Intelligent jamming and anti-jamming techniques using Cognitive Radios

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Kresimir Dabcevic

PhD Programme in Computational Intelligence

University of Genoa

A thesis submitted for the degree of

Doctor of Philosophy

Genoa, April 2015

You only do two days in your PhD – the day you get in, and the day you come out.

(a *somewhat* modified quote from the legendary TV series *The Wire*)

Preface

If you download any one among the many scientific papers related to Cognitive Radios, chances are they are going to mention "Dynamic Spectrum Access" or "cross-compatibility and interoperability" as the motivating factors for the research of the Cognitive Radio technology. For me, though, the motivating reason for deciding to dedicate no less than three years of my life to researching this topic is somewhat more banal: Cognitive Radio is simply cool! A radio system that re-configures, adapts, and ultimately learns on its own? Well, sign me in!

I have first come to learn about this exciting novel communication paradigm somewhat accidentally, while researching potential topics for my final-year M.Sc. project. With the aid of my mentor-at-the-time, prof. Mislav Grgić of the University of Zagreb, I have gained plenty of interesting insights into the topic. This was followed by a wonderful five-month spell as a visiting researcher with the Mälardalen University's Wireless Communications group, where I have gained invaluable hands-on experience with off-the-shelf Software Defined Radio platforms. Ultimately, it was this introduction to the world of the academic research that has shaped my desire to do a PhD on this particular topic. Hence, I didn't hesitate to jump at the opportunity to apply for a position as the PhD candidate in Cognitive Radio research at the University of Genoa. And so, three years later – years comprised of sometimes tiring, occasionally frustrating but for the biggest part truly great and exciting moments - here I am, trying to summarize everything important I have done throughout my PhD, in one meaningful, well-structured document.

I would like to provide a clarification as to why, throughout this thesis, I am occasionally switching between writing in first person singular ("I") and first person plural ("we"). The reason is as follows: the former is typically used to express my own personal beliefs and opinions on the matters in question. These are a result of three years of research on the

topic, meeting and talking with the peers and experts in the field, and in general observing the way that the Cognitive Radio technology has progressed. The latter, conversely, is used whenever actions and inflections denote collaborative effort between me and my colleagues – Alejandro Betancourt, Ozair Mughal, Lucio Marcenaro and Carlo Regazzoni. Since much of my work has relied on collaboration and cooperation, "we" has established itself as a predominant form in the thesis.

I would like to dedicate a few lines to giving thanks to important people in my life, starting with my family – to my parents Branimir and Milena, and my brother Zvonimir – thank you for providing me with support and encouragement throughout my life.

My gratitude extends to all the great friends I am lucky to have: Šime, Ante, Filip, Marinko, Grof, Danijel, Nikolina, Bruno, Nataša, Albert, Jorge, Isah, Alex, Mohamed, Alejandro, Francesca, Camilla, Bo and others - even though thousands of kilometers may separate us at any point in the future, let us keep contact and not forget why we have come to be friends in the first place! And let us not forget about all the cheap airlines out there...

Thank you to all of the present and former fellow researchers and the supporting staff at the ISIP40 group, for building a pleasant and healthy working environment, and for making me come to the office every morning with a smile on my face.

My special thanks goes to my wonderful girlfriend and life companion Maira, who has been by my side throughout, making me a happy and fulfilled person, day-in, day-out. Going through life with you has been nothing short of amazing.

Finally, I would like to thank you, dear reader, for taking the time to go through this document. I hope that you can find something of interest on the following pages.

Abstract

Cognitive Radio can be defined as a radio that is aware of its surroundings and adapts intelligently. While being cited mainly as an enabler for solving spectrum scarcity problems by the means of Dynamic Spectrum Access (DSA), perspectives and potential applications of Cognitive Radio technology far surpass the DSA alone. For example, cognitive capabilities and on-the-fly reconfiguration abilities of Cognitive Radios constitute an important next step in the communications electronic warfare. They may provide the jamming entities with abilities of devising and deploying advanced jamming tactics. Similarly, they may also aid development of advanced intelligent self-reconfigurable systems for jamming mitigation.

This thesis studies the impacts of Cognitive Radio technology on tactical battlefield solutions. A Software Defined Radio/Cognitive Radio test bed architecture was implemented in order to study principles and practice related to Radio Frequency (RF) jamming and anti-jamming problems. In addition, the test bed is used for developing and testing of the novel algorithms and solutions proposed within this thesis. The central part of the thesis is the proposed Spectrum Intelligence for Interference Mitigation algorithm, which performs real-time monitoring, analysis and online learning of relevant Radio Frequency spectrum activities, and takes proactive measures to improve communication robustness and continuity. Finally, the thesis proposes a game-theoretical framework for analyzing intelligent jamming and anti-jamming behaviour between Cognitive Radio systems.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation and objectives

Majority of the components comprising the legacy radio systems are defined in hardware, making the systems inflexible and, oftentimes, mutually noninteroperable. This has motivated the research of *Software Defined Radios*, which introduce programmable processors and highly modular software components into the system architecture. *Cognitive Radios* further embody Software Defined Radios with self-awareness and Radio Frequency (RF)-awareness potentials, as well as the abilities to reconfigure their operating parameters automatically.

Cognitive Radio has so far been given particular attention from the research community as an enabling technology for Opportunistic Spectrum Access. The focus of the work presented in this thesis, however, follows a different line – we study the potential impacts of Cognitive Radio technology to the communications electronic warfare domain. Namely, the work presented within this thesis addresses the following question: "how can a Cognitive Radio be utilized to devise and deploy jamming or anti-jamming tactics with higher probabilities of success by observing the patterns and anomalous occurrences in the RF spectrum and autonomously acting upon these observations?". The desired outcome of the undertaken research is to create an impact on future tactical battlefield solutions. For ensuring that our work reaches our target audience, a close collaboration with Selex ES – a leading Italian provider of military radio solutions – was established and maintained throughout.

1.2 Research contributions

The main contributions of the thesis are summarized as follows:

- A comprehensive overview of the main security issues related to Cognitive Radios and Cognitive Radio Networks is given.
- Technical details of the assembled Software Defined Radio/Cognitive Radio test bed architecture used for algorithm development, testing and validation are presented.
- An intelligent anti-jamming algorithm for Cognitive Radios called *Spectrum Intelligence for Interference Mitigation* is proposed, and the corresponding details of its implementation on the assembled test bed architecture are presented.
- A game-theoretical model for analyzing jamming/anti-jamming behaviour between Cognitive Radio systems is proposed. The parameters for the model are obtained using the assembled test bed architecture.

1.3 Thesis outline

The thesis is comprised of eight chapters that are based on a number of peer-reviewed journals, conference and workshop papers, and a book chapter. Each chapter is intended to serve as a stand-alone technical textbook, and re-introduces all relevant concepts needed to gain a comprehensive insight into the topics it discusses, along with the corresponding bibliography. The exceptions are several cross-references to Chapter 4, which describes the test bed architecture used for testing and validation of the algorithms presented in Chapters 5–7.
The thesis is organized as follows:

Chapter 2 gives background on the Cognitive Radio technology, introducing basic concepts, interesting research topics, and common use cases. In addition, it provides my own outlook on where Cognitive Radio technology currently is, and where it is heading. In great way, this outlook was shaped by my conversations and attended seminars with some of the pioneers and the leading minds of the Cognitive Radio research and development – names such as Joseph Mitola, James Neel and Pramod Varshney, among others. Finally, the chapter provides an overview of the state-of-the-art literature related to intelligent jamming and anti-jamming systems that utilize Cognitive Radio technology. These may be categorized as theoretical, experimental, and game-theoretical advances in the field.

Chapter 3 provides a comprehensive overview of the major security issues related to Cognitive Radios and Cognitive Radio Networks. In addition, security issues that Cognitive Radios inherit from Software Defined Radios as well as from legacy radio

systems are discussed. Besides the state-of-the-art review of the most relevant security issues, the chapter proposes a simple location-based method for identifying Primary User Emulation attackers.

Chapter 4 describes the Software Defined Radio/Cognitive Radio test bed architecture that was assembled with the goal of porting and testing of all of the relevant developed algorithms. Because of the high number of abstractions introduced by even the most complex and accurate simulation environments, assembling a real-life test bed was paramount for performing a meaningful study of jamming and anti-jamming behaviour. The algorithms and use cases demonstrated using the assembled architecture represent a good example of how Software Defined Radios may be embodied with self-awareness and self-reconfigurability capabilities, thus ultimately evolving towards Cognitive Radios.

Chapter 5 discusses traditional RF jamming and anti-jamming concepts and techniques, i.e., those relying on legacy radio systems for achieving their respective goals. Even though RF jamming is a concept almost as old as the wireless communication itself, the problems related to both the jamming and anti-jamming systems remain far from solved, as the "arms race" between the two continues to be ever-evolving. In order to understand how Software Defined Radios and Cognitive Radios may be used to successfully impact the domain of the jamming and anti-jamming systems, it is mandatory to understand the underlying principles and practice of traditional RF jamming and anti-jamming solutions. In addition, the chapter presents experimental results of jamming efficiencies of various interfering signals on the wideband QPSK-modulated waveform under different jamming-to-signal regimes.

Chapter 6 is the central part of the thesis, focused on explaining the "cognitive" part of the Cognitive Radio jamming/anti-jamming systems. Particular attention is given to the conceptualization and the implementation of the Spectrum Intelligence for Interference Mitigation – an intelligent anti-jamming system that deploys several Cognitive Radio functionalities, such as energy detection spectrum sensing, feature detection and waveform classification, and self-reconfiguration and self-awareness. The chapter places focus on giving practical solutions to overcome issues and constraints involved with the successful design and deployment of the proposed system.

Chapter 7 analyzes the intelligent jamming/anti-jamming systems from a game-theoretical perspective. Game theory was shown to be an excellent tool for the mathematical formalization of the jamming/anti-jamming events. Main contributions of the chapter with respect to the state-of-the-art include analysis of the role of spectrum sensing mechanisms in deploying advanced jamming/anti-jamming tactics, and

bridging the gaps between the game theory and practical systems by using the implemented test bed architecture to infer all the parameters necessary for the meaningful game-theoretical analysis.

Chapter 8 concludes the thesis, wrapping up the most important concepts, highlighting major findings, and proposing possible future extensions.

Chapter 2

Background and related work

This chapter introduces the concepts associated with Cognitive Radio and Software Defined Radio technologies, discussing their advances since early days up to present. It also presents the most interesting applications associated with Cognitive Radio systems, as well as the underlying enabling technologies. Finally, review of the state of the art advances in the field of Cognitive Radio jamming and anti-jamming is presented.

2.1 Cognitive radio technology – preliminaries

Over the past decade, Cognitive Radio has emerged as a "hot topic" in the telecommunications industry and research. However, there is no unanimous definition of what Cognitive Radio technology precisely constitutes. Thus, it is useful to introduce Cognitive Radio by summarizing definitions of some of the visionaries and the leading authorities in the fields of the Cognitive Radio research, development and regularization:

- Joseph Mitola [22]:
  "A really smart radio that would be self-, RF- and user-aware, and that would include language technology and machine vision along with a lot of high-fidelity knowledge of the radio environment."

- Simon Haykin [17]:
  "A radio capable of being aware of its surroundings, learning, and adaptively changing its operating parameters in real-time with the objective of providing reliable anytime, anywhere, and spectrally efficient communication."

- The Institute of Electrical & Electronic Engineers (IEEE):
  "A radio frequency transmitter/receiver that is designed to intelligently detect whether a particular segment of the radio spectrum is currently in use, and to jump into (and out of, as necessary) the temporarily-unused spectrum very rapidly, without interfering with the transmissions of other authorized users."

- ITU's Radiocommunication Study Group [19]:
  "A radio or system that senses, and is aware of, its operational environment and can dynamically and autonomously adjust its radio operating parameters accordingly."

Clearly, the definitions somewhat vary – occasionally it is only a matter of semantics, whereas sometimes the definition is pertinent to a specific application of the Cognitive Radio technology. However, two common underlying features are present in all of the definitions: intelligence and self-adaptivity of the operational parameters. Our definition of Cognitive Radio follows the same path: the work presented in this thesis is focused precisely on exploring how the combination of self-adaptivity and intelligence – as two vital characteristics of Cognitive Radio systems – may be applied to devise and deploy jamming and anti-jamming systems with higher probability of success.

Cognitive Radios by and large utilize Software Defined Radios (SDRs) as underlying platforms, further embodying them with machine learning mechanisms, and also potentially equipping them with smart antennas, geolocation capabilities, biometrical identification, etc. Because of this strong connection between the two communication paradigms, SDR technology warrants a brief introduction.

Just like Cognitive Radio, SDR is not a standardized technology. For this reason, there is no stringent definition on what criteria a radio has to satisfy in order to be considered "software defined". One of the most adopted, and in the same time very intuitive ones is the definition offered by the Wireless Innovation Forum, which recognizes SDR as "a radio in which some or all of the physical layer functions are software defined" [12].

An "ideal" SDR would have all the radio-frequency bands and modes defined in software, meaning it would consist only of an antenna, Digital-to-Analog Converter (DAC) and/or Analog-to-Digital Converter (ADC), and a programmable processor. However, in practical systems, a Radio Frequency (RF) front-end has to be implemented as well in order to support the receive/transmission mode. Typically, an RF front-end of an SDR consists of antenna circuitry, amplifiers, filters, local oscillators, and ADCs/DACs. The processing is done by the deployed computational

resources: most commonly General Purpose Processors (GPPs), Digital Signal Processors (DSPs) and Field Programmable Gate Arrays (FPGAs), or a combination of the aforementioned [9]. A typical hardware architecture of a modern SDR transceiver is shown in Figure 2.1.

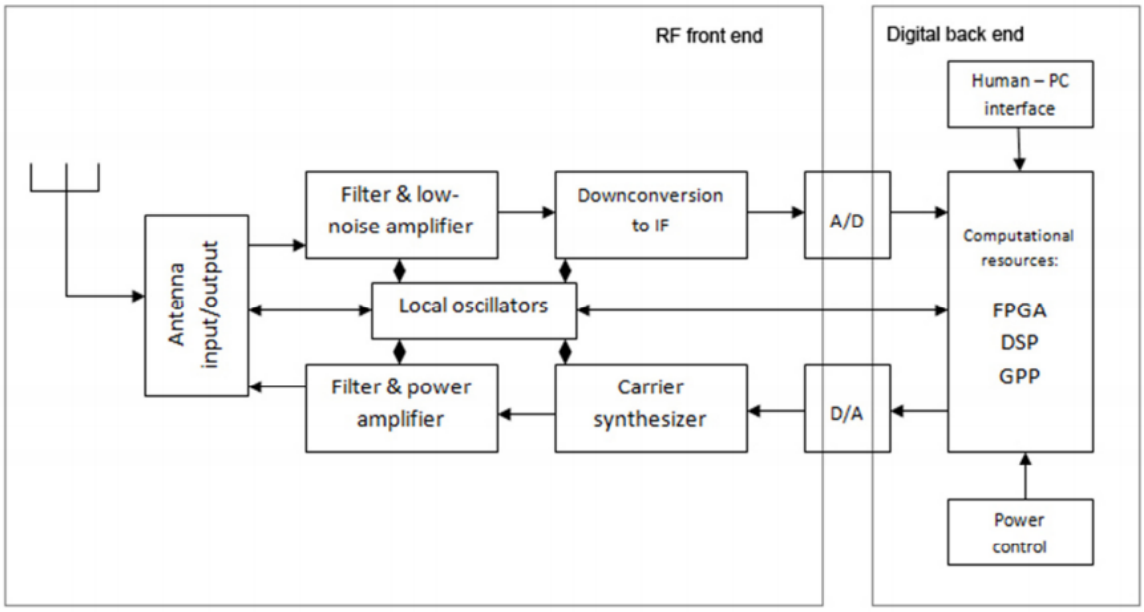


Figure 2.1: Basic hardware architecture of a modern SDR

However, perhaps even more than by the abstraction of their hardware components, SDRs are represented by the modular and reusable manner of developing the corresponding firmware, software and waveforms. Indeed, a standardized manner of introducing new waveforms to the platform and compatibility with other platform implementations is usually at the heart of any SDR design.

2.1.1 From legacy radio systems to Cognitive Radios

Shifting from legacy hardware-based systems to software defined architectures and, eventually, their embodiment with self-adaptivity and machine learning capabilities, is a gradual process that started in the early 1990s. Whereas SDR and Cognitive Radio paradigms were initially of interest primarily to the military, over the past years they have started to attract significantly more interest from the industry and academia as well. Figure 2.2 illustrates some of the most important milestones in Cognitive Radio development.

Arguably the first system that started deploying some of the functionalities of what will later become known as the SDR paradigm, was the Integrated Communica-

Figure 2.2: Timeline of Cognitive Radio development

tions, Navigation, and Identification Architecture (ICNIA) [6], dating back to 1987. The ICNIA was a multiple-radio system consisting of a number of self-testing line replaceable modules that comprised an aircraft radio suite.

The term SDR itself was coined somewhat later when, in 1991, Joseph Mitola published his seminal paper [24] describing the architecture of a possible SDR system.

SDR technology started gaining particular prominence in the military communications domain, where it was viewed as a potential facilitator for interoperable tactical radio solutions, where a multitude of mutually incompatible technologies were deployed in the 2 MHz–2 GHz part of the frequency band. SpeakEasy and SpeakEasy II projects, which took place during the 1990s, have established the basic structure of today's SDRs. These were eventually refined, leading to the Joint Tactical Radio System (JTRS) – an effort by the United States army to create an integrated network of military radio technologies. Even though the project was abandoned in 2011, it has left a valuable legacy in the form of the Software Communications Architecture (SCA) – an open-architecture framework that details the software structure and interfaces for the designs of the SDRs. SCA has up to date remained a dominant framework for the design of military SDR systems and solutions.

In 1996, the first SDR-dedicated industry association was created, which would soon become known as the SDR Forum. The organization comprised experts from the industry, military, regulatory agencies and academia, and had a goal of creating innovative products, solutions and standards in the SDR domain. In 2010, it was renamed to Wireless Innovation Forum.

In 2000, Mitola introduced and described the concepts of Cognitive Radios [25]. Built on the SDR architecture, Mitola's ideas of Cognitive Radios introduced several concepts that would later become popular and relevant research topics, such as more efficient use of the RF spectrum, interference avoidance, and the radios' potential impacts on the end users' daily routines.

The interest of the academic community for the Cognitive Radio research was further sparked by Simon Haykin's 2006 paper [17], up to date the most cited paper in the Cognitive Radio research community. Haykin highlighted Opportunistic Spectrum Access (OSA) as a particular application of interest, eventually leading many researchers to associate the whole Cognitive Radio technology solely with the application of OSA.

Concurrently, significant efforts were being made by the industry and regularization bodies, resulting in the first IEEE standard for Cognitive Radios: 802.22 WRAN

[31]. The standard specified technical requirements for the opportunistic use of the TV white spaces.

In late 2000s, development of low-cost off-the-shelf SDR/Cognitive Radio platforms brought the possibility of Cognitive Radio development and experimentation to a wider part of the academia, as well as to home enthusiasts. Some of the most popular platforms up to date remain Ettus Research's Universal Software Radio Peripherals (USRPs) [28]. Significant part of their appeal lies in the open-source nature of the underlying software architecture, called GNU Radio [16].

2.1.2 Enabling technologies

In order to successfully exploit numerous opportunities and exciting applications associated with Cognitive Radio technology, technical difficulties related to the underlying enabling technologies need to be adequately addressed. Two technologies most commonly associated with proper functioning of Cognitive Radios are spectrum sensing and databases.

Spectrum sensing is a method for inferring spectrum occupancy information that has so far been given the most attention in the research community. Using these inferences, Cognitive Radio can adapt its operating parameters, such as transmission frequency, transmission power, modulation scheme, and deployed waveform, in order to achieve its goal. Different spectrum sensing approaches have been proposed and analyzed in the past, the most popular ones being energy detection, matched filters and feature detectors. These are mainly differentiated by their computational complexity, necessity for a priori knowledge of the observed signals, and the means of extracting features of the recognized signals.

Energy detection [26] is the simplest and thus easiest to implement among the aforementioned methods. The energy detector aims at solving the decision problem between the following two hypotheses [11]:

$$Y(n) = \begin{cases} W(n) & H_0 \\ X(n) + W(n) & H_1 \end{cases} \tag{2.1}$$

where $Y(n)$, $X(n)$ and $W(n)$ are the received signals, transmitted signals and noise samples, respectively, H_0 is the hypothesis corresponding to the absence of the signal, and H_1 is the hypothesis corresponding to the presence of the signal. The decision on the spectrum occupancy is made by comparing the test statistic T with the detection threshold λ. T may, for example, be defined as the average energy of the observed

samples, i.e.:

$$T = \frac{1}{N} \sum_{n=1}^{N} |Y(n)|^2. \tag{2.2}$$

Main advantages of energy detectors: implementational simplicity and blind sensing, are often overshadowed by their major setbacks: unreliability in low Signal-to-Noise Ratio (SNR) regimes, high probability of false alarm due to noise uncertainty problems, and inability to differentiate between the sensed signals.

A popular method that relies on the prior knowledge of the sensed channel and/or user's signal is called *matched filters* [20]. Matched filters correlate the received signal with the already known signal, comparing their frequencies, bandwidths, modulation types, etc. While typically exhibiting the best performance in low SNR regimes among the three mentioned approaches, matched filters require complex signal processing and additional hardware equipment, since each type of signal present in the system requires its separate receiver and the corresponding algorithm.

Feature detectors are based on extracting certain features of the received signal, and comparing them to the features of the already known signals. These features may be cyclostationary characteristics of the signal [37], which are consequence of periodicities such as modulation rate. Alternatively, certain reference features may be extracted from the outputs of the energy detector, such as the signal's bandwidth, shape and magnitude. Feature detectors typically achieve better performance than energy detectors in low-SNR regimes, but their performance falls short from the perfect matched filters.

An alternative approach to spectrum sensing for obtaining spectrum information is utilized by *geolocation-database* Cognitive Radios. These radios are assumed to be geographically aware, and to have the ability to access a database containing relevant spectrum information. Among several approaches for constructing such databases, arguably the best well known are *Radio Environment Maps (REMs)* [40]. REM is a database that contains multi-domain information describing the environment in a certain geographical area. This information typically includes spectral regulations, terrain features, and the locations and activities of radios.

2.1.3 Interesting applications

Among a plethora of potential applications of Cognitive Radios, four of them stand out: interoperability, Dynamic Spectrum Access, cognitive Multiple Input Multiple Output (MIMO), and advanced Communications Electronic Warfare (CEW) solutions.

One of the primary motivations for the development and application of the SDR technology, particularly in the military domain, is waveform and software cross-compatibility and *interoperability* [30]. The SCA describes software components of an SDR and defines its interfaces. This in turn provides the basis for re-use of modules and radio functions. As Cognitive Radios are by and large defined as upgraded SDRs, interoperability as a motivating application may be extended to the Cognitive Radio domain, since a Cognitive Radio can be implemented under the SCA standard. Importance and popularity of the SCA as the underlying software architecture for SDR and Cognitive Radio development is illustrated by Figure 2.3, which shows recent national and international programs focused on SDR and Cognitive Radio development that have adopted the SCA standard [13].

DSA techniques are expected to bring about means for better radio frequency spectrum utilization. These may be categorized under three models: Dynamic Exclusive Use, Open Sharing, and Hierarchical Access Models [39]. Opportunistic Spectrum Access is a form of the Hierarchical Access Model, where unlicensed Cognitive Radios (secondary users) are allowed to utilize the spectrum as long as the communication of licensed (primary) users is protected. In order to access the spectrum opportunistically, secondary users need to be able to acquire the spectrum occupancy information, using one of the technologies described in section 2.1.2. From a commercial perspective, OSA is the most interesting application of Cognitive Radios, as efficient spectrum sharing could bring significant revenues to the spectrum lessors. From a regulatory standpoint, it is one of the most challenging issues to solve, due to rigid requirements for protecting licensed users' communication.

