau)] = R_r(t,\tau)$ are both periodic with period T_0,

$$M_r(t+T_0) = M_r(t), \qquad R_s(t+T_0,\tau) = R_r(t,\tau). \tag{6.4}$$

The autocorrelation function of a wide-sense cyclostationary process can be expressed in terms of its Fourier series components.

$$R_r(t,\tau) = E[r(t+\tau/2)r^*(t+\tau/2)] \tag{6.5}$$

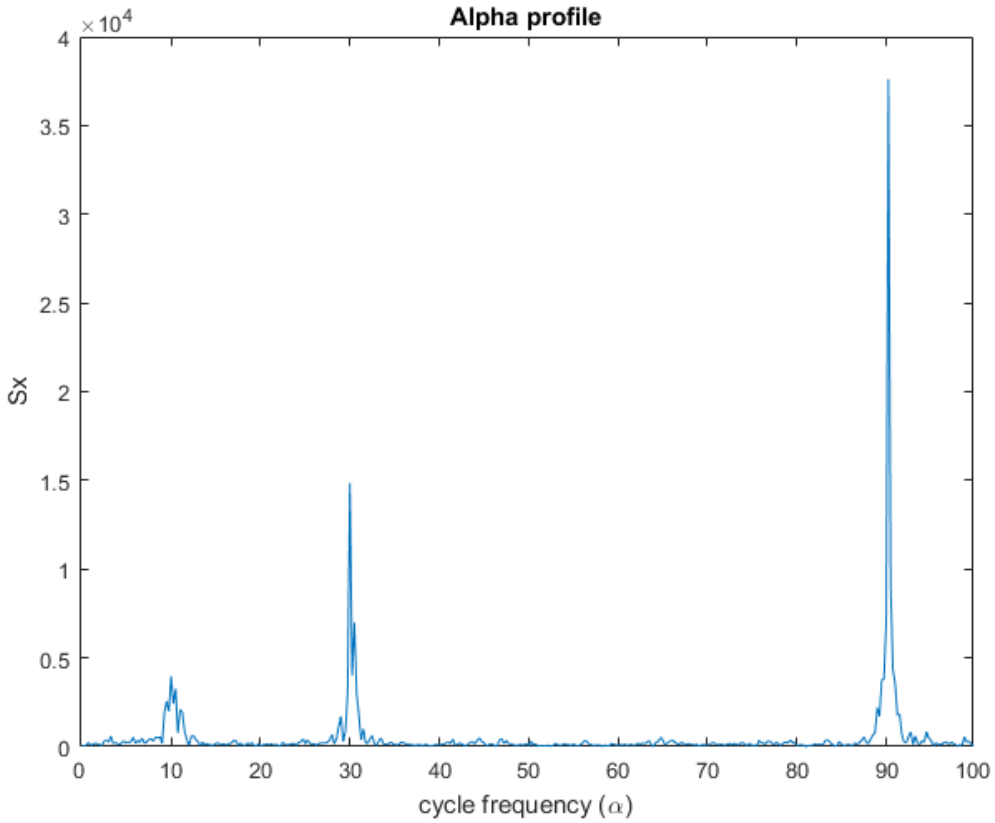


Figure 6.3: Cyclic frequency profile of a wide-band spectrum hosting BPSK, QPSK and a tone signal at different cyclic frequencies.

$$R_r(t,\tau) = \sum_{\alpha} R_r^{\alpha} e^{j2\pi\alpha t} \tag{6.6}$$

where, $\alpha = \frac{a}{T_0}$ and a is an integer. $E[.]$ is the expectation operator, α is the cyclic frequency, and $R_r^{\alpha}(\tau)$ present the cyclic autocorrelation function (CAF) and give Fourier components. CAF is given by

$$R_r^{\alpha}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} R_r(t,\tau) e^{-j2\pi\alpha t} dt \tag{6.7}$$

The Fourier Transform of the CAF is known as SCF and is given by

$$S_r^{\alpha}(f) = \int_{-\infty}^{\infty} R_r^{\alpha}(\tau) e^{-j2\pi f\tau} d\tau \tag{6.8}$$

where α is cyclic frequency and f is the angular frequency.

The major benefit of spectral correlation is its insensitivity to background noise. Since, correlation measures the temporal correlation of different spectral components, and the spectral components of noise are completely uncorrelated in time due to the

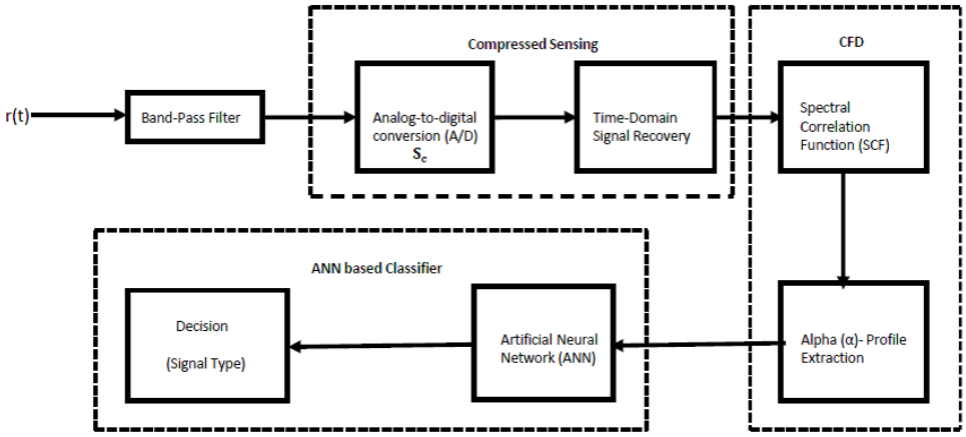


Figure 6.4: A generic block diagram of the implementation of proposed algorithm.

fact that noise is wide-sense stationary process. Therefore, noise does not play significant factor in the SCF. This fact allows the spectral correlation of a signal to be accurately calculated even at low SNRs. Furthermore, different types of modulated signals (BPSK, AM, FSK, MSK, QAM, PAM) with overlapping power spectral densities have highly distinct SCFs. Our simulations are restricted to the BPSK and QPSK modulation schemes due to the fact that higher order QAM and higher order PSK do not exhibit second order periodicity or exhibits the same features as QPSK. Therefore, these signals can be distinguished by higher order spectral analysis [43]. An example of the SCF of WB signal is depicted in Fig. 6.2.

SCF computation requires large amount of data, which makes it unreasonable for a classifier to operate on it in real time. We used here $\alpha - profile$ as features for classification given in (6.10) . The $\alpha - profile$ of SCF for WB signal is shown in Fig. 6.3.

$$I(\alpha) = max_f[S_r^\alpha] \tag{6.9}$$

6.4.2 Compressed sensing

In this section, an overview of CS process is presented. The frequency response of the observed WB signal shown in (1) can be obtained by taking N-point discrete fourier

transform (DFT) on $r(t)$, as follows:

$$r_f = \sum_{n=1}^{N} D_h^{(n)} S_f^{(n)} + w_f \tag{6.10}$$

where r_f is a $N \times 1$ vector of obtained frequency-domain samples, $D_h^{(n)} = diag(h_f^{(n)})$ is an $N \times N$ diagonal channel matrix, and $h_f^{(n)}$, $S_f^{(n)}$ and w_f are the frequency-domain samples of $h_n(t)$. $s_n(t)$ and $w(t)$, respectively. This signal model in (10) can be written in more generalized form as follows:

$$r_f = H_f \bar{S_f} + w_f \tag{6.11}$$

where $\bar{S_f} = [(S_f^{(1)})^T ....(S_f^{(N)})^T]^T$ is used to denote the spectrum of transmitted signals, and $H_f = [(D_f^{(1)}) ....(D_f^{(N)})]$ to denote the corresponding channel matrix for the receiver. From the above expression it can be observed that the spectrum sensing task requires to estimate S_f in (6.11) provided we have H_f and $r(t)$. We have WB signal at our disposal, to alleviate Nyquist rate sampling requirements at the receiver A/D converter, we can take advantage of the advances in signal recovery algorithms to recover Nyquist rate signal from sub-Nyquist samples. Several computationally reasonable algorithms, such as, BP [16] or Orthogonal Matching Pursuit (OMP)[104], were developed to reliably estimate the received signal sampled at sub-Nyquist rate sampling. The compressed time-domain samples are required to be collected at receiver. Therefore, a CS matrix S_c is constructed to collect a $K \times 1$ sample vector X_t from $r(t)$ as follows:

$$x_t = S_c r_t \tag{6.12}$$

where s_c is the $k \times n$ projection matrix and r_t is the $N \times 1$ vector of discrete-time representations of $r(t)$ at the Nyquist rate with $K <= N$. There are different designs introduced in literature for compressive sampler such as non uniform sampler [92] and random sampler [117]. It is worth noting that $r_t = F_N^- 1 r_f$, and given K compressed measurements, the frequency response S_f^- can now be estimated in (6.12), as follows:

$$x_t = S_c^T F_N^{-1} H_f \bar{S_f} + \tilde{w_f} \tag{6.13}$$

where $\tilde{w_f} = S_c^T F_N^{-1} w_f$ presents the noise sample vector which is white Gaussian. In the context of cognitive radio networks, due to low spectrum occupancy by licensed users, the signal vector S_f is sparse in frequency domain. The sparsity of signal vector is measured by p-norm $||S_f||_p$, $p \in [0, 2)$, where $p = 0$ indicates exact sparsity. Thus,

equation (13) is a linear regression problem with signal $\bar{S_f}$ being sparse. The signal $\bar{S_f}$ can be estimated by solving the following linear convex optimization problem:

$$\hat{S_f} = \underset{\bar{S_f}}{argmin} ||\bar{S_f}||_1, \quad s.t. \quad x_t = S_c^T F_N^{-1} H_f \bar{S_f} \tag{6.14}$$

This optimization problem can be solved for example, by means of Convex Programming as in BP [16]. After the reconstructed Nyquist rate WB signal have been obtained from sub-Nyquist samples, CFD can be used to estimate the SCF of the reconstructed signal. The estimated SCF in this case is definitely dependent on how well the WB signal was estimated from CS, which in turn depends on the sparsity of the signal and the compression rate. The procedure of SCF computation is given in Sec. 6.4.3. Then the features are extracted from obtained SCF of the WB signal and used to train ANN. The $\alpha - profile$ is used as features to train ANN based classifier. The detail of ANN based classifier is given in following section.

6.4.3 Neural Network Classifier

The proposed system uses an ANN as classifier due to its ease of implementation and potential to generalize any parameter, such as carrier frequency, symbol rate, phase offset and compression ratio. The system is designed to classify signals as BPSK, QPSK, Jammer (single tone), QPSK plus Jammer and BPSK plus Jammer. This is done with one ANN, trained to identify the above five classes of signals. The SCF of WB produces a large amount of data, which makes impossible for a classifier to work on it in near real time. In order to reduce the amount of data for a classification stage, we used $\alpha - profile$ as input features for an ANN. The proposed ANN is composed by 80 inputs related to the $\alpha - profile$, a single hidden layer whose neurons use the hyperbolic tangent sigmoid as a neural transfer function; and an output layer of five neurons relevant to each type of signal taken into account in this work. The value is in the range $[0, 1]$. Therefore, the output class with the highest vlaue between $[0, 1]$ is considered as the signal class. ANN is trained based on the scale conjugate gradient propagation [69]. The selection of a single hidden layer is proposed due to the classification process simplicity of this particular problem, it was found with a single hidden layer ANN, over the 90% accuracy was achieved. These results show that considering more hidden layers would increment the training time and overall results would not be significantly improved. According to this, in order to choose the proper number of neurons such that does not compromise notably the training time and guarantees robustness at repeating the training process for new ANNs, it

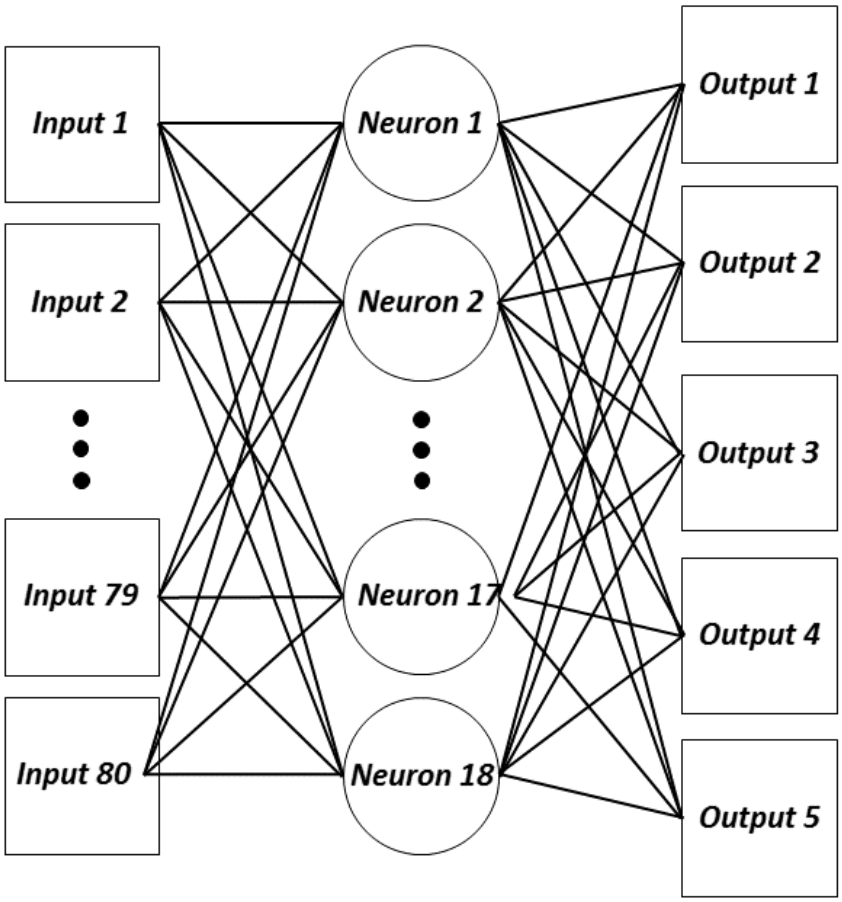


Figure 6.5: Proposed Neural Network

is proposed to train multiple times 20 different architectures in which the number of neurons in the single layer is varied from 1 to 20. A total of 100 trains are executed for each ANN architecture. For each run, weights are initialized randomly and a data set composed by 80,000 signals is used in order to train (70%), validate (15%) and test (15%) each architecture. In order to evaluate and compare to overall performance of each architecture, the expression of equation (6.15) was taken into consideration.

$$\Psi_k = W_e(ANN_{er}^k)(std_{er}^k) + W_t(ANN_t^k)(std_t^k) \tag{6.15}$$

Where k is an indicator of the ANN architecture. ANN_{er}^k represents the normalized average error of the 100 trained ANNs for the particular architecture k. ANN_t^k is the normalized average time that an architecture m took in the training phase. std_{error}^k and std_{time}^k are the standard deviations of the normalized error and training time respectively for a particular ANN architecture k. W_e and W_t are global weights

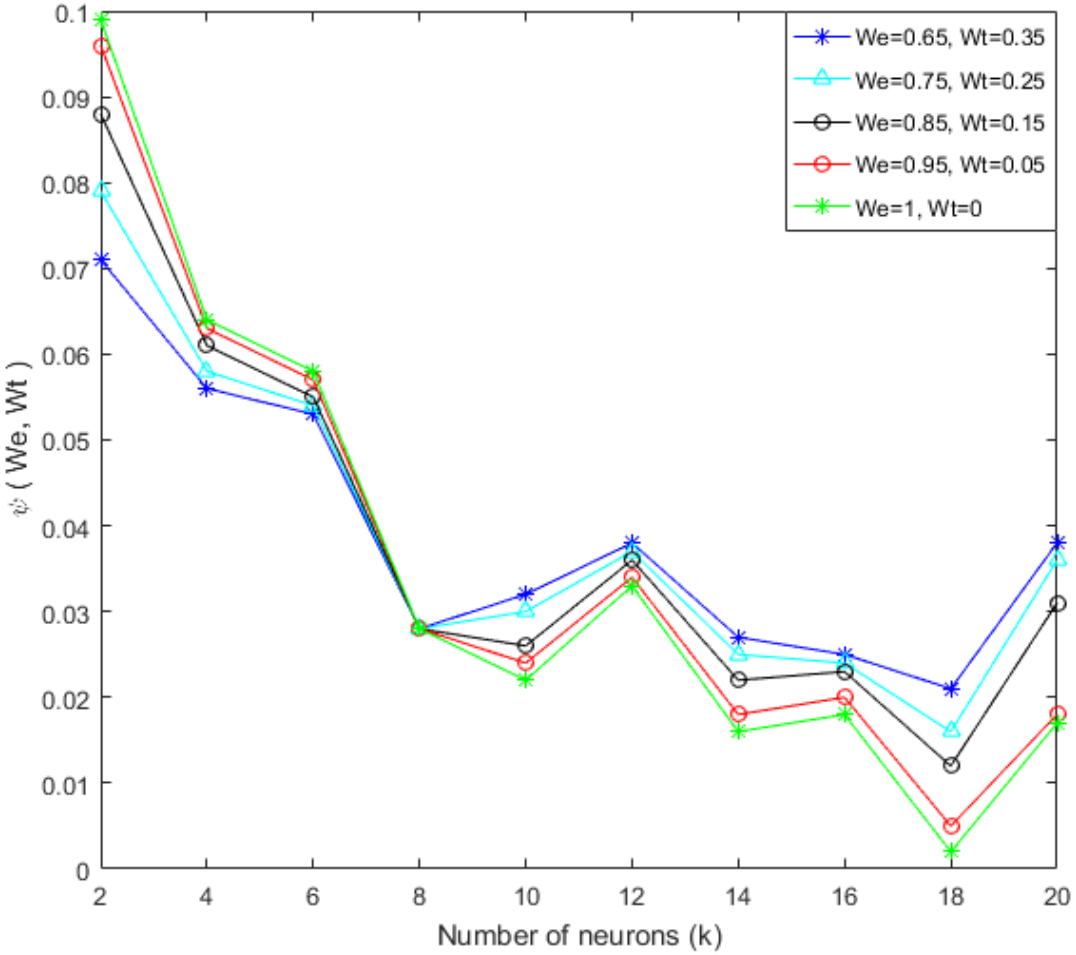


Figure 6.6: Neural Network performance for different number of neurons

which indicate the impact that errors and training times have respectively in the performance expression. Both parameters are related in the following way: $W_e + W_t = 1$. In this work the overall performance of each architecture k is considered for high values of W_e and therefore low values of W_t. This constrain is considered in the present work in order to give more relevance to the error optimization instead of the consumed training time.

From Fig. 6.6, it is possible to observe that the architecture of 18 neurons in the hidden layer presents the best overall performance in terms of error and training time minimization. According to this, the ANN architecture of 18 neurons that presented the highest performance among the 100 trains was used for classification purposes. The final ANN architecture used in this work is shown in Fig. 6.5.

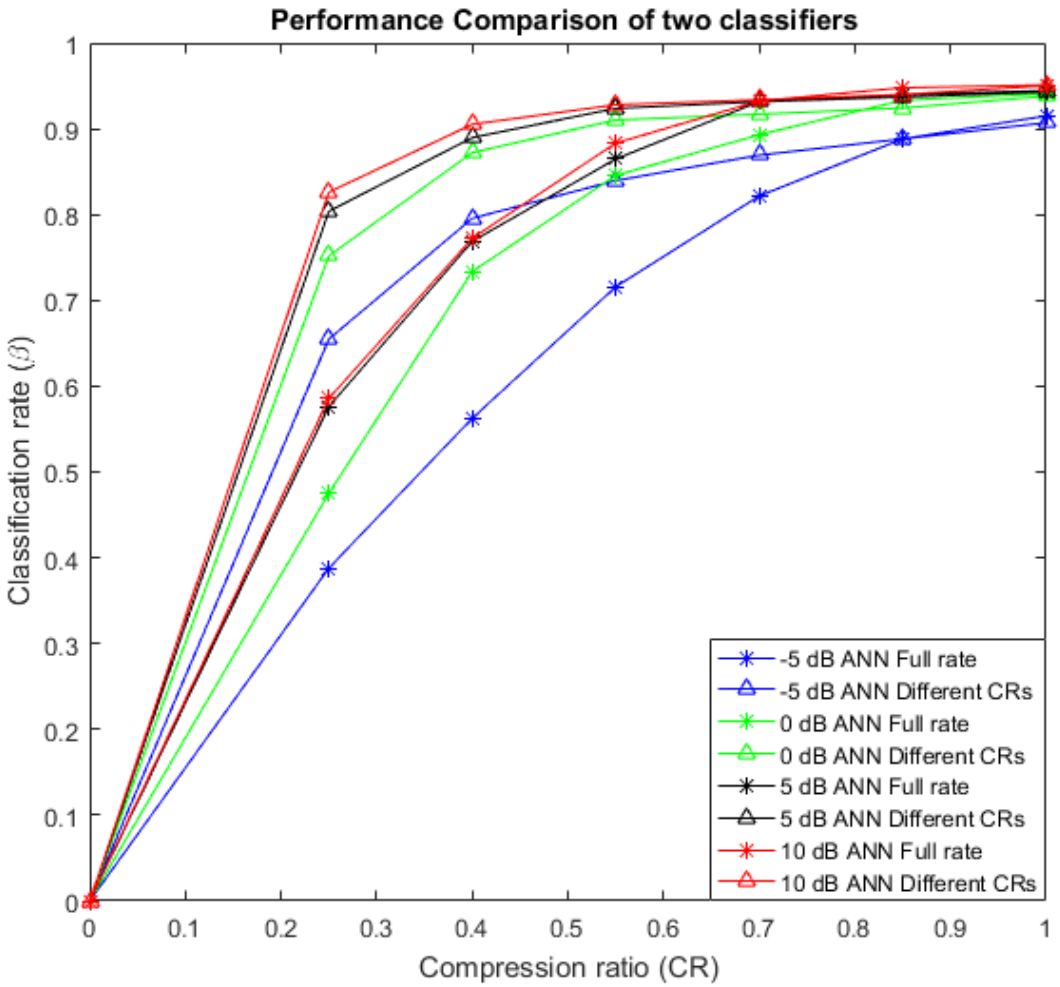


Figure 6.7: Performance comparison of the two proposed ANN based classifiers. One is trained at Nyquist rate samples and the other is trained for samples obtained with different compression ratios.

The proposed algorithm can be summarized as follows: the receiver observers a WB spectrum, which consists of multiple NB signals. The compression ratio is set to a particular value and WB is sampled using random sampling. Then the measurement matrix, S_c is collected at receiver and WB is estimated from sub-Nyquist samples using BP. After the reconstruction of Nyquist rate WB signal from sub-Nyquist samples, SCF is computed and features related to $\alpha-profile$ are extracted for different type of signals. Then, these extracted features are fed into previously trained ANN in order classify NB signals. The ANN classifies each NB signal as "legitimate" or "jamming" signal and eventually, optimum value for SNR and compression ratio is obtained. The pseudo-code of the proposed algorithm is outlined in Algorithm 4

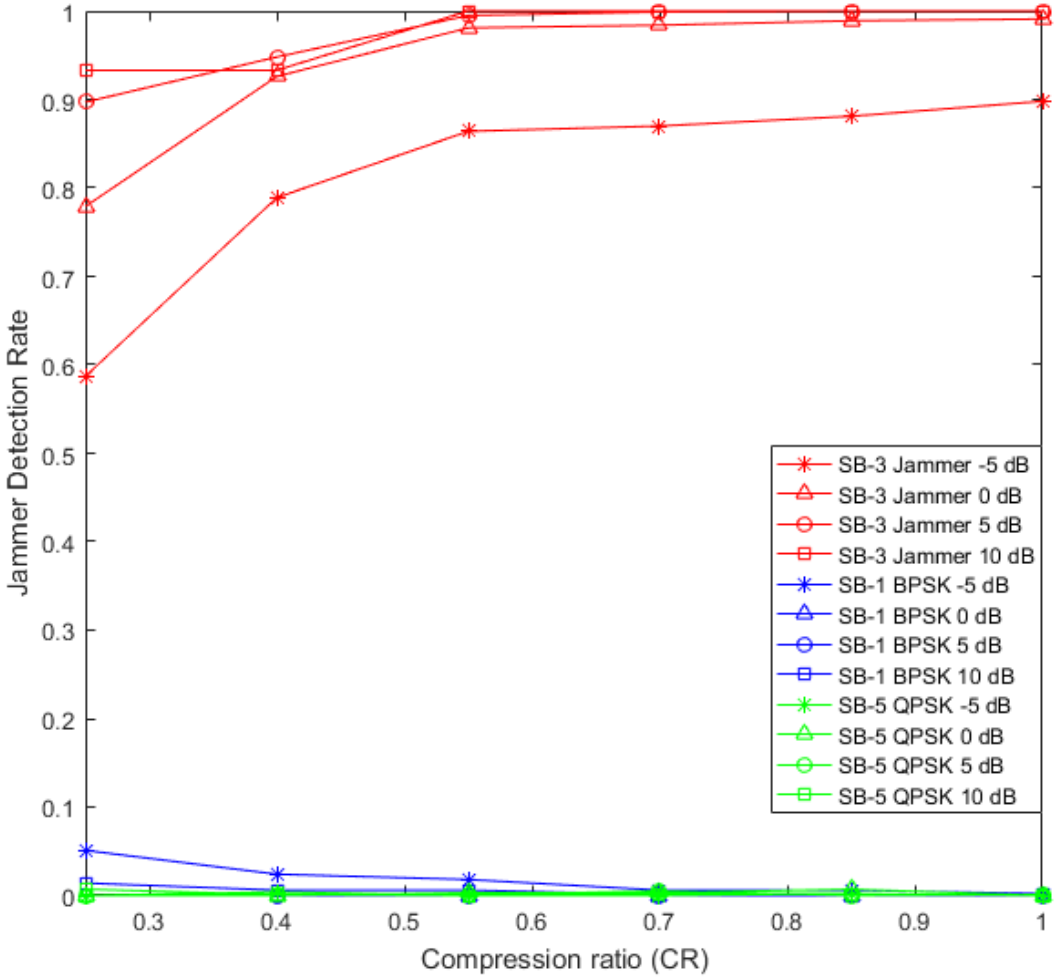


Figure 6.8: Performance of Jammer Detection Algorithm over various compression ratios and SNRs. SB-1 is used by BPSK, SB-5 is occupied by QPSK and SB-3 is occupied by jammer.

and a block diagram describing the different steps involved is depicted in Fig. 6.4 .

In this work, two different approaches are adopted to train ANN. In first case, the ANN is trained for full rate (Nyquist rate) and tested against different compression ratios. In second case, the ANN is trained for different compression ratios and tested against various compression ratios.

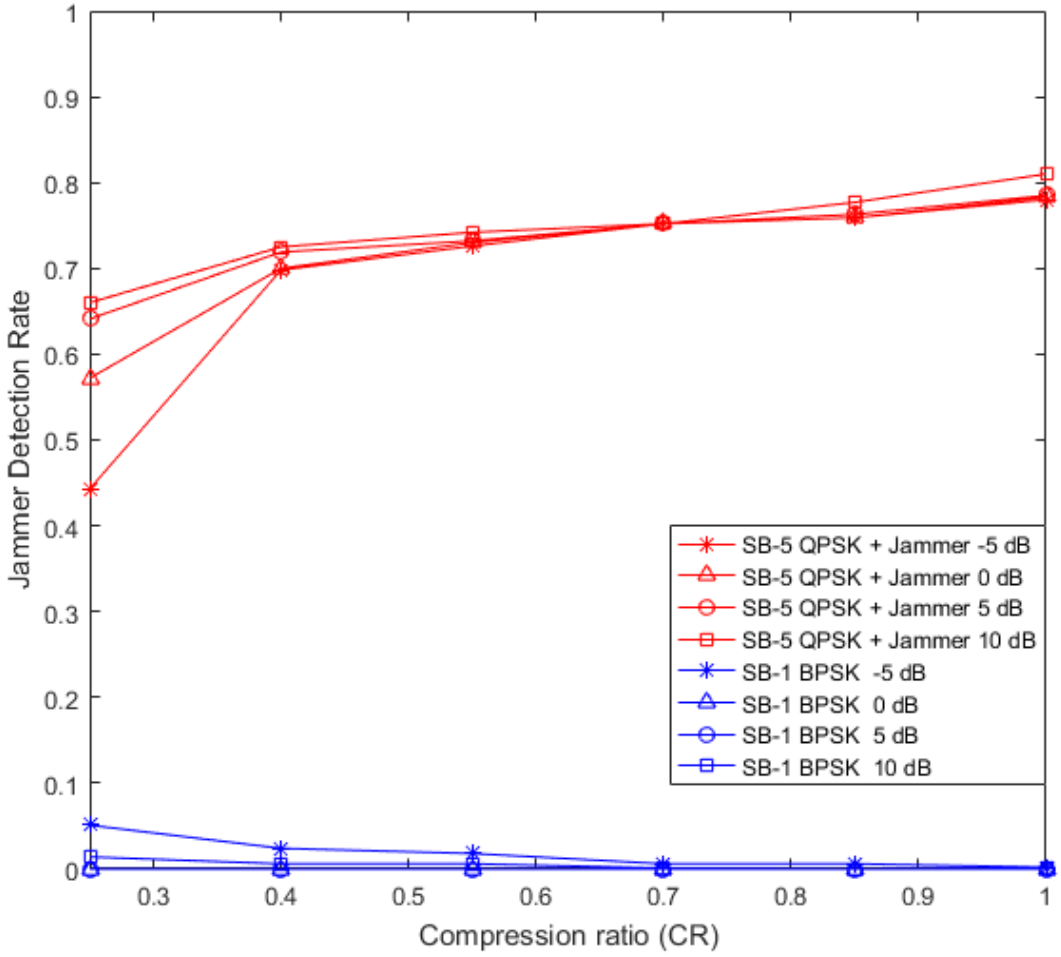


Figure 6.9: Performance of Jammer Detection Algorithm over various compression ratios and SNRs. SB-1 is occupied by BPSK signal while jammer has jumped from SB-3 to SB-5 to jam QPSK signal.

6.5 Experimental Results and Discussion

A WB spectrum of 50 Hz is assumed to be under observation by a cognitive radio terminal. This WB is divided into 5 SBs. These SBs can be occupied by NB signals or empty. For testing our proposed algorithm, we assume BPSK and QPSK to be our legitimate signals and sine wave is treated as a jamming signal. The receives WB signal is assumed to be affected by AWGN. From various recovery algorithms, we use BP algorithm for signal recovery through CS. The performance of proposed system is evaluated for various compression ratios $K/N = 0.25$ to $K/N = 1$ at different SNRs -5 dB, 0 dB, 5 dB and 10 dB respectively. We configured the system in three different

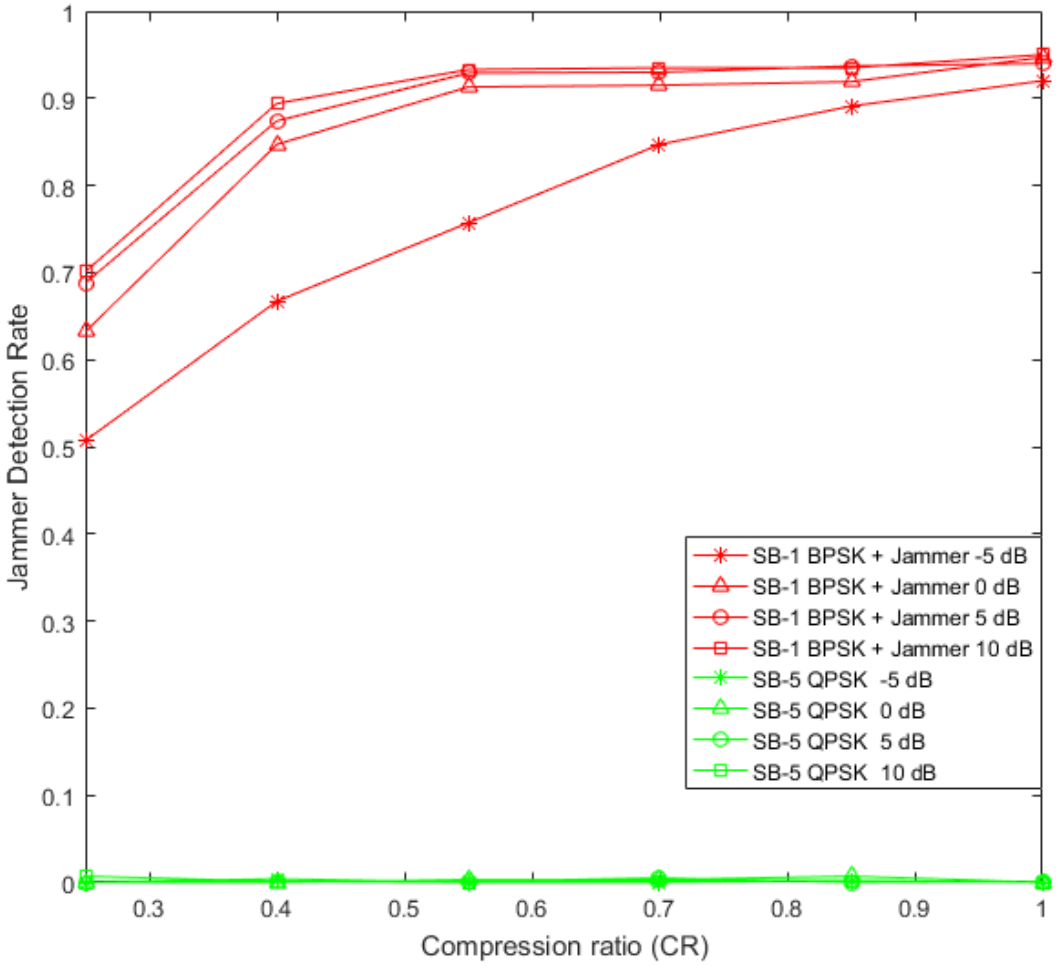


Figure 6.10: Performance of Jammer Detection Algorithm over various compression ratios and SNRs. SB-1 is occupied by BPSK signal while jammer has jumped from SB-3 to SB-5 to jam QPSK signal.

ways: (a) we placed the BPSK signal in SB-1, QPSK in SB-5 and jamming signal in SB-3; (b) BPSK signal is in SB-1 while jamming signal jumps to SB-5 to jam the QPSK signal; and (c) QPSK signal is in SB-5 while jamming signal jumps to SB-1 to jam the BPSK signal. The sampling rate is set at Nyquist rate of 100 Hz. Having the knowledge of presence of the licit signals, classification is performed at $\alpha \neq 0$, where AWGN exhibits no spectral features. The Monte-Carlo simulations are run for 1000 iterations for each signal type and for different compression ratios at each SNR. The results are shown for two different types of ANN based classifiers.

Algorithm 4 Pseudo-code for proposed algorithm

function JAMMER DETECTOR
    Initialize all SB states to "empty"
    Receive the WB signal (1)
    Set compression rate ← K/N
    Sample the WB using random sampling (12)
    Construct the measurement matrix ← S_c (12)
    Estimate the WB spectrum from compressed samples using BP (14)
    Compute the SCF of WB signal (8)
    Extract the $\alpha - profile$ (9)
    Divide WB into i SBs
    for $i = 1\,to\,I$, **do**
        Feed the $\alpha - profile$ for SB_i to previously trained ANN (15)
        Decision ← Signal type
    end for
    Performance: Classification rates (β) Vs Compression ratios (CR_S)
    Select → Best (K/N,SNR)
end function

6.5.1 Proposed classifier

The two ANNs selected based on the process described in 6.4.3, as mentioned previously, both the systems are trained with 80,000 signals, the first system is trained with full rate (Nyquist rate) samples and the second system is trained with various compression ratios. Both the classifiers are trained at different SNRs and carrier frequencies so that the system performance does not depend on the information of these parameters. The proposed systems correctly classifies signals with total classification rate of 0.93 and 0.885 respectively.