MIMO design may bring several enhancements to the radio system, such as capacity enhancement, providing spatial diversity, effective co-channel interference reduction, and spatial multiplexing. However, introduction of multiple antennas brings several challenges, such as increased complexity, real-time tracking of ever-changing channel characteristics, and adapting to users' needs. The role of the cognitive element may then be to determine the "optimal" transmission scheme based on the observable parameters. These techniques are commonly referred to as *cognitive MIMO* [4].

Maintaining reliable communication with the friendly units, while preventing the adversaries from successfully doing so can give a crucial edge on the tactical battlefield. For this reason, interoperability and advanced self-adaptive capabilities provided by Cognitive Radio technology are of particular interest in the *Communications Electronic Warfare (CEW)* domain. By taking advantage of the on-the-fly reconfiguration capabilities and learning techniques, more robust communication systems, as well as

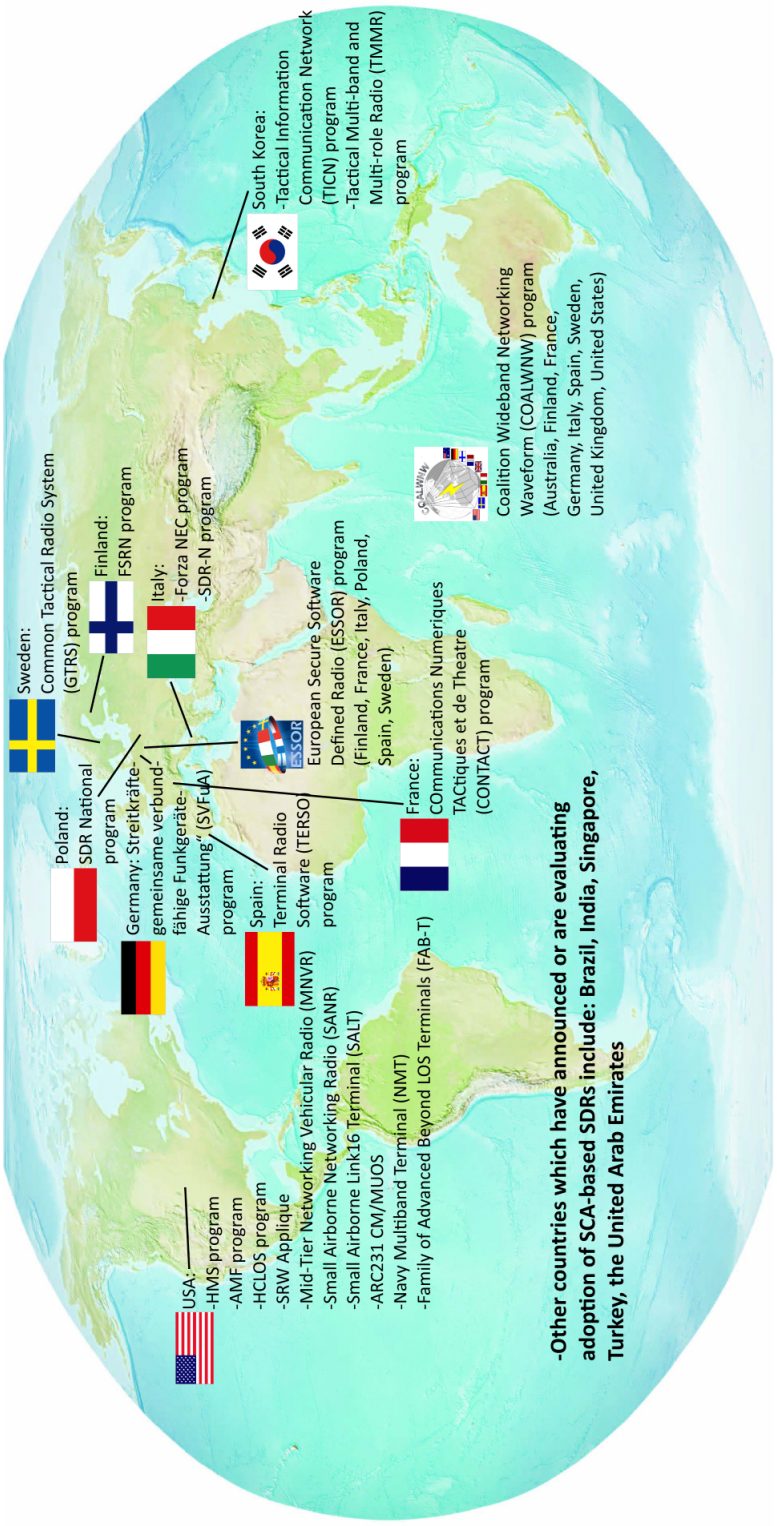


Figure 2.3: SDR and Cognitive Radio research programmes that have adopted the SCA standard [13]

jamming/interception systems with higher probability of success, may be constructed and deployed [10].

2.1.4 Current status and future developments

SDR and Cognitive Radio paradigms continue to attract particular interest in the military domain. Since the early days of the SDR technology approximately 25 years ago, most western countries have had tremendous progress with making their tactical battlefield solutions software-defined. The United States Department of Defense has arguably been the largest investor in R&D of SDR military equipment (e.g., through the aforementioned JTRS programme). As a result, almost all of the United States army's military radio solutions are now software-defined. In turn, the United States army is currently starting to look towards embodying the radios with certain levels of self-adaptability and, ultimately, cognitivity. In Europe, great efforts are currently being put forward by NATO partners for creating interoperable (STANAG-based) waveforms for tactical SDR solutions, and deploying them to the battlefield. One of the most pressing issues, however, is the lack of standardization – a problem which is currently being tackled by the European Defence Standardisation System and NATO, who recently presented a "Roadmap for the development of defence standards". The ultimate objective is worldwide standardization of SDR-based solutions, although reaching this goal still seems to be several years ahead.

Current trends, however, indicate that huge monetary investments from the military into SDR and Cognitive Radio R&D are becoming a matter of past. This is particularly highlighted with the development of low-cost off-the-shelf programmable processors, and even full SDR/Cognitive Radio platforms. Having recognized these potentials, the military is nowadays turning towards the industry in order to develop systems that can be fielded faster and at lower costs, and that are able to provide open architectural solutions and commonality as a basis for interoperability. United States Department of Defense has stated that it "wants their radio solutions to be more spectrally efficient, and to take more advantage of the concepts that the Cognitive Radio technology proffers". The ultimate goal is "deploying portable, affordable and energy efficient Cognitive Radios in the field." [23]

In the academia, Cognitive Radio continues to be a hot research topic. Figure 2.4, which plots the number of research articles with the most common keywords related to Cognitive Radio, is a good illustration of the recent research trends. As indicated by the figure, database Cognitive Radios and Cognitive Radios deploying compressed

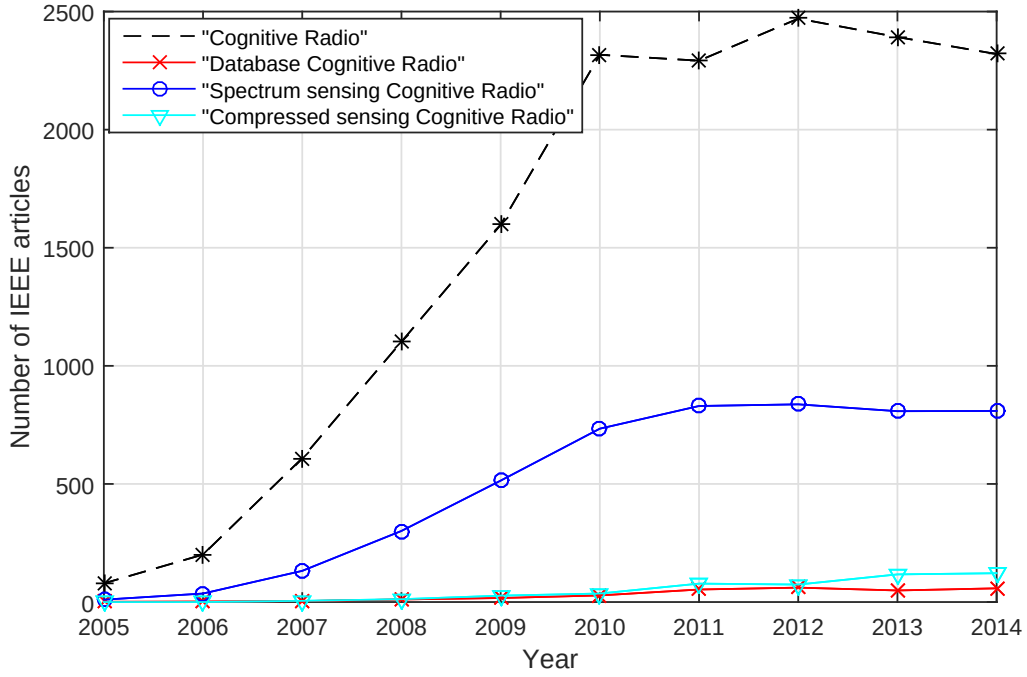


Figure 2.4: Number of articles available on IEEExplore indicating "hot topics" in the Cognitive Radio research community

sensing have started gaining significant interest from the academic community over the last 4–6 years, and continue to represent popular research topics.

Compressed sensing, a set of techniques that enable successful spectrum estimation and reconstruction from sub-Nyquist rate sampling, may relax the burdens on the sampling rates of the radios' ADCs. This may in turn significantly reduce the hardware costs of the deployed equipment, making it a topic of particular interest. Compressed sensing is, however, as of now still largely considered an "academic exercise" – both the industry and the military are yet to match the recent advances in the field, and to start deploying them in their solutions.

Geolocation-databases have started gaining attention as more practical alternatives (or, in some cases, complementary mechanisms) to spectrum sensing for enabling OSA. They manage to overcome many of the uncertainty, reliability and safety issues associated with Cognitive Radios utilizing spectrum sensing, such as hidden node problems, user emulation attacks, and noise uncertainties. Although arguably not as exciting research topic as various spectrum sensing methods (highlighted by the disproportion in the number of articles between the two topics in Figure 2.4), geolocation/databases continue to affirm themselves as primary enablers for OSA in future

Cognitive Radio Networks. Spectrum sensing will most probably continue to serve as a supporting technology, e.g., as in case of the 802.22 WRAN standard [31].

Besides the tremendous interest from the military, the academia and, lately, the industry, SDRs and Cognitive Radios have recently started finding their place among the home radio enthusiasts as well. This is largely due to the increase in availability and affordability of the necessary components. A good example is reported by Cass [7], where the author presented an SDR assembled for only $40 using low-cost off-the-shelf components. The SDR was able to receive a large variety of transmissions with different modulation schemes, and to monitor wideband RF spectrum activities in real-time.

Whereas many of the technical issues related to Cognitive Radios have already been, or are on their way to be, solved, some of the major obstacles for commercial deployment of Cognitive Radio systems remain to be of regulatory nature. This is particularly true for the application of OSA. Since RF spectrum is an expensive resource, licensed users want assurances that reliable, tested spectrum auction mechanisms are in place before agreeing to subrent their parts of the spectrum to unlicensed users.

Cognitive Radio research is currently in its very exciting phase – as SDR is becoming a dominant design architecture for wireless systems, serious deployment of Cognitive Radios is finally on the horizon. As military, industry and the academics continue to cross paths and exchange knowledge, and as standardization and regularization bodies started placing more focus on Cognitive Radio technology, it is not unreasonable to expect the Cognitive Radio systems deployed ubiquitously by the year 2020.

2.2 Intelligent RF jamming and anti-jamming – related work

RF jamming is a process of creating intentional harmful interference at the targeted systems. Devices that create such interference are referred to as the *jammers*, and may mutually differ in design, strategies, and capabilities. Conversely, *anti-jamming systems* are designed with the goal of precluding RF jamming from successfully taking place. When Cognitive Radios are used to devise RF jamming or anti-jamming systems, such systems are called *intelligent*. This section introduces state-of-the art contributions in the domain of intelligent RF jamming and anti-jamming systems.

The contributions are categorized as theoretical, experimental, and game-theoretical advances in the field.

2.2.1 Theoretical contributions

Theoretical contributions mostly focus on proposing different jamming and anti-jamming tactics, and studying their influence under different system parameters. Typically, proposed methods are supported by simulations performed in the commercial and open-source network simulation environments, such as OMNEST [18], OPNET [32], and Network Simulator 3 [14].

One of the seminal theoretical works on intelligent jamming and anti-jamming systems was presented by Xu et al. [36]. The authors have introduced four different types of jamming attacks: constant, deceptive, random, and reactive, and studied their effects on a wireless network. In addition, the paper has proposed several methods that an anti-jamming system could deploy in order to detect the presence of a jamming attack. Among them, signal strength consistency check and location information consistency check proved to be the most reliable methods.

Sampath et al. [29] have studied impacts that a Cognitive Radio jammer capable of transmitting on multiple channels simultaneously can have on targeted 802.11 network. Simulation results performed in Qualnet have indicated the jamming impacts for different numbers of channels, jamming packet size, and channel switching delays.

Thuente and Acharya [33] have considered an intelligent jammer that possesses awareness of the protocol of the targeted communication system, and is able to exploit crucial timings and control packets. Simulations performed in OPNET have indicated the benefit of using intelligent jamming over continuous jamming in terms of efficiency of signal duration leading to lower energy costs. Amuru and Buehrer [2] have extended this methodology to a more general case when the jammer may have delayed knowledge of the environment state as a result of processing delay.

2.2.2 Experimental contributions

Experimental contributions related to intelligent jamming/anti-jamming are still relatively scarce, mainly due to issues related to implementation complexity of intelligent jamming and anti-jamming systems and strict real-time requirements for signal detection and automatic reconfiguration of the parameters.

Wilhelm et al. [35] were among the first to demonstrate how off-the-shelf SDR platforms can be used to devise and deploy fast reactive jammers, i.e., jammers that

are able to reconfigure themselves in order to target the packets that are already transmitted over the air. The authors have presented an implementation of an intelligent jammer on a USRP2 SDR, and have demonstrated jamming performance of different jamming signals: single-tone, narrowband noise, and random modulated signals, in a 802.15.4 network.

Nguyen et al. [27] have presented an implementation of a real-time, protocol-aware, reactive jammer targeted for high-speed wireless networks. The implementation was done on a USRP N210 SDR. A combination of two algorithms for signal detection was implemented at the jamming side: signal cross-correlation and energy detection. The authors have performed study of the susceptibility of 802.16e networks to reactive jamming attacks.

Yao and Peng [38] have proposed an anti-jamming algorithm that is able to maintain communication in the presence of a broadband, high power reactive jammer by exploiting the jammer's reaction time (the time needed to perform spectrum sensing and to start transmitting). The proposed algorithm was based on a novel technique to identify unjammed bits from a received bit stream. In addition, it proposed an encoding and decoding technique that is able to recover the original message from message fragments with unknown positions in the original message. The implementation of both the reactive jammer, and the anti-jamming system consisting of a transmitter-receiver pair was done using USRP SDRs. The results indicated significant improvement in performance over the traditional spread spectrum anti-jamming systems.

Li et al. [21] have proposed a protocol that is capable of recovering regular network communications in the presence of jamming attacks. The protocol integrates jammer identification, jammer isolation, and key management schemes, and communicates new channels suitable for communication to all the users. The implementation was done on a USRP SDR.

2.2.3 Game-theoretical contributions

Conflict of interest between the RF jamming and the anti-jamming systems is obvious: the former aim to disrupt the successful communication of the latter, whereas the latter try to ensure that the communication takes place. For this reason, game theory – a mathematical framework for analysis of conflicts between rational players – is a suitable tool for analyzing jamming/anti-jamming problems. Namely, it allows for finding optimal and near-optimal strategies for jamming and anti-jamming entities, and to design learning algorithms that are able to converge to such strategies.

Most of the state-of-the-art contributions in the literature on application of game theory to intelligent jamming problems consider either channel surfing or power allocation as anti-jamming strategies. Furthermore, they are mutually differentiated mostly by the objective function subjected to optimization (Signal-to-Noise Ratio, Bit Error Rate, Shannon capacity); various forms of uncertainty (user types, physical presence, system parameters); game formulation (zero-sum vs. non-zero-sum, single-shot vs. dynamic), considered learning algorithms (Q-learning, SARSA, policy iteration), etc.

Altman et al. [1] have proven the existence and uniqueness of Nash equilibrium for a class of games with transmission cost. In addition, they have derived analytical expressions for the Nash equilibrium and have formulated the jamming game as the generalization of the water-filling optimization problem. Jamming game for OFDM system with 5 channels was analyzed.

Wang et al. [34] have formulated the problem of jamming in Cognitive Radio networks with primary users as a zero-sum stochastic game, where channel hopping was considered as the anti-jamming scheme, and minimax-Q as the learning algorithm. They have compared the performance of the developed stationary policy with the myopic decisioning policy which didn't consider the environment dynamics. The former was shown to exhibit significantly better performance in terms of overall spectrum-efficient channel throughout.

The method was extended by Chen et al. [8], who compared the results of Q-learning with those of the policy iteration scheme. The performance of the proposed scheme was evaluated against attackers of varying levels of sophistication.

Buchbinder et al. [5] and Garnaev et al. [15] have considered multi-carrier power allocation as an anti-jamming strategy, and have formulated the games as zero-sum. Buchbinder et al. [5] have derived lower bounds on the overall system performance for the proposed online learning algorithm. Garnaev et al. [15] have provided formal proofs of existence and uniqueness of Nash equilibrium points for a system where considered players have incomplete information on the channel gains.

Amuru and Buehrer [3] have studied optimal jamming strategies in terms of deployed modulation of the jamming waveform, depending on the deployed modulation types of the targeted system. For example, the authors have shown that, when the targeted system deploys either binary phase shift keying (BPSK) or quaternary phase-amplitude modulation (4-PAM), the optimal jamming signal is modulated using BPSK. Conversely, when the targeted system deploys either quaternary phase

shift keying (QPSK) or 2^4 quadrature amplitude modulation (16-QAM), the optimal jamming signal is modulated using QPSK.

Bibliography

[1] E. Altman, K. Avrachenkov, and A. Garnaev. A jamming game in wireless networks with transmission cost. In *Proceedings of the 1st EuroFGI International Conference on Network Control and Optimization*, NET-COOP'07, pages 1–12, Berlin, Heidelberg, 2007. Springer-Verlag.

[2] S. Amuru and R.M. Buehrer. Optimal jamming using delayed learning. In *Proceedings of the 2014 IEEE Conference on Military Communications*, pages 1528–1533, October 2014. doi: 10.1109/MILCOM.2014.252.

[3] S. Amuru and R.M. Buehrer. Optimal jamming strategies in digital communications–impact of modulation. In *Proceedings of 2014 IEEE Global Communications Conference (GLOBECOM), Austin, TX*, 2014.

[4] L. Bixio, G. Oliveri, M. Ottonello, M. Raffetto, and C.S. Regazzoni. Cognitive radios with multiple antennas exploiting spatial opportunities. *Signal Processing, IEEE Transactions on*, 58(8):4453–4459, August 2010. doi: 10.1109/TSP.2010.2048322.

[5] N. Buchbinder, L. Lewin-Eytan, I. Menache, J. Naor, and A. Orda. Dynamic power allocation under arbitrary varying channels: an online approach. *IEEE/ACM Transactions on Networking*, 20(2):477–487, April 2012. doi: 10.1109/TNET.2011.2170092.

[6] P. Camana. Integrated communications, navigation, identification avionics (ICNIA)-the next generation. *Aerospace and Electronic Systems Magazine, IEEE*, 3(8):23–26, Aug 1988. doi: 10.1109/62.890.

[7] S. Cass. A 40$ software-defined radio. *Spectrum, IEEE*, 50(7):22–23, July 2013. doi: 10.1109/MSPEC.2013.6545114.

[8] C. Chen, M. Song, C. Xin, and J. Backens. A game-theoretical anti-jamming scheme for cognitive radio networks. *Network, IEEE*, 27(3):22–27, 2013. doi: 10.1109/MNET.2013.6523804.

[9] K. Dabcevic. Evaluation of software defined radio platform with respect to implementation of 802.15.4 ZigBee. Master's thesis, Malardalen University, School of Innovation, Design and Engineering, 2011.

[10] K. Dabcevic, M.O. Mughal, L. Marcenaro, and C.S. Regazzoni. Spectrum intelligence for interference mitigation for cognitive radio terminals. In *Proceedings of SDR'14 -WinnComm-Europe*, November 2014.

[11] 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):21–25, 2007.

[12] Wireless Innovation Forum. Sdrf cognitive radio definitions working document, sdrf-06-r-0011-v1.0.0. URL `http://groups.winnforum.org/d/do/1585`. [Accessed: 2015-01-13].

[13] Wireless Innovation Forum. SCA standards for defense communications, 2015. URL `http://www.wirelessinnovation.org/assets/sca%20standards%20-%20global%20adoption%20version%201.0%20high%20res%20final.pdf`. [Accessed: 2015-02-13].

[14] National Science Foundation. Network simulator 3. `http://www.nsnam.org`, 2014. [Accessed: 2015-01-13].

[15] A. Garnaev, Y. Hayel, and E. Altman. A bayesian jamming game in an OFDM wireless network. In *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2012 10th International Symposium on*, pages 41–48, 2012.

[16] GNU Radio Website. URL `http://www.gnuradio.org`. [Accessed: 2015-01-14].

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

[18] Simulcraft Inc. Omnest. `http://www.omnest.com`, 2013. [Accessed: 2015-01-13].

[19] International Telecommunication Union. Report ITU-R SM.2152 Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS), 2009.

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

[21] L. Li, S. Zhu, D. Torrieri, and S. Jajodia. Self-healing wireless networks under insider jamming attacks. In *Communications and Network Security (CNS), 2014 IEEE Conference on*, pages 220–228, Oct 2014. doi: 10.1109/CNS.2014.6997489.

[22] P. Mannion. Smart radios stretch spectrum. *Electronic Engineering Times (EE-Times)*, 2006(8), 2006.

[23] J. McHale. Military market trends: Funding cutbacks drive commonality in electronics. Keynote lecture presented at the WinnComm-Europe-2014 conference, 2014.

[24] J. Mitola III. Software radios - survey, critical evaluation and future directions. In *Telesystems Conference, 1992. NTC-92., National*, pages 13/15–13/23, May 1992. doi: 10.1109/NTC.1992.267870.

[25] J. Mitola III. *Cognitive Radio — An Integrated Agent Architecture for Software Defined Radio*. DTech thesis, Royal Institute of Technology (KTH), Kista, Sweden, May 2000.

[26] M.O. Mughal, A. Razi, S.S. Alam, L. Marcenaro, and C.S. Regazzoni. Analysis of energy detector in cooperative relay networks for cognitive radios. In *Next Generation Mobile Apps, Services and Technologies (NGMAST), 2013 Seventh International Conference on*, pages 220–225, September 2013. doi: 10.1109/NGMAST.2013.47.

[27] D. Nguyen, C. Sahin, B. Shishkin, N. Kandasamy, and K.R. Dandekar. A real-time and protocol-aware reactive jamming framework built on software-defined radios. In *Proceedings of the 2014 ACM Workshop on Software Radio Implementation Forum*, SRIF '14, pages 15–22, New York, NY, USA, 2014. ACM. doi: 10.1145/2627788.2627798.

[28] Ettus Research. USRP product categories. URL `http://www.ettus.com/product`. [Accessed: 2015-01-14].

[29] A. Sampath, H. Dai, H. Zheng, and B.Y. Zhao. Multi-channel jamming attacks using cognitive radios. In *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*, pages 352–357, August 2007. doi: 10.1109/ICCCN.2007.4317844.

[30] D. Scaperoth, B. Le, T. Rondeau, D. Maldonado, C.W. Bostian, and S. Harrison. Cognitive radio platform development for interoperability. In *Military Communications Conference, 2006. MILCOM 2006. IEEE*, pages 1–6, October 2006. doi: 10.1109/MILCOM.2006.302233.

[31] C.R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S.J. Shellhammer, and W. Caldwell. IEEE 802.22: The first cognitive radio wireless regional area network standard. *IEEE Communications Magazine*, 47(1):130–138, January 2009. doi: 10.1109/MCOM.2009.4752688.

[32] Riverbed Technology. Opnet. `http://www.riverbed.com/products/performance-management-control/opnet.html`, 2015. [Accessed: 2015-01-13].

[33] D.J. Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In *Proceedings of the 2006 IEEE Conference on Military Communications*, MILCOM'06, pages 1075–1081, Piscataway, NJ, USA, 2006. IEEE Press.

[34] B. Wang, Y. Wu, K.J.R. Liu, and T.C. Clancy. An anti-jamming stochastic game for cognitive radio networks. *Selected Areas in Communications, IEEE Journal on*, 29(4):877–889, 2011. doi: 10.1109/JSAC.2011.110418.

[35] M. Wilhelm, I. Martinovic, J.B. Schmitt, and V. Lenders. Short paper: Reactive jamming in wireless networks: How realistic is the threat? In *Proceedings of the Fourth ACM Conference on Wireless Network Security*, WiSec '11, pages 47–52, New York, NY, USA, 2011. ACM. doi: 10.1145/1998412.1998422.

[36] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, pages 46–57, New York, NY, USA, 2005. ACM. doi: 10.1145/1062689.1062697.

[37] L. Yang, Z. Chen, and F. Yin. Cyclo-energy detector for spectrum sensing in cognitive radio. *AEU - International Journal of Electronics and Communications*, 66(1):89 – 92, 2012. doi: http://dx.doi.org/10.1016/j.aeue.2011.05.004.

[38] L. Yao and N. Peng. Bittrickle: Defending against broadband and high-power reactive jamming attacks. In *INFOCOM, 2012 Proceedings IEEE*, pages 909–917, March 2012. doi: 10.1109/INFCOM.2012.6195840.

[39] Q. Zhao and B.M. Sadler. A survey of dynamic spectrum access. *Signal Processing Magazine, IEEE*, 24(3):79–89, May 2007. doi: 10.1109/MSP.2007.361604.

[40] Y. Zhao, L. Morales, J. Gaeddert, K.K. Bae, Jung-Sun Um, and J.H. Reed. Applying radio environment maps to cognitive wireless regional area networks. In *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pages 115–118, April 2007. doi: 10.1109/DYSPAN.2007.22.

Chapter 3

Security issues of Cognitive Radios

Cognitive Radio can be described as an intelligent and dynamically reconfigurable radio that can adaptively regulate its internal parameters as a response to changes in the surrounding environment. Namely, its parameters can be reconfigured in order to accommodate the current needs of either the network operator, the spectrum lessor, or the end user.

Cognitive Radio is usually defined as an upgraded and enhanced *Software Defined Radio (SDR)*. Typically, full Cognitive Radios will have learning mechanisms based on some of the deployed machine learning techniques, and may potentially also be equipped with smart antennas, geolocation capabilities, biometric identification, etc.

One of the most important capacities of Cognitive Radio systems is their capability to optimally adapt their operating parameters based on observations and previous experiences. There are several possible approaches towards realizing such cognitive capabilities, such as:

- Reinforcement learning;
- Learning based on neural networks;
- Game-theoretical approach;
- etc.

Reinforcement learning refers to machine learning methods in which the radio learns through trial-and-error interactions in a scenario without perfect contextual information. It is a mathematical method used in the learning stage of the cognitive cycle (an example of a cognitive cycle is given in section 6.1). Radio learns the information based on the consequences of its previous actions, and chooses new actions by observing the numerical rewards previously received. The goal of the radio is to

select strategies in a way that would maximize the expected accumulated reward over time [15].

Artificial Neural Networks (ANNs) are mathematical models inspired by the structure and functioning of biological neural networks [3]. ANNs can change and adapt their structure based on data used during the learning phase. Furthermore, they are able to discover and model complex relationships among acquired data. ANNs can be trained by automatically selecting one model from the set of the allowed models for the network. This is typically done by cost function minimization (cost functions are directly dependent on the desired tasks). There are multiple algorithms available for training neural network models; most of them can be viewed as a straightforward application of optimization theory and statistical estimation. Most of the algorithms used in training ANNs employ some form of gradient descent. This is done by taking the derivative of the cost function with respect to the network parameters, and then changing those parameters in a gradient-related direction. Evolutionary methods [16], simulated annealing [19], expectation-maximization, non-parametric methods and particle swarm optimization [18] are some of the commonly used methods for training Artificial Neural Networks.

Game theory is a mathematical study of strategic interaction processes between multiple independent decision makers. Since users within Cognitive Radio Networks can be modeled as such decision makers, game theory presents itself as a natural structure for analyzing users' behaviors and actions, as well as for modeling suitable strategies in order to overcome the crucial interoperability issues. Application of game theory to Cognitive Radio Networks is multifold – ranging from formalization of the issues pertaining to Dynamic Spectrum Sharing (DSS), through supplying different optimality criteria for the spectrum sharing, to deriving efficient distributed approaches for DSS by using the non-cooperative game theory. Simpler game-theoretical solutions typically do not account for the learning capabilities of Cognitive Radios; however, it is possible to model more advanced games, such as Bayesian games, in order to account for the algorithms with learning capabilities. Game theory can furthermore be viewed as a set of tools for analyzing security-related issues, as has been studied for example by Liu and Wang [23].

Deployment of learning techniques represents one of the fundamental parts of the Cognitive Radio paradigm. By using one of the approaches described above, Cognitive Radios are able to observe and learn the status of the surrounding environment, which in turn allows them to utilize the Radio Frequency (RF) spectrum in a more efficient manner. The outcome of this learning process may then be used by Cognitive Radio

devices to improve efficiency in accessing available spectrum resources. In other words, Cognitive Radios can, for example, learn different patterns of licensed users' activities in order to be able to forecast availability of the resources and to adapt dynamically to the sensed conditions. Knowledge about spectrum usage can be built by each user without interacting with other users. Alternatively, users can collaborate in order to not only exchange network information, but also to model and update the observed patterns in the radio environment.

The aforementioned cognitive capabilities of Cognitive Radios are exactly what makes them susceptible to a whole new set of possible security issues and breaches. For example, if a malicious user is aware of the learning capabilities of the Cognitive Radio devices in the network, it can adopt a specific activity pattern in order to deceive the Cognitive Radios, thus possibly dramatically decreasing the overall performance of the targeted radios and of the network. It is thus important to understand the possible threats in order to be able to adequately respond to them. Furthermore, the threats that Cognitive Radios inherit from Software Defined Radios, as well as from legacy radio systems, also need to be taken into account.

This chapter describes the most common security threats and the corresponding state-of-the-art solutions for legacy radio systems, SDRs, and Cognitive Radios/Cognitive Radio networks.

3.1 Threats to legacy wireless systems

There are several established security standards for wireless networks in use today. In this section, general security issues in cellular networks, as well as the most widespread mechanisms for WLAN security – WEP, WPA and WPA2 – are reviewed.

3.1.1 Security issues in wireless cellular networks

The openness of communication characteristic to wireless cellular networks brings a set of security issues that need to be addressed. Hereafter follows the description of main issues associated with the most widely used communication standards: GSM, GPRS, 3G, and LTE.

Being the standard that had the highest impact in the evolution of commercial wireless cellular networks, *Global System for Mobile Communications (GSM)* has throughout its existence been given particular attention from a security standpoint. GSM incorporates several built-in security features responsible for ensuring subscribers' safety and privacy, namely [17]:

- Authentication of the registered subscribers only;
- Secure data transfer through the use of encryption;
- Subscriber identity protection;
- Inoperability of mobile phones without a SIM;
- Forbiddenness of duplicate SIMs on the network;
- Securely stored Ki.

Most of the security mechanisms in GSM are based on cryptographic algorithms, which vary depending on the functionality that they are designed to protect. The main algorithms are A5 (a stream cipher used for encryption), A3 (an authentication algorithm), and A8 (a key agreement algorithm). Among the two initial A5 algorithms, A5/1 is the stronger one, and is used to achieve security and privacy of voice-over-the-air interface. While originally kept secret, it became publicly known after being reverse-engineered, and has continued to serve as a good example for crypto-related security hazards. A5/2 is the version without any export limitations, which was also subjected to reverse-engineering and cryptoanalysis, in turn demonstrating the need for a more powerful algorithm. Hence, in 2002, A5/3 was introduced using the block-cipher called KASUMI. Besides in GSM, KASUMI is used as a cryptography algorithm in General Packet Radio Service (GPRS) and 3G networks as well.

Barkan et al. [1] have analyzed several attacks against A5 cyphers, namely:

- Class-Mark Attack: the attacker changes the class-mark information that the phone sends to the network at the beginning of the conversation, so that the network thinks that the phone supports only A5/2. Although the network prefers to use A5/1, this leads the phone to using either A5/2 (weaker encryption) or A5/0 (no encryption). The attacker can then exploit these weaker mechanisms and eavesdrop on the communication.
- Recovering crypto key of past or future conversations: an attacker recovers the encryption key of an encrypted conversation that was recorded in the past.
- Man in the Middle Attack: The attacker uses a fake base station in its communications with the mobile phone, impersonates the mobile phone, and forwards the authentication request, that it got from the network, to the victim. The

victim sends the 32-bit Signed Response to the attacker, who holds on to it and, by performing a cyphertext attack, finds the cypher key, which enables him to authenticate himself on the network.

General Packet Radio Service (GPRS) is a protocol that enables packet radio access for GSM users. From a security viewpoint, GPRS inherits many security problems from GSM; however, the upgraded network architecture also brings several new issues. The GPRS architecture is associated with the following weaknesses [33]:

- Compromise of the confidentiality of subscriber identity: whenever the serving network cannot associate the Temporary Mobile Subscriber Identity (TMSI) with the International Mobile Subscriber Identity (IMSI), the Service GPRS Support Node should request from the Mobile Station (MS) to identify itself by means of IMSI on the radio path. This leaves the possibility for the adversary to pretend to be a new serving network, to which the user has to reveal his permanent identity.

- One-way subscriber authentication: GPRS architecture does not assure that a mobile user is connected to an authentic serving network, thus enabling active attacks using a false Base Station (BS) identity. Furthermore, the A3 and A8 vulnerabilities are inherited from the GSM network, whereas re-using authentication triplets makes it possible to launch Man in the Middle Attack, or Replay Attack.

- Optional encryption of signalling and user data: optional encryption enables the potential attacker to mediate in the exchange of authentication messages between the legitimate user and the Base Station.

- Unsupported security protection by the SS7 technology: this deficiency of the SS7 technology, which is used for signaling exchange in GPRS, increases the probability of an adversary to get access to the network, or a legitimate operator to act maliciously as well, resulting in the unprotected exchange of signaling messages between the location registers.

Compared to its 2G and 2.5G predecessors, *3G* has brought significantly better security features, mainly through the deployment of the aforementioned KASUMI block cipher instead of the A5 stream cipher, and the Authentication and Key Agreement (AKA) protocol instead of CAVE-based authentication. Furthermore, 3G integrity algorithm with an Integrity Key (IK) introduces the feature of Data Integrity, whereas

User to User Services Integrity Module (USIM) and USIM to Terminal Authentication provide the secure access to MS.

Long Term Evolution (LTE)'s security is largely built upon the 3G one (primarily, usage of the AKA protocol), with several modifications, such as extended key hierarchy, introduction of longer keys, better backhaul protection, and integrated interworking security for legacy and non-3GPP networks.

3.1.2 Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) was "designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication" [21]. It is an optional encryption standard, implemented in the Media Access Control (MAC) layers, which provides user authentication, data privacy, and data integrity in a way that is supposed to make a wireless LAN equivalent to a wired LAN.

The RC4 algorithm, also known as a stream cipher, is a symmetric cipher in which every binary digit in a data stream is subjected separately to an encrypting algorithm, by logically XOR-ing the key with the data. The key is shared between communicating nodes, clients and access points, hence ensuring its secure exchange is needed.

One of the main vulnerabilities of the WEP protocol lies in the usage of the random Initialization Vector (IV), used in the encryption process. Namely, WEP's IV is only 24 bits long, allowing for only relatively low number of unique combinations, that can be reached fairly easily in busy network conditions, thus bringing the need for the re-use of certain IVs. Hence, if RC4 for a certain IV is found, a potential attacker can decrypt the packets with the same IV.

Furthermore, WEP does not define a key management protocol, leading to the need for manual change of the key for each wireless device by the network administrator. This presents a big security leak, since in case of a potential security breach, all keys need to be changed. Due to the lack of synchronization, this task is far from trivial.

The use of the RC4 algorithm also brings an issue of weak keys; the high correlation factor between the key and the output means that the attacker can somewhat easily filter out the "interesting packets", substantially decreasing the number of combinations for possible keys that will allow him the access to the network.

There are two forms of authentication within 802.11 standards: Shared key and Open system. While the latter gives a satisfactory performance in terms of security,

the Shared key authentication, based on encryption of a challenge, brings a potential security breach in cases where the attackers are able to monitor the encryption process.

Borisov et al. [4] define four basic types of attacks present in WEP-based wireless networks:

- Passive Attack: a passive eavesdropper can intercept all wireless traffic, until an IV collision occurs. Once the attacker obtains the XOR of the two plaintext messages, the resulting XOR can be used to infer data about the contents of the two messages. IP traffic is often very predictable and includes a lot of redundancy, which can be used to eliminate many possibilities regarding the contents of messages.

- Active Attack to Inject Traffic: if the attacker knows the exact plaintext for one encrypted message, he can use this knowledge to construct correctly encrypted packets. The procedure involves constructing a new message, calculating the CRC-32, and performing bit flips on the original encrypted message to change the plaintext to the new message.

- Active Attack from Both Ends: the attacker makes a guess about the headers of a packet, which is usually easy to obtain or guess. The attacker can flip appropriate bits to transform the destination IP address to send the packet to a machine he controls, and transmit it using a rogue mobile station. Most wireless installations have internet connectivity; the packet will be successfully decrypted by the access point and forwarded unencrypted through appropriate gateways and routers to the attacker's machine, revealing the plaintext.

- Table-based Attack: the limited number of unique combinations of possible IVs allows an attacker to build a decryption table. Once that the attacker learns the plaintext for one packet, he can compute the RC4 key stream generated by the IV that is in use, which can then be used to decrypt all other packets that use the same IV. Over time, the attacker can build up a table of the IVs and the corresponding key streams.

3.1.3 Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is an open standard aimed at solving problems present in WEP-based systems. Encryption is realized through the Temporal Key Integrity

Protocol (TKIP), which provides per-packet key mixing function for reducing correlation between IVs from the weak keys. In addition, a message integrity check and a re-keying mechanism are added. TKIP also relies on RC4, and an addition of hashing makes for a significantly more robust mechanism.

The improvements that WPA brings over WEP may be summarized as [21]:

- A cryptographic message integrity code, or MIC, to defeat forgeries;
- A new IV sequencing discipline, to prevent replay attacks;
- A per-packet key mixing function, to de-correlate the public IVs from weak keys;
- A re-keying mechanism, to provide fresh encryption and integrity keys, thus mitigating the threat of attacks stemming from key reuse.

For home networks, a so-called *WPA Pre-Shared Key (WPA-PSK)* variation has been designed. It is a simplified algorithm, in which an individual user must set a passphrase (key). The difference from WEP lies in the automatic alteration of the key every n time intervals, making it more difficult for attackers to identify the deployed keys.

However, WPA-PSK algorithm has proven to be more attack-prone than WPA. Several dictionary attacks were devised to somewhat efficiently exploit the Pairwise Master Key (a feature obtained from the concatenation of the passphrase, the Service Set Identifier, its length, and a number of bit strings used in a session).

3.1.4 Wi-Fi Protected Access version 2

Wi-Fi Protected Access 2 (WPA2), also known as 802.11i, is an amendment to the WPA standard, aiming at improving not only security and reliability, but also the ease of access of the WPA-based networks.

One of the most important novelties is the introduction of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP is based on the Advanced Encryption Standard (AES) – an open-source algorithm that provides significant robustness improvements.

As is the case with WPA, the most exploitable vulnerability of WPA2 stems out from using the Pre-Shared Key (PSK).

In WPA2, user authentication is separated from ensuring the privacy and integrity of the messages, and, like WPA, it operates in two modes:

- *WPA-Personal*, or PSK: performed between the client and the access point, and typical for home networks;

- *WPA-Enterprise*, or Extensible Authentication Protocol (EAP): typical for business networks. Authentication server named RADIUS is used for authorization decisions – it provides the Master Session Key to the client and to the access point.

Up to this date, WPA2 is considered the most reliable Wi-Fi security protocol; however, several vulnerabilities are still present. For example, the following attacks on WPA2-secured systems were devised:

- PSK Brute Force Dictionary Attack: based on attacking the PSK, recognized as the biggest weakness of WPA2. To perform an attack on the passphrase, the attacker must eavesdrop on the network during the 4-way handshake, where he receives everything except for the passphrase, and then performs the attack.

- Security Level Rollback Attack: based on WPA2's feature of defining a Transient Security Network. The attacker sends wrong Beacon or Probe requests to establish a pre-Robust Security Network Association (RSNA) connection, even if both would support a more secure RSNA connection, namely WPA2. As pre-RSNA does not support a cipher suite, the fraud may go through undetected, resulting in accepting the insecure connection. This in turn allows the attacker to obtain the default keys by exploiting WEP's weaknesses.

- Reflection Attack: present in ad-hoc networks, where a device is not allowed to play both the supplicant and the authenticator roles at the same time. The original device starts the handshake as the authenticator, while the attacker starts another 4-way handshake using the same parameters, but with the device representing the supplicant. Once that the device starts to send messages as the supplicant, the attacker can use these messages as a valid message for the initial 4-way handshake with its target.

In addition to the aforementioned security issues, the so-called "Hole196" vulnerability which exposes WPA2-secured network to insider attacks, was discovered [26]. The attack is enabled by use of the Group Temporal Key (GTK), shared among all authorized clients in a WPA2 network. The data traffic encrypted using the GTK should be transceived between an access point and a legitimate user. However, a malicious insider can potentially eavesdrop and decrypt data from other authorized

users, as well as scan their Wi-Fi devices for vulnerabilities, install malware, in turn compromising their security.

The Wi-Fi Alliance continuously works on improving the WPA and WPA2 standards, offering different EAP types that allow greater interoperability and higher security. Nevertheless, certain security issues still exist, and improvements still need to be made.

In many future Cognitive Radio Networks, it will be necessary to enable interoperability with the legacy systems. In addition, the wireless nature of SDRs and Cognitive Radios will make them prone to inheriting some of the threats presented in this section. Hence, ensuring maximum security and privacy of such systems will be paramount. Consequently, addressing the known security issues in the current state-of-the-art security standard for WLAN, i.e. WEP2, can be considered a good starting point.

3.2 Threats to SDR architecture

As mentioned in Chapter 2, there is no unanimous definition of which requirements a radio must satisfy in order to be considered software defined. Depending on the level of software reconfigurability, some authors and organizations have established a division between, for example, Software Capable, Software Programmable and Software Defined Radios. For the sake of the simplicity, all of these will from now on be referred to as Software Defined Radios, since, from the security point of view, they mostly share common threats and problems.

It is useful to categorize the types of software present in Software Defined Radios, as per the Wireless Innovation Forum's guidelines, since this categorization is widely accepted and commonly referred to in the scientific environment. Following that, it is possible to classify the software in SDRs as [12]:

- Radio Operating Environment (ROE): consists of the core framework, the operating system, device drivers, middleware, installer, and any other software fundamental to the operation of the radio platform;
- Radio Applications (RA): software which controls behavior of the RF function of the radio. This includes any software defining the air interface and the modulation and communication protocols, as well as software used to manage or control the radio in a network environment;

- Service Provider Applications (SPA): software used to support network and other service providers' support for the user of the radio. It includes voice telephone calls, data delivery, paging, instant messaging service, emergency assistance, and geolocation;
- User Applications (UA): application software not falling into any of the above categories.

3.2.1 General SDR-related security threats

One of the potential hazards for SDRs lies in the possibility of tampering with their hardware. Since these hazards apply to all wireless systems and are not unique to the new features that SDRs bring, the focus of this section is on the other types of threats: the ones stemming out from the software's reconfigurability. Main threats to reconfigurability come from faulty and buggy software – hence, the deployed schemes need to protect the system from download and usage of improper software. In general, security-enabling mechanisms for SDRs can be divided into hardware-based and software-based ones, each with their own advantages and disadvantages.

Hardware-based mechanisms include hardware modules for monitoring the SDR's reconfigurable parameters. However, unlike the SDRs that they are securing, these mechanisms themselves are typically not easily reconfigurable, and updating the security parameters or policies may be problematic and expensive. Software-based mechanisms, in their turn, rely on deploying the tamper-resistance techniques, providing safe and secure authentication, communication security and integrity, as well as safe algorithms for downloading, updating and distributing the software. The potential vulnerability of such schemes is the openness to malicious modifications.

Chunxiao et al. [9] present a security architecture based on separation of the application environment and the ROE, so that the compromise of one does not affect the other. Furthermore, SDR reconfiguration parameters produced by the application environment are verified against security policies before they are executed in the radio environment. So, in cases where the application environment is tampered with and becomes malicious, it cannot infect the radio environment, and thus the RF characteristics can be ensured to be in compliance with the desired policies. For software classification, the authors have used the Wireless Innovation Forum's guidelines, as was described before, where, on top of the ROE, RA, and SPA they define the User Application Environment (UAE) as the environment (OS) where UA are executed. The authors proceed to define a new separate layer called Secure Radio Middleware

(SRM) – a layer implemented below UAE, which includes the most security-critical components, namely RA and ROE. SRM is composed of:

- Bypass: the component in charge of non-critical operations;
- Memory Management Unit: the unit that controls the behavior of the OSM;
- Virtualized Hardware: the layer where all the radio applications are performed;
- Security Policy Monitor: the component that tries to decide a normal value or range for the radio parameters and compare them to the ones that the OS passes to Virtualized Hardware, leading to initialization of the appropriate recovery mechanisms in cases of violation.

As the authors themselves note, their implementation has several constraints. Since a desktop PC has been used as a testbed, the implementation does not reflect the performance in the potential real-life scenarios, where platforms will typically be far more resource-constrained. Furthermore, their architecture does not incorporate mechanisms for encryption/decryption, information integrity, access control and secure radio software download, which are issues that need to be addressed separately.

Brawerman et al. [5] propose a lightweight version of the Secure Socket Layer (SSL) protocol. SSL provides bulk encryption, end point authentication, and data integrity protection. For encryption, symmetric key algorithms are used, whereas for authentication, client and server can mutually authenticate each other. *Light SSL* redesigns the SSL protocol in order to decrease the computational complexity of the performed operations and to perform most of the cryptography at the server side, thus making it suitable for power-constrained devices such as SDR terminals. The authors have defined several possible attacks, and the corresponding defense features employed within the protocol, namely:

- Access control: countered by the authentication mechanism;
- Masquerade attack: attacker emulates the manufacturer server or a client, countered by the use of mutual authentication;
- Confidentiality: secrecy of information is ensured by establishing secure connections;
- Replay: attacker re-transmits messages after a certain time period, countered by using timestamps;

- R-CFG validation: installation of the non-approved R-CFG, resolved by digitally signing every R-CFG by the regulatory agency;
- R-CFG integrity: possibility of modifying R-CFG after it has been approved, countered by using one-way hash functions.