The performance of both systems is further evaluated for independent test signals, with different compression ratios and SNRs (-5 dB to 10 dB) from training signals. The comparison of overall classification accuracy for two classifiers is given in Fig. 6.7. The plot shows that at low SNRs and high compression ratios the system trained for different compression ratios outperforms the other system, which is trained only for Nyquist rate samples. For example, at -5 dB, it can be seen that the classification rate is 0.38 for first classifier and 0.65 for second classifier at $K/N = 0.25$. The classification accuracy is increased as K/N is elevated, and it is 0.56, 0.71, 0.82 and 0.80, 0.85, 0.86 at $K/N = 0.40, 0.55, 0.70$ respectively for two classifiers. However, for the high compression rates such as $K/N = 0.85, 1$, the classification rate is approximately same for both the classifiers and it is 0.88 and 0.90 respectively. The second classifier, which is trained for different compression ratios is selected for jammer detection on

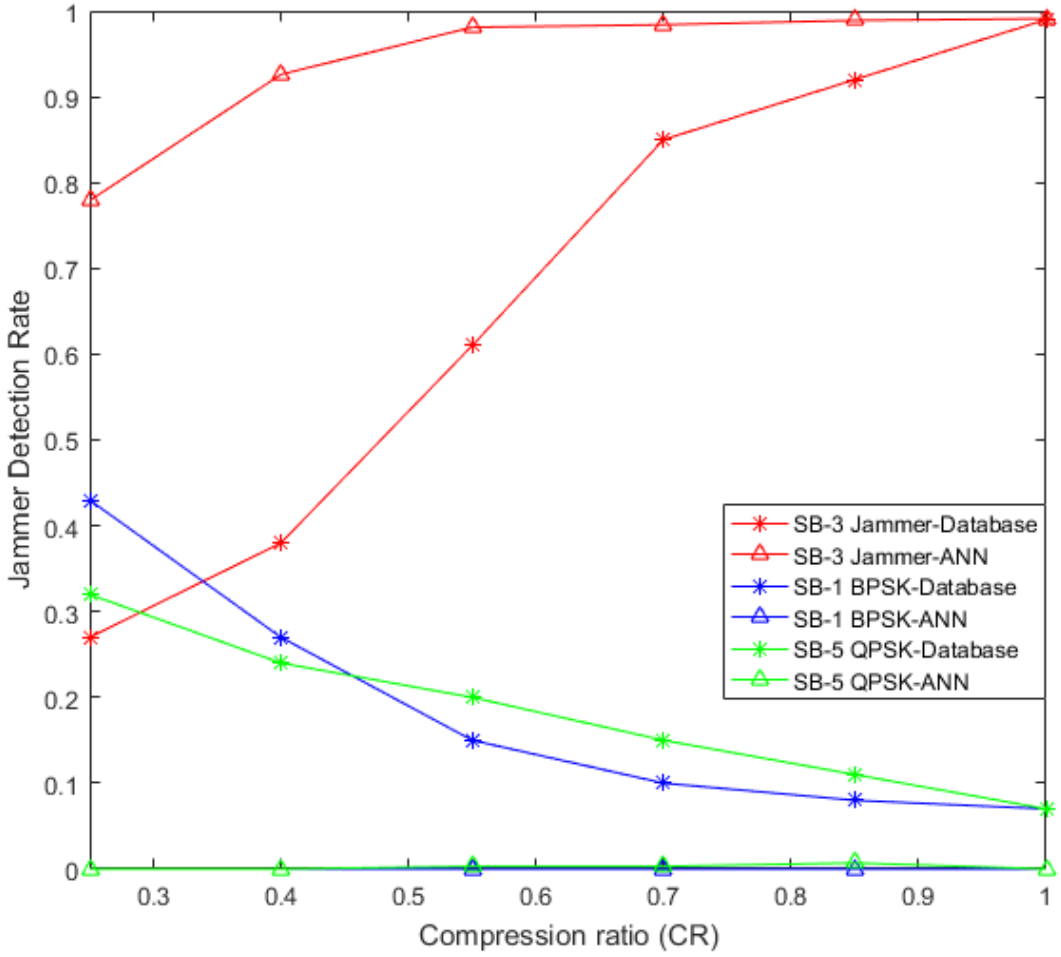


Figure 6.11: Performance comparison with database matching method

the basis of the above discussions.

6.5.2 Jammer Detection Rate

Fig. 6.8 shows the jammer detection rate versus the compression ratio for occupied SBs. It can be noticed from the figure that at 0 dB, the jammer detection rate in SB-3 is 1 for $K/N = 1.0$ while for that of SB-1 and SB-5 is approximately 0.0. This means that both in SB-1 and SB-5, the algorithm correctly classified the legitimate signals (BPSK as BPSK and QPSK as QPSK) with 98% accuracy, and miss classified with rate 0.02 BPSK as QPSK and QPSK as BPSK. By decreasing K/N ratio, the less samples are available for recovery of signal. As a consequence, the estimated SCF by the CFD is also an approximation. The jammer detection rate is 0.93, even K/N is

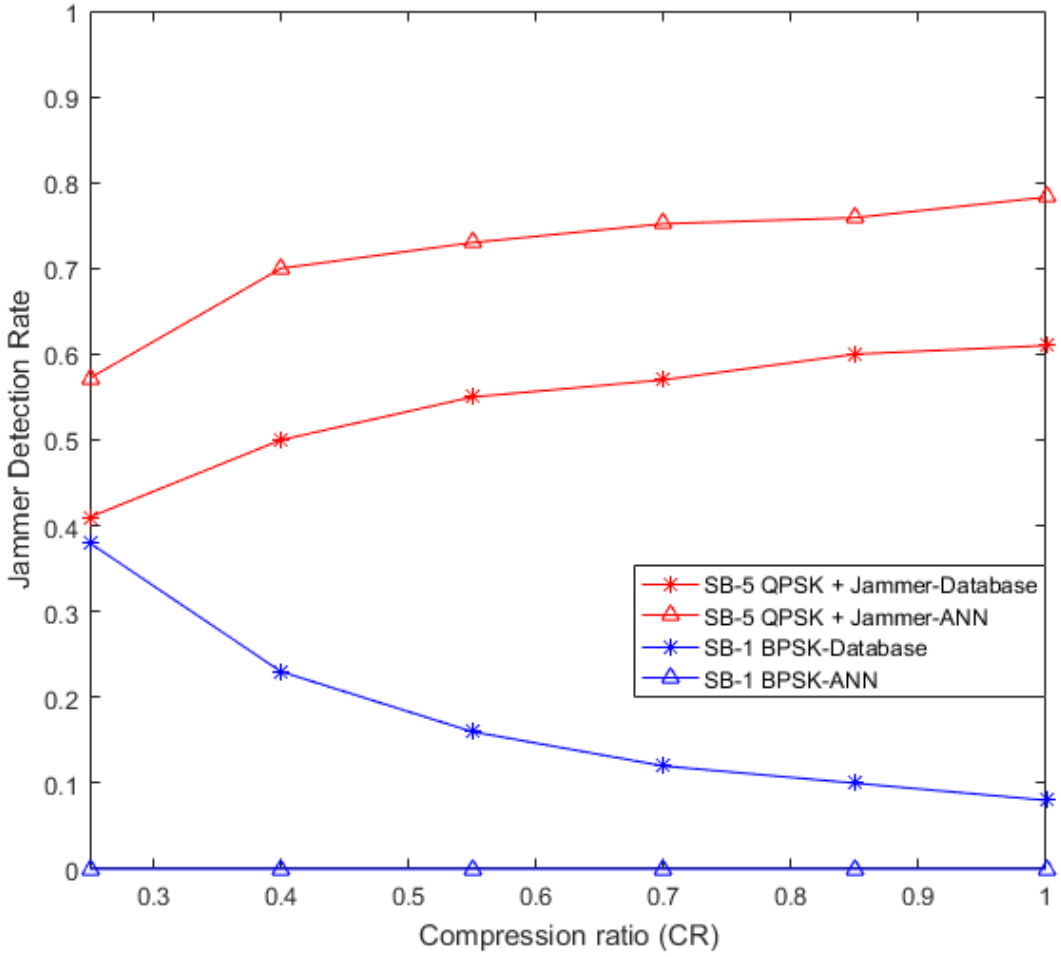


Figure 6.12: Performance comparison with database matching method

fallen to 0.4. This high accuracy is achieved due to the use of ANN as a classifier and training it for various compression ratios. When $K/N = 0.25$, the jammer detection rate is reduced to 0.779 while wrong classification of jammer as BPSK is 0.049 and that of jammer as QPSK is 0.039. It is worth noticing that jammer is classified as BPSK plus jammer class for rate of 0.13, which is in fact an illegitimate signal class.

Jammer detection rate versus the compression rate is plotted in Fig. 6.9 for second test configuration where the jammer jumped into SB-5 to jam the licit QPSK signals. It can be seen that the jammer detection rate falls to 0.78 in SB-5 as compared to 1 in SB-3 from first test scenario. It is because the algorithm is now classifying a mixture of Jammer and QPSK in SB-5 with a rate of 0.21. The jammer detection rate once again falls as the compression ratio is decreased due to the poor recovery of the WB

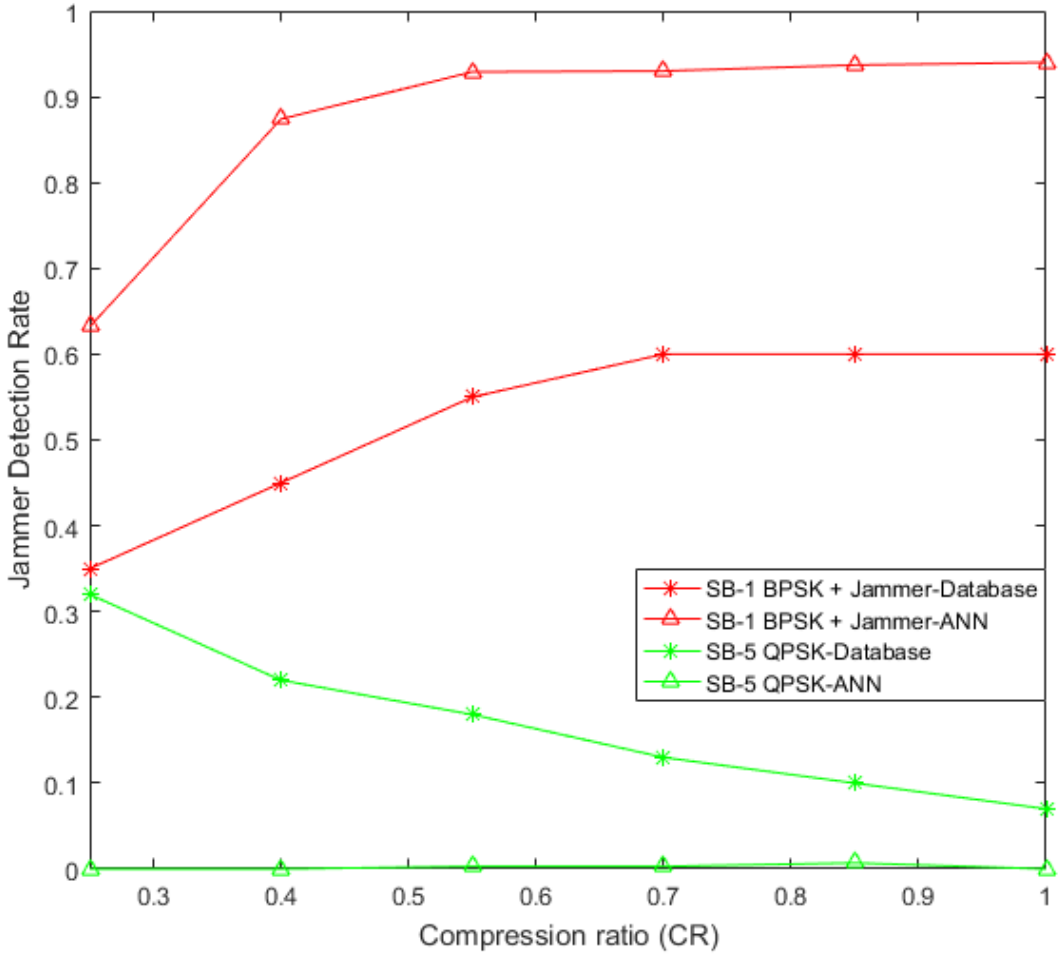


Figure 6.13: Performance comparison with database matching method

signal at low compression rates. For instance, at $K/N = 0.40$ the jammer detection rate is apporimately 0.7 in SB-5 with wrong classifications as QPSK to be 0.27.

In third test configuration, the jammer jumped to SB-1 in order to jam the BPSK signals. The jammer detection rate in this case is shown in Fig. 6.10. The jammer detection rate is 0.94 in SB-1, a 0.06 decreased is observed as compared to 1 in SB-3 from first test scenario. The detection rate is dropped as K/N is decreased and it is 0.87 at $K/N = 0.40$ and its mistaken rate as BPSK and QPSK is 0.038 and 0.019 respectively. The proposed algorithm performance is compared with[73] and it can be seen from Fig. 6.11-6.13 that the introduction of ANN not only increases the classification rate, but also greatly improve the jammer detection rate. In [73] classification was made on simple comparison of parameters from database. The

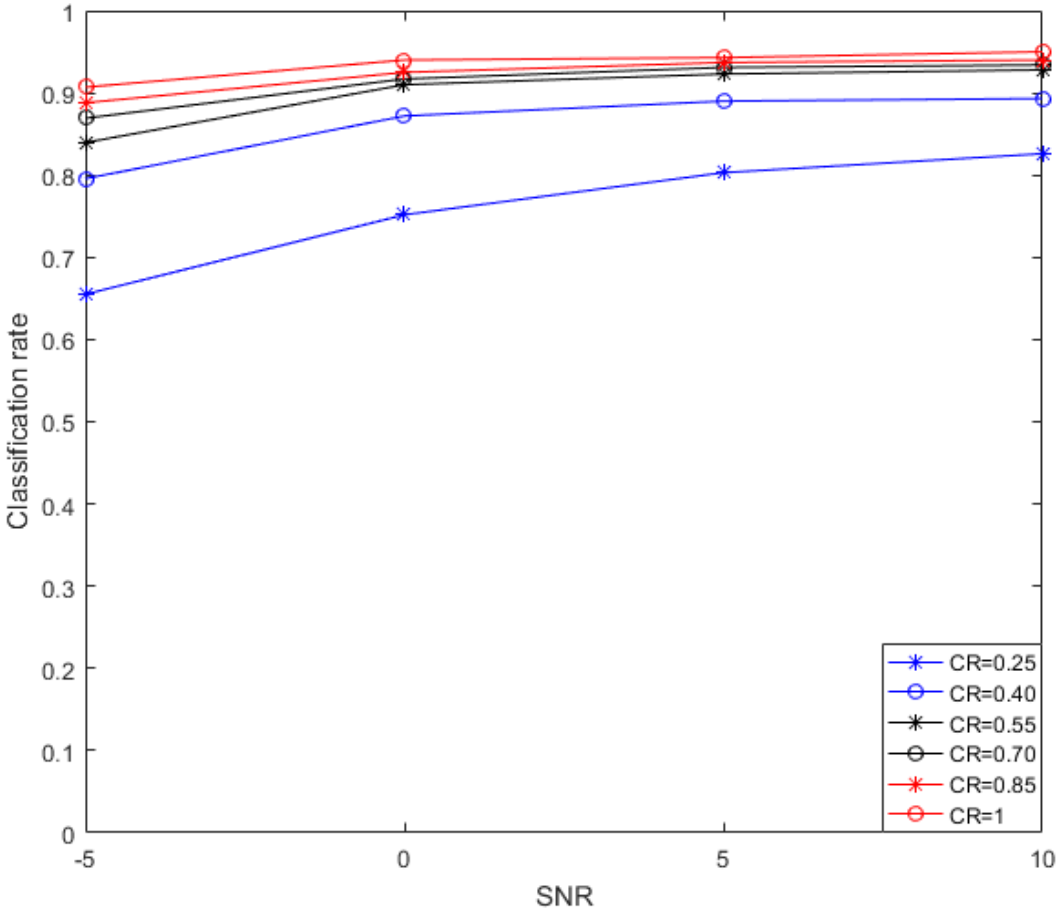


Figure 6.14: Robustness of proposed algorithm

robustness of the algorithm is shown in Fig. 6.14. It can be seen, even for low compression ratio of 0.4, the classification rate is approximately 0.87 at 0 dB and 0.8 at -5 dB. This demonstrates that proposed algorithm can efficiently work in an environment where noise level exceeds the signal level. Therefore, this algorithm is robust against noise.

The purpose of the designed algorithm is also to determine an optimum value for compression ratio and SNR, which reduces the overall cost of the system under consideration. The signals can be further categorized into two broad classes, licit signals (BPSK, QPSK) and illicit signals (Jammer, BPSK plus Jammer, and QPSK plus Jammer). The illicit case is more harmful for any communication system and the SBs occupied by these signals must be avoided. Table 6.1 presents the classification rate for $SNR = -5$ dB and $K/N = 0.40$. The algorithm classified BPSK and

QPSK for 95% and 98% as a legitimate signals (BPSK, QPSK) consecutively, while for 5% and 2% algorithm wrongly classified as the jamming signal (Jammer, BPSK plus Jammer and QPSK plus Jammer). Similarly, Jammer, BPSK plus Jammer and QPSK plus Jammer are correctly classified for 96%, 90% and 73% as illicit signals and wrongly classified as legitimate signals for 4%, 10%, and 27% respectively.

Table 6.2 shows signal classification rate at $SNR = 0$ dB and $K/N = 0.40$. The BPSK and QPSK are classified 100% and 98.5% as licit users, respectively. Similarly, jammer is correctly detected as illicit signal for 97%. When the jammer jumps into the band occupied by the BPSK signal, the band is for 94.3% classified as illegitimate band. When the jammer jumps to jam QPSK, the algorithm correctly classify it as illegitimate signal for 73%.

Therefore, by analyzing the Fig. 6.7, Table 6.1 and Table 6.2, it can be concluded that a -5 dB and 0.40 would be a smart choice for SNR and compression ratio, which means this technique is robust to noise and can save 60% of sensing energy . Hence, it is definitely an adequate choice for two broad signal classes.

This work, considered a constant jammer that send out random bits without following any medium access control (MAC)-layer protocols. It will be interesting to use this algorithm to detect other types of jammers, for example deceptive and reactive jammers [20].

6.6 Conclusion

In this chapter, we proposed a cyclic feature based jammer detection algorithm for WB cognitive radio using ANN. The WB is considered to be composed of several NB signals. To ease the A/D complexity, CS was used for recovering the Nyquist rate samples of the WB signal from sub-Nyquist sampling. The recovered WB signal was then fed to the CFD to compute the SCF of the signal. The $\alpha - profile$ is extracted and fed to two different ANNs which were previously trained. The classification performance of both the ANN based classifiers was evaluated at various SNR and compression rate values. The classier trained for different compressed ratios is selected on the basis of its good performance at low SNR and K/N as compared to the classifier trained at Nyquist rate samples. The proposed algorithm appears to perform well at various SNRs values down to -5 dB. Since the SCF of different signals are quite different, it appears to be a very effective parameter to use in classification. Furthermore, it is shown that the ANN based classifier significantly increase the performance as compared to plain database matching methods.

Table 6.1: Signal classifications for CR = 0.40 at -5 dB

Test Signal	BPSK	QPSK	Jammer	BPSK Plus Jammer	QPSK Plus Jammer
BPSK	935	15	24	26	0
QPSK	100	889	4	1	6
Jammer	26	14	789	163	8
BPSK Plus Jammer	79	18	218	667	18
QPSK Plus Jammer	2	273	13	14	698

Table 6.2: Signal classifications for CR = 0.40 at 0 dB

Test Signal	BPSK	QPSK	Jammer	BPSK Plus Jammer	QPSK Plus Jammer
BPSK	938	62	0	0	0
QPSK	35	950	0	0	15
Jammer	17	12	926	40	5
BPSK Plus Jammer	38	19	79	847	17
QPSK Plus Jammer	2	268	12	18	700

In the end, algorithm determine the optimum value for compression ratio and SNR, in order to reduce the sensing energy and to work in an environment where noise level exceeds the signal level. The algorithm appears to classify the signals with a high accuracy in noisy channels and can save more than half of the sensing energy. Additionally, such a jammer detection algorithm could be helpful in formulating intelligent anti-jamming strategies for WB cognitive radio systems.

Chapter 7

Practical Implementation of Spectrum Characterization for Wide-band Radios

7.1 Introduction

In the framework of cognitive radio (CR) and dynamic spectrum access (DSA), spectrum sensing is the fundamental method which provides radio devices with information about the wireless spectrum in the surrounding environments consisting of signals with different characteristics, such as different modulation schemes, different communication standards, or different objectives. In the later case, signals are defined as legitimate signals or jammers. In this chapter, a new Cyclic Spectral Intelligence (CSI) algorithm is proposed which exploits the cyclostationary features of digitally modulated signals and use an artificial neural network as a classifier. This algorithm is based on the cognitive cycle to acquire self-awareness from spectrum measurements.

The process for the realization of a large dataset consisting of experimental data generated by spectrum measurements is also described in this chapter. The main purpose for which the proposed dataset has been created is research in the field of PHY-layer security and Cognitive Radio. A Software Defined Radio (SDR) platform has been used to generate modulated signals in a specified band which are stored for off-line applications. The proposed CSI algorithm has been validated on the collected experimental dataset and the results highlight a classification rate of approximately 1 even at low transmit power.

The remainder of the chapter is organized as follows: Section 7.2 outlines the background related to this work. The proposed cyclic spectral intelligence algorithm is introduced in Section 7.3 which is based on a cognitive cycle consisting of five

steps. *Sensing* described in Section 7.4 along with the testbed architecture and the data acquisition, *processing* is presented in Section 7.5. The *cyclostationary feature analysis* and the *neural network classifier* are both described in Section 7.6, while *acting* and *learning* steps in Section 7.7 conclude the cognitive cycle. Validation of the proposed algorithm on experimental data is made in Section 7.8. Finally, chapter is concluded in Section 7.9.

7.2 Background

Recent advances in software defined devices and machine learning, in addition to results obtained in neuroscience, open new horizons towards innovative technologies in different fields including Cognitive Radio (CR) [37], [48].

CR can be defined as an intelligent and dynamically reconfigurable radio that can adaptively regulate its internal parameters in response to the changes in the surrounding environment. To this end, research is now focussing on learning mechanisms based on some of the existing machine learning techniques [24].

Basically, CR deals with the growing demand and shortage of the wireless spectrum. In order to utilize the spectrum efficiently, TV white spaces (TVWS) [89] allows secondary users to use licensed spectrum bands provided that they change their access strategies to care for the primary users. With respect to unlicensed communications, the available channel is not fixed and, consequently, the transmitter operates at different carrier frequencies, modulation techniques, and transmit powers.

In literature, various spectrum sensing techniques have been proposed for CRs, such as, energy detection [17], cyclostationary feature detection (CFD) [56], matched filtering detection [112] wavelet transform [123]. Among these methods, the CFD is capable of detecting the primary signal from the interference and noise even in very low signal-to-noise ratio (SNR) regions [49]. This performance is achieved at the cost of increased implementation complexity. The Federal Communications Commission (FCC) of the United States has suggested CFD as an alternative to improve the detection sensitivity in CR networks. Generally, energy detector fails at low SNRs while matched filtering detector requires a dedicated receiver structure which may not be possible in a practical cognitive radio terminal. CFD exploits the cyclostationarity of modulated signals by detecting spectral peaks in spectral correlation function (SCF) or spectral coherence function (SOF) [45, 93, 96], which are sparse in both angular (f) and cyclic (α) frequency domain. Major advantage of CFD based detector lies on its abilities to perform better than energy detector at low SNR values and to distinguish

different modulated signals. Furthermore, the cyclic spectral analysis has been used as a robust tool for signal classification when the carrier frequency and bandwidth information is unavailable [111], [61]. A comparison among the most common sensing methods in terms of complexity and accuracy is made by [118].

On the other hand, though, radio communications in wireless environments introduce security issues due to external attacks from malicious devices owing to the broadcast nature of radio propagation. In particular, the PHY-layer is extremely vulnerable to jamming attacks.

Radio frequency (RF) jamming refers to the process of illegitimate RF transmission on one or more RF channels with the objective of causing maximum distortion to the communication of the targeted system. Spectrum sensing information plays a key role in anti-jamming systems. This information may be used to detect potential jamming entities [80], [72], [73] and to take proactive measures to ensure communication continuity [70] and security [21]. Moreover, a history of observations can be maintained and used to devise more effective anti-jamming tactics [78].

Considering that, a Software Defined Radio (SDR) platform has been used to generate modulated signals in a specified band. The testbed is remotely controlled and can be employed in on-line applications. Moreover, the generated data can be also stored in datasets and used off-line.

Although previous work based on the aforementioned platform was carried out in anti-jamming scenarios such in [23] and [74], there has never been stored a large amount of data and organized for off-line applications.

7.3 Cyclic Spectral Intelligence

The principal idea behind the Cyclic Spectrum Intelligence algorithm is to continuously monitor relevant RF spectrum activities, identify potential threats to the communication, and take proactive measures to ensure communication robustness and secrecy. For doing so, the algorithm relies on the reliable spectrum sensing mechanism, correct identification and extraction of the relevant parameters, and secure software unsubjected to tampering. In comparison with the Spectrum Intelligence algorithm in [25], the proposed algorithm employs a cyclostationary feature algorithm to extract the α-profile feature from the detected signals which is then fed to a neural network to classify the waveforms present into the observed spectrum. The functional process of the Cyclic Spectrum Intelligence algorithm can be represented in the form of the Cognitive Cycle, as shown in Fig. 7.1, consisting of 5 blocks: *Sensing*,

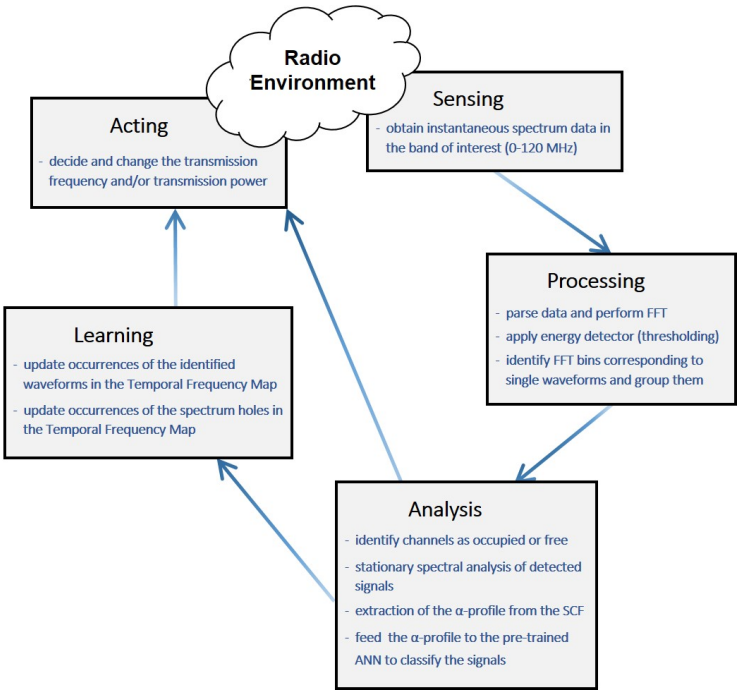


Figure 7.1: Diagram of the Cognitive Cycle for the proposed Cyclyc Spectral Intelligence algorithm.

Processing, *Analysis*, *Learning*, and *Acting*. *Sensing* and *Acting* blocks represent the interface with the external radio environment. The Cognitive Cycle is described in the following sections.

7.4 Sensing

Acquisition of the wideband RF spectrum, is performed periodically for the frequency band of interest. This may be done by taking either a quiet or an active approach, depending on the implementation of the architecture. Quiet approach implies that the radio is able to performing sensing simultaneously with transmitting/ receiving, whereas in active sensing, the radio needs to stop transmitting/receiving while sensing takes place.

In order to describe the *sensing* step, the testbed architecture is firstly introduced along with the data acquisition.

7.4.1 Testbed Architecture

The testbed employed to generate real-data is a SDR platform which consists of two Secure Wideband Multi-role - Single-Channel Handheld Radios (SWAVE HHs) shown in Fig. 7.2(a), the first one is the transmitter while the second one receives the wideband signal, connected through a dual directional coupler [25].

The fully operational SDR radio terminal SelexES (2013), SWAVE HH (from now on referred to as HH), is capable of generating a multitude of wideband and narrowband waveforms. Currently, two functional waveforms are installed on the radio: SelfNET Soldier Broadband Waveform (SBW), whose channel bandwidth is adjustable in the range 1.25 MHz to 5 MHz with channel spacing of 2 MHz and data is modulated using a fixed digital modulation technique, and VHF/UHF Line Of Sight (VULOS), which supports two analog modulation techniques, Amplitude Modulation (AM) and Frequency Modulation (FM), while both channel bandwidth and channel spacing are adjustable up to 25 kHz [24].

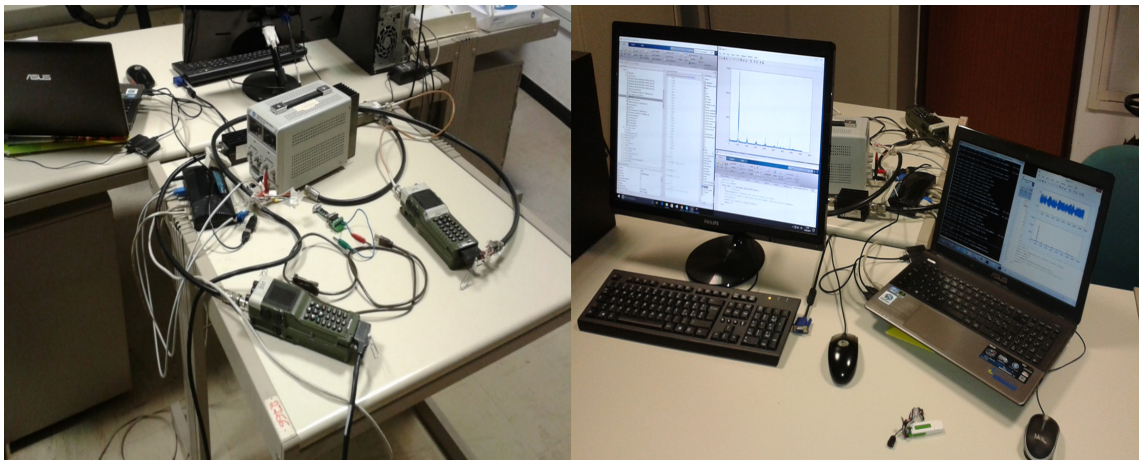
The radio provides operability in both Very High Frequency band, VHF (30 - 88 MHz), and Ultra High Frequency band, UHF (225 - 512 MHz). In VHF, analog to digital conversion is performed directly at RF and the frequency band scanned is always 0-120 MHz, while in UHF, the conversion is performed at intermediate frequency (IF) and the frequency band scanned depends on the center carrier frequency f_c of the radio ($[f_c - 35; f_c + 85]$ MHz) [23]. No selective filtering is applied before ADC. Broadband digitized signal is then issued to the FPGA, where it undergoes digital down conversion, matched filtering and demodulation.

Several interfaces are provided by the hypertach expansion placed at the bottom of each HH, specifically, 10/100 Ethernet, USB 2.0, RS-485 serial, DC power interface (max 12.7V), and PTT. The software architecture of the radio is compliant with the Software Communications Architecture (SCA) 2.2.2 standard.

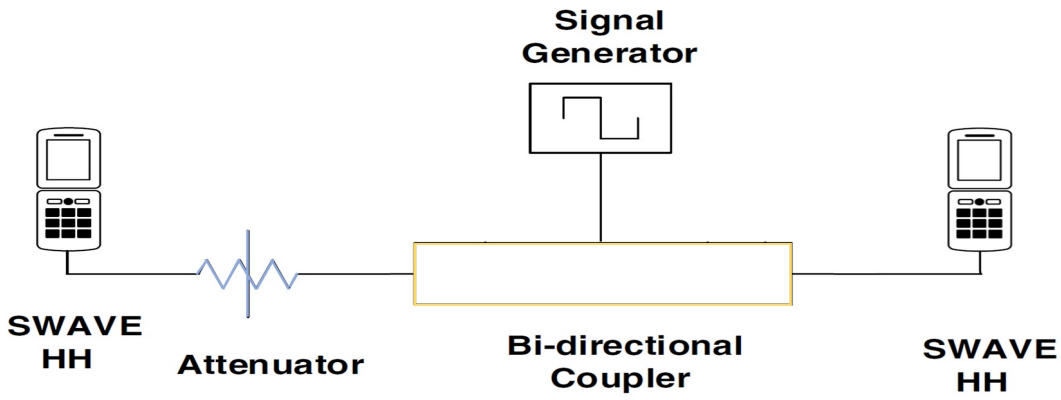
Maximum transmit power of the HH is 5W, with the harmonics suppression at the transmit side over -50 dBc. Superheterodyne receiver has specified image rejection better than -58 dBc. Because of the high output power of the radios, one programmable attenuator is included in the communication path and programmed to their maximum attenuation value - 30 dB.

Agilent 778D 100MHz-2GHz dual directional coupler with 20dB nominal coupling is used as communication medium between the two HHs.

Guided propagation exhibits several important advantages with respect to the over-the-air implementation: accurate and stable RF levels, repeatability of the experiments without the uncertainties characteristic to wireless transmission, possibil-



(a)



(b)

Figure 7.2: SDR testbed utilised to generate the dataset with wideband spectrum measurements: a) hardware platform, b) diagram of the main components of the testbed and their connections.

ity to connect test instruments and generators, avoiding regulatory issues related to transmitting outside of the allowed frequency bands.

The testbed provides support for remote control of HH's transmit and receive parameters through Ethernet and the Simple Network Management Protocol (SNMP v3) [25]. A general diagram of the testbed is shown in Fig. 7.2(b). Full details on the testbed architecture may be found in [24].

Concerning the spectrum sensing process, the HH's 14-bit Analog-to-Digital-Converter (ADC) performs sampling at 250 Msamples/s. Every 3 seconds, a burst of 8192 consecutive samples is buffered, and then outputted over the serial port at 115200 bauds. The samples are then parsed and transformed into the frequency domain using the Fast Fourier Transform (FFT). The bandwidth of the corresponding spectrum is 120

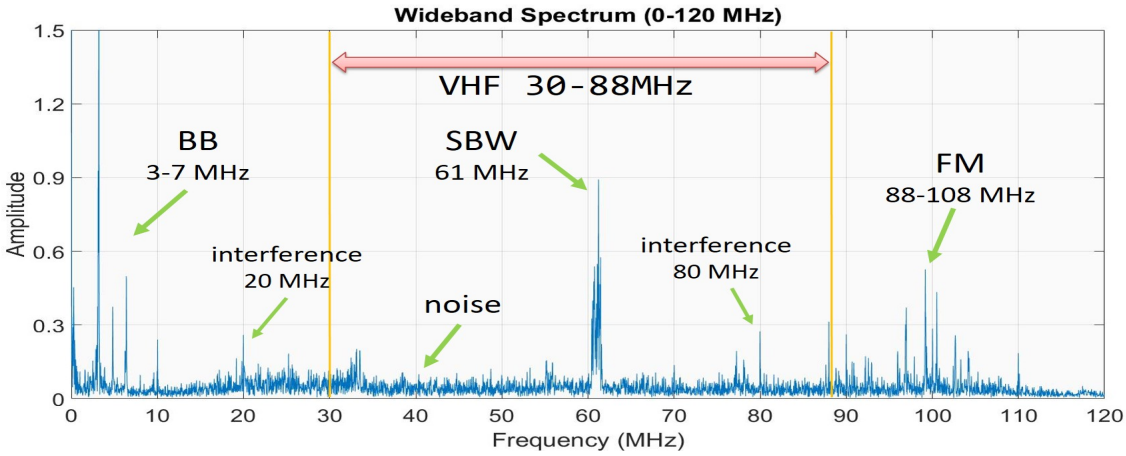


Figure 7.3: Spectrum observation in the 0-120 MHz (1 burst) which includes the SBW signal at 61 MHz and with transmitt power equal to -3dBm.

MHz wide around the center carrier frequency of the radio. Consequently, the effective resolution is 29.3 kHz/sample. In order to obtain higher frequency resolutions, two possible changes to the testbed are increasing the buffer size on the HHs, and finding ways to transfer spectrum data at higher baud rate [23]. Further details can be found in [24].

7.4.2 Data Acquisition

By means of the testbed described in the previous section, real-data is collected and stored in a dataset. To this end, the VHF transmission band where the radios are operable has been utilized, meaning that the spectrum sensing is performed for the frequency band of 0-120 MHz. The data consists of a large amount of spectrum observations containing a number of narrowband signals. More specifically, as shown in Fig. 7.3 (the blue line), each spectrum consists of a SBW signal (digitally modulated signal) transmitted by the transmitting HH device and a number of signals (from the environment) such as the FM signal (in the 88-108 MHz band) and an unknown signal at 0-7 MHz. The parameters of the SBW signal can be set remotely and, for the proposed research (described later in this report), the transmit power and the carrier frequency of the transmitted SBW signal have been considered which are given 4 different values (7dBm-full, 4dBm-half, -3dBm-one-tenth, and -12dBm-minimum for the transmit power; 41MHz - 51MHz - 61MHz - 71MHz for the carrier frequency). Consequently, the dataset consists of spectrum measurements grouped in 16 different configurations, as shown in Table 7.1. Each configuration consists of more than 2500 bursts. The corresponding time-domain samples have also been stored in the dataset.

7dBm - Full Power

f_c	I 41 MHz	II 51 MHz	III 61 MHz	IV 71 MHz

4dBm - Half Power

f_c	V 41 MHz	VI 51 MHz	VII 61 MHz	VIII 71 MHz

-3dBm - One-tenth Power

f_c	IX 41 MHz	X 51 MHz	XI 61 MHz	XII 71 MHz

-12dBm - Minimum Power

f_c	XIII 41 MHz	XIV 51 MHz	XVI 61 MHz	XVI 71 MHz

Table 7.1: Configurations for transmit parameters of the SBW signal in the collected dataset: carrier frequency and transmitting power.

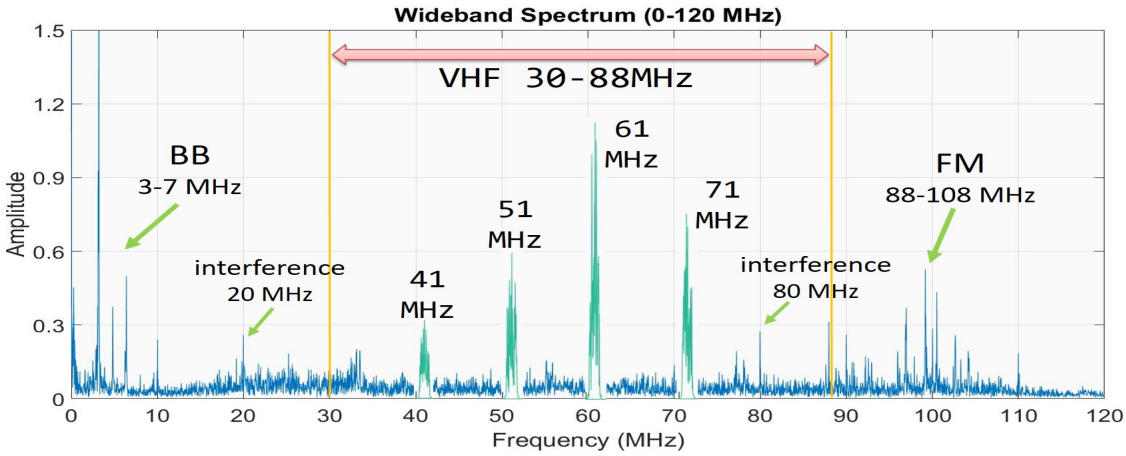
For the sake of clarification, in Fig. 7.4(a) the SBW signal has been overlapped to the 0-120 MHz spectrum, inside the VHF band, at the four different carrier frequencies with fixed transmit power (3dBm). While in Fig. 7.4(b), the 16 different configurations for the SBW signal can be seen. The minimum power for the transmit power makes the SBW level comparable with the noise level making difficult to differentiate them. In this chapter, only full and half transmit power have been considered for the experimental step in Sec. 7.8.