3.2.2 Potential threats to common SDR architectures

Currently, there are two dominant open-source architectures for SDRs: GNU Radio, which is particularly appealing to academic community due to the relative simplicity of use and compatibility with low-cost off-the-shelf SDR platforms such as Universal Software Radio Peripheral (USRP), and Software Communications Architecture, which is the architecture adopted by the Wireless Innovation Forum.

GNU Radio is an open-source software toolkit that, coupled with hardware equipment such as USRP, allows for a complete platform for building Software Defined Radios. GNU Radio can also be used as a stand-alone simulation environment. Most of GNU Radio's applications are written in Python, whereas C++ is used for implementing signal processing blocks. Python commands are used to control all of the USRP's software defined parameters, such as transmission power, gain, frequency, antenna selection, etc. GNU Radio is built on two main structural entities: signal processing blocks and flow graphs. Blocks are structured to have a certain number of input and output ports, consisting of small signal-processing components. When the blocks are appropriately connected, a flow graph is made.

Hill et al. [14] have analyzed threats related to GNU Radio-based SDR systems. By considering the GNU Radio Software Applications, written in C++, as the Radio Applications (RA), and the Python functions as the Radio Operating Environment (ROE), the authors identify the following shortcomings related to the ROE of GNU Radio:

- At the moment, there is no embedded functionality for verification, i.e., securing the SDR device from being reconfigured by a malicious code;
- There are risks related to the execution of models in the graph. Since a single address space is shared among all the software modules, there is a possibility for the malicious user to alter the data in the whole address space. To counter this, the authors propose restricting each module to only be able to access its dedicated address space;

- There is the possibility of a buffer overflow, stemming from the use of the shared buffer. Mechanisms for restricting the amount of data that can be written to the buffer are needed.

They also define three possible attacks, depending on the parameter targeted:

- Modulation attack: improper change of the modulation format;
- Frequency attack: jamming attack where an impostor is transmitting on the frequencies that it is not allowed to;
- Output power attack: where an attacker can continuously transmit at high power, forcing other users to increase their power level, which leads to increased battery drain.

The authors go on to suggest that GNU Radio ROE has to provide mechanisms for evaluating and enforcing policies for specifying the operating constraints of the SDRs, defined by the network administrators and regulators.

Software Communications Architecture (SCA) was originally defined by the United States government with the purpose of securing waveform portability and improving software reuse. Built originally for the United States military's Joint Tactical Radio System (JTRS) program, it has been accepted as a communication standard in military services of many other countries, as well as by the commercial organizations such as Wireless Innovation Forum. It is an always-evolving standard, with first version dating back to 2000, that provides standardized set of methods for installing, managing, and uninstalling new waveforms, therefore maintaining interoperability between various SDR systems.

Security is a very important aspect of radios featuring SCA. The architecture provides the foundation to solve issues such as programmable cryptographic capability, certificate management, user identification and authentication, key management, and multiple independent levels of classification. Manufacturers and users are embracing the approach, albeit at a relatively slow rate. For example, the Security Supplement to the JTRS SCA [20] requires that the SDR devices "shall only accept cryptographic algorithms/algorithm packages signed by National Security Agency (NSA)", that "NSA shall digitally sign all Security Policy XML files", and that "the operating system invocation method shall be a NSA digitally signed script". However, SDR middleware and tools vendors supporting JTRS customers do not yet support digital signature features within their products, although they generally express openness to including such features in future releases. Similarly, user and manufacturer representatives

in the Wireless Innovation Forum's Public Safety Special Interest Group are trying to identify alternatives to digital signatures before committing to such an approach, largely due to perceptions regarding the complexity of the Public Key Infrastructure (PKI) technology.

3.3 Threats to Cognitive Radios and Cognitive Radio Networks

As described before, Cognitive Radios can be considered as intelligent devices that are able to learn from experiences and dynamically adapt to the features of the environment. Major research efforts have been devoted towards the study and development of learning and reasoning techniques without considering security related issues in detail. Typically, security issues are tackled by means of adding an authentication on encryption mechanism to the data communication within the network. However, this is not always sufficient due to the improved capabilities of the cognitive paradigm. In particular, as artificial intelligence engines represent the core of cognitive devices, potential threats that are able to feed Cognitive Radios with false sensory inputs – thus purposely affecting their trained knowledge and subsequently their behavior – need to be considered.

Table 3.1 summarizes the attacks and the proposed defense mechanisms addressed in this section, also describing their basic characteristics.

3.3.1 Primary user emulation attacks

Two types of users can be differentiated in Cognitive Radio Networks deploying Opportunistic Spectrum Access (OSA): Primary Users (PUs) and Secondary Users (SUs). The main premise of OSA lies in the SUs' ability to access the channels normally assigned to PUs when they are free of occupancy. In order to decide whether the channel is momentarily free, or is in use by the PU or the other SU, the Cognitive Radio needs to perform spectrum sensing [1]. Several spectrum sensing approaches, such as energy detection, cyclostationary feature detection, second-order statistics detection, filterbank-based detection, etc., have been proposed up to date, each with its advantages and disadvantages in terms of ease of implementation, decoding complexity and sensing accuracy in various channel conditions. In case that the Cognitive

[1] Alternatively, two other methods for inference of the spectrum occupancy information: geolocation/database, and beacon signals are proposed in the literature; they are addressed in Section 3.3.3

Table 3.1: Taxonomy of Cognitive Radio attacks and threats

Attack type	Contribution	Attacker's special characteristics	Proposed defense scheme
PUEA: emulating characteristics of a primary user to acquire exclusive spectrum rights	[7]	Altering its transmission power, modulation mode and frequency; injecting false data to the localization system	3-step mechanism: verification of signal characteristics, RSS measurement, localization of the signal
	[8]	Applying the estimation techniques to enhance its performance	Assumes that emulating the channel features is not feasible for the attacker. Invariants of communication channels are used as means of differentiating between the PUE attackers from legitimate PUs
	[24]	-	Novel physical layer authentication mechanism, which incorporates cryptographic and wireless link signatures
	[11] (proposed)	Ability to emulate any of the PU's transmission characteristics	Location integrity checking as means of deciding on the credibility of a user
Byzantine: providing wrong data to other nodes in collaborative spectrum sensing	[32]	Two operating modes: causing False Alarm attack, or causing False Alarm & Misdetection	Each user is attributed a suspicious level, turned into a trust value, but also a consistency value
	[25]	Two types of attacks: false-positive and false-negative. The attackers are assumed to be able to estimate the channel occupancy with 100% precision	Double-defense mechanism: the correlations between the reported RSS values using correlation filters are observed and the suspicious nodes are outlined; weight-combining data fusion rule is used
	[27]	Hit-and-run attacker: able to estimate its current suspicious level and adapt its attacking scheme	Novel reputation algorithm - the user is permanently excommunicated once his reputation value is below a threshold
OFA: disrupting CR's learning mechanism	[28]	-	Set of general guidelines, e.g., Multi-Objective Programming module verifies all the reconfigured parameters in each iteration
Lion attack: multi-layer attack with the goal of causing DoS at the transport layer	[13]	-	Set of general guidelines for reducing the efficiency of the attack
Attacks on CCC	[34]	two types of attacks: DoS attack in multi-hop networks, and the greedy MAC layer behavior	-
	[29]	-	Authentication of communicating Cognitive Radionodes as the key security feature
Spectrum trading security issues	[35]	Attacker decreases the QoS while declaring that it remains the same	Once it observes illegal behavior, PU decreases the amount of spectrum shared with SU, thus reducing its overall utility
802.22-specific	[2]	Identification of the possible attacks: DoS; Replay; Jamming in QPs; PUEA; Threats to WMBs; Attacks on Self-Coexistence mechanism	Security sublayer deals with some of the vulnerabilities, mainly through: Privacy Key Management v2; message authentication codes; Advanced Encryption Standard

Radio decides that the specific channel is momentarily not in use by the PU, it competes with other potentially present SUs in order to acquire the rights to access the channel. Furthermore, once that it has been assigned the rights to use the channel, the Cognitive Radio will still need to periodically perform spectrum sensing and, should it sense the presence of a PU, vacate the channel immediately.

Primary User Emulation Attack (PUEA) is a type of attack where a secondary user falsely advertises itself as a primary user, either to acquire exclusive right to the spectrum occupancy, or to cause Denial of Service (DoS) within the network. Depending on the spectrum sensing technique that the legitimate SUs use, the adversary emulates certain characteristics of a PU, e.g., in Cognitive Radio Networks where SUs use energy detectors, the PUE attacker will try to create signals of similar power, whereas in networks with feature-based detectors, the attacker will emulate the corresponding features of the PU. To counter the PUE attacks, an appropriate defense scheme able to distinguish between real and mimicking PUs needs to be implemented within the network. One of the aggravating factors in devising such a scheme is Federal Communication Commission's instruction that "no modification to the incumbent signal should be required to accommodate opportunistic use of the spectrum by SUs" [10].

PUEAs have arguably been given the most attention in the literature out of all the threats specific to Cognitive Radio Networks. The PUEA-defense contributions can be divided into those where the locations of the PUs are assumed to be known a priori, such as in cases when PUs are, for example, TV towers or base stations, and those where the PUs' locations cannot be assumed to be known beforehand.

Chen et al. [7] have proposed a location-based method, applicable to networks where PUs are TV towers with high transmission power and high transmission range. The authors model a Cognitive Radio attacker capable of altering its transmission power, modulation mode and frequency. Two types of attacks are considered: in the first one, the attacker alters Received Signal Strength (RSS) measurements by changing the transmission power, whereas in the second one, the attacker injects false data to the localization system. To counter such attackers, the authors propose a scheme that: i) estimates location of the signal source and compares it to known locations of the TV towers, and ii) checks whether the signal's characteristics resemble those of the PU. Based on these comparisons, the scheme estimates the likelihood that a signal source is launching a PUE attack, assuming that "it would be infeasible for an attacker to mimic both the primary user signal's transmission location and energy level since the transmission power of the attacker's Cognitive Radio is several orders

of magnitude smaller than that of a typical TV tower". The scheme consists of three steps: i) verification of signal characteristics, ii) RSS measurement, and iii) localization of the signal source. Simulation results demonstrate the effectiveness of the scheme, designed for the networks in which PUs have fixed locations and high transmission powers. In cases of mobile PUs with relatively small power (directly leading to higher RSS fluctuations), alternative approaches would need to be considered.

Another location-based method for discovering advanced PUE attackers is proposed by Chen et al. [8]. The modeled attacker is capable of applying the estimation techniques to enhance its performance, i.e., it is able to employ a maximum likelihood estimator to infer the transmission power of the PU and a channel parameter, and to use those parameters and a mean-field approach to generate and launch a PUEA. It is assumed that the attacker has the information about the location of all the entities in the network. The authors also assume the use of energy detectors as spectrum sensing mechanisms, meaning that the attacker needs to try and transmit signals whose received energy at the targeted SU's receiver will be as similar as possible to the one transmitted by the legitimate PU. To do this, the attacker estimates the PU's transmission power and the channel parameter and then, taking into account its distance to the targeted SU and PU's distance to the SU, launches a PUEA. The designed defense mechanism lies on the assumption that the attacker cannot successfully emulate the channel features. Invariants of communication channels are used as a criteria for differentiating between the PUE attackers and the legitimate PUs. The simulation results show that, while such an attacker could successfully defeat a "naive" detection method, the proposed mechanism distinguishes between real PUs and the emulators with high accuracy.

Liu et al. [24] have modeled a non-location-based mechanism, which uses a helper node placed proximate to the PU in order to counter PUEAs. The helper node serves as a "bridge" to enable a SU to verify the cryptographic signature carried by the helper node's signals, and then obtain the helper node's authentic link signatures in order to verify the PU's signals. The authors propose a novel physical layer authentication mechanism, which incorporates cryptographic and wireless link signatures. It is assumed that all SUs have reliable ways to obtain the correct public key of each helper node, and that the helper node cannot be compromised by an attacker.

We presented a naive location-based method for identifying PUE attackers, with the assumption of the a priori knowledge of the locations of all users [11]. The method is based on the credibility calculation for all SUs, and the final decision of whether

the SU is the actual PU or the PUE attacker is done by comparing its credibility to the predefined threshold for a given Signal-to-Noise Ratio (SNR) level.

The system model is based on the following assumptions:

- Each user has a priori information of other users' locations;
- The attackers are capable of emulating one or more of the PU's features, including the ability to transmit with the same power as the PU;
- Prior to encountering the PUE attacker, the Cognitive Radio is ensured to have established communication with the legitimate PU, in order to derive the appropriate threshold value for user classification for a given channel.

The algorithm decides on the credibility of the user in the following manner: based on the coordinates on the playground, the distance between the SU (Cognitive Radio) and the legitimate PU is calculated. The RSS values of the legitimate PU transmitting a signal at constant power are calculated for different SNR values. The expected distance between the SU and the legitimate PU can be derived from the RSS value. The credibility of each user is calculated as the ratio of the real distance (derived from coordinates) and approximated distance (derived from RSS values). This value is used as a "ground truth", and the threshold value for future user classifications is derived from this credibility.

The RSS values of subsequent users are calculated depending on their distance and transmission power, and their credibility is derived using the previous method. The credibility is then compared to the threshold, when it is decided whether a user is a legitimate PU or a PUE attacker. It should be noted that the performance of the algorithm is impacted significantly by the number of samples that can be obtained from the legitimate PUs for calculating the threshold.

In the simulations, a free-space path loss channel with Additive White Gaussian Noise (AWGN) was modeled. The transmission powers of the legitimate PU and the emulating SU were equal. For calculating the threshold, we have performed Monte Carlo simulations with 1000 iterations, where position on the playground was randomized in every iteration. The threshold is calculated as: $\gamma = 0.995 \cdot (total\_trust)$. The credibility of each subsequent user is then compared to the threshold and, if its value is higher than the threshold, the user is regarded as a legitimate PU.

Figure 3.1 shows the distribution of the average calculated credibility over 1000 iterations, versus SNR. Probabilities of the correct detection of the legitimate PU, and the successful detection of the attacker are given in Figure 3.2.

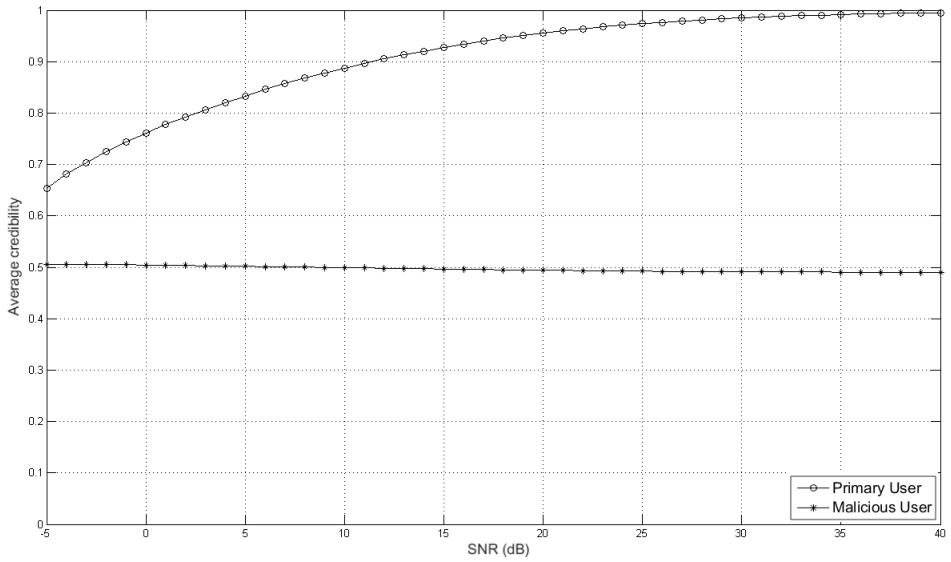


Figure 3.1: Average credibility of the users vs. SNR

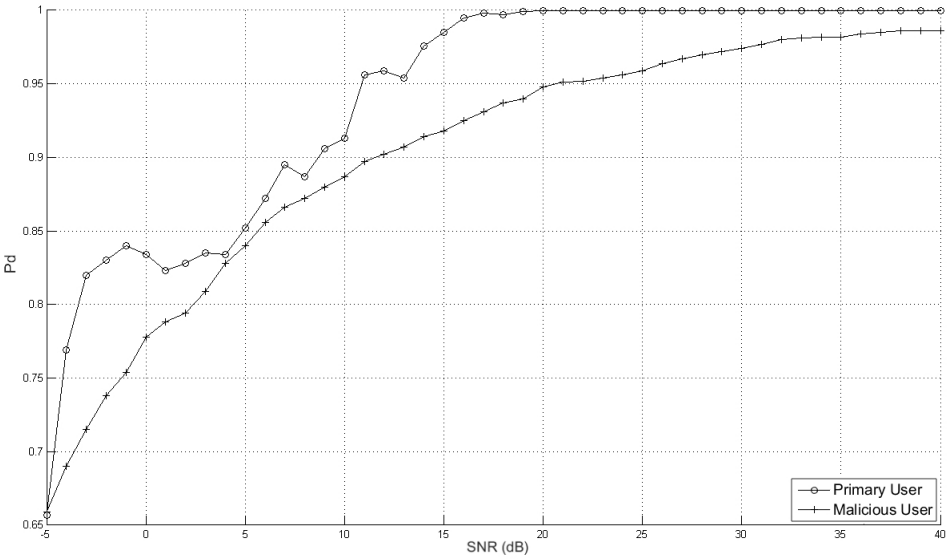


Figure 3.2: Probability of the correct detection vs. SNR

Because of the noise power causing high RSS fluctuations in low-SNR environments, the credibility of the legitimate PUs is relatively low in such harsh channel conditions. The algorithm does substantially better in higher-SNR environments. For SNR=15dB, the algorithm is able to correctly identify legitimate PUs with 98% accuracy, and malicious users with 92% accuracy, whereas for SNR=25 dB, legitimate

PUs are correctly categorized with a 100%, and malicious users with 98% accuracy. Different results can be obtained depending on the threshold constraint.

Alongside the aforementioned poor channel conditions, the main vulnerabilities of the algorithm arise when the attacker's location is close to that of the real PU. In those cases, either a more complex RSS-based scheme, such as the one proposed by Chen et al. [7], or an alternative, non-RSS-based scheme need to be used for the successful detection of PUEAs.

3.3.2 Byzantine attacks

Once that the sensing part is finished, a Cognitive Radio needs to decide how to use the acquired data in order to correctly estimate the channel occupancy state. While it is possible for each entity to make this decision based only on their own spectrum sensing outputs, more precise results can be achieved if users can exchange information among themselves. This is the idea behind collaborative spectrum sensing, where SUs send their results of spectrum sensing either to each other, or to a centralized entity which then decides on the channel occupancy and sends this decision back to the SUs. In this way, correct detection probability of a channel occupancy, potentially impaired by the problems such as a "hidden node", equipment malfunction, or poor channel conditions, can be improved significantly.

However, collaborative spectrum sensing also has its drawbacks. Besides an increase in computational complexity (in cases where each node has to make the decision for themselves based on the data acquired from multiple users), and the need for use of the additional data fusion entity (in cases of centralized collaborative sensing), certain security issues arise as well.

Byzantine attackers send false spectrum sensing information to other users or a centralized entity, thus increasing probability of wrong decisions regarding the spectrum occupancy. Furthermore, a malfunctioning node may also unintentionally cause faulty reports. In both cases, the ability to correctly estimate channel availability – arguably the most important feature of Cognitive Radios – can be severely degraded.

Hence, users can be classified in the following categories, depending on the type of the misbehaving Cognitive Radio node:

- Greedy: those with the intention of acquiring exclusive privileges to vacant channels by constantly sending the information that a channel is being occupied;
- Malicious: those with the intention of causing harmful interference between the other users, or reducing the spectrum usage efficiency;

- Temporarily malfunctioning: those which unknowingly send incorrect information regarding the spectrum occupancy.

Devising a reliable method for countering byzantine failures imposes itself as a critical task in order to implement collaborative sensing safely and successfully. Various strategies for addressing byzantine issues have been proposed in the literature, mutually differentiated mainly with respect to the data fusion algorithm, reputation algorithm and the special features of the considered attackers.

Wang et al. [32] proposed a relatively simple defense scheme for recognizing a malicious user by computing the suspicious level, the trust values and the consistency values for every user in the system. The authors consider a single malicious attacker, and show how the algorithm, which eliminates the observations from the node marked as malicious, performs depending on which collaborative sensing scheme is used. An attacker can operate in two modes: causing False Alarm attack, where it reports a higher sensed power whenever the power is below its set threshold, or causing False Alarm & Misdetection, where it reports higher sensed power when it is below the threshold, or lower sensed power when it is above the threshold. Each user is attributed a suspicious level, which is then turned into a trust value. Since the trust value itself is not reliable in cases when there are either not enough observations, or when there is no malicious user present, each user is also assigned a consistency value. By eliminating reports of the users whose trust values are consistently low, and then using the OR rule for the remaining nodes, the scheme shows satisfying improvements compared to simpler, more straightforward schemes, for both attacking strategies. The main limitation of the scheme is the fact that it is able to deal with only a single malicious user.

Min et al. [25] proposed a double-defense mechanism for centralized collaborative sensing, which they refer to as the *Attack-tolerant Distributed Sensing Protocol*. Two types of attacks are taken into account: false-positive, which classifies a non-primary user as a primary and thus increases the probability of a misdetection, and false-negative, which causes a failure to detect a primary signal and increases the probability of a false alarm. Attackers are assumed to be able to correctly estimate whether the PU is using the channel or not at all times, regardless of the decision that the centralized entity makes, and are therefore able to switch between their attacking modes. The proposed defense framework consists of three building blocks:

- Sensing manager: manages sensor clusters and directs the sensors to report their readings at the end of each scheduled sensing period;

- Attack detector: detects and discards (or penalizes) the abnormal sensing reports based on pre-established shadowing correlation profile;
- Data fusion center: determines the presence or absence of a primary signal based on the filtered sensing results.

The mechanism is implemented in a way that the clustered sensors send their RSS values and location information to the data fusion center, which is done in two phases. First, the correlations between the reported RSS values using correlation filters are observed, and the nodes whose reports appear inconsistent with the others are deemed suspicious, so their reports are not taken into account for making the decision regarding the channel occupancy. The other line of defense – implemented because of the inaccuracy of the first one when the attackers produce low-strength attacks – is a weight-combining data fusion rule, where weights to sensors are allocated based on their Conditional Probability Density Function (CPDF). This way, misbehaving sensors are likely to be given low weight factors, meaning that their reports to the data fusion center will be less likely to affect the final decision. The simulation results show that the proposed algorithm is able to minimize the probability of a false-alarm by up to 99.2% (for the first type of attack), and to achieve a probability of correct detection of up to 97.4% (for the second type of attack), showing significantly better performances than other state-of-the-art algorithms.