7.5 Processing

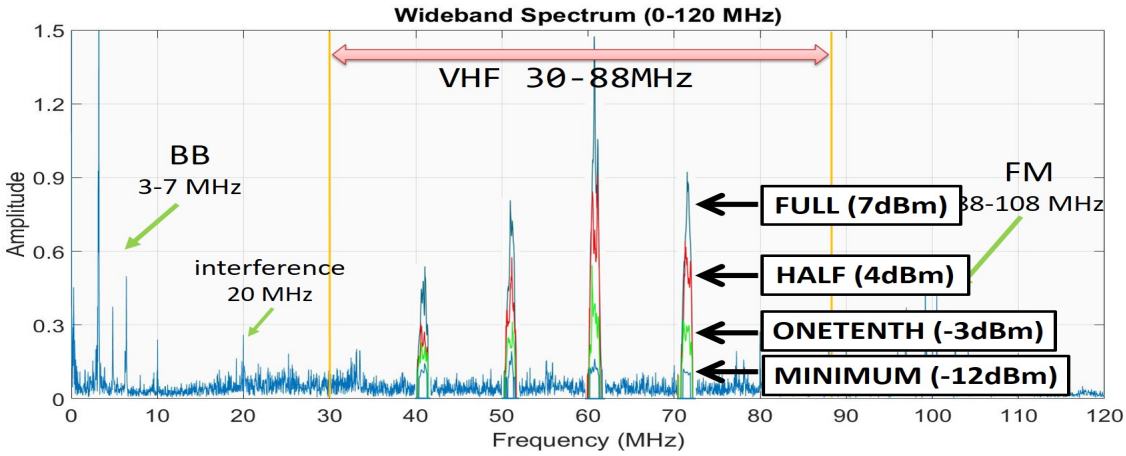
This section describes the pre-precessing step of real-data to detect frequency bins belonging to the different waveforms inside the spectrum. The main parameters for the pre-precessing process are also described.

First of all, the received spectrum observations are smoothed in the frequency domain through a simple moving average applied to the samples in order to reduce the wide/sharp fluctuations due to noise which can be seen in each received spectrum.

Then, based on a sensible choice for a specific threshold, the background noise is eliminated, keeping only the FFT bins corresponding to actual signals. Basically,



(a) SBW signal at four different carrier frequencies (41-51-61-71 MHz) in the 0-120 MHz spectrum



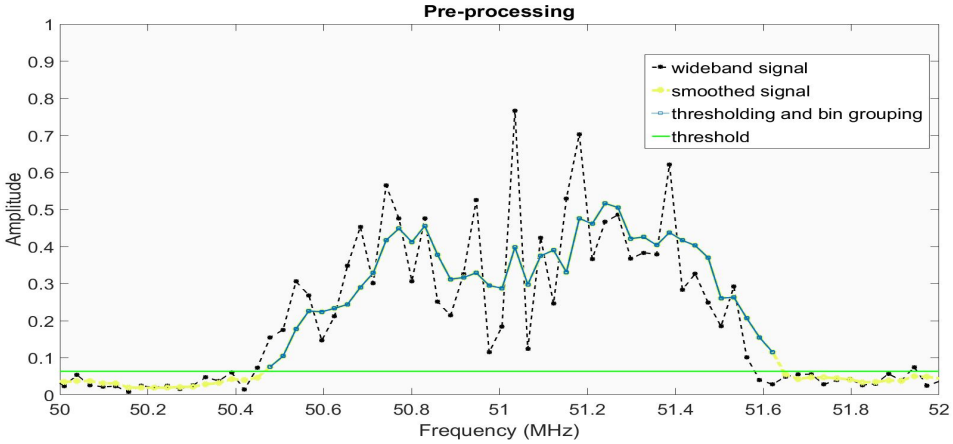
(b) SBW signal at four different carrier frequencies (41-51-61-71 MHz) and four transmit powers (full, half, one-tenth, minimum)

Figure 7.4: Spectrum observation (1 burst) with 16 different configuration for the carrier frequency and transmit power. In both the figures, the SBW signal is overlapped to the wideband spectrum for the sake of clarification.

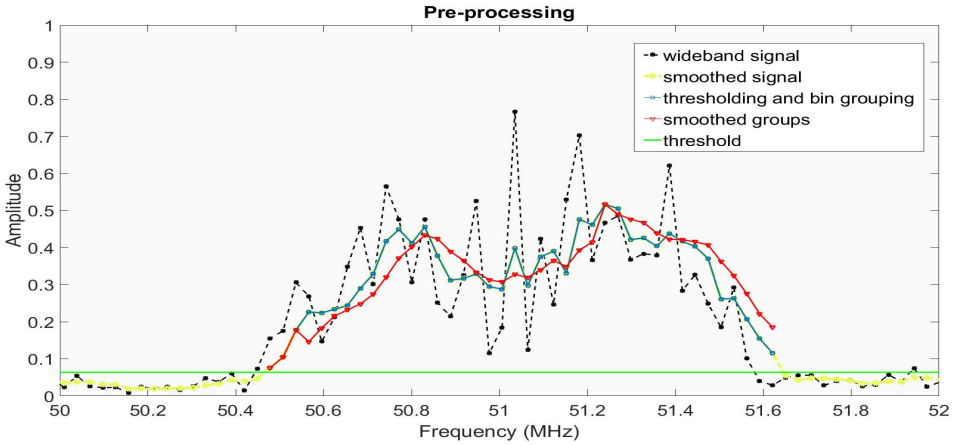
this process can be thought as an Energy Detector (ED) and formally corresponds to solving the decision problem between the following two hypotheses [25, 29]:

$$Z(n) = \begin{cases} \eta(n) & H_0 \\ S(n) + \eta(n) & H_1 \end{cases} ; \quad n = 1, ..., N_S \tag{7.1}$$

where $Z(n)$, $S(n)$ and $\eta(n)$ are the received signal, the transmitted signal and the noise samples, respectively. H_0 is the *null hypothesis* corresponding to the absence of the signal (in this case, received signal consists only of noise), and H_1 is the *alternative hypothesis* corresponding to the presence of the signal, while N_S is the



(a)



(b)

Figure 7.5: Pre-processing applied to the WB signal (in both the pictures, only the SBW signal is shown): (a) *WB signal*, *smoothed signal*, *thresholding and bin grouping*, and *threshold*; (b) also includes the waveform after *group smoothing*.

number of samples acquired during the sampling process.

Based on the Neyman-Pearson lemma, the most common approaches to finding the appropriate threshold are the Constant Detection Rate (CDR) and Constant False Alarm Rate (CFAR) detectors, where threshold is set adaptively depending on the SNR regime and the characteristics of the sensed wideband signal. However, even in adaptive thresholding, presence of interference may make the energy detector come to incorrect decisions.

In most applications, the analysed spectrum is underutilised (usage of licensed bands is an example [89]) which means that there is only a limited number of actual narrowband signals in the scanned wideband signal at any instant of time [23]. In

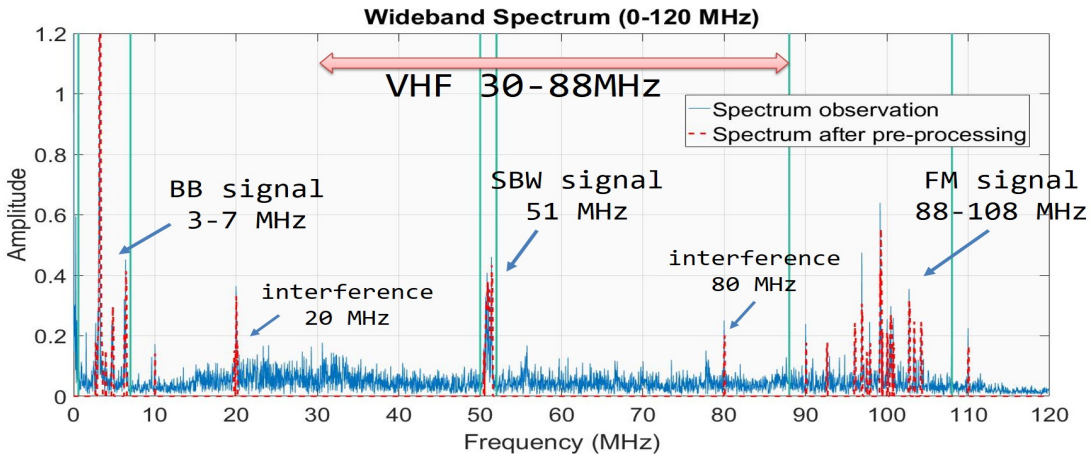


Figure 7.6: Wideband spectrum measurement before pre-processing (blue line) and after pre-processing (red line).

this scenario, suboptimal thresholding algorithms with low computational complexity, where CFAR or CDR performance is not necessarily achieved, can be considered. Indeed, it has been shown that the threshold $\hat{\delta}$ may be adaptively set based only on the mean value of the magnitudes of the scanned wideband signal [25], and given by:

$$\hat{\delta} = 2 \cdot \frac{1}{n} \sum_{n=1}^{N_S} |Z(n)| \tag{7.2}$$

K frequency bins are identified as a result of the thresholding process.

In a wideband and sparse spectrum observation there are L actual signals ($K > L$) each of them consists of a number of bins. For this reason, frequency bins corresponding to the same signal need to be grouped together. In high-SNR environments, consecutive samples can be grouped together and classified as single waveforms. However, in practical situations, some frequency bins may have erroneous magnitude values as a result of imperfect sampling and would thus be discarded during the thresholding phase. In this case, the bin grouping process considers two (o more) groups of consecutive bins as a single signal if they are close enough each other. More formally, the maximum acceptable distance (in Hz) between the two samples belonging to the same waveform is defined as:

$$d_{MAX} = M \cdot d_f \tag{7.3}$$

M is the maximum number of consecutive samples that could be erroneously disregarded, and d_f is the frequency resolution of the FFT, given by:

$$d_f = \frac{2 \cdot f_{max}}{N_S} \tag{7.4}$$

where f_{max} is the maximum resolvable frequency (which in case of Nyquist sampling equals to half of the sampling frequency). After the thresholding step, grouped waveforms undergo smoothing, in order to reduce impacts of the imperfect and erroneous sampling. For achieving this, a second stage moving average filter has been implemented. For a waveform that consists of nG grouped bins with magnitudes $S_1, \ldots, S_{nG}$, filtering with the window length W results in the filtered bins given by [23]:

$$S_f(n_i) = \frac{1}{P} \sum_{j=i-P+1}^{i} S_j; \quad i = P, ..., nG \tag{7.5}$$

So, each element in Eq. (7.5) is an average of the preceding P points.

Fig. 7.5(a) illustrates the difference between the original transmitted SBW signal, the corresponding smoothed signal, the sensed FFT bins, and the estimated signal after performing thresholding/bin grouping. While, in Fig. 7.5(b), the smoothed group corresponding to the SBW signal is also shown.

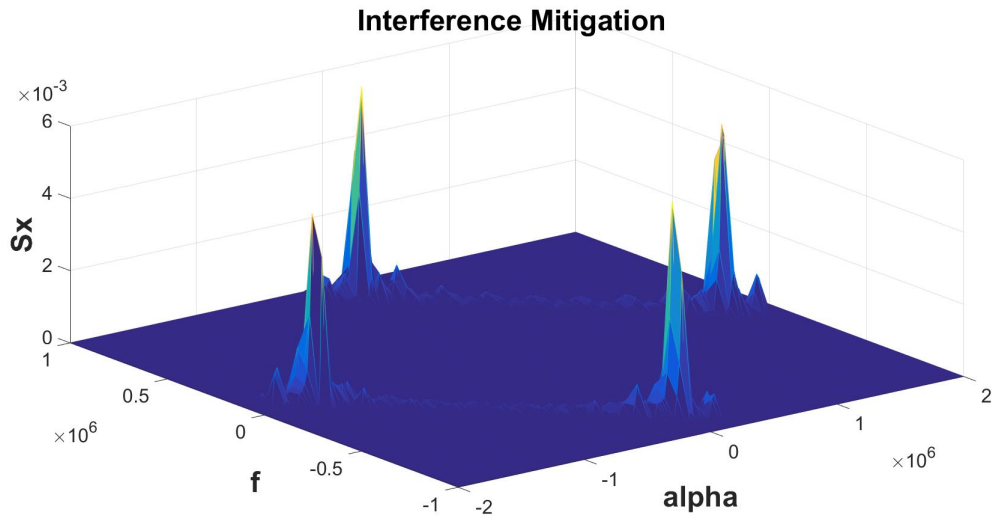
A comparison between the original wideband signal and the corresponding signal after having undergone the pre-processing is made in Fig. 7.6.

This concludes the frequency domain pre-processing phase which is applied to the collected wideband signals.

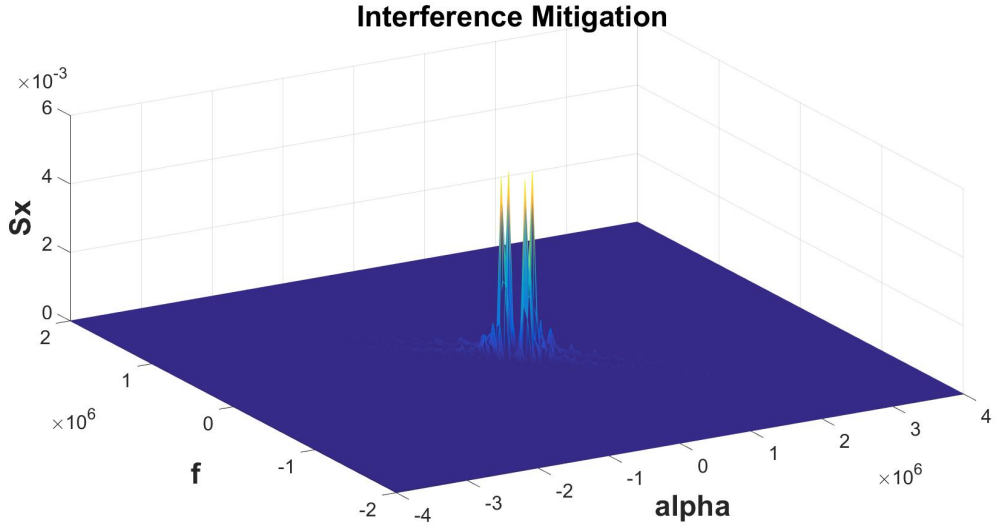
After this phase, the inverse Fourier transform is applied to produce the corresponding time domain signals from the pre-processed wideband spectrum measurements and, then, the SFD algorithm produces both alpha- and f- profile from the time-domain sub-signals as described in the following section.

7.6 Analysis

In this section, the classification process is described in order to present an application of the dataset to theoretical framework. After the pre-processing phase in Sec. 7.5, the waveforms are classified as either potentially malicious (PM) or friendly (FR). The former class refers to signals which aim to disrupt or degrade communications among legitimate users (belonging to the latter class). In the 0-120MHz wideband spectrum, the jammer is supposed to be the SBW signal (which is capable of changing its transmit parameters), while legitimate waveforms are the BB signal, interference at 20 MHz and 80 MHz, and the FM signal. In order to differentiate them, a cyclostationary feature based algorithm [77] with an Artificial Neural Network (ANN) as classifier [78] is applied to the dataset.



(a) SCF of the 3-7 MHz BB signal



(b) SCF of the SBW signal

Figure 7.7: CSF of two of the detected signals in the WB spectrum: (a) BB signal and (b) SBW signal.

7.6.1 Cyclostationary Feature analysis

A process $x(t)$ is said to be wide-sense cyclostationary with period T_0 if its mean $E[x(t)] = \mu_x(t)$ and autocorrelation $E[x(t)x^*(t+\tau)] = R_x(t,\tau)$ are both periodic with period T_0, in such case, they can be defined respectively as:

$$\mu_x(t+T_0) = \mu_x(t)\,; \quad R_x(t+T_0,\tau) = R_x(t,\tau)\,. \tag{7.6}$$

The autocorrelation function of a wide-sense cyclostationary process can be expressed in terms of its Fourier series components:

$$R_x(t,\tau) = \sum_{\alpha} R_x^{\alpha}(\tau)\, e^{j2\pi\alpha t} \tag{7.7}$$

Where $\alpha = \frac{a}{T_0}$ with a integer, $E[\cdot]$ is the expectation operator, α is the set of Fourier components, and $R_x^{\alpha}(\tau)$ represents the cyclic autocorrelation function (CAF) and gives Fourier components. CAF is given by:

$$R_x(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} R_x(t,\tau) e^{-j2\pi\alpha t} dt\,. \tag{7.8}$$

When $R_x(t,\tau)$ is periodic in t with period T_0, (7) can be expressed as:

$$R_x^{\alpha}(\tau) = \frac{1}{T_0} \int_{\frac{-T_0}{2}}^{\frac{T_0}{2}} R_x(t,\tau) e^{-j2\pi\alpha t} dt\,. \tag{7.9}$$

The Fourier Transform of the CAF is known as SCF and is given by:

$$S_x^{\alpha}(f) = \int_{-\infty}^{\infty} R_x^{\alpha}(\tau) e^{-j2\pi f\tau} d\tau \tag{7.10}$$

where α is the cyclic frequency and f the angular frequency. The major benefit of spectral correlation is its insensitivity to background noises. Since the temporal correlation of different spectral components are measured; and the spectral components of noise are completely uncorrelated in time due to the fact that noise is wide-sense stationary process, such noise does not play significant factor in the SCF. This fact allows the spectral correlation of a signal to be accurately calculated even at low SNRs. Furthermore, different types of modulated signals (BPSK, AM, FSK, MSK, QAM, PAM) with overlapping power spectral densities have highly distinct SCFs.

The SCF of the SBW signal and the 3-7 MHz signal in the 0-120 MHz spectrum are shown in Figs. 7.7(a) and 7.7(b), respectively.

Since SCF computation requires large amount of data, which makes it unreasonable for a classifier to operate on it in real time, the cycle frequency profile (α-profile) has been employed in this chapter as feature for classification. Specifically, the α-profile of SCF for a signal x is given by:

$$I(\alpha) = max_f[S_x^{\alpha}] \tag{7.11}$$

The α-profile of signals in the wideband spectrum of interest is shown in Sec. 7.8.

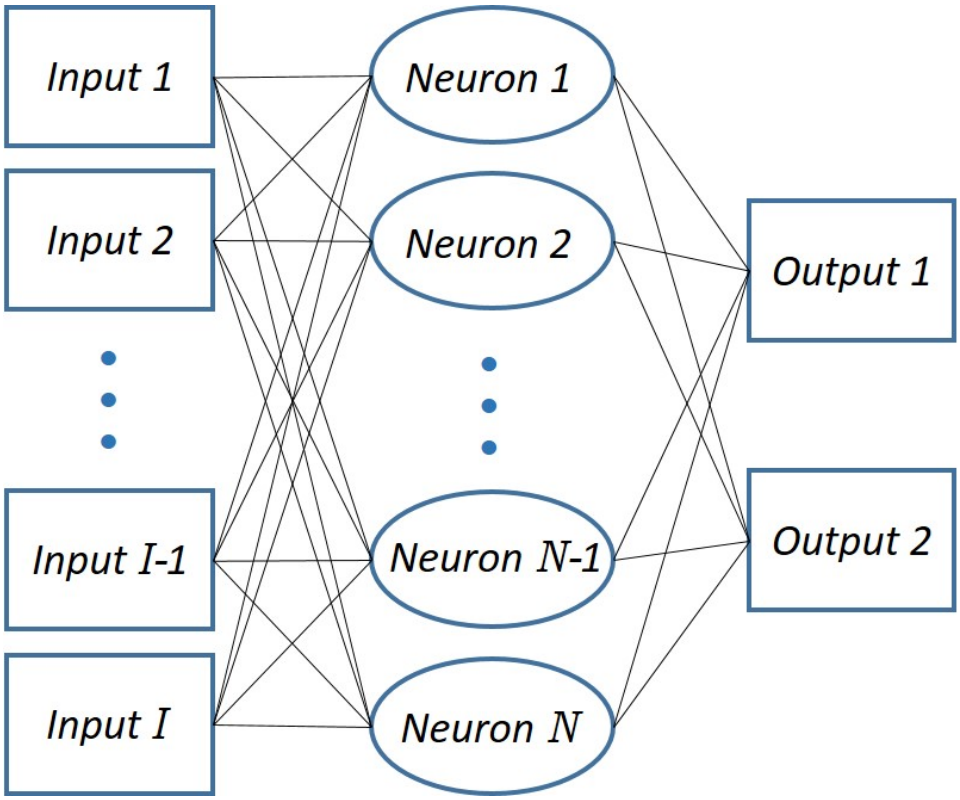


Figure 7.8: Proposed Artificial Neural Network used as classifier in the CSI algorithm with I inputs, one hidden layer with N neurons, and 2 outputs.

7.6.2 Neural Network Classifier

Our proposed system uses an Artificial Neural Network (ANN) as classifier due to its ease of implementation and potential to generalize any carrier frequency, symbol rate and phase offset. The system was designed to classify potential malicious (PM) and friendly (FR) signals. We trained the ANN to identify the two classes of signals defined at the beginning of this section. The SCF of the detected signals produces a large amount of data, which makes impossible for a classifier to work on it in real time. In order to reduce the amount of data for a classification stage, we used the α-profile as input feature for an ANN. Accordingly, the proposed ANN is composed by I inputs related to the dimensionality of α-profile, a single hidden layer whose N neurons use the hyperbolic tangent sigmoid as neural transfer function, and an output layer of two neurons related to each class of signal considered in this work. Each output value is in the range $(0, 1)$. Accordingly, the output class with the highest value between $(0, 1)$ is considered as the signal class. An ANN training based on the scale conjugate gradient propagation [69] is adopted.

The selection of a single hidden layer is proposed due to the classification process

simplicity of this particular problem, it was found that with a single layer results over the 99% of true positive classification were obtained for the 2 types of signal classes

Algorithm 5 Pseudo-code for proposed algorithm

function SIGNAL RECOGNITION IN WB SPECTRUM
    Set the number of bursts to be acquired $\rightarrow k$
    Receive and sample the wideband signal at or above Nyquist rate for all k bursts $\rightarrow N_S$ amplitude values
    Data parsing $\rightarrow N_S = 2^x$ amplitude values
    Perform FFT $\rightarrow \frac{N_S}{2}$ frequency bins with magnitudes M
    Fisrt smooth by moving average
    Calculate mean value of $M \rightarrow M_{mean}$
    Based on M_{mean}, set the energy thethreshold $\rightarrow \hat{\eta}$
    for $i = 1$ to $\frac{N_S}{2}$ **do** (for each frequency bin)
        if $M(i) > \hat{\eta}$ **then**
            Bin i belongs to the signal
            Change channel state of bin i to "occupied"
            if any of $M(i-K) : M(i-1) > M_T$ **then**
                Group these bins as a single waveform
                Perform waveform smoothing
            end if
        end if
    end for
    Estimate the SCF of detected signals
    Extract the α-profile
    Feed α-profile to previously trained Neural Network
    Decision $\leftarrow$ Licit or Jammer
end function

considered in this work. Employing more hidden layers would increment the training time and overall results would not be significantly improved.

The corresponding pseudo-code of the proposed algorithm is outlined in Algorithm 1. It can be summarized as follows: the receiver observes a WB signal and then energy detection and pre-processing are performed. The α-profile of SCF for each detected sub-signal is subsequently extracted. After that, detected signals go through the classification process. The α-profile of detected signals are fed to a previously trained ANN. The ANN classifies the received NB signal in each SB as either a licit or a potential malicious user.

7.7 Further Steps to the Algorithm

Leaning and *Acting* steps in [23] conclude the proposed Cyclic Spectrum Intelligence algorithm.

7.7.1 Learning

After having identified occupied channels and spectrum holes in the 0-120 MHz band of interest, and classified the detected signals through the cyclostationary feature algorithm with the neural network as classifier, the cyclic spectral intelligence algorithm is thought to include a *learning* process strategy based on the Temporal Frequency Map where previous occurrences of spectrum activities are stored. In each cycle of the Cognitive strategy, the proposed algorithm accesses the Temporal Frequency Map which is a $n \times 3$ matrix that keeps track of the number of occurrences of friendly waveforms (m_F), potentially malicious waveforms (m_{PM}), and spectrum holes (m_{SH}) for each of the n channels-of-interest. Then previous values are updated with the newly acquired and processed information. Temporal forgiveness can be implemented within the algorithm, i.e., spectrum activities corresponding only to the last k spectrum readouts are taken into account while making future decisions. This reduces the probability of data becoming obsolete, at the expense of the lower amount of accessible information.

7.7.2 Acting

Finally, based on the processed spectrum information, current transmission parameters (channel and transmit power) and the history obtained from the Temporal Frequency Map, the CR may decide to *act* in order to improve its chances of reliable transmission. The actions constitute of proactively changing the transmission frequency (channel surfing), or the transmission power whenever a threat has been detected. The system is considered under threat when a potentially malicious waveform has been identified on the channel close to the channel currently used for transmission. The new channel for the transmission is then chosen according to:

$$c_{t+1} \in (c_t = SH | X(c_t) = min). \tag{7.12}$$

This means that the new channel c_{t+1} is selected among all the channels c_t that are currently spectrum holes, such that the $X(c_t)$ is minimum. $X(c_t)$ represents the expected channel reliability, defined as:

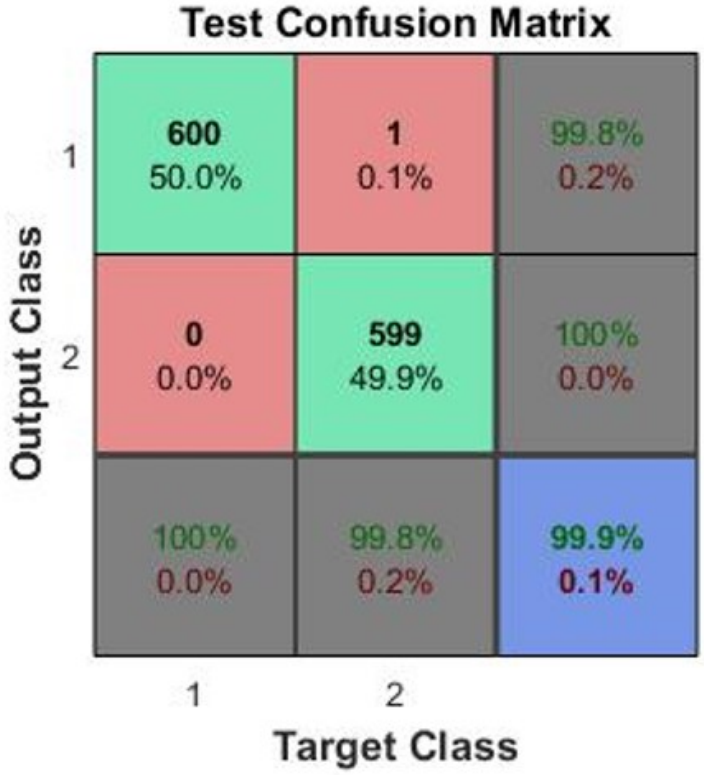


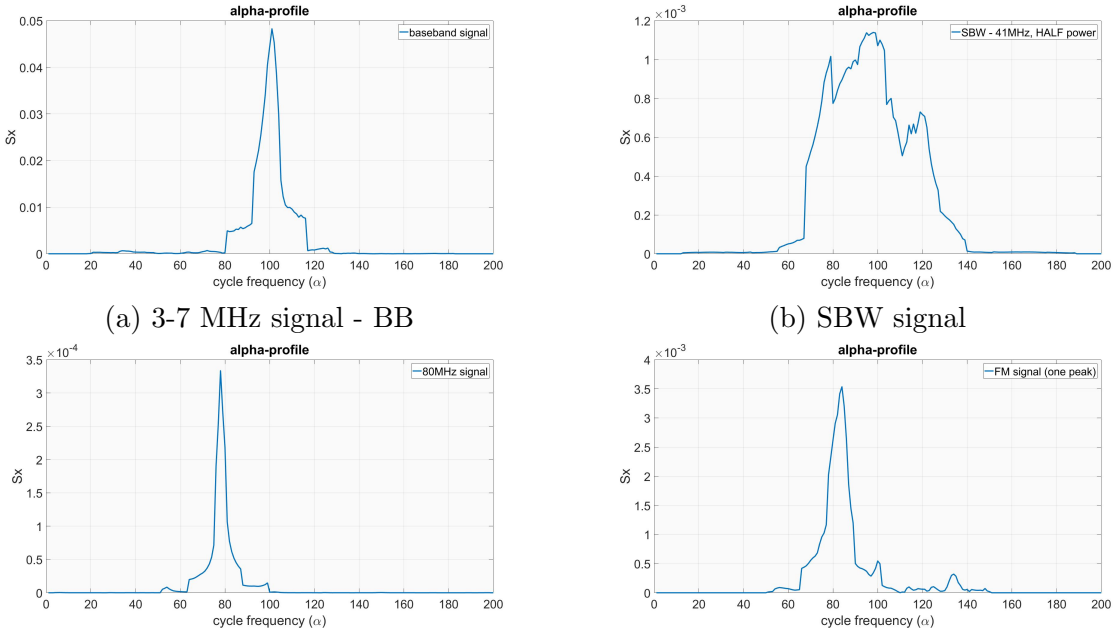
Figure 7.9: Confusion matrix of the proposed ANN with two classes: *FR* and *PM*.

$$X\left(c_t\right) = l^2 \cdot m_{PM/c_t} + (l+1) \cdot m_{F/c_t} - m_{SH/c_t}, \tag{7.13}$$

where m_{PM/c_t}, m_{F/c_t} and mSH/c_t represent the numbers of occurrences of the potentially malicious waveforms, friendly waveforms and spectrum holes on the channel c_t over the last l steps, respectively. The coefficients l^2 and $(l+1)$ are assigned in order to give highest priority of action to avoiding channels with history of occurrences of potentially malicious waveforms, followed by the channels with history of occurrences of friendly waveforms. In this way, it is ensured that each possible channel reliability corresponds to a unique combination of friendly waveforms, potentially malicious waveforms, and spectrum holes. The new transmission power is chosen according to:

$$P_{t+1} \in P | P_R > 10 \log_{10} \hat{\lambda} + 3dB. \tag{7.14}$$

Another application of interest is the possibility of the cognitive system to learn from the actions of a human operator through a graphical user interface (GUI) allowing the human operator to overrule the decision of the cognitive algorithm and



(a) 3-7 MHz signal - BB

(b) SBW signal

(c) 80 MHz signal - HB

(d) one peak of the FM signal

Figure 7.10: α-profiles of four different detected signals.

change transmit parameters such as the operating frequency and the transmission power. The role of the GUI is then to allow the human operator to take decisions irrespectively of the decisions of the Cyclic Spectral Intelligence algorithm. However, it also presents an interesting motivation for considering principles of cognitive refinement, i.e., refining the reasoning behaviour of the algorithm, which is currently policy-based, by learning from the actions of the human operator.

7.8 Validation of the Proposed Algorithm

In order to evaluate the performance of the jammer detection algorithm based on spectral correlation detector and neural network classifier, a set of experiments is performed using the software defined testbed architecture described in Sec. 7.4.1. The sampling rate is set at Nyquist rate for each type of detected signals. In our experiments, the SBW signal represents the potentially malicious waveform and is transmitted by the transmitting HH. Its transmit parameters are given different values according to the half upper part of Table 7.1, namely the SBW signal is in one among the first eight configurations with full and half transmit power. All other detected signals, described in Sec. 7.4.2 are considered as friendly.

The objective of this section is to show the performance of the proposed algorithm in classifying the signals detected in the band-of-interest based on the α-profile, ex-

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	999	1
PM	0	1000

(1) SBW: full - 41MHz

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	996	4
PM	0	1000

(2) SBW: full - 51MHz

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	1000	0
PM	0	1000

(3) SBW: full - 61MHz

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	1000	0
PM	0	1000

(4) SBW: full - 71MHz

Table 7.2: Confusion matrices for the testing step obtained by feeding the ANN with the α-profile of 1000 independent samples at 7 dBm transmit power.

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	1000	0
PM	0	1000

(1) SBW: half - 41MHz

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	999	1
PM	0	1000

(2) SBW: half - 51MHz

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	1000	0
PM	0	1000

(3) SBW: half - 61MHz

SIGNAL$^{\text{CLASS}}$	FR	PM
FR	999	1
PM	0	1000

(4) SBW: half - 71MHz

Table 7.3: Confusion matrices for the testing step obtained by feeding the ANN with the α-profile of 1000 independent samples at 4 dBm transmit power.

tracted from each detected waveform in the wideband spectrum, which passes through the neural network used as classifier. Each NB waveform in the wideband spectrum,

SIGNAL \ CLASS	FR	PM
FR	991	9
PM	10	990

(1) SBW: one tenth - 41MHz

SIGNAL \ CLASS	FR	PM
FR	992	8
PM	0	1000

(2) SBW: one tenth - 51MHz

SIGNAL \ CLASS	FR	PM
FR	993	7
PM	0	1000

(3) SBW: one tenth - 61MHz

SIGNAL \ CLASS	FR	PM
FR	995	5
PM	0	1000

(4) SBW: one tenth - 71MHz

Table 7.4: Confusion matrices for the testing step obtained by feeding the ANN with the α-profile of 1000 independent samples at -3 dBm transmit power.

obtained after the pre-processing step in Sec. 7.5, is characterized by the cyclostationary feature through the α-profile. Specifically, each generated α-profile consists of 200 cyclic frequency points which are the input of the ANN ($I = 200$ in Fig. 7.8). Figs. 7.10 (a)-(d), show the α-profiles for the 4 different signals detected in the 0-120 MHz band: the 3-7 MHz signal, SBW signal, interference at 80 MHz, one peak of the FM signal.

A total of 1000 trains are executed for an ANN architecture with 9 neurons in the hidden layer ($N = 9$ in Fig. 7.8). For our experiments, a dataset composed by 2.000 signals is used in order to train (70%), validate (15%) and test (15%) the ANN architecture. The overall performance can be observed in the 2-classes confusion matrix of Fig. 7.9 for the testing phase which highlights a classification rate approximately equal to 1. Furthermore, after having trained the ANN, the waveforms are tested by using the trained neural network.

The performance of the system is evaluated for 1000 independent testing signals, with different carrier frequencies and transmit powers (7 dBm, 4 dBm and -3 dBm) from training signals. Tables 7.2, 7.3, and 7.4 show the classification accuracy for different system configurations. The proposed cyclostationary algorithm combined with a neural network provides good performance because the classification rate is approximately 1 even for very low power of -3 dBm. The analyzed cyclostationary

feature detector with artificial neural network shows significant performance increase compared to common methods of signal classification, which required 7 dBm for comparable classification rates [25].

7.9 Conclusion

A new Cyclic Spectral Intelligence algorithm is proposed. It is based in a Cognitive Cycle consisting of 5 steps: *Sensing*, *Processing*, *Analysis*, *Learning*, and *Acting*. The Cognitive Cycle interacts with the radio environment through the *sensing* block which obtains instantaneous spectrum data in the band of interest (0-120 MHz) and the *acting* block whose task is to decide and change the transmit parameters such as the carrier frequency and the transmission power. The main novelty introduced by this work is the *Analysis* block. After having identified occupied channels and spectrum holes in the observed wideband signal, the stationary spectral analysis is performed, based on the cyclostationary feature of digitally modulated signals, to extract the α-profile from the SCF of the detected signals. Afterwards, the extracted α-profile of a number of samples of the different waveforms detected in the wideband spectrum, are fed to a pre-trained ANN to classify the waveforms as friendly or potential malicious. In addition, a software defined radio testbed has been employed to generate an experimental dataset to validate the *analysis* block. Real data consists of spectrum measurements in the 0-120 MHz in which there are different signals including the SBW signal whose carrier frequency and transmit power are given different values. Eight configurations of these values have been used in the validation step. Results show that the classification rate is approximately 1 in all the considered configurations making the cyclostationary feature detector with artificial neural network a promising method for the spectrum intelligence processing. Future work includes analysis of fully autonomous systems capable of dynamically access the spectrum in a cognitive radio framework for applications such as PHY-layer security against jamming attacks as well as TVWS. In particular, Stealthy Jammer Detection Algorithm investigated in [79] and in [81] is to be validated on the experimental dataset described in this work.

Chapter 8

Summary and Future Directions

This thesis was focused on the problem of wide-band spectrum sensing and characterization for cognitive radios. Wide-band spectrum sensing is a key enabling functionality for cognitive radios since it detects the spectral holes and allows throughput increase. Due to prioritized spectrum sharing between cognitive radios and primary users, it is not only sufficient to detect spectrum holes, but also distinguish among different users in order to mange interference and jamming. In this dissertation, various algorithms were proposed for spectrum characterization/classification in order to address the problem of jamming in cognitive radios. These newly developed algorithms were applied to detect different types of jamming attacks, namely, tone, modulated and stealthy jamming. In the end of the dissertation, practical implementation of the wide-band spectrum sensing and characterization was addressed on a Software Defined Radio (SDR) test-bed.

This chapter presents the summary of thesis by reviewing the main achieved results of chapters 3, 4, 5, 6 and 7.