Noon and Li [27] present a specific type of an advanced attacking strategy, called *Hit-and-run*, and the corresponding defense mechanism. The attacking strategy is based on the assumption that an attacker is able to estimate current suspicious level assigned to it by the data fusion center, and act appropriately. Namely, when he feels that his suspicious level is high, and there is a potential for him to be expelled from the network, he stops sending false observations and starts acting honestly. It restarts its malicious behavior once that it calculates that it is safe again to do so, and from there on continues to use this Hit-and-run strategy. It is assumed that the attacker is aware of the other nodes' reports to the data fusion center, and can model its report based on this information. Conventional reputation-based schemes are unable to counter this kind of attacker, hence the authors propose a new point-system. The system permanently bans a user from the network once that he has accumulated enough negative reputation points, where each negative point is assigned to the user whenever his suspicion level surpasses a pre-defined threshold. By applying the Wald's equality, the algorithm can approximate the expected time for the attacker to reach the threshold, as well as the time for the attacker to decrease its suspicion level.

By combining these approximations, the time needed to detect the attacker can be estimated. For the set number of 10 secondary users in the network, the authors show how the algorithm fares when faced with up to three attackers. As the number of attackers increases, the algorithm needs more iterations for successful detection; however, it still successfully manages to excommunicate the malicious users.

3.3.3 Alternative spectrum occupancy decision methods and the related security threats

Besides spectrum sensing, two other methods have been proposed by the Notice of the Proposed Rule Making – Unlicensed Operation in the TV Broadcast Bands [6] as alternative ways of acquiring spectrum occupancy information: geolocation/databases, and beacon signals.

Geolocation/database approach has recently sparked particular interest in the Cognitive Radio research community because it overcomes some of the drawbacks of spectrum sensing approaches (which vary depending on the sensing technique used), such as potentially long sensing periods, unknown/incomplete waveform information, and poor channel conditions. This approach requires a Cognitive Radio to have perfect awareness of its location, and to be able to access the database containing the list of currently available frequencies at that particular location. One feature makes the geolocation/database approach particularly appealing from the regulatory point of view: the possibility of easier management of the frequencies or the frequency bands that the lessor wishes to declare as "available" or "busy" at any given time. However, this approach brings its own set of security issues and concerns, primarily:

- Continuous database accessibility: ensuring that the database is always "up-and-running", and updated with the list of (un)available frequencies is a necessity;

- Database management and updating: since databases need to be regularly updated, there is a need for a reliable mechanism for the processes of updating and downloading the updated content to a Cognitive Radio device;

- Database tampering: whereas the communication between a database and a Cognitive Radio is by default intended to be one-way (Cognitive Radio downloading the content from a database), ensuring that malicious content cannot be uploaded by a Cognitive Radio – by deploying anti-tampering methods – is paramount;

- Database emulation: similarly to PUEA, if the SU retrieves information from a source pretending to be a spectrum lessor in a given geographical area, it can make wrong estimations of the spectrum occupancy of a given frequency band – i.e., it may attempt to access a channel currently marked as "busy" by the spectrum lessor (malicious attack), or may refrain itself from accessing a channel that is in reality marked as "available" (selfish attack);

- Providing false geolocation information: whereas many Cognitive Radio devices are expected to have direct geolocation capabilities due to embedded navigation systems such as the Global Positioning System (GPS), there might be instances where this is not the case, or where a navigation system is malfunctioning. In this case, Cognitive Radios may have the capability of calculating their coordinates by triangulation with other cooperative or non-cooperative devices. This, however, opens the possibility of providing false data, thus causing the targeted device to perform the triangulation erroneously.

Beacon signals method refers using RF beacons as means of providing the prospective SUs information about the vacant channels in their proximity. SUs tune to a dedicated channel in order to extract the information of the spectrum availability from the beacons, and then decide upon the optimal way to proceed. In case of absence of the beacon, SUs should refrain themselves from using the spectrum opportunistically. Main issues from a security and privacy standpoint are as follows:

- Beacon emulation: emulation attacks are a common security issue in Cognitive Radio Networks, regardless of the approach taken towards realizing the spectrum occupancy inference. With this in mind, Beacon signals seem particularly prone to such attacks, since they represent a single point of failure. The attacker may intercept the beacon, alter the information it contains, and/or predict the behavior of the Cognitive Radio users;

- Security of the Common Control Channel (CCC): with the assumption that the beacons are transmitted over a dedicated channel, it is necessary to address the related security problems. CCC-related security issues and the proposed defense mechanisms are discussed in Section 3.3.5;

- Beacon misinterpretation: one of the challenges lies in preventing the beacon from being received outside of the designated geographical area, thus causing the incorrect interpretation of the contained information. As an example, a SU

receiving a beacon from the neighbouring cell might mistakenly conclude that a certain channel is free to be accessed opportunistically. Furthermore, in case of multiple beacons co-existing in the same location at the same time, there is a problem of deciding on which beacon is the one carrying the information pertaining to that particular geographical spot.

Whereas beacon designs have been proposed in the literature, for example by Lei and Chin [22], a complete architecture that is able to successfully address the aforementioned security problems is still an open issue.

3.3.4 Threats to reputation systems

In Cognitive Radio Networks, using reputation systems has particular purposefulness in networks where some sort of collaboration between the users exists, such as in the context of collaborative spectrum sensing. Whereas threats to the reputation systems were partially covered in Section 3.3.2, it is useful to provide a more detailed coverage of the potential attacks and issues.

Sun and Liu [31] have given a detailed comparison of the attacks on feedback-based reputation systems, recognizing:

- Whitewashing and traitor attacks: the whitewashing attacker is able to discard his current ID, and re-enter the system (network) with a new ID. The traitor attacker is able to restore his reputation score by behaving non-maliciously for a certain time period (see "Hit-and-run attacker" in Section 3.3.2). As a defense strategy against whitewashing, the authors propose increasing the cost/complexity for acquiring a new user ID, as well as low initial reputation for new users. Against traitor attacks, an adaptive forgetting scheme with a fading factor is proposed;

- Attacking object quality reputation through dishonest feedback: refers to providing false feedback information in order to lead the reputation system towards an erroneous decision. The authors recognize three different approaches towards tackling dishonest feedback attacks:

  - Increasing the cost of dishonest feedback: users are required to have certain credentials in order to be able to provide feedback;
  - Detection of dishonest feedback: deployment of a defense scheme that detects dishonest feedback based on the majority rule, i.e., the feedback that significantly differs from the majority's opinion is disregarded;

  - Mitigating the effects of dishonest feedback: feedback of users with lower feedback reputation will have less impact on the overall score. There are several proposed methods for calculating the feedback reputation of a user, such as computing a weight of an user's feedback in the feedback aggregation algorithm as the inverse of the variance in all of his feedbacks;

- Self-promotion attacks: attackers can provide honest feedback for the objects they are not interested in; for example, in case of collaborative spectrum sensing, for frequency bands that they are not interested in opportunistically accessing. For countering self-promoting attacks, the defense schemes used against whitewashing and traitor attacks can be applied.

- Complicated collusion attacks: in order to enhance the efficiency of attacks and reduce the probability of being detected, attackers may collude. The authors differentiate two types of complex collaboration attacks:

  - Oscillation attack: malicious users are divided into different groups, where each group performs a different role at a given time – e.g., while one group focuses on providing a dishonest feedback, the other may focus on improving its reputation by providing honest feedback to the non-targeted objects. The focuses of these groups may switch dynamically;
  - RepTrap attack: malicious users focus on breaking the "majority rule" of an object by making the majority of feedback for the given object dishonest.

  For countering the complicated collusion attacks, two different defense schemes were proposed: a scheme using temporal analysis, which explores the information over time (e.g., changing trend of the rating values), and a user correlation analysis, which aims at finding patterns between the malicious users.

3.3.5 Other attacks and threats

Several other attacks that are directly related to the cognitive functionalities of Cognitive Radios have been devised and studied in the literature.

Objective Function Attacks (OFAs) are aimed at disrupting the most complex of the functionalities of the Cognitive Radio – its learning mechanism. A learning mechanism will typically be on top of triggering the reconfiguration process of most of the reconfigurable radio parameters, such as frequency, modulation type, transmission

power, and coding rate, in order to improve the overall performance, e.g., increasing data rate, decreasing energy consumption, or enabling or disabling certain security protocols and functions. Malicious users can try and tamper with some of these parameters in order to prevent the targeted Cognitive Radio from adapting in an optimal way. To counter OFAs, Pei et al. [28] proposed a simple method called *Multi-Objective Programming module*, which verifies all of the reconfigured parameters. The model is based on Particle Swamp Optimization (PSO) – a computational method for solving optimization problems in which software agents move through the problem space, trying to improve the candidate solution. Upon reconfiguration, the algorithm should be able to detect the attackers, and reset the parameters to previous state.

Lion attack is a cross-layer attack pertinent to Cognitive Radio Networks, where the malicious node targets the physical layer in order to cause DoS at the transport layer. The attacker performs either a PUEA, or a jamming attack, thus forcing the SU that is currently using the channel to perform frequency handoff. Because of the high latencies of data flow within the Transmission Control Protocol (TCP), the situation where the transport layer is unaware of the temporary disconnection due to the handoff, can occur. The transport layer keeps streaming data, which is then not transmitted, but queued at the lower layers, leading to certain TCP segments being delayed, or even permanently lost, and the throughput suffering substantially. Hernandez-Serrano et al. [13] evaluate the impacts of Lion attack on TCP performance, validating its efficiency through simulations. The authors provide general guidelines for reducing the efficiency of Lion attacks, namely: freezing the TCP connection parameters during the frequency handoffs, and deploying the intrusion detection systems for Cognitive Radio Networks.

Common Control Channel (CCC) is expected to be present in most Cognitive Radio Networks, both centralized (for enabling the communication between base station and SUs) and distributed (for the communication between SUs). As such, it imposes itself as one of the potential points of attack. The attacker can, for example, forge the MAC frames in multi-hop networks, where there is no mechanism for the MAC frames authentication, thus causing DoS. Zhu and Zhou [34] analyze two types of attacks on the CCC: the aforementioned DoS attack in multi-hop networks, and the greedy MAC layer behavior. In the latter, a Cognitive Radio device may be subjected to reconfiguration in order to exploit implicit fairness mechanisms in lower-layer wireless network protocols, thus increasing the attacker's performance. Alternatively, greedy nodes may refuse to transmit data to legitimate nodes in order to obtain better channel allocation for themselves. Safdar and O'Neill [29] proposed

a framework for a secure CCC in multi-hop Cognitive Radio Networks. They suggest that channel announcements, selection and reservation takes place in the CCC, whereas data exchange in the selected data channel between two Cognitive Radios occurs in the data channel part of the MAC super frame. They highlight the authentication of the communicating Cognitive Radio nodes as the key feature of the framework.

Spectrum trading refers to assigning the RF spectrum through administrative means, thus allowing a spectrum license holder to directly control the process of spectrum leasing or selling to a non-licensed user. As such, it is one of the most interesting capacities of Cognitive Radios from the license holders' point of view. Whereas security of spectrum trading by itself has mainly regulatory significance – thus differing from the technical mechanisms considered throughout the rest of this chapter – it is useful to give a brief introduction to such mechanisms as well. Zhu et al. [35] have addressed the security aspects of the spectrum trading by using a game-theoretical approach, formulating the process as a reversed Stackelberg game. The authors assume cooperation between a PU and a SU, where the primary Base Station (BS) communicates with the PUs, and trades unused frequency spectrum with the secondary network. Then, the secondary BS could act as a relay for the primary network, where a contract is required between the primary network and the secondary network to ensure a Quality of Service (QoS) level in the relay work. The secondary network can gain some utility from the relay work. Moreover, unused frequency spectrum in secondary network could also be leased to secondary users. Applying a game theoretical framework to a desired model and searching for its Nash equilibrium(s) requires defining a finite set of actions that each of the players can take, as well as defining each player's utility functions. The authors define five factors that compose PUs' utility function: i) satisfaction with its transmission, ii) profit from selling spectrum, iii) gain and iv) payment from the SUs' relay work, and v) performance loss due to the shared spectrum with SUs. SUs' utility is comprised by: i) gain from its data transmission, ii) profit and iii) cost from acting as a relay, and iv) payment for the purchased spectrum. The considered security issue refers to the scenario where the SU tries to cheat the primary PU by decreasing the QoS while declaring that the QoS remains the same. The proposed scheme tackles this by continuously supervising SU's performance parameter and, in case that illegal behavior occurs, the PU punishes the SU by decreasing the shared spectrum with SU, thus reducing its overall utility.

3.3.6 802.22 standard for Cognitive Radio Networks and the related security threats

The IEEE 802.22 [30] is a Cognitive Radio standard for Wireless Regional Area Networks (WRANs) developed by the IEEE 802 LAN/MAN standards committee. It specifies the methods for opportunistic use of white spaces in the 54–862 MHz TV bands. Following the general paradigms of Opportunistic Spectrum Access, the 802.22 standard prescribes a set of rules for OSA, whilst ensuring that the normal operation of the TV services remains undisrupted by interference. The standard considers two approaches for achieving the knowledge about the spectrum occupancy: spectrum sensing and geolocation/database. A centralized network architecture is defined, where, in the case that the spectrum sensing method is used as means for determining the occupancy, secondary base stations are in charge of directly coordinating the Cognitive Radio users in order to achieve spectrum sensing synchronously. Sensing outputs are then forwarded to a centralized entity (data fusion center), which makes a decision regarding the spectrum occupancy.

Several security threats directly related to 802.22 standard were identified. Whereas the standard defines existence of the security sublayer that is able to tackle several common security issues, it does not specify any particular technique for protecting spectrum sensing or geolocation information, or the data coming from the database. Examples of potential 802.11-related security threats are [2]:

- Denial of Service: attackers create messages for disturbing spectrum sensing and allocation processes. This type of threat is managed by the 802.22 security sublayer through the Privacy Key Management v2 and message authentication codes;

- Replay Attacks: the attacker captures and replays the local sensing reports sent by wireless terminals to their base station. This may cause the base station to make incorrect spectrum sensing decision. IEEE 802.22 uses Advanced Encryption Standard (AES) for dealing with this type of attack;

- Spurious transmissions in quiet periods: the attacker transmits spurious data (jamming) in quiet periods. In this way, the attacker can interfere with the various coexistence-related control mechanisms carried out during those periods;

- Incumbent Signal Emulation: In PUEAs, a malicious Cognitive Radio transmits signals whose characteristics emulate those of the incumbent signals. This type of attack is also known as “incumbent ghosting”;

- Security Threats against Wireless Microphone Beams (WMBs): the IEEE 802.11 standard proposes two solutions for detecting the presence of Part 74 devices (i.e., low-power wireless devices, such as wireless microphones, which are licensed to operate in the TV broadcast bands). If Part 74 signals are detected, a wireless terminal sends a WMB to collocated base stations in its vicinity. The 802.22 standard specifies that each wireless terminal needs to possess preprogrammed security keys that enable the use of an authentication mechanism to prevent forgery and modification of WMBs. The security sublayer protects WMBs from replay attacks in the same way that it protects intra-cell management messages.

- Security vulnerabilities in coexistence mechanism: One of the most significant security oversights in IEEE 802.22 is the lack of protection provided to inter-cell beacons. All inter-cell control messages are vulnerable to unauthorized modification, forgery, or replay.

Since it represents one of the main novelties that the standard defines, the last point warrants a somewhat more in-depth explanation. Self-coexistence is a cooperation mechanism performed between the overlapping WRANs with the intention of improving performance and minimalizing interference. In cases where the base station wishes to perform a spectrum handoff to a channel whose Signal-to-Interference Ratio is lower than acceptable, the On-Demand Spectrum Contention protocol is used. The protocol includes transmitting the inter-cell beacons between base stations with the goal of sharing spectrum occupancy information. However, attackers may disrupt the synchronization and the exclusive spectrum sharing process by sending false, modified, or replayed beacons. This is known as the *Beacon Falsification attack*.

3.4 Conclusions

Cognitive Radio, and some of the most important features associated with it – Opportunistic Spectrum Access and Dynamic Spectrum Access – undoubtedly make for exciting, innovative and above all highly relevant research topics. However, the advanced features linked with Cognitive Radio technology bring new sets of potential security breaches and issues. Adequately addressing these issues is paramount for constructing safe and efficient Cognitive Radio Networks.

This chapter has given a detailed categorization of the main standards, security problems, and corresponding solutions for legacy wireless networks, Software Defined

Radio networks, and Cognitive Radio Networks, respectively, where each subsequent network inherits the issues found in the previous ones.

Most of the considered security issues stem from deployment of one of the spectrum occupancy inference methods, typically one of the spectrum sensing methods, and the self-reconfigurability of the radios. As such, main identified threats to spectrum occupancy inference mechanisms are Primary User Emulation Attacks, Byzantine Attacks and Intelligent Jamming Attacks (the latter are addressed in Chapter 6). Depending on the type of the learning mechanism deployed, a major security hazard is present in the form of the Objective Function Attack, which targets the learning mechanism of a Cognitive Radio.

As device capabilities and prospective ideas behind the Cognitive Radio technology continue to evolve, so do the existing threats and attacks, with some new ones arising on the go. Because of the numerous possibilities of variations, being able to match them from a security perspective is often not an easy task, with challenges on multiple fields still waiting to be resolved.

Bibliography

[1] E. Barkan, E. Biham, and N. Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 600–616. Springer, 2003.

[2] K. Bian and J.-M. "Jerry" Park. Security vulnerabilities in IEEE 802.22. In *Proceedings of the 4th Annual International Conference on Wireless Internet*, WICON '08, pages 9:1–9:9, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[3] C.M. Bishop. *Neural Networks for Pattern Recognition*. Oxford University Press, Inc., New York, NY, USA, 1995.

[4] N. Borisov, I. Goldberg, and D. Wagner. Security of the WEP algorithm, 2001. URL `http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html`. [Accessed: 2015-02-05].

[5] A. Brawerman, D. Blough, and B. Bing. Securing the download of radio configuration files for software defined radio devices. In *Proceedings of the Second International Workshop on Mobility Management &Amp; Wireless Access Protocols*, MobiWac '04, pages 98–105, New York, NY, USA, 2004. ACM. doi: 10.1145/1023783.1023802.

[6] W.A. Check, A. Scott, S.L. Mace, D.L. Brenner, and D.L. Nicoll. Notice of the proposed rule making - unlicensed operation in the TV broadcast bands. Fcc, Washington, D.C., Washington, USA, 2004.

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

[8] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez. Modeling primary user emulation attacks and defenses in cognitive radio networks. In *Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International*, pages 208–215, December 2009. doi: 10.1109/PCCC.2009.5403815.

[9] L. Chunxiao, A. Raghunathan, and N.K. Jha. An architecture for secure software defined radio. In *Design, Automation Test in Europe Conference Exhibition, 2009. DATE '09.*, pages 448–453, April 2009. doi: 10.1109/DATE.2009.5090707.

[10] Federal Communications Commission. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies. ET Docket, (03-108), December 2003.

[11] K. Dabcevic, L. Marcenaro, and C.S. Regazzoni. Security in cognitive radio networks. In T. D. Lagkas P. Sarigiannidis M. Louta and P. Chatzimisios, editors, *Evolution of Cognitive Networks and Self-Adaptive Communication Systems*. IGI Global, 2013.

[12] Wireless Innovation Forum. SDRF cognitive radio definitions working document, SDRF-06-R-0011-V1.0.0. URL `http://groups.winnforum.org/d/do/1585`. [Accessed: 2015-01-13].

[13] J. Hernandez-Serrano, O. León, and M. Soriano. Modeling the lion attack in cognitive radio networks. *EURASIP Journal on Wireless Communications and Networking*, 2011:2:1–2:10, January 2011. doi: 10.1155/2011/242304.

[14] R. Hill, S. Myagmar, and R. Campbell. Threat analysis of GNU software radio. In *Proceedings of World Wireless Congress (WWC'05)*, May 2005.

[15] N. Hu. *Investigations of Radio Behavior and Security Threats in Cognitive Radio Networks*. PhD thesis, Stevens Institute of Technology, 2012.

[16] J. Ilonen, J.-K. Kamarainen, and J. Lampinen. Differential evolution training algorithm for feed-forward neural networks. *Neural Processing Letters*, 17(1): 93–105, 2003. doi: 10.1023/A:1022995128597.

[17] European Telecommunications Standards Institute. Recommendation GSM 02.09, "security aspects". Etsi, Sophia Antipolis, Valbonne, France, 1996.

[18] J. Kennedy and R. Eberhart. Particle swarm optimization. In *Neural Networks, 1995. Proceedings., IEEE International Conference on*, volume 4, pages 1942–1948, November 1995. doi: 10.1109/ICNN.1995.488968.

[19] S. Kirkpatrick, C.D. Gelatt, and M.P. Vecchi. Optimization by simulated annealing. *Science*, 220(4598):671–680, 1983. doi: 10.1126/science.220.4598.671.

[20] M. Kurdziel, J. Beane, and J.J. Fitton. An SCA security supplement compliant radio architecture. In *Military Communications Conference, 2005. MILCOM 2005. IEEE*, pages 2244–2250 Vol. 4, October 2005. doi: 10.1109/MILCOM.2005.1606003.

[21] A.H. Lashkari, M.M.S. Danesh, and B. Samadi. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). In *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 48–52, August 2009. doi: 10.1109/ICCSIT.2009.5234856.

[22] Z. Lei and F. Chin. A reliable and power efficient beacon structure for cognitive radio systems. *Broadcasting, IEEE Transactions on*, 54(2):182–187, June 2008. doi: 10.1109/TBC.2008.917737.

[23] K.J.R. Liu and B. Wang. *Cognitive Radio Networking and Security: A Game-Theoretic View*. Cambridge University Press, New York, NY, USA, 1st edition, 2010.

[24] Y. Liu, P. Ning, and H. Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In

Security and Privacy (SP), 2010 IEEE Symposium on, pages 286–301, May 2010. doi: 10.1109/SP.2010.24.

[25] A.W. Min, K.G. Shin, and X. Hu. Attack-tolerant distributed sensing for dynamic spectrum access networks. In *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*, pages 294–303, October 2009. doi: 10.1109/ICNP.2009.5339675.

[26] AirTight Networks. WPA2 hole196 vulnerability. URL `http://www.airtightnetworks.com/WPA2-Hole196`. [Accessed: 2015-02-05].

[27] E. Noon and H. Li. Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system. In *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*, pages 1–5, May 2010. doi: 10.1109/VETECS.2010.5494003.

[28] Q. Pei, H. Li, J. Ma, and K. Fan. Defense against objective function attacks in cognitive radio networks. *Chinese Journal of Electronics*, 20(4):138–142, 2011.

[29] G.A. Safdar and M. O'Neill. Common control channel security framework for cognitive radio networks. In *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*, pages 1–5, April 2009. doi: 10.1109/VETECS.2009.5073450.

[30] C.R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S.J. Shellhammer, and W. Caldwell. IEEE 802.22: The first cognitive radio wireless regional area network standard. *Communications Magazine, IEEE*, 47(1):130–138, January 2009. doi: 10.1109/MCOM.2009.4752688.

[31] Y. Sun and Y. Liu. Security of online reputation systems: The evolution of attacks and defenses. *Signal Processing Magazine, IEEE*, 29(2):87–97, March 2012. doi: 10.1109/MSP.2011.942344.

[32] W. Wang, H. Li, Y.L. Sun, and Z. Han. Attack-proof collaborative spectrum sensing in cognitive radio networks. In *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on*, pages 130–134, March 2009. doi: 10.1109/CISS.2009.5054704.

[33] C. Xenakis. Malicious actions against the GPRS technology. *Journal in Computer Virology*, 2(2):121–133, 2006. doi: 10.1007/s11416-006-0021-1.

[34] L. Zhu and H. Zhou. Two types of attacks against cognitive radio network MAC protocols. In *Computer Science and Software Engineering, 2008 International Conference on*, volume 4, pages 1110–1113, December 2008. doi: 10.1109/CSSE.2008.1536.

[35] Y. Zhu, D. Suo, and Z. Gao. Secure cooperative spectrum trading in cognitive radio networks: A reversed stackelberg approach. In *Multimedia Communications (Mediacom), 2010 International Conference on*, pages 202–205, August 2010. doi: 10.1109/MEDIACOM.2010.33.

Chapter 4

Assembled Cognitive Radio test bed architecture

Cognitive Radio has so far received significant attention from the research community from a theoretical standpoint. Many researchers rely on simulation environments for developing and testing cognitive algorithms. As useful as the simulation environment is for the algorithm research and development, simulators of wireless systems necessarily introduce many abstractions, often leading to losing track of important real-life constraints and obstacles. As such, demonstrating effectiveness of wireless systems' cognitive features on a simulation basis only is not sufficient. This has inspired us to go a step further and assemble an experimental Software Defined Radio/Cognitive Radio test bed, which may be used for testing and validating all relevant developed algorithms. This chapter describes the assembled architecture and its main functionalities.

4.1 Existing Cognitive Radio test beds and platforms

Prior to describing our assembled test bed architecture, a brief overview of the hardware and software characteristics and the developed functionalities for several state-of-the-art Cognitive Radio test bed architectures is given.

Researchers at the Berkeley Wireless Research Center have developed an experimental Cognitive Radio platform based on the *Berkeley Emulation Engine (BEE2)*, and reconfigurable 2.4 GHz RF front-ends, using fiber links for inter-communication. BEE2 engine consisted of five Xilinx Virtex-2 Field Programmable Gate Arrays (FPGAs), and supported connection of up to 18 individual RF front-ends, making the

Multiple Input Multiple Output (MIMO) experimentation possible. The RF front-ends support up to 25 MHz bandwidth in an 85 MHz frequency range. All signal processing is done directly on the platform. The software architecture is based on Matlab Simulink, coupled with the Xilinx System Generator library enhanced by a set of blocks in order to support interfaces with Analog-to-Digital Converters and Double data rate memory. The focus of the research is placed upon the spectrum sensing implementations, showing the practical performance and constraints of energy detectors [1] and cyclostationary feature detectors [6] in imperfect channel conditions.

Kansas University Agile Radio (KUAR) [4] is a low-cost experimental SDR platform based on an embedded 1.4 GHz General Purpose Processor (GPP), Xilinx Virtex-2 FPGA, and a RF front-end with 30 MHz bandwidth. The RF front-end is designed to operate in the 5–6 GHz frequency band. Majority of the signal processing is delegated to the FPGA, which is targeted using the software libraries running Linux OS. KUAR's software architecture consists of a set of Application Programming Interfaces (APIs) that comprise the KUAR Control Library. Some of the topics of interest are implementation of agile transmission techniques; distributed radio spectrum survey, and channel sounding techniques.

Maynooth Adaptable Radio System (MARS) [3] is another experimental SDR/ Cognitive Radio platform, consisting of an RF front end interconnected with a personal computer, where all the signal processing is done on the PC's GPP. The platform operates in the 1.75–2.45 GHz range, with the direct conversion architecture implemented both at the transmitting and the receiving side. The proprietary software architecture, called IRiS, is highly reconfigurable, and compatible with both Windows and Linux. A set of use-cases, such as spectrum sensing, image and video transmission, and interoperability with other SDR platforms, was studied and implemented using the platform.

A summary of the characteristics of the three aforementioned architectures, along with our proposed SDR/Cognitive test bed architecture, is given in Table 4.1.

4.2 Test bed description

The proposed SDR/Cognitive Radio test bed [2] is implemented as a coaxial architecture. Compared to over-the-air implementation, a coaxial test bed exhibits several important practical advantages:

- possibility to set accurate and stable RF levels;

Table 4.1: State of the art Cognitive Radio architectures

SDR/Cognitive Radio architecture	Signal processing	Operating RF band	RF bandwidth	Applications
BEE2, [1,6]	FPGA (on board)	2.4 GHz	25 MHz	Spectrum sensing; Cognitive MIMO
KUAR, [4]	FPGA (on board)	5-6 GHz	30 MHz	Agile transmission; distributed spectrum sensing
MARS, [3]	GPP (external)	1.75-2.45 GHz	?	Spectrum sensing; interoperability
Our proposed architecture, [2]	DSP+FPGA (external)	30-88 MHz; 256-512 MHz	120 MHz	Advanced communications electronic warfare

- repeatability of the experiments without the uncertainties characteristic to wireless transmission;
- possibility to connect test instruments and generators to one or more branches;
- avoiding regulatory issues related to transmitting outside of the Industrial, Scientific and Medical (ISM) frequency bands.

The proposed architecture consists of two Secure Wideband Multi-role – Single-Channel Handheld Radios (SWAVE HHs) [5], each interconnected with the OMBRA v2 – a powerful System-on-Module (SoM) embodied with a DSP and an FPGA. Inbetween, a dual directional coupler is placed. Vector signal generator allows for injecting noise/interference to the system, whereas spectrum analyzer provides reliable monitoring of the relevant RF activities in real-time. Block diagram of the test bed architecture is provided in Figure 4.1.

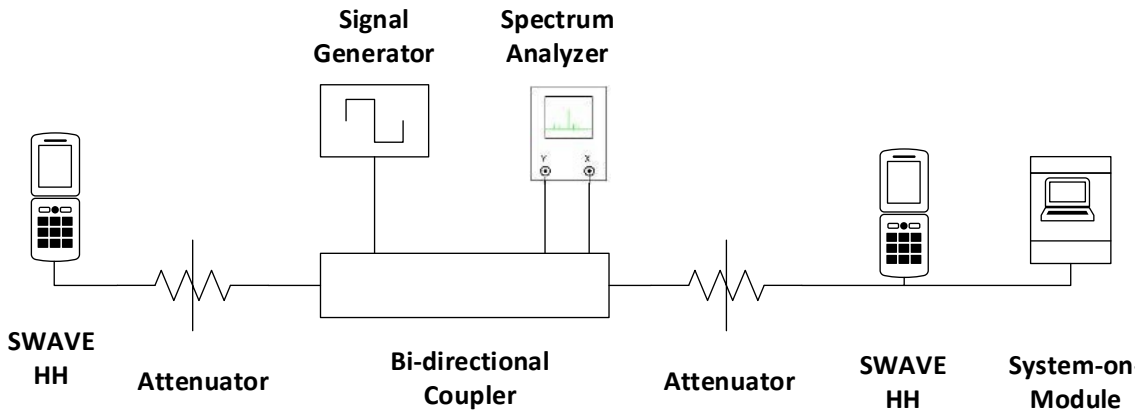


Figure 4.1: Cognitive Radio test bed block diagram

SWAVE HH (from now on referred to as HH) is a fully operational SDR terminal operable in Very High Frequency (VHF) and Ultra High Frequency (UHF) parts of the RF band, and capable of hosting a multitude of wideband and narrowband waveforms. Maximum transmission power of HH is 5W, with the harmonics suppression at the transmission side over -50 dBc. Superheterodyne receiver has a specified image rejection better than -58 dBc. The receiver is fully digital. In VHF part of the band, 12-bit 250 MHz Analog-to-Digital (AD) converters perform the conversion directly at RF, while in UHF part of the band, AD conversion is performed at an intermediate frequency (IF). No selective filtering is applied before AD conversion. Wideband digitized signal is then issued to the FPGA, where it undergoes digital down conversion, matched filtering and demodulation. HH has an integrated commercial Global Positioning System (GPS) receiver, but also provides the interface for an external GPS receiver. The radio is powered by Li-ion rechargeable batteries, however it may also be externally powered through a 12.6V direct current (DC) source. Relatively small physical dimensions ($80 \times 220 \times 50$ mm), long battery life (8 hours at the maximum transmission power for a standard 8:1:1 duty cycle), and acceptable weight (960g with battery) allow for portability and untethered mobile operation of the device. Hypertach expansion at the bottom of the HH provides several interfaces, namely: 10/100 Ethernet; Universal Serial Bus (USB) 2.0; RS-485 serial, DC power interface (maximum 12.7V), and Push-To-Talk (PTT).

The OMBRA v2 platform (from now on referred to as SoM) is composed of a small form factor SoM with high computational power, and the corresponding carrier board. It is based on an ARM Cortex A8 processor running at 1GHz, encompassed with powerful programmable Xilinx Spartan 6 FPGA and Texas Instruments TMS320C64+ DSP. The platform can be embodied with up to 1 GB LPDDR RAM, proffers support for microSD card up to 32 GB, and provides interfaces for different RF front-ends. IEEE 802.11 b/g/n and ANT protocol standards are supported. Furthermore, several other external interfaces are provided, namely: 16-bit Video Graphics Array (VGA) interface; Mic-in, line-in and line-out audio interfaces; USB 2.0; Ethernet; and RS-232 serial. The SoM is DC-powered, and has Windows CE and a Linux distribution installed.

All signal processing is delegated to the SoM. Connection between the HH and the SoM is achieved through Ethernet and serial ports. Ethernet is used for the remote control of the HH's parameters, using Simple Network Management Protocol (SNMP) v3. Furthermore, Ethernet is currently used as the port for the data communication with external systems (e.g., another HHs) – alternatively, it is possible to configure

the HH to utilize the USB port for data communication. Serial port is used to transfer raw spectrum data from the HH to the SoM. Interfaces between the HH and the SoM, as well as some of the most relevant SNMP commands, are denoted in Figure 4.2 . The actual implementations of the HH and the SoM are shown in Figure 4.3.

Two functionalities that are critical for encompassing the radios with the cognitive features: remote control of the HH's transceiving parameters, and spectrum acquisition, are described in Sections 4.2.1 and 4.2.2, respectively. The two waveforms that are currently installed on the HH are detailed in Section 4.2.3.

4.2.1 Remote control of the HH's parameters

SNMP v3 is a protocol used for externally controlling the parameters of the HH. A single host (running on the SoM) may be used to control multiple agents (HHs) in the network, provided that they are connected through an Ethernet hub and registered on the same domain. By utilizing two basic SNMP commands – `GET` and `SET` – it is possible to read the current value, or set a new value of the parameter, respectively. The parameters that can be controlled and the corresponding values that they can take are stored in a Management Information Base (MIB), which is loaded onto the host. MIB contains all the definitions of the properties of the controllable parameters, and assigns a unique Object IDentifier (OID) to each of them. Complete list of the parameters that may be controlled externally, with the corresponding input data types and the SNMP commands that may be invoked, is presented in Table 4.2.

4.2.2 Spectrum acquisition

The spectrum acquisition process using the HH's wideband front end architecture, presented in Figure 4.4, is described as follows. HH's 14-bit AD converter performs sampling at 250 Msamples/s. Every time that a `GET_SpectrumSnapshot` command is invoked on the SoM, a burst of 8192 consecutive samples is stored into a buffer on the HH's FPGA, and then outputted at 115200 bauds over the serial port to the SoM, where it may undergo further analysis. The samples correspond to the frequency spectrum of $[0, 120]$ MHz if the radio is operating in the VHF part of the band, or the $[f_C - 35, f_C + 85]$ MHz if the radio is operating in the UHF part of the band, where f_C is the center carrier frequency that the radio is currently using for transceiving.

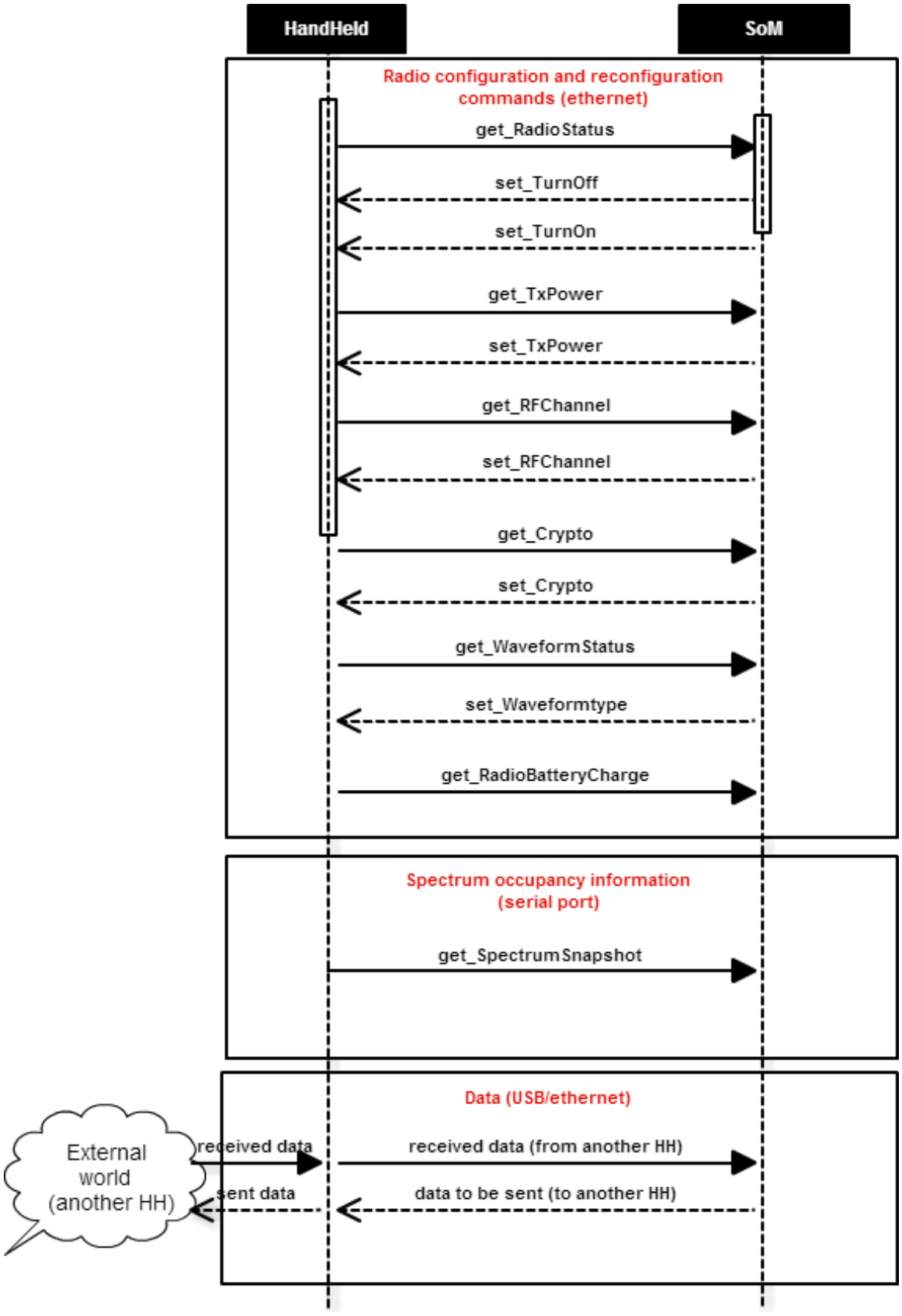


Figure 4.2: Interfaces HandHeld–SoM

Figure 4.3: Implementations of HandHeld and SoM

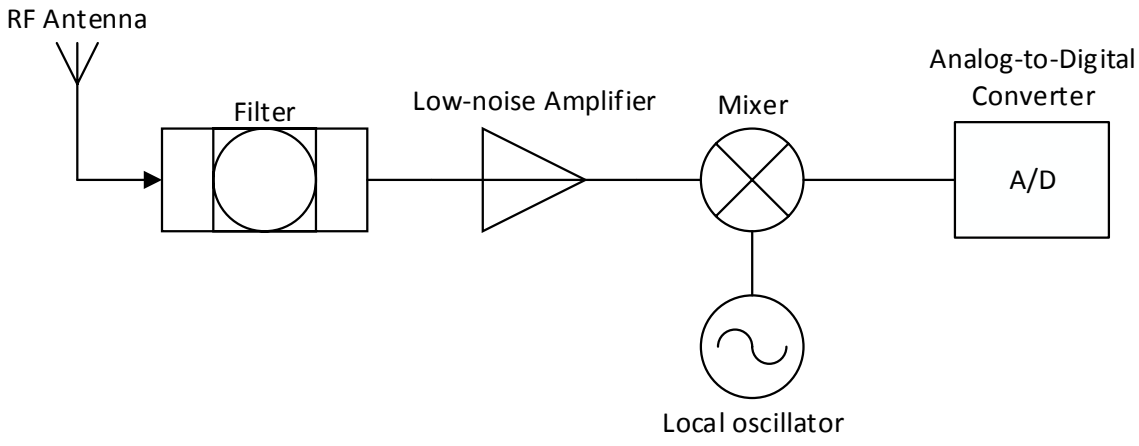


Figure 4.4: HandHeld's wideband RF front end architecture

Table 4.2: Parameters of the HH that may be externally controlled via SNMP v3

Parameter	**Type**	**SNMP commands**
File Transfer Activation	string	SET/GET
File Transfer Type	string	SET/GET
FTP User Name	string	SET/GET
FTP Password	string	SET/GET
FTP Address	string	SET/GET
Login Username	string	SET/GET
Login Password	string	SET/GET
Transmission Power	integer	SET/GET
Transmitter On/Off	integer	SET/GET
Currently Installed Waveform	string seq	GET
Waveform's MIB Root	string	GET
Waveform Status [ON/OFF]	integer	SET/GET
Audio Message ID	string	SET/GET
Create New Waveform	string	SET/GET
Activate Preset	string	SET/GET
Activate Mission File	string	SET/GET
Audio Output Gain	float	SET/GET
Battery Charge Percentage	integer	GET
File Download Status	integer	GET
Trap Receiver's IP Address	string	SET/GET
Turn Crypto [ON/OFF]	integer	SET/GET
Zeroize All Crypto Keys	integer	SET/GET
Crypto Key Loaded	integer	GET
System End Boot	integer	GET
RF Channel	integer	SET/GET

4.2.3 Installed waveforms

Currently, two functional waveforms are installed on the HHs: Soldier Broadband Waveform (SBW) and VHF/UHF Line Of Sight (VULOS). A wideband spectrum analyzer enables us to monitor the transmitted waveforms in real-time, and analyze their parameters.

SBW is a digital multi-hop Mobile Ad-hoc NETwork (MANET) waveform that provides self-(re)configurability and self-awareness of the network structure and topology, for up to 50 nodes and up to 5 hops. Furthermore, possibility of simultaneous streaming of voice and data services is provided, with prioritization for voice streaming (in case of exceeded bandwidth). Allocated channel bandwidth is adjustable – from 1.25 MHz to 5 MHz – with channel spacing of 2 MHz. Data is modulated using a Quaternary Phase Shift Keying (QPSK) digital modulation technique. Self-awareness is exercised by monitoring the network topology for changes every n seconds (monitor interval n is adjustable). Two QoS monitoring mechanisms are provided: Bit Error Rate (BER) Test, and the statistics data for the transmitting/receiving side. These mechanisms proffer means for analyzing and comparing the quality of communication in regular and impaired channel conditions. Figure 4.5 shows the shape of the envelope and properties of the SBW waveform in the frequency domain, for the maximum signal bandwidth (5 MHz), transmitted with power -3 dBW on the carrier frequency 225 MHz.

VULOS is a narrowband single-hop waveform designed for short-distance voice or data communication. It supports operation in both VHF (30–88 MHz) and UHF (225–512 MHz) parts of the frequency band. The waveform supports two analog modulation techniques: Amplitude Modulation (AM) and Frequency Modulation (FM). The modulation technique, as well as the modulation index, may be configured on-the-fly. Channel bandwidth is 25 kHz, with channel spacing also equaling 25 kHz. Furthermore, the VULOS waveform is able to utilize both digital and analog voice Coder–Decoders (CODECs) installed on the radio. Figure 4.6 shows envelope shape and properties of the FM-modulated VULOS waveform, transmitted with 1 dBW power on the carrier frequency 30 MHz.

4.3 Conclusions

The chapter has provided a technical description of the assembled SDR/Cognitive Radio test bed architecture. At the core of the architecture is the fully reprogrammable military SDR interconnected with the computationally powerful System-on-Module.

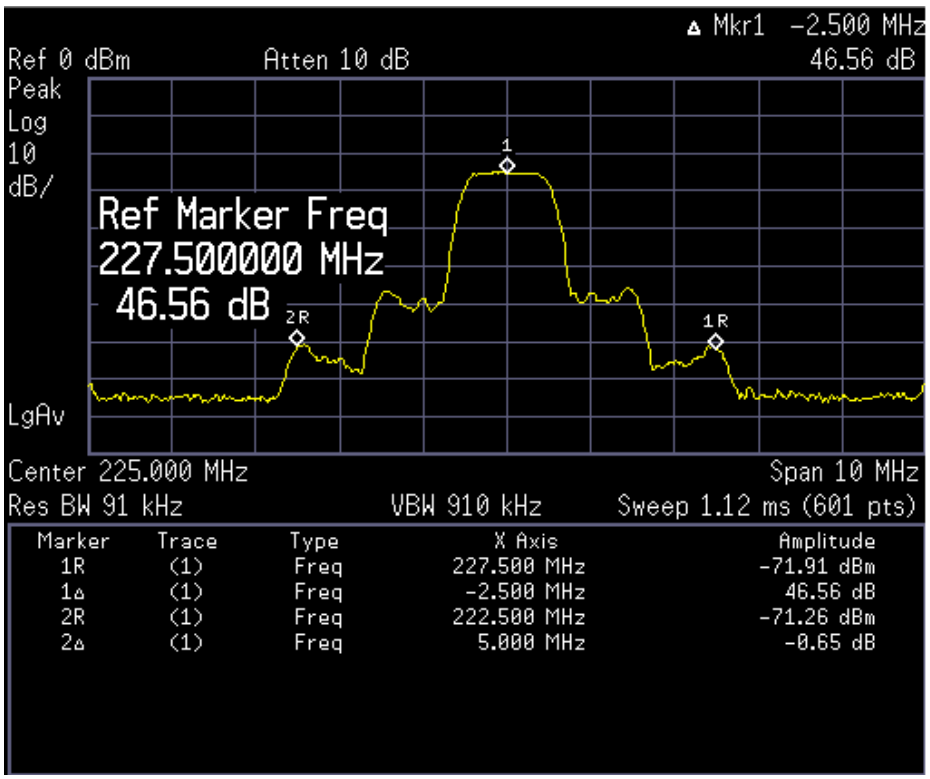


Figure 4.5: SBW waveform in the frequency domain – max hold

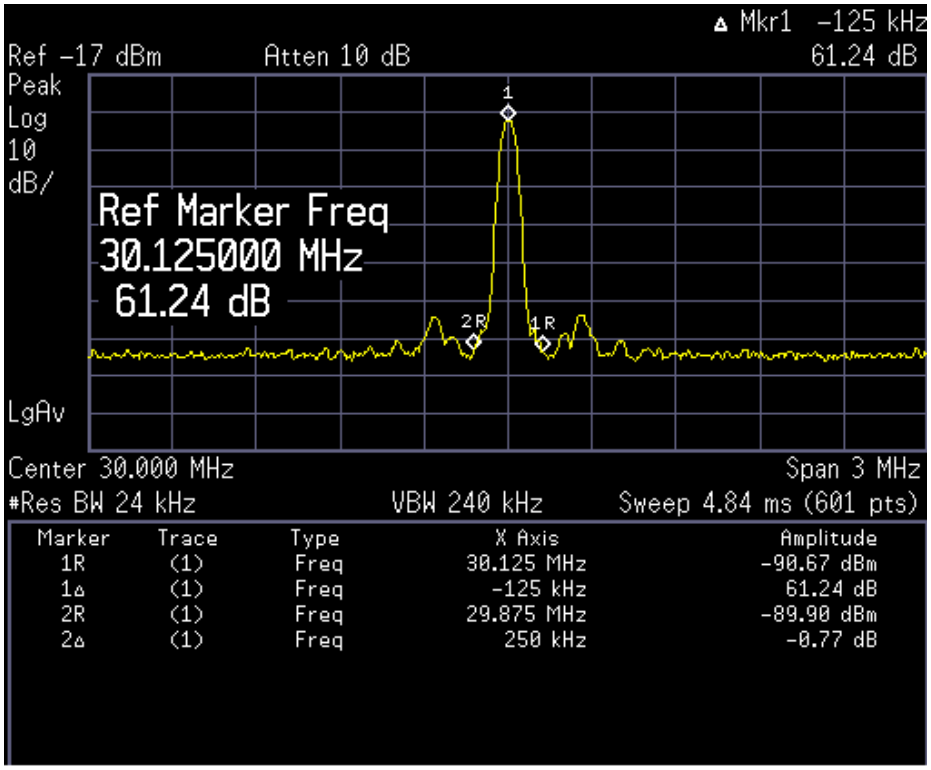


Figure 4.6: VULOS waveform in the frequency domain – max hold

Details of all the relevant hardware and software parameters and interfaces, as well as the currently supported waveforms, were included. The assembled architecture allows for testing and validation of the algorithms presented in the following sections.