8.1 Chapters 3, 4

Out of the various sensing methods, cyclostationary feature detector is capable of detecting the primary signals from interference and noise even at very low signal-to-noise-ratio (SNR). On the other hand, energy detector fails at low SNR and unable to differentiate between different type of signals while matched filtering detector requires a dedicated receiver structure, which may not be possible in practical cognitive radio terminal. Therefore, we selected cyclostationary feature detector over other spectrum sensing techniques, because it is also able to characterize the spectrum in low SNR regions.

Chapter 3 introduced a novel algorithm for jammer detection in wide-band radios. A wide-band was assumed to be consisted of multiple sub-band, each of them is occupied by a narrow-band signal or free. These narrow-band signals could be legitimate or jammers. Firstly, the cyclostationary feature detector was used to compute the spectral correlation function of the received wide-band spectrum. After that, cyclic frequency profile (alpha profile) and angular frequency profile (frequency profile) were extracted from the spectral correlation function. The alpha and frequency profiles were then fed to previously trained artificial neural network. Based on the output of the classifier, each narrow-band signal was characterized as a legitimate or jamming signal. Finally, the proposed algorithm's performance was evaluated for various SNRs to observe the effects of diverse parameters on the classification.

Chapter 4 presented a new physical layer approach for stealthy jammer detection in wide-band cognitive radio networks. Stealthy jammer is an adaptive reactive jammer with same capabilities as a cognitive radio user. These type of jammers only transmit when a legitimate transmission is detected and stop transmitting when the legitimate transmission stops. Therefore, the jamming activities of such jammers are hard to detect by the popular sensing approaches such as energy detection at physical layer. Hence, we presented a novel cyclostationary feature detector based approach to detect such types of jammers at physical layer. The proposed algorithm considered a wide-band composed of multiple narrow-band sub-bands, which could be occupied by licit or stealthy jamming signals . The cyclostationary spectral analysis was performed on this wide-band spectrum to compute spectral correlation function. The alpha profile was then extracted from the spectral correlation function and used as input features to artificial neural network, which classified each signal as a licit signal or a stealthy jamming signal. In the end, the performance of the proposed approach was shown with the help of Monte-Carlo simulations under different empirical setups. The above discussed algorithms, not only successfully characterize the jamming signals, but also able to correctly classify the modulation schemes of legitimate users. Therefore, these algorithms can not only find applications in communications electronic warfare, but also be adapted for future commercial communications systems to increase the throughput by allowing in-band transmissions.

8.2 Chapters 5, 6, 7

When the radios are operating on a wide-band, the task of spectrum estimation becomes complex due to high rate analog-to-digital converter requirements. Com-

pressed sensing is an appealing solution to alleviate requirements of high sampling rates provided that the signal is sparse in some given transform domain.

In chapter 5, a new algorithm was proposed for jammer detection using compressed sensing and cyclostationary spectral analysis for wide-band cognitive radios. The wide-band spectrum was assumed to be occupied by various narrow-band signals with sparsity. In first step, the algorithm recovered the Nyquist rate wide-band spectrum from sub-Nyquist samples using compressed sensing. The recovered signal was then fed to the cyclostationary feature detector to estimate the spectral correlation function of the recovered signal. After that, the cyclic profile of spectral correlation function was extracted and peaks in the cyclic profile were then compared with the corresponding values of the legitimate signal peaks, which were stored in a database. Based on this comparison, each of the detected signals were classified either as a licit signal or a jamming signal. This algorithm was applied to mitigate three different types of jamming attacks, namely tone, modulated and stealthy jamming attacks. The performance of the designed algorithm was evaluated for various compression ratios at low SNR to observe the effects of various parameters on classification performance. The proposed algorithm appeared to perform well within limitation imposed by simple classification using licit waveform parameters stored in a database. Further, it was difficult to maintain databases.

In order to address the classification challenges faced in chapter 5, a new algorithm based on artificial neural network as classifier was proposed in chapter 6. Two different approaches were adopted to train artificial neural network. First approach was to train neural network for Nyquist rate samples at various SNRs, and the second approach used sub-Nyquist rate samples to train the network for different SNRs. The classier trained for different compressed ratios was selected for jammer detection on the basis of its good performance at low SNRs and compression ratios as compared to the classifier trained for Nyquist rate samples. The algorithms can be explained as following. The first step was to recover the Nyquist rate wide band spectrum, which consists of various narrow-band signals, from sub-Nyquist samples using compressed sensing. This reconstructed signal was then fed to the cyclostationary feature detector to estimate the spectral correlation of the wide-band signal. The cyclic frequency profile was extracted and was used as input features for an artificial neural network based classifier. Based on the classifier, each of the narrow-band signal was classified either as a legitimate or a jamming signal. Finally, the performances of the proposed algorithm were shown for various compression ratios and SNRs. The applications of

such algorithms can be found in communications electronic warfare and TV white space (TVWS).

Finally, chapter 7 outlines some practical aspects of sensing and characterization of wide-band spectrum when porting proposed algorithms onto real-world implementation. A large datset was created using a software defined radio (SDR) platform, which consisted of military radios, signal generators, spectrum analyzers and the corresponding auxiliaries. This SDR was used to generate modulated signals in a specified band which were stored for off-line applications. Further, a cyclic spectrum intelligence algorithm was implemented for interference/non-legit mitigation in wide-band radios. The algorithm was based on learning capability and on-the-fly re-configurability of the transmission related parameters in cognitive radio technology. The algorithm first performed the energy detection and necessary pre-processing, then the cyclic spectral analysis of detected narrow-band signals were performed to compute the spectral correlation function. The spectral correlation function produces large amount of data, which made it impossible to work on it in near real time applications. Therefore, cyclic frequency profile was extracted from spectral correlation function. This profile was then fed to a pre-tarined artificial neural network based classifier to identify the signal as legitimate or potential malicious. The results were shown with the help of confusion matrices for various system configurations.

8.3 Suggestions for Future Directions

The work presented in this thesis opened various interesting future research avenues. Some of the important ones are discussed below:

Adversaries that uses the cognitive radio learning mechanisms to improve their jamming capabilities are considered intelligent. Intuitively, being equipped with such learning capabilities may also aid the licit users in improving their anti jamming capabilities. The goals of licit transceivers and jammers are typically negatively correlated. This can allows us to use game theory; a mathematical study of decision-making in situations involving conflicts of interest, as a tool for mathematical formalization of the intelligent jamming /anti jamming problems.

A large data set was created as a part of this thesis to study PHY layer security and cognitive radios. This thesis considered expert features, namely, cyclic features, it will be interesting to use deep learning techniques to classify various types of signals. These deep learning techniques, for example convolution neural networks are being used in speech prepossessing and computer vision fields.

In future, the cyclic intelligence algorithm can be improved by incorporating compressed sensing, to alleviate the high rate analog to digital conversion (A/D) requirements for wide-band sensing. Further, an artificial neural network trained with sub-Nyquist rate can be used to improve the classification performance of cyclic intelligence algorithm. Another interesting future work, would be, validating the proposed stealthy jammer detection algorithm on cognitive radio test-bed.

Publications

Refereed Journal Articles

- T. Nawaz, L. Marcenaro and C. S. Regazzoni, " Cyclostationary-Based Jammer Detection for Wide-band Radios using Compressed sensing and Artificial Neural Network," *International Journal of Distributed Sensor Networks (IJDSN),* Nov. 2017.
- T. Nawaz, A. Toma, L. Marcenaro and C. S. Regazzoni, " Interference Mitigation in Wide-band Radios using Spectrum Correlation and Neural Network," in process.

Refereed Conference Articles

- A. Toma and T. Nawaz and L. Marcenaro and C. S. Regazzoni and Y. Gao, "A Dual Resolution Discrete S-Transform for Cognitive Radio," submitted in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, Canada, April. 2018.
- T. Nawaz, L. Marcenaro and C. S. Regazzoni, "Stealthy Jammer Detection Algorithm for Wide-band Radios: A Physical Layer Approach," *IEEE 10th International Workshop on Selected Topics in Wireless and Mobile computing (STWiMob' 17)*, Rome, Italy, Oct. 2017.
- T. Nawaz, L. Marcenaro and C. S. Regazzoni, "Defense against Stealthy Jamming Attacks in Wide-band Radios: A Physical Layer Approach," *IEEE Global Conference on Signal and Information Processing (GlobalSIP' 17)*, Montreal, Canada, Oct. 2017.
- T. Nawaz, L. Marcenaro and C. S. Regazzoni, "Defense against Jamming Attacks in Wide-band Radios using Cyclic Spectral Analysis and Compressed Sensing," *IEEE 9th International Conference on Ubiquitous and Future Networks (ICUFN' 17)*, Milan, Italy, Jul. 2017.
- T. Nawaz, D. Campo, M. O. Mughal, L. Marcenaro and C. S. Regazzoni, "Jammer Detection Algorithm for Wide-band Radios using Spectral Correlation and Neural Networks," *IEEE 13th International Conference on Wireless Communications and Mobile Computing (IWCMC' 17)*, Valencia, Spain, Jun 2017.

- M. O. Mughal, T. Nawaz, L. Marcenaro, C. S. Regazzoni, "Cyclostationary based Jammer Detection Algorithm for Wide-band Radios using Compressed Sensing," *IEEE Global Conference on Signal and Information Processing (IEEE GlobalSIP' 15)*, Orlando, Florida, Dec. 2015.
- T. Nawaz, M. O. Mughal, L. Marcenaro, C. S. Regazzoni, "Exploiting Cyclic Features for Jammer Detection in Wideband Cognitive Radios," *WInnComm-Europe' 15*, Erlangen, Germany, Oct. 2015.

Book chapters

- Chapters 3 and 10 of the book entitled, "Measurable and Composable Security, Privacy, and Dependability," Dec. 2017.

Acknowledgements

First and foremost, I would like to thank my advisor, Prof. Carlo S. Regazzoni, for his support and guidance over the past three years at University of Genova. His valuable advice and assistance were essential in achieving this work and in helping me to develop my research career. Working with Prof. Carlo has been a great learning experience for me. I am grateful for his encouragement and help during this work period.

I would like to express my gratitude to Prof. Lucio Marcenaro for his smooth management of our research group, participating in group discussions and for inspiring questions, which opens new challenges and broaden our research spectrum.

I am grateful to my lab colleagues and PhD fellows for making the work environment at ISIP40 a more friendly place. I am so grateful for their collaboration and the time we spent together throughout our journey at ISIP40. Thanks Irfan, Subhan, Andrea, Ozair, Damian, Kadian, Veranika, Marzia, Pietro, Sandeep, Kresmir, Vahid, Waqar, Suleman, Mohammad, Sebastian, and Oscar.

Last, but not least, I would like to thank my all family members for their support and encouragement. Special thanks to my parents, Mr. and Mrs. Prof. Shah Nawaz Khan for their patience, their sacrifice and their continual support in all my pursuits. Thanks to my siblings, and extended family , for being so encouraging and supportive during all this period of time.

Bibliography

[1] Ian F Akyildiz, Won-Yeol Lee, Mehmet C Vuran, and Shantidev Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer networks*, 50(13):2127–2159, 2006.

[2] S. Amuru and R. M. Buehrer. Optimal jamming strategies in digital communications-impact of modulation. In *2014 IEEE Global Communications Conference*, pages 1619–1624, Oct 2014. doi: 10.1109/GLOCOM.2014.7037040.

[3] S. Amuru and R. M. Buehrer. Optimal jamming against digital modulation. *IEEE Transactions on Information Forensics and Security*, 10(10):2212–2224, 2015. ISSN 1556-6013. doi: 10.1109/TIFS.2015.2451081.

[4] A. Annamalai and A. Olaluwe. Energy detection of unknown deterministic signals. In *2014 International Conference on Computing, Networking and Communications (ICNC)*, pages 761–765, Feb 2014.

[5] A. H. Ansari and S. M. Gulhane. Investigation of roc parameters using monte carlo simulation in cyclostationary and energy detection spectrum sensing. In *2015 International Conference on Information Processing (ICIP)*, pages 266–271, Dec 2015. doi: 10.1109/INFOP.2015.7489391.

[6] I. G. Anyim, J. Chiverton, M. Filip, and A. Tawfik. The implementation of wideband cyclostationary feature detector with receiver constraints. In *2017 European Conference on Networks and Communications (EuCNC)*, pages 1–5, June 2017. doi: 10.1109/EuCNC.2017.7980722.

[7] D. B, A. P. Iyer, and C. R. Murthy. Cyclostationary-based architectures for spectrum sensing in ieee 802.22 wran. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–5, Dec 2010.

[8] B. F. Beidas and C. L. Weber. Asynchronous classification of mfsk signals using the higher order correlation domain. *IEEE Transactions on Communications*, 46(4):480–493, Apr 1998.

[9] M. Bkassiny, S. K. Jayaweera, Y. Li, and K. A. Avery. Wideband spectrum sensing and non-parametric signal classification for autonomous self-learning cognitive radios. *IEEE Transactions on Wireless Communications*, 11(7):2596–2605, July 2012.

[10] M. Bkassiny, S. K. Jayaweera, Y. Li, and K. A. Avery. Blind cyclostationary feature detection based spectrum sensing for autonomous self-learning cognitive radios. In *2012 IEEE International Conference on Communications (ICC)*, pages 1507–1511, June 2012.

[11] D. Cabric, S. M. Mishra, and R. W. Brodersen. Implementation issues in spectrum sensing for cognitive radios. In *Proc. of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, volume 1, pages 772–776, November 2004.

[12] Danijela Branislav Cabric. *Cognitive radios: System design perspective*. University of California, Berkeley, 2007.

[13] C. Chang, J. Wawrzynek, and R. W. Brodersen. Bee2: a high-end reconfigurable computing system. *IEEE Design Test of Computers*, 22(2):114–125, 2005.

[14] S. Chatterjee, S. Ray, S. Dutta, and J. S. Roy. Performance analysis of spectrum sensing in cognitive radio at low snr environment. In *2017 1st International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech)*, pages 1–4, April 2017. doi: 10.1109/IEMENTECH.2017.8076996.

[15] R. Chen, J. M. Park, and J. H. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, Jan 2008. ISSN 0733-8716. doi: 10.1109/JSAC.2008.080104.

[16] Scott Shaobing Chen, David L. Donoho, and Michael A. Saunders. Atomic decomposition by basis pursuit. *SIAM Journal on Scientific Computing*, 20(1):33–61, 1998. doi: 10.1137/S1064827596304010.

[17] W.L. Chin, J.M. Li, and H.H. Chen. Low-complexity energy detection for spectrum sensing with random arrivals of primary users. *IEEE Transactions on Vehicular Technology*, 65(2):947–952, February 2015.

[18] D. Cohen, E. Rebeiz, V. Jain, Y. C. Eldar, and D. Cabric. Cyclostationary feature detection from sub-nyquist samples. In *2011 4th IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, pages 333–336, Dec 2011. doi: 10.1109/CAMSAP.2011.6136018.

[19] T. Cui, F. Gao, and A. Nallanathan. Optimization of cooperative spectrum sensing in cognitive radio. *IEEE Transactions on Vehicular Technology*, 60(4): 1578–1589, May 2011.

[20] Kresimir Dabcevic. *Intelligent Jamming and Anti-Jamming Techniques using Cognitive Radios*. PhD thesis, PhD thesis, University of Genova, Genova, Italy, 2015.

[21] Krešimir Dabčević, Lucio Marcenaro, and Carlo S Regazzoni. Security in cognitive radio networks. *Evolution of Cognitive Networks and Self-Adaptive Communication Systems*, page 301, 2013.

[22] Kresimir Dabcevic, Alejandro Betancourt, Lucio Marcenaro, and Carlo S. Regazzoni. Intelligent cognitive radio jamming - a game-theoretical approach. *EURASIP Journal on Advances in Signal Processing*, 2014(1):1–18, 2014. ISSN 1687-6180. doi: 10.1186/1687-6180-2014-171. URL `http://dx.doi.org/10.1186/1687-6180-2014-171`.

[23] Kresimir Dabcevic, Muhammad Ozair Mughal, Lucio Marcenaro, and Carlo S. Regazzoni. Cognitive radio as the facilitator for advanced communications electronic warfare solutions. *Journal of Signal Processing Systems*, 83(1):29–44, 2015. ISSN 1939-8115. doi: 10.1007/s11265-015-1050-0. URL `http://dx.doi.org/10.1007/s11265-015-1050-0`.

[24] K. Dabčević, L. Marcenaro, and C. S. Regazzoni. Spd-driven smart transmission layer based on a software defined radio test bed architecture. In *4th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS) - Lisbon, Portugal*, January 2014.

[25] K. Dabčević, M.O. Mughal, L. Marcenaro, and C. S. Regazzoni. Spectrum intelligence for interference mitigation for cognitive radio terminals. In *Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (WInnComm- Europe), Rome, Italy*, November 2014.

[26] A. V. Dandawate and G. B. Giannakis. Statistical tests for presence of cyclostationarity. *IEEE Transactions on Signal Processing*, 42(9):2355–2369, Sep 1994.

[27] Guillaume de la Roche, Andrs Alayn-Glazunov, and Ben Allen. *Cognitive Radio Networks: Sensing, Access, Security*, pages 568–. Wiley Telecom, 2012. ISBN 9781118410998. doi: 10.1002/9781118410998.ch16. URL `http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=8043780`.

[28] M. Derakhshani, T. Le-Ngoc, and M. Nasiri-Kenari. Efficient cooperative cyclostationary spectrum sensing in cognitive radios at low snr regimes. *IEEE Transactions on Wireless Communications*, 10(11):3754–3764, November 2011.

[29] F.F. Digham, M.S. Alouini, and M.K. Simon. On the energy detection of unknown signals over fading channels. *IEEE Transactions on Communications*, 55(1):21–24, January 2007.

[30] D. L. Donoho. Compressed sensing. *IEEE Transactions on Information Theory*, 52(4):1289–1306, April 2006. ISSN 0018-9448. doi: 10.1109/TIT.2006.871582.

[31] Marco F. Duarte, Michael B. Wakin, and Richard G. Baraniuk. Fast reconstruction of piecewise smooth signals from random projections. In *Online Proceedings of the Workshop on Signal Processing with Adaptative Sparse Structured Representations (SPARS)*, Rennes, France, 2005.

[32] B. Farhang-Boroujeny. Filter bank spectrum sensing for cognitive radios. *IEEE Transactions on Signal Processing*, 56(5):1801–1811, May 2008.

[33] R. Farrell, M. Sanchez, and G. Corley. International journal of digital multimedia broadcasting. *IEEE Transactions on Signal Processing*, 2009.

[34] US FCC and ET Docket. Second report and order and memorandum opinion and order, in the matter of unlicensed operation in the tv broadcast bands additional spectrum for unlicensed devices below 900 mhz and in the 3 ghz band. *Washington, DC: Federal Communnications Commission*, 2008.

[35] A. Fehske, J. Gaeddert, and J. H. Reed. A new approach to signal classification using spectral correlation and neural networks. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 144–150, Nov 2005. doi: 10.1109/DYSPAN.2005.1542629.

[36] S Force. Spectrum policy task force report. *Federal Communications Commission ET Docket 02, vol. 135*, 2002.