Bibliography

[1] D. Cabric, A. Tkachenko, and R.W. Brodersen. Experimental study of spectrum sensing based on energy detection and network cooperation. In *Proceedings of the first international workshop on Technology and policy for accessing spectrum*, TAPAS '06, New York, NY, USA, 2006. ACM. doi: 10.1145/1234388.1234400.

[2] K. Dabcevic, L. Marcenaro, and C. S. Regazzoni. SPD-driven smart transmission layer based on a software defined radio test bed architecture. In *Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems*, pages 219–230, 2014. doi: 10.5220/0004876302190230.

[3] R. Farrell, M. Sanchez, and G. Corley. Software-defined radio demonstrators: An example and future trends. *Int. J. Digital Multimedia Broadcasting*, 2009, 2009.

[4] G.J. Minden, J.B. Evans, L. Searl, D. DePardo, V.R. Petty, R. Rajbanshi, T. Newman, Q. Chen, F. Weidling, J. Guffey, D. Datla, B. Barker, M. Peck, B. Cordill, A.M. Wyglinski, and A. Agah. Kuar: A flexible software-defined radio development platform. In *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pages 428–439, 2007. doi: 10.1109/DYSPAN.2007.62.

[5] SelexES. SWAVE HH specifications. URL `http://www.selexelsag.com/internet/localization/IPC/media/docs/SWave-Handheld-Radio-v1-2012Selex.pdf`. [Accessed: 2015-02-08].

[6] A. Tkachenko, D. Cabric, and R.W. Brodersen. Cognitive radio experiments using reconfigurable BEE2. In *Signals, Systems and Computers, 2006. ACSSC '06. Fortieth Asilomar Conference on*, pages 2041–2045, 2006. doi: 10.1109/ACSSC.2006.355125.

Chapter 5

Traditional RF jamming and anti-jamming techniques

Wireless communication is fundamentally susceptible to attacks due to the open nature of the wireless medium. Typically, over-the-air attacks may be categorized as either passive or active. In the former, attackers aim at eavesdropping on the targeted communication channels, thus posing threat to communication privacy. Active attackers, conversely, try to degrade quality of the communication link on the targeted channels by creating intentional interference. The latter types of attacks are also referred to as the *Radio Frequency (RF) jamming attacks*.

RF jamming and anti-jamming systems have particular applications in the electronic battlefield situations. This is commonly referred to as the *Communications Electronic Warfare (CEW)*. In the CEW domain, *Electronic Attack (EA)* typically refers to the set of techniques and solutions aimed at intercepting or denying the communication on the targeted systems, whereas *Electronic Defense (ED)* comprises actions aimed at preventing EAs from successfully occurring.

Figure 5.1 shows model of the communication system considered within this chapter. The system consists of a transmitter–receiver pair and an active attacker (jammer). The signal from the legitimate transmitter propagates through the channel and, on its way to the receiver, undergoes deterioration due to thermal noise, multipath effects, and different types of interference. The jammer may be located either in the immediate proximity of the receiver (denoted in the figure by the standoff radius), or further away. In both cases, its intention is to interfere with the receiver, not the transmitter. The signal from the jammer to the receiver also undergoes deterioration due to the aforementioned channel effects. However, since the transmitter–receiver and the jammer–receiver propagation paths may be – and typically will be – independent of each other, the two respective signals will undergo different levels of

deterioration.

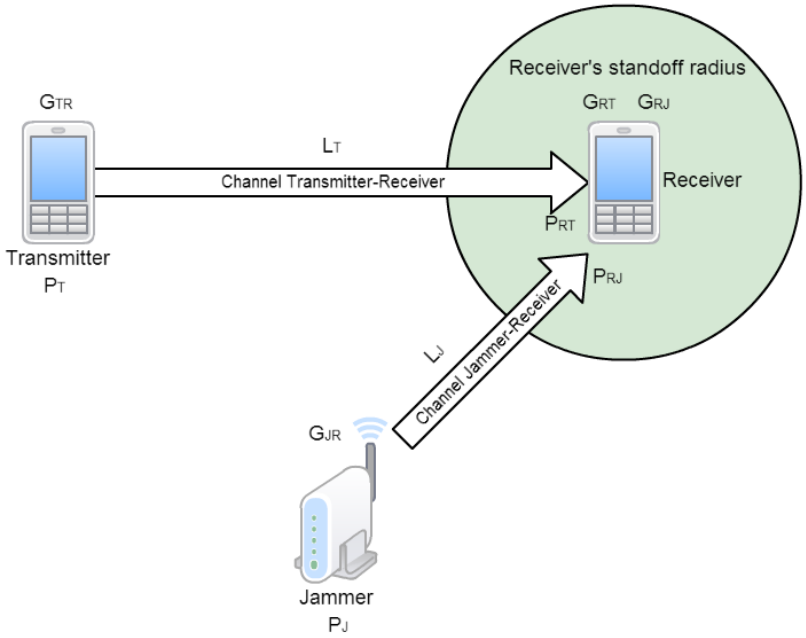


Figure 5.1: Model of the considered communication system

This chapter presents traditional jamming and anti-jamming techniques in wireless systems, and discusses their efficiencies depending on the properties and parameters of the overall system. An analysis of the crucial aspects that influence the success rate of jamming and anti-jamming systems is performed from a theoretical perspective. These results are complemented by the experimental analysis using the SDR/Cognitive Radio test bed architecture presented in Chapter 4. Understanding these factors is an important basis for an efficient design of jamming/anti-jamming systems that utilize the advanced capabilities of the Software Defined Radio/Cognitive Radio technology, discussed in Chapter 6.

5.1 Jamming techniques

Deployment of different jamming tactics and techniques directly influences the probability of jamming success. In this section, we explain some of the most commonly employed jamming tactics and analyze their performance in digital communication systems. Deployment of jamming tactics will often be restricted by the hardware capabilities of the jamming entity. An advanced jammer may switch between different tactics in order to adapt to the targeted communication system.

The jamming success rate depends on multiple parameters of the communication system, namely:

- Received power of the jamming signal;
- Received power of the targeted transmitted signal;
- Type, modulation and bandwidth of the jamming signal;
- Modulation and bandwidth of the targeted transmitted signal;
- Error correction mechanisms implemented within the transmitted signal;
- Sensitivity of the receiver;
- Type of detector implemented at the receiver (coherent or non-coherent).

We present a theoretical analysis of jamming efficiency for various levels of transmission power for both the jamming and the transmitted signal. The analysis is done for two different modulation techniques of the targeted transmitted signal: Binary Phase Shift Keying (BPSK) and Quaternary Phase Shift Keying (QPSK). These techniques represent the most common digital modulation choices for anti-jamming systems based on Direct Sequence Spread Spectrum (DSSS), which are described in Section 5.2.2. The presented derivations and results correspond to the receiver architectures that implement coherent detection, as these are the only suitable design choices for the aforementioned modulation techniques. The considered targeted transmitted signals do not contain error correction mechanisms [1]. It should be noted that most error correction techniques provide good improvement only at already relatively low Bit Error Rate (BER) levels (e.g., less than 10^{-3}), whereas at high BER levels (more that 10^{-1}), the added protection is negligible [4, p. 41].

When all the parameters of the communication systems are defined as above, the performance of the jammer will be a function of Jamming-to-Signal Ratio (JSR). Prior to introducing the JSR, let us describe parameters of the communication model presented in Figure 5.1.

The received power at the receiver's antenna with gain G_{RT} in the direction of the receiver, for the transmitter transmitting with power P_T with transmission losses L_T,

[1] An interested reader is referred to Torrieri [9] for a detailed evaluation of the influence of error correction mechanisms on the quality of communication.

with antenna gain in the direction of the receiver G_{TR}, and with propagation losses on the transmitter-receiver path L_{TR}, can be expressed as:

$$P_{RT} = \frac{P_T G_{RT} G_{TR}}{L_T L_{TR}}. \tag{5.1}$$

Similarly, the received power at the receiver's antenna with gain G_{RJ} in the direction of the jammer, for the jammer transmitting with power P_J with transmission losses L_J, with antenna gain in the direction of the receiver G_{JR}, and with propagation losses on the jammer-receiver path L_{JR}, can be expressed as:

$$P_{RJ} = \frac{P_J G_{RJ} G_{JR}}{L_J L_{JR}}. \tag{5.2}$$

Then, the JSR ξ is defined as:

$$\xi = \frac{P_{RJ}}{P_{RT}}. \tag{5.3}$$

Signal-to-Jamming Ratio (SJR) is the reciprocal value of JSR, and is denoted by γ:

$$\gamma = \frac{1}{\xi}. \tag{5.4}$$

In order to achieve its goal, a jammer can deploy several different jamming tactics – each with its own advantages and disadvantages, depending on the constraints of the jamming entity and the characteristics of the targeted system. Some of the commonly deployed jamming tactics are described below.

Narrowband noise jamming corresponds to the jammer that uses all its power to generate and transmit a random Gaussian noise waveform on a single channel. The bandwidth of such signal may be equal to the width of the targeted channel, or may be restricted to a specific part of the channel – ideally, the part equaling to the data signal width of the targeted transmitted signal.

Partial band noise jamming tries to improve jamming efficiency by distributing the available energy over multiple channels used by the targeted system. This type of jamming is often used against systems relying on spread spectrum techniques.

Full band noise jamming, sometimes referred to as *barrage jamming*, can be viewed as a special case of partial band noise jamming, where the jammer distributes its energy over all of the channels utilized by the targeted communication system. This type of jamming, however, often requires impractically large amounts of jamming power and/or physical placement in the immediate proximity of the targeted communication system – typically within its standoff radius. When successfully deployed

against a spread spectrum system, full band noise jamming can have impact not only on the successful decoding of the targeted signal, but also on the synchronization and tracking phases of transmitter–receiver pair. For example, for a targeted system that deploys frequency hopping spread spectrum with fine tracking, the receiver may be prevented from successfully tracking the transmitter, since it will not be able to adequately tune its clock/oscillator [5, pp. 472–475].

Single-tone jamming refers to transmitting a single tone – typically, a sinusoidal signal – on a given carrier frequency. Single-tone jamming can have high success rates when the target is a narrowband signal. It may often represent the best strategy for jammers with limited transmission power, as it allows them to concentrate all of their power on a single data channel.

Multi-tone jamming occurs when the jammer distributes its power on multiple tones, which may be placed on specific frequencies, or randomly. These types of jammers are sometimes referred to as *comb jammers*, and typically have higher success rates against wideband communication systems than single-tone jammers, provided that they are able to transmit with sufficient power to cause degradation to the targeted system. Furthermore, they may be particularly suitable for jamming systems that employ Frequency Shift Keying (FSK) modulation, where the carrier frequency is changed according to the modulating digital signal, resulting in different frequencies each representing a different symbol. Frequency Hopping Spread Spectrum systems deploy FSK modulation – typically, Binary FSK (BFSK).

Figure 5.2 sketches the possible transmitted narrowband signal, transmitted DSSS signal, and the aforementioned types of jamming signals.

We focus our analysis on two types of jamming signals: narrowband noise, and single-tone jamming, in different SNR and SJR regimes.

5.1.1 Jamming the BPSK-modulated signals

In Phase Shift Keying (PSK), the phase of the carrier is changed according to the modulating digital signal. We consider the relative phase changes of the signal, as opposed to the differential changes which characterize the Differential PSK (DPSK) techniques. Among all the PSK techniques, BPSK has the lowest spectral efficiency, amounting to 1 bit/s/Hz. Its phases are separated by π rad. A signal $s(t)$ modulated using BPSK during time interval k can be represented as:

$$s_k(t) = \sqrt{2R}cos(2\pi f_0 t + d_k\frac{\pi}{2}), \quad (k-1)T \leq t < kT \tag{5.5}$$

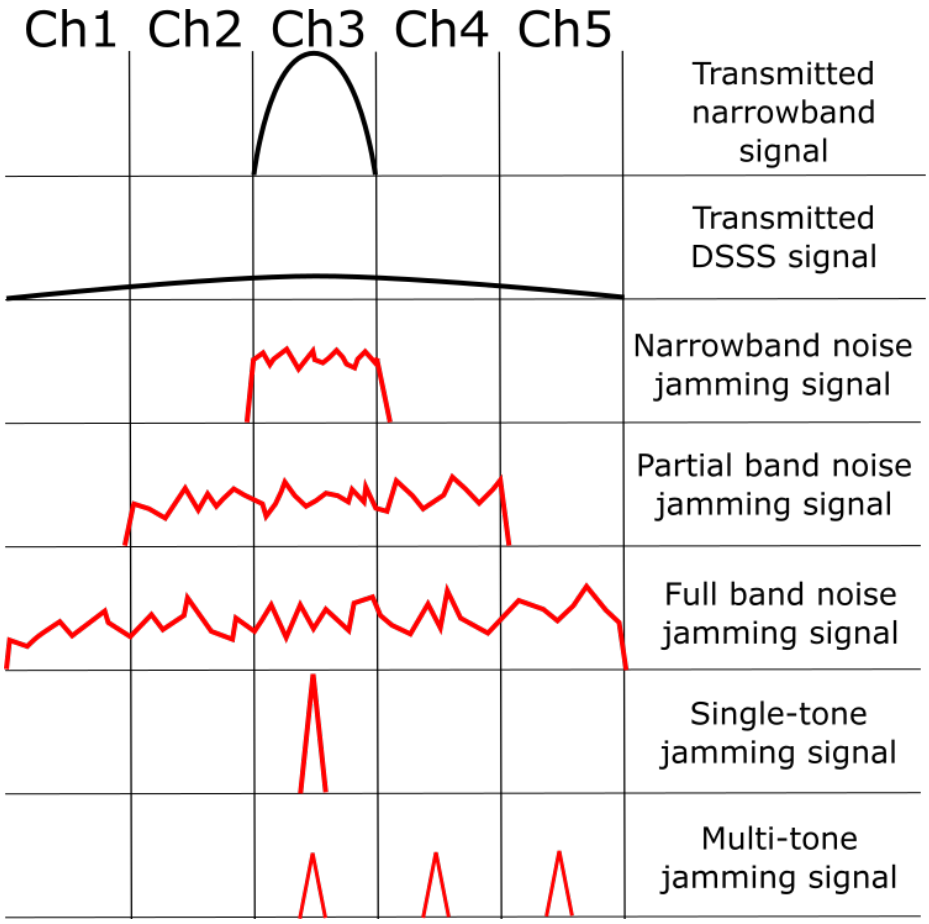


Figure 5.2: Examples of targeted transmitted signals and considered jamming signals

where R is the average signal power, $d_k \in \{+1, -1\}$ determines the data bit, f_0 is the carrier frequency, and T is the symbol period.

5.1.1.1 AWGN channel only

The received signal $r(t)$ during time interval k can be written as:

$$r_k(t) = s_k(t) + n(t), \tag{5.6}$$

where $n(t)$ incorporates Additive White Gaussian Noise (AWGN) and any eventual interfering signals.

The corresponding probability density function (pdf) of $r(t)$ is:

$$p(r|d_k) = \frac{1}{\sqrt{\pi N_0}} e^{-\frac{(r-d_k\sqrt{E_S})^2}{N_0}}, \tag{5.7}$$

where E_S represents the average signal energy, and N_0 represents noise energy.

The decoder differentiates between the symbols by comparing the received signal with the threshold γ, for example:

$$symbol = \begin{cases} s_0, & r(t) < \gamma \\ s_1, & r(t) > \gamma \end{cases} \tag{5.8}$$

Then, the probability of error given that s_1 is transmitted can be expressed as:

$$\Pr\{\mathrm{e}|\mathrm{s}_1\} = \frac{1}{\sqrt{\pi N_0}} \int_{-\infty}^{0} e^{-\frac{(r-\sqrt{E_S})^2}{N_0}} dr = \frac{1}{2}\mathrm{erfc}(\sqrt{\frac{E_S}{N_0}}), \tag{5.9}$$

where $\mathrm{erfc}(x)$ is the complementary error function of x given by:

$$\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_{x}^{\infty} e^{-z^2} dz. \tag{5.10}$$

Assuming that both symbols are equally likely, i.e., $\Pr\{e|s_1\} = \Pr\{e|s_0\} = 0.5$, the symbol error probability of the BPSK corrupted by the AWGN is given by:

$$P_e = \frac{1}{2}\mathrm{erfc}(\sqrt{\frac{E_S}{N_0}}). \tag{5.11}$$

The influence of AWGN on the Symbol Error Rate (SER) performance of BPSK is shown in Figure 5.3.

5.1.1.2 AWGN channel with narrowband noise jamming

When the jammer injects narrowband Gaussian noise on the targeted channel, the symbol error probability increases correspondingly:

$$P_e = \frac{1}{2}\mathrm{erfc}(\sqrt{\frac{E_S}{J + N_0}}), \tag{5.12}$$

where J is the average power of the injected noise signal at the decoder of the receiver.

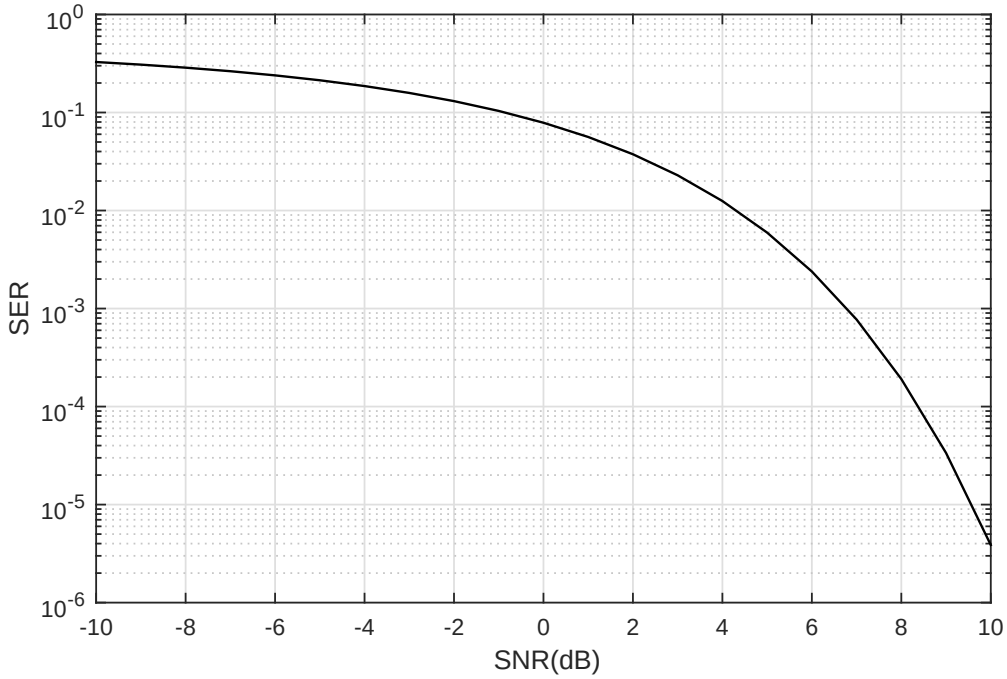


Figure 5.3: Influence of AWGN on SER for coherent BPSK

5.1.1.3 AWGN channel with tone jamming

Similar to (5.5), the jamming tone $j(t)$ during time interval k can be described as:

$$j_k(t) = \sqrt{2J}cos(2\pi f_0 t + \theta_J), \quad (k-1)T_S \leq t < kT_S \tag{5.13}$$

where J is the average power in the jamming tone, θ_J is the phase offset of the interfering signal compared to the jamming signal, and T_S is the symbol period.

Then, the overall received signal is:

$$r_k(t) = s_k(t) + n_k(t) + i_k(t), \quad (k-1)T_S \leq t < kT_S. \tag{5.14}$$

When the jammer injects a single tone onto the center carrier frequency of the channel used for communication, the probability of symbol error depends on the phase of the jamming signal – namely [6, p. 673]:

$$\mathrm{P_e} = \mathrm{Q}(\sqrt{2\frac{R}{N_0}}(1 - \sqrt{\frac{2J}{R}}sin(\theta^J))), \tag{5.15}$$

where $\mathrm{Q}(x)$ represents the Q-function, defined as:

$$\mathrm{Q}(x) = \frac{1}{2}\mathrm{erfc}(\frac{x}{\sqrt{(2)}}). \tag{5.16}$$

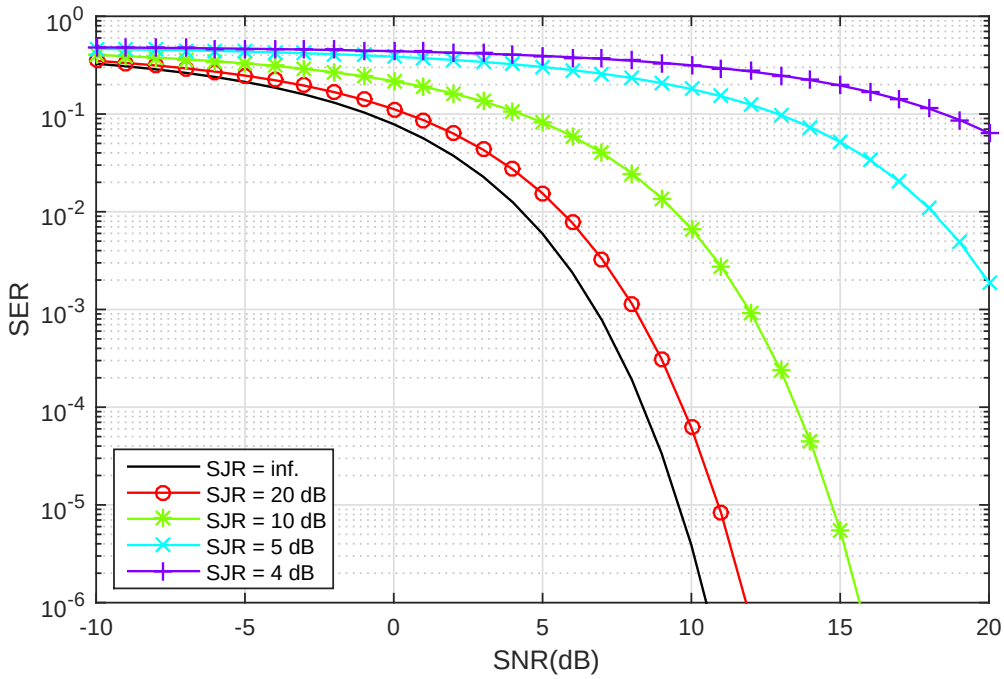


Figure 5.4: Influence of AWGN with single tone jamming on SER for coherent BPSK

Hence, in order for the jammer to successfully jam the signal, the phases between the jamming and the targeted signal must not coincide.