[37] K. Friston, B. Sengupta, and G. Auletta. Cognitive dynamics: From attractors to active inference. *Proceedings of the IEEE*, 102(4):427–445, April 2014.

[38] M. Gandetto and C. Regazzoni. Spectrum sensing: A distributed approach for cognitive terminals. *IEEE Journal on Selected Areas in Communications*, 25 (3):546–557, April 2007.

[39] G. Ganesan and Y. Li. Cooperative spectrum sensing in cognitive radio, part i: Two user networks. *IEEE Transactions on Wireless Communications*, 6(6): 2204–2213, June 2007.

[40] G. Ganesan and Y. Li. Cooperative spectrum sensing in cognitive radio, part ii: Multiuser networks. *IEEE Transactions on Wireless Communications*, 6(6): 2214–2222, June 2007.

[41] W. Gardner. Spectral correlation of modulated signals: Part i - analog modulation. *IEEE Transactions on Communications*, 35(6):584–594, June 1987.

[42] W. Gardner, W. Brown, and Chih-Kang Chen. Spectral correlation of modulated signals: Part ii - digital modulation. *IEEE Transactions on Communications*, 35(6):595–601, June 1987.

[43] W. A. Gardner. Signal interception: a unifying theoretical framework for feature detection. *IEEE Transactions on Communications*, 36(8):897–906, Aug 1988. ISSN 0090-6778. doi: 10.1109/26.3769.

[44] W. A. Gardner, A. Napolitano, and L. Paura. Cyclostationarity: Half a century of research. *Signal Process*, 84(4):595–601, 2006.

[45] William Gardner and James A Cadzow. Statistical spectral analysis: a non-probabilistic theory. *Applied Optics*, 29:1399, 1990.

[46] A. H. Gholamipour, A. Gorcin, H. Celebi, B. U. Toreyin, M. A. R. Saghir, F. Kurdahi, and A. Eltawil. Reconfigurable filter implementation of a matched-filter based spectrum sensor for cognitive radio systems. In *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*, pages 2457–2460, May 2011. doi: 10.1109/ISCAS.2011.5938101.

[47] S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 23(2):201–220, Feb 2005. ISSN 0733-8716. doi: 10.1109/JSAC.2004.839380.

[48] S. Haykin. Cognitive dynamic systems: Radar, control, and radio [point of view]. *Proceedings of the IEEE*, 100(7):2095–2103, July 2012.

[49] S. Haykin, D. Thomson, , and J. Reed. Spectrum sensing for cognitive radio. *Proceedings of the IEEE*, 97(5):849–877, April 2009.

[50] Chung-Yu Huan and A. Polydoros. Likelihood methods for mpsk modulation classification. *IEEE Transactions on Communications*, 43(2/3/4):1493–1504, Feb 1995.

[51] Maria Stella Iacobucci. *Cognitive Radio: Concept and Capabilities*, pages 304–. Wiley Telecom, 2013. ISBN 9781118398401. doi: 10.1002/9781118398401.ch2. URL `http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=8044507`.

[52] Md Habibul Islam, Choo Leng Koh, Ser Wah Oh, Xianming Qing, Yoke Yong Lai, Cavin Wang, Ying-Chang Liang, Bee Eng Toh, Francois Chin, Geok Leng Tan, et al. Spectrum survey in singapore: Occupancy measurements and analyses. In *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, pages 1–7. IEEE, 2008.

[53] S. Kapoor, S. Rao, and G. Singh. Opportunistic spectrum sensing by employing matched filter in cognitive radio network. In *2011 International Conference on Communication Systems and Network Technologies*, pages 580–583, June 2011. doi: 10.1109/CSNT.2011.124.

[54] Y. M. Kim, G. Zheng, S. H. Sohn, and J. M. Kim. An alternative energy detection using sliding window for cognitive radio system. In *2008 10th International Conference on Advanced Communication Technology*, volume 1, pages 481–485, Feb 2008.

[55] V. I. Kostylev. Energy detection of a signal with random amplitude. In *2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No.02CH37333)*, volume 3, pages 1606–1610 vol.3, 2002.

[56] S. Kozlowski. Implementation and verification of cyclostationary feature detector for dvb-t signals. *IET Signal Processing*, 10(2):162–167, March 2016.

[57] L. B. Le and E. Hossain. Resource allocation for spectrum underlay in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 7(12):5306–5315, December 2008.

[58] K. B. Letaief and W. Zhang. Cooperative communications for cognitive radio networks. *Proceedings of the IEEE*, 97(5):878–893, May 2009.

[59] S. Li, M. Sun, Y. C. Liang, B. Li, and C. Zhao. Spectrum sensing for cognitive radios with unknown noise variance and time-variant fading channels. *IEEE Access*, 5:21992–22003, 2017. doi: 10.1109/ACCESS.2017.2758848.

[60] Y. Li, S. K. Jayaweera, and C. G. Christodoulou. Wideband phy/mac bandwidth aggregation optimization for cognitive radios. In *2012 3rd International Workshop on Cognitive Information Processing (CIP)*, pages 1–6, May 2012.

[61] E. Like, V. Chakravarthy, R. Husnay, and Z. Wu. Modulation recognition in multipath fading channels using cyclic spectral analysis. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–6, Nov 2008. doi: 10.1109/GLOCOM.2008.ECP.584.

[62] J. Lunden, V. Koivunen, A. Huttunen, and H. V. Poor. Collaborative cyclostationary spectrum sensing for cognitive radio systems. *IEEE Transactions on Signal Processing*, 57(11):4182–4195, Nov 2009.

[63] J. Ma, G. Y. Li, and B. H. Juang. Signal processing in cognitive radio. *Proceedings of the IEEE*, 97(5):805–823, May 2009.

[64] A. Mandal and S. Chatterjee. A comprehensive study on spectrum sensing and resource allocation for cognitive cellular network. In *2017 Devices for Integrated Circuit (DevIC)*, pages 100–102, March 2017. doi: 10.1109/DEVIC.2017.8073915.

[65] Y. G. Marn, D. F. Celis, A. Londoo, and W. D. Jimnez. Evaluation of blind detection algorithms for spectrum sensing. In *2017 IEEE Colombian Conference on Communications and Computing (COLCOM)*, pages 1–6, Aug 2017. doi: 10.1109/ColComCon.2017.8088209.

[66] M. Mishali and Y. C. Eldar. From theory to practice: Sub-nyquist sampling of sparse wideband analog signals. *IEEE Journal of Selected Topics in Signal Processing*, 4(2):375–391, April 2010. ISSN 1932-4553. doi: 10.1109/JSTSP.2010.2042414.

[67] Mitola and Joseph. Cognitive radio: an integrated agent architecture for software defined radio. 2000.

[68] J. Mitola and G. Q. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6(4):13–18, Aug 1999. ISSN 1070-9916. doi: 10.1109/98.788210.

[69] Martin Fodslette Møller. A scaled conjugate gradient algorithm for fast supervised learning. *Neural networks*, 6(4):525–533, 1993.

[70] P. Morerio, K. Dabčević, L. Marcenaro, and C.S. Regazzoni. Distributed cognitive radio architecture with automatic frequency switching. In *2012 Complexity in Engineering (COMPENG). Proceedings*, pages 1–4, June 2012.

[71] E. Moser, M. K. Moran, E. Hillen, D. Li, and Z. Wu. Automatic modulation classification via instantaneous features. In *2015 National Aerospace and Electronics Conference (NAECON)*, pages 218–223, June 2015. doi: 10.1109/NAECON.2015.7443070.

[72] M. O. Mughal, K. Dabcevic, L. Marcenaro, and C. S. Regazzoni. Compressed sensing based jammer detection algorithm for wide-band cognitive radio networks. In *Compressed Sensing Theory and its Applications to Radar, Sonar and Remote Sensing (CoSeRa), 2015 3rd International Workshop on*, pages 119–123, June 2015. doi: 10.1109/CoSeRa.2015.7330276.

[73] M. O. Mughal, T. Nawaz, L. Marcenaro, and C. S. Regazzoni. Cyclostationary-based jammer detection algorithm for wide-band radios using compressed sensing. In *2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 280–284, Dec 2015. doi: 10.1109/GlobalSIP.2015.7418201.

[74] MO Mughal, K Dabcevic, G Dura, L Marcenaro, and CS Regazzoni. Experimental study of spectrum estimation and reconstruction based on compressive sampling for cognitive radios. In *2014 Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (WInnComm-Europe 2014)*, 2014.

[75] A. K. Nandi and E. E. Azzouz. Algorithms for automatic modulation recognition of communication signals. *IEEE Transactions on Communications*, 46(4): 431–436, Apr 1998.

[76] V. Havary Nassab, S. Hassan, and S. Valaee. Compressive detection for wide-band spectrum sensing. In *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 3094–3097, March 2010.

[77] T. Nawaz, M.O. Mughal, L. Marcenaro, and C.S. Regazzoni. Exploiting cyclic features for jammer detection in wide-band cognitive radios. In *WInnComm-Europe' 15, Erlangen, Germany*, October 2015.

[78] T. Nawaz*, D. Campo, M. O. Mughal, L. Marcenaro, and C. S. Regazzoni. Jammer detection algorithm for wide-band radios using spectral correlation and neural networks. In *13th International Conference on Wireless Communications and Mobile Computing*, volume 1, pages 890–897 vol.1, Nov 2017. doi: 10.1109/ACSSC.2001.987051.

[79] T. Nawaz, L. Marcenaro, and C. S. Regazzoni. Defense against stealthy jamming attacks in wide-band radios: A physical layer approach. In *IEEE Global Conference on Signal and Information Processing (GlobalSIP' 17), Montreal, Canada*, October 2017.

[80] T. Nawaz, L. Marcenaro, and C. S. Regazzoni. Defense against jamming attacks in wide-band radios using cyclic spectral analysis and compressed sensing. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 874–879, July 2017.

[81] T. Nawaz, L. Marcenaro, and C.S. Regazzoni. Stealthy jammer detection algorithm for wide-band radios: A physical layer approach. In *IEEE 10th International Workshop on Selected Topics in Wireless and Mobile computing (STWiMob' 17), Rome, Italy*, October 2017.

[82] Ser Wah Oh, Yugang Ma, Ming-Hung Tao, and Edward Peh. *Introduction to Cognitive Radio and Television White Space*, pages 360–. Wiley-IEEE Press, 2017. ISBN 9781119110491. doi: 10.1002/9781119110491.ch1. URL `http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7656858`.

[83] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys Tutorials*, 13(2):245–257, Second 2011. ISSN 1553-877X. doi: 10.1109/SURV.2011.041110.00022.

[84] R. A. Poiselr. Introduction to communication electronic warfare systems. In *2014 IEEE Global Communications Conference*, 2008.

[85] Y. L. Polo, Ying Wang, A. Pandharipande, and G. Leus. Compressive wide-band spectrum sensing. In *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2337–2340, April 2009.

[86] A. Polydoros and K. Kim. On the detection and classification of quadrature digital modulations in broad-band noise. *IEEE Transactions on Communications*, 38(8):1199–1211, Aug 1990.

[87] John G Proakis. *Companders*. Wiley Online Library, 2001.

[88] Lijun Qian, Xiangfang Li, and Shuangqing Wei. Anomaly spectrum usage detection in multihop cognitive radio networks: A cross-layer approach. *JCM*, 8: 259–266, 2013.

[89] Z. Qin, Y. Gao, M. Plumbley, and C.G. Parini. Wideband spectrum sensing on real-time signals at sub-nyquist sampling rates in single and cooperative multiple nodes. *IEEE Transactions on Signal Processing*, 64(12):3106–3117, June 2016.

[90] Z. Quan, S. Cui, A. H. Sayed, and H. V. Poor. Optimal multiband joint detection for spectrum sensing in cognitive radio networks. *IEEE Transactions on Signal Processing*, 57(3):1128–1140, March 2009.

[91] M. J. A. Rahman, M. Krunz, and R. Erwin. Interference mitigation using spectrum sensing and dynamic frequency hopping. In *2012 IEEE International Conference on Communications (ICC)*, pages 4421–4425, June 2012. doi: 10.1109/ICC.2012.6363744.

[92] M. Rashidi and S. Mansouri. Parameter selection in periodic nonuniform sampling of multiband signals. In *2010 3rd International Symposium on Electrical and Electronics Engineering (ISEEE)*, pages 79–83, Sept 2010. doi: 10.1109/ISEEE.2010.5628538.

[93] R. S. Roberts, W. A. Brown, and H. H. Loomis. Computationally efficient algorithms for cyclic spectral analysis. *IEEE Signal Processing Magazine*, 8(2): 38–49, April 1991. ISSN 1053-5888. doi: 10.1109/79.81008.

[94] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao. Multi-channel jamming attacks using cognitive radios. In *2007 16th International Conference on Computer Communications and Networks*, pages 352–357, Aug 2007.

[95] M. Sardana and A. Vohra. Analysis of different spectrum sensing techniques. In *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, pages 422–425, July 2017. doi: 10.1109/COMPTELIX.2017.8004006.

[96] C. M. Spooner. On the utility of sixth-order cyclic cumulants for rf signal classification. In *Conference on Signals, Systems and Computers*, volume 1, pages 890–897 vol.1, Nov 2001. doi: 10.1109/ACSSC.2001.987051.

[97] S. Srinivasa and S. A. Jafar. Cognitive radios for dynamic spectrum access - the throughput potential of cognitive radio: A theoretical perspective. *IEEE Communications Magazine*, 45(5):73–79, May 2007.

[98] P. D. Sutton, K. E. Nolan, and L. E. Doyle. Cyclostationary signatures in practical cognitive radio applications. *IEEE Journal on Selected Areas in Communications*, 26(1):13–24, Jan 2008.

[99] A. Swami and B. M. Sadler. Hierarchical digital modulation classification using cumulants. *IEEE Transactions on Communications*, 48(3):416–429, Mar 2000.

[100] Z. Tian. Cyclic feature based wideband spectrum sensing using compressive sampling. In *2011 IEEE International Conference on Communications (ICC)*, pages 1–5, June 2011. doi: 10.1109/icc.2011.5963015.

[101] Z. Tian and G. B. Giannakis. A wavelet approach to wideband spectrum sensing for cognitive radios. In *2006 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pages 1–5, June 2006.

[102] Z. Tian and G. B. Giannakis. Compressed sensing for wideband cognitive radios. In *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*, volume 4, pages 1357–1360, April 2007.

[103] Z. Tian, Y. Tafesse, and B. M. Sadler. Cyclic feature detection with sub-nyquist sampling for wideband spectrum sensing. *IEEE Journal of Selected Topics in Signal Processing*, 6(1):58–69, Feb 2012. ISSN 1932-4553. doi: 10.1109/JSTSP.2011.2181940.

[104] J. A. Tropp and A. C. Gilbert. Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Transactions on Information Theory*, 53 (12):4655–4666, Dec 2007. ISSN 0018-9448. doi: 10.1109/TIT.2007.909108.

[105] J. Unnikrishnan and V. Veeravalli. Cooperative sensing for primary detection in cognitive radio. *IEEE Journal of Selected Topics in Signal Processing*, 2(1): 18–27, Feb 2008.

[106] S. Upadhyay and S. Deshmukh. Blind parameter estimation based matched filter detection for cognitive radio networks. In *2015 International Conference on Communications and Signal Processing (ICCSP)*, pages 0904–0908, April 2015. doi: 10.1109/ICCSP.2015.7322627.

[107] L. Wang and A. M. Wyglinski. A combined approach for distinguishing different types of jamming attacks against wireless networks. In *Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pages 809–814, Aug 2011. doi: 10.1109/PACRIM.2011.6032998.

[108] Wen Wei and J. M. Mendel. Maximum-likelihood classification for digital amplitude-phase modulations. *IEEE Transactions on Communications*, 48(2): 189–193, Feb 2000.

[109] H. Wu and S. Wang. An efficient and robust approach for wideband compressive spectrum sensing. In *2012 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2012)*, pages 499–502, Aug 2012.

[110] Y. Wu, B. Wang, and K. J. R. Liu. Optimal defense against jamming attacks in cognitive radio networks using the markov decision process approach. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–5, Dec 2010.

[111] Z. Wu, E. Like, and V. Chakravarthy. Reliable modulation classification at low snr using spectral correlation. In *4th IEEE Consumer Communications and Networking Conference*, pages 1134–1138, Jan 2007. doi: 10.1109/CCNC.2007.228.

[112] Z. Xinzhi, G. Feifei, C. Rong, and J. Tao. Matched filter based spectrum sensing when primary user has multiple power levels. *China Communications*, 12(2): 21–31, April 2015.

[113] y Simon Haykin, David J. Thomson, and Jeffrey H. Reed. Spectrum sensing for cognitive radio. *Proceedings of the IEEE*, 97(5):849–877, 2009.

[114] Yawpo Yang and Ching-Hwa Liu. An asymptotic optimal algorithm for modulation classification. *IEEE Communications Letters*, 2(5):117–119, May 1998.

[115] P. Semba Yawada and A. J. Wei. Cyclostationary detection based on non-cooperative spectrum sensing in cognitive radio network. In *2016 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pages 184–187, June 2016. doi: 10.1109/CYBER.2016.7574819.

[116] H. B. Yilmaz, T. Tugcu, F. Alagz, and S. Bayhan. Radio environment map as enabler for practical cognitive radio networks. *IEEE Communications Magazine*, 51(12):162–169, December 2013. ISSN 0163-6804. doi: 10.1109/MCOM.2013.6685772.

[117] Zhuizhuan Yu, S. Hoyos, and B. M. Sadler. Mixed-signal parallel compressed sensing and reception for cognitive radio. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 3861–3864, March 2008. doi: 10.1109/ICASSP.2008.4518496.

[118] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys Tutorials*, 11(1):116–130, First 2009. ISSN 1553-877X. doi: 10.1109/SURV.2009.090109.

[119] F. Zeng, C. Li, and Z. Tian. Distributed compressive spectrum sensing in cooperative multihop cognitive networks. *IEEE Journal of Selected Topics in Signal Processing*, 5(1):37–48, Feb 2011. ISSN 1932-4553. doi: 10.1109/JSTSP.2010.2055037.

[120] Y. Zeng and Y. C. Liang. Covariance based signal detections for cognitive radio. In *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pages 202–207, April 2007.

[121] W. Zhang, R. K. Mallik, and K. B. Letaief. Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 8(12):5761–5766, December 2009.

[122] X. Zhang, R. Chai, and F. Gao. Matched filter based spectrum sensing and power level detection for cognitive radio network. In *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 1267–1270, Dec 2014. doi: 10.1109/GlobalSIP.2014.7032326.

[123] Y. Zhao, Y. Wu, J. Wang, X. Zhong, and L. Mei. Wavelet transform for spectrum sensing in cognitive radio networks. In *International Conference on Audio, Language and Image Processing (ICALIP), Shanghai, China*, pages 565–569, June 2014.

[124] Q. Zhu, H. Li, Z. Han, and T. Basar. A stochastic game model for jamming in multi-channel cognitive radio systems. In *2010 IEEE International Conference on Communications*, pages 1–6, May 2010.