Figure 5.4 shows the SER performance for coherent BPSK when the interfering tone is present on the center carrier frequency of the data channel and $\theta = \frac{\pi}{2}$, for different levels of γ.

Here, $\gamma = \infty$ corresponds to the situation with no jamming tone present, as was shown in Figure 5.3. As the power of the jamming signal increases, the performance of the communication system starts decreasing rapidly. The objective of the jammer will often be to cause SER$\geq 10^{-1}$ in order to efficiently disable the communication, although the exact value is situation-dependent.

5.1.2 Jamming the QPSK-modulated signals

Compared to BPSK, QPSK technique doubles the spectral efficiency, increasing it to 2 bit/s/Hz. This is done by simultaneously transmitting two BPSKs in quadrature, achieving the phase separation of $\pi/2$ rad. A signal $s(t)$ modulated using QPSK

during time interval k can be represented as:

$$s_k(t) = \sqrt{2R}sin(2\pi f_0 t + d_k\frac{\pi}{4}) \tag{5.17}$$

$$= \pm\sqrt{R}cos(2\pi f_0 t) \pm \sqrt{R}sin(2\pi f_0 t), \quad (k-1)T \leq t < kT \tag{5.18}$$

where $d_k \in \{1, 3, 5, 7\}$.

5.1.2.1 AWGN channel only and AWGN channel with narrowband noise jamming

The received signal can once again be expressed as (5.6).

Similarly to (5.11), and assuming that all four symbols are equally likely, the derivation of the probability of symbol error can be expressed as:

$$P_e = \text{erfc}(\sqrt{\frac{E_S}{2N_0}}) - \frac{1}{4}\text{erfc}^2(\sqrt{\frac{E_S}{2N_0}}) \tag{5.19}$$

$$\approx \text{erfc}(\sqrt{\frac{E_S}{2N_0}}). \tag{5.20}$$

Analogously to (5.12), the symbol error probability in the presence of the narrowband noise jammer becomes:

$$P_e \approx \text{erfc}(\sqrt{\frac{E_S}{2(J+N_0)}}). \tag{5.21}$$

The influence of AWGN on the SER performance of QPSK is shown in Figure 5.5.

5.1.2.2 AWGN channel with tone jamming

Since QPSK can be represented as two antipodal BPSK signals, the tone jammer needs to efficiently jam either the quadrature, or the in-phase component of the targeted signal. The probability of causing a symbol error on each of these components is given by [6, pp. 673–674]:

$$\mathrm{P_e}^I = \mathrm{Q}(\sqrt{\frac{R}{N_0}}(1 - \sqrt{\frac{2J}{R}}sin(\theta^J))) \tag{5.22}$$

$$\mathrm{P_e}^Q = \mathrm{Q}(\sqrt{\frac{R}{N_0}}(1 + \sqrt{\frac{2J}{R}}cos(\theta^J))). \tag{5.23}$$

The average symbol error probability for the QPSK signal, conditioned on the phase θ^J of the jamming signal may then be computed as:

$$\mathrm{P_e} = \mathrm{P_e}^I + \mathrm{P_e}^Q - \mathrm{P_e}^I\mathrm{P_e}^Q \tag{5.24}$$

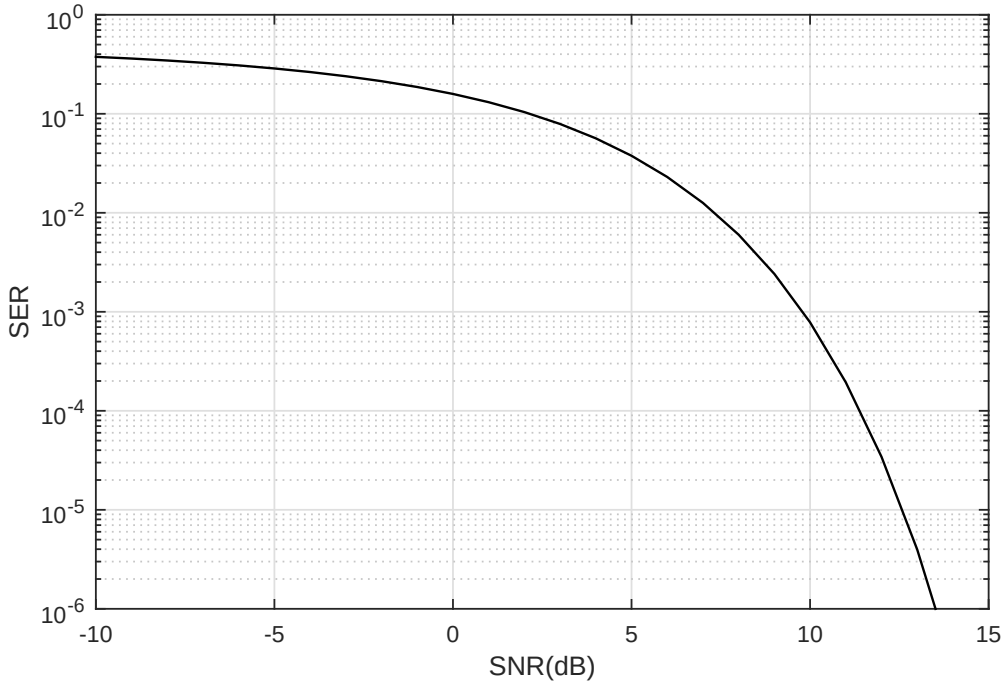


Figure 5.5: Influence of AWGN on SER for coherent QPSK

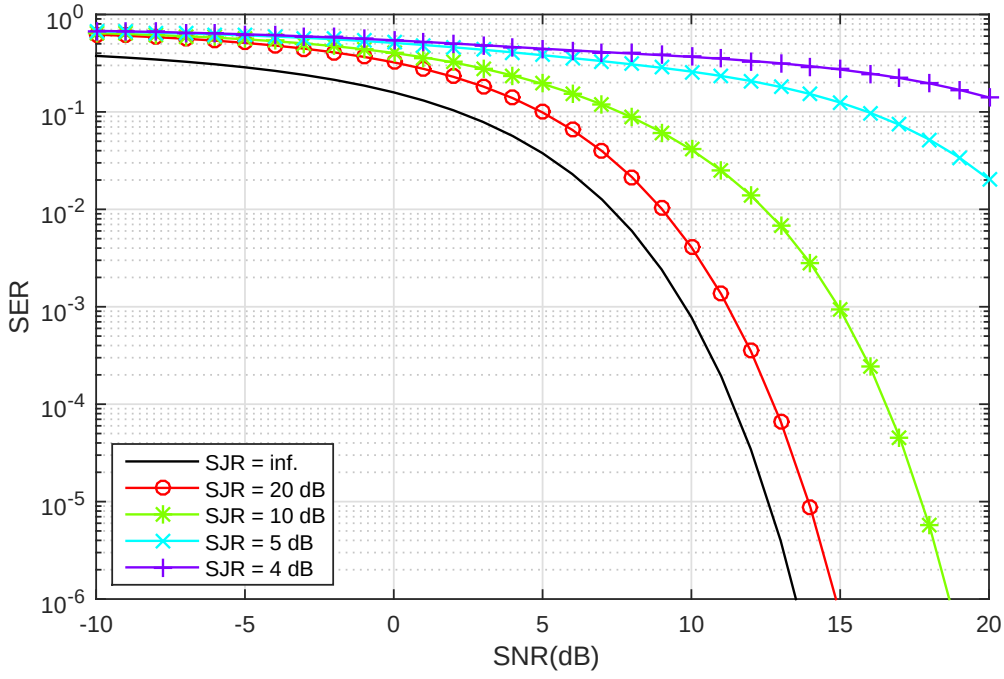


Figure 5.6: Influence of AWGN with single tone jamming on SER for coherent QPSK when $\theta = \frac{\pi}{2}$

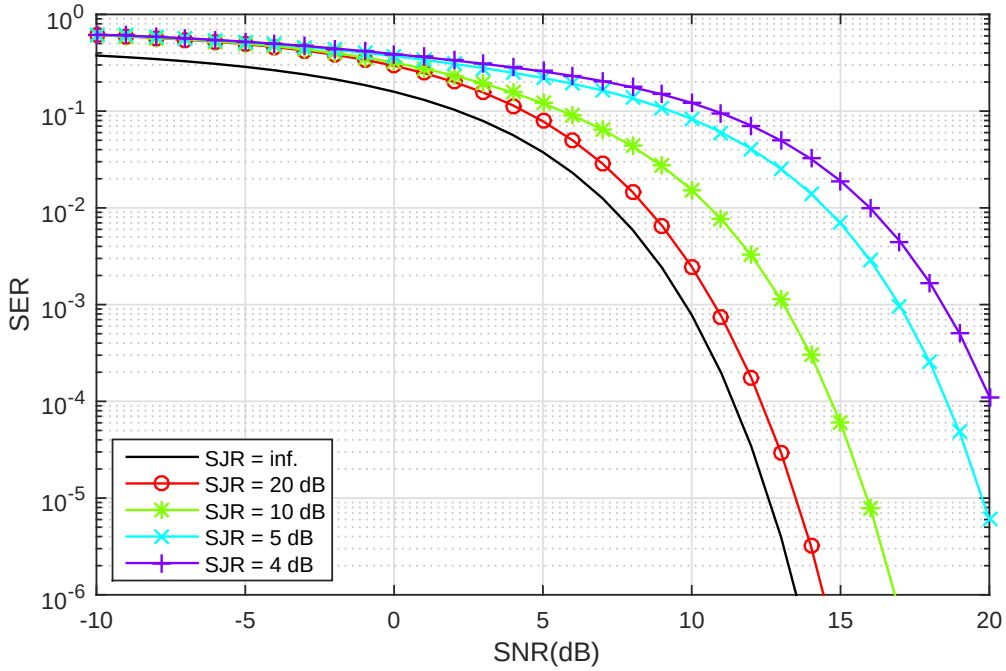


Figure 5.7: Influence of AWGN with single tone jamming on SER for coherent QPSK when $\theta = \frac{\pi}{4}$

Figure 5.6 shows the SER performance for coherent QPSK when the interfering tone is present on the center carrier frequency of the data channel and $\theta = \frac{\pi}{2}$, for different levels of γ.

The results show that, for $\theta = \frac{\pi}{2}$, the performance of QPSK for achieving SER= 10^{-6} is approximately 3dB worse when compared to BPSK, i.e., the jammer will need to invest 2 times less power to cause the same SER.

The influence of θ is highlighted in Figure 5.7, which shows the SER performance when the interfering tone has a phase delay of $\theta = \frac{\pi}{4}$ with respect to the transmitted signal: In high-SNR and low-SJR environments, in order to achieve the same SER, the jammer needs to invest approximately 3dB more power compared to when $\theta = \frac{\pi}{2}$.

Assuming that the phase of the jamming signal is evenly distributed over $[0, 2\pi]$, the unconditional average symbol error probability can be computed as:

$$\mathrm{P_e}^{uncond.} = \frac{1}{2\pi} \int_0^{2\pi} \mathrm{P_e} d\theta^J. \tag{5.25}$$

Which jamming tactic a jammer should deploy depends primarily on the characteristics of the targeted communication system, however it depends also on the

capabilities and constraints of the jammer. Wideband jammers equipped with multiple antennas may decide to perform transmission on multiple channels simultaneously, however, power constraints may force them to limit the number of channels to a relatively small value. Finding a compromise between a number of channels to transmit on, and ways of distributing the available power across them is a principle challenge of any power-constrained jamming entity.

5.2 Anti-jamming techniques

Anti-jamming techniques designed for the tactical battlefield solutions may broadly be divided in two categories: i) those aiming to achieve *Low Probability of Detection (LPD)*, and ii) those focusing on *Low Probability of Interception (LPI)*. LPD systems focus on "hiding" transmitted signals from potential adversaries. This can be done either by refraining from transmitting in certain time periods – the so-called EMissions CONtrol techniques – or by spreading the transmitted signal over a wide frequency band, as deployed in Direct Sequence Spread Spectrum systems. Conversely, LPI systems imply that the signal may be detected relatively easily, while being difficult to intercept or to jam. The best example of LPI is given by Fast Frequency Hopping Spread Spectrum signals, which are relatively easily to detect, but due to rapid changes in the frequencies used for transmission may not be readily jammed. The three aforementioned techniques are presented below.

5.2.1 Emissions control techniques

In order to protect the communication, the radios comprising the system may take coordinated actions aimed at preventing the adversaries from eavesdropping and/or successfully jamming the communication. Among the electronic protect methods in the CEW domain, the most widely deployed techniques are referred to as *EMissions CONTtrol (EMCON)* [3]. EMCON techniques limit the communication between the friendly systems in defined time periods (usually periods estimated as most critical). The systems are allowed to receive data, however, they may not acknowledge any data reception.

5.2.2 Spread spectrum techniques

Spread spectrum systems use large RF bandwidth to spread the original signal. Two spread spectrum systems that are most common are DSSS, and FHSS.

In *DSSS* [2], the original signal is multiplied with a pseudo random noise spreading code, thus significantly increasing the utilized RF bandwidth. However, DSSS systems are still somewhat vulnerable to tone and narrowband noise jamming signals, in particular when the jammers are placed in the standoff radius of the targeted receiver. Sufficiently powerful jamming signal may then overcome the processing margin of the receiver, causing the noise leak in the demodulation process, and in turn raising the noise floor at the baseband [4, p. 42]. DSSS systems most commonly deploy BPSK or QPSK modulation, hence the analysis performed in Section 5.1 is pertinent to these systems.

In *FHSS* systems, the transmitter–receiver pair continuously changes the operating frequency according to a pre-defined pattern. Depending on the hopping rate – the time during which the signal stays on the same carrier frequency – there are two types of FHSS systems: slow and fast. In the former, one or more data bits are transmitted over the same carrier, whereas in the latter, each bit is transmitted over several carriers. While fast frequency hopping systems typically provide lower probability of interception, they are also more complex to implement and require fine tracking. This makes them particularly vulnerable to powerful wideband jamming that may prevent the tracking phase from successfully occurring. Independent Mark-Space signalling [7] was developed to make frequency hopping a more robust anti-jam technique. FHSS systems typically deploy BFSK modulation, whose performance under various types of interference was evaluated by Viswanathan and Taghizadeh [10], Teh et al. [8].

5.3 Experimental results

This section presents experimental results of jamming efficiency, performed using the test bed architecture presented in Chapter 4. The goal of the experiments is to evaluate the impact of different jamming signals on the quality of communication, and the corresponding robustness of the targeted waveform.

Soldier Broadband Waveform (SBW), introduced in Section 4.2.3, is used as the waveform deployed by the transmitter–receiver pair. SBW is a wideband QPSK-modulated digital waveform operable in 30–88 MHz part of the VHF band and the 225–512 MHz part of the UHF band. It implements turbo coding with code rate 1/2 [1] as an error correction mechanism. Packetized data transmission is used, with each packet consisting of 29 bytes.

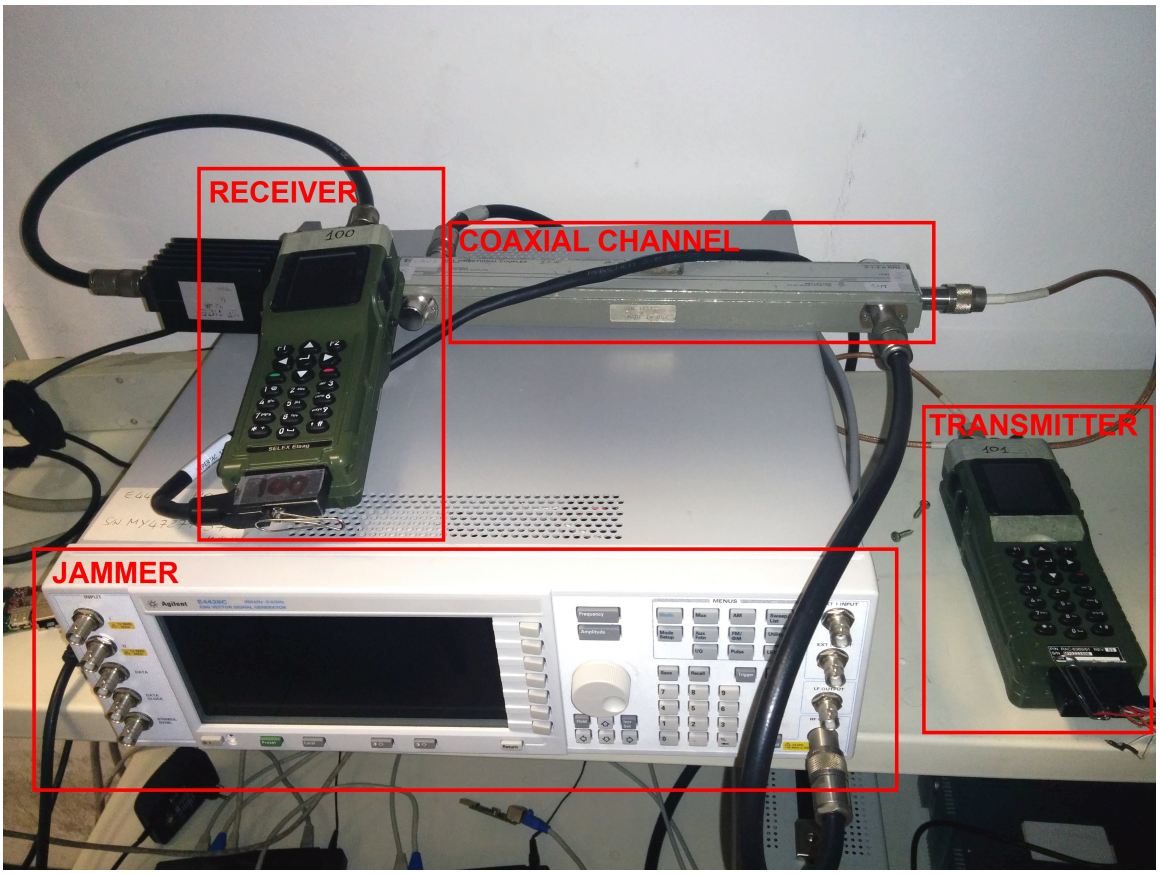


Figure 5.8: Experimental setup

For the experiments, communication is established in the UHF part of the band – namely, 225 MHz is used as the frequency of the transmitter–receiver pair. The bandwidth of the SBW waveform is set to 1.3 MHz. A vector signal generator, capable of producing both narrowband and wideband non-modulated as well as modulated waveforms, is used to create interference on the targeted channels. The experimental architecture is denoted in Figure 5.8.

First, the transmitter and the receiver establish communication on the given channel, with the transmitter placed in the *constant transmission mode*. Then, the jamming signal is placed on the targeted channel, resulting in the degradation of the quality of communication. In order to evaluate impact of the jamming signal on the targeted system, a high SNR-regime is established – namely, SNR= 29.3 dB, which makes impacts of channel noise and other sources of interference negligible. The transmission power of the targeted signal is kept equal, while the jamming power is modified in order to achieve different SJR regimes. The quality of communication is

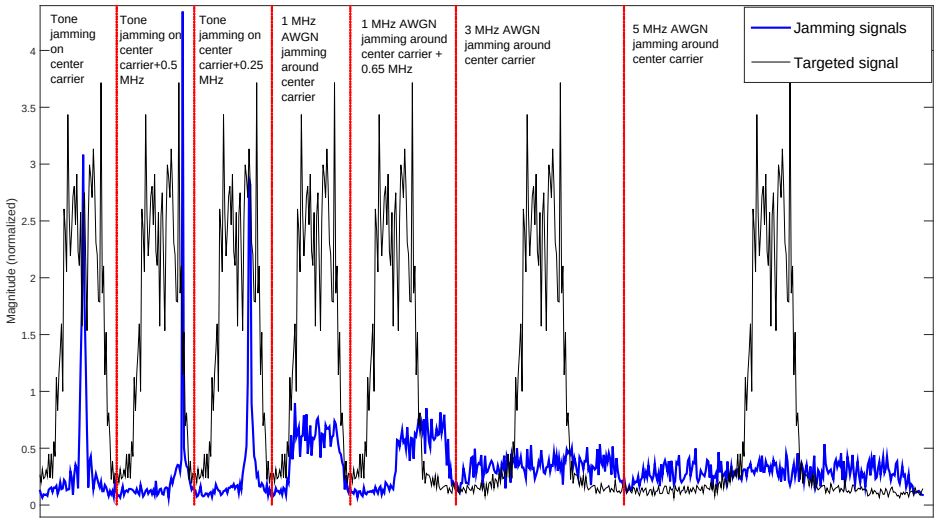


Figure 5.9: Jamming tactics in a high SJR environment

evaluated by measuring the Packet Delivery Rate (PDR), defined as:

$$PDR = \frac{N(Packets\_received)}{N(Packets\_transmitted)} \tag{5.26}$$

Figure 5.9 illustrates the considered jamming signals for high SJR ($S > J$) environment. Figure 5.10, conversely, illustrates the signals in a low SJR ($S < J$) environment.

The first set of experiments evaluates impact of single tone jamming under different SJR regimes. The jamming signals are created with three different frequency offsets with respect to the center carrier frequency of the targeted signal: 0, 0.25, and 0.5 MHz. At any instance of time, the phase of the jamming signal may take any random value over $[0, 2\pi]$. The results showing the PDR for a total of 1000 transmitted packets for each SJR-regime are presented in Figure 5.11.

The performance of the jamming tones without any offset and with the 0.25 MHz offset with respect to the center carrier frequency of the targeted signal f_C is almost identical. This is because the envelope of the SBW waveform shows that the signal energy is spread equally over the $[f_C - 0.4, f_C + 0.4]$ MHz. However, the tone placed on the $f_C + 0.5$ MHz achieves a performance approximately 4 dB worse, which stems from the fact that the frequencies corresponding to the edges of the envelope contain significantly less signal energy. Hence, for the tone jammer to be successful against wideband digital signals, it needs to be able not only to find the channel occupied

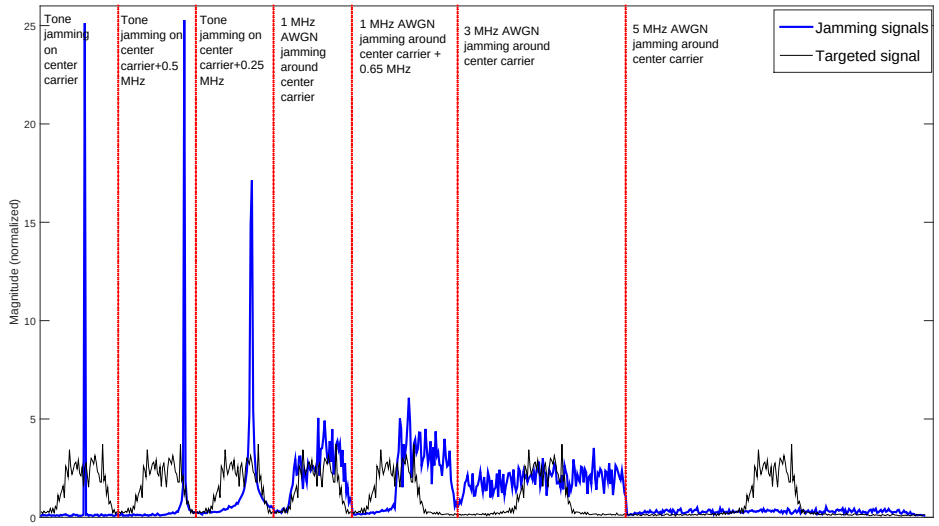


Figure 5.10: Jamming tactics in a low SJR environment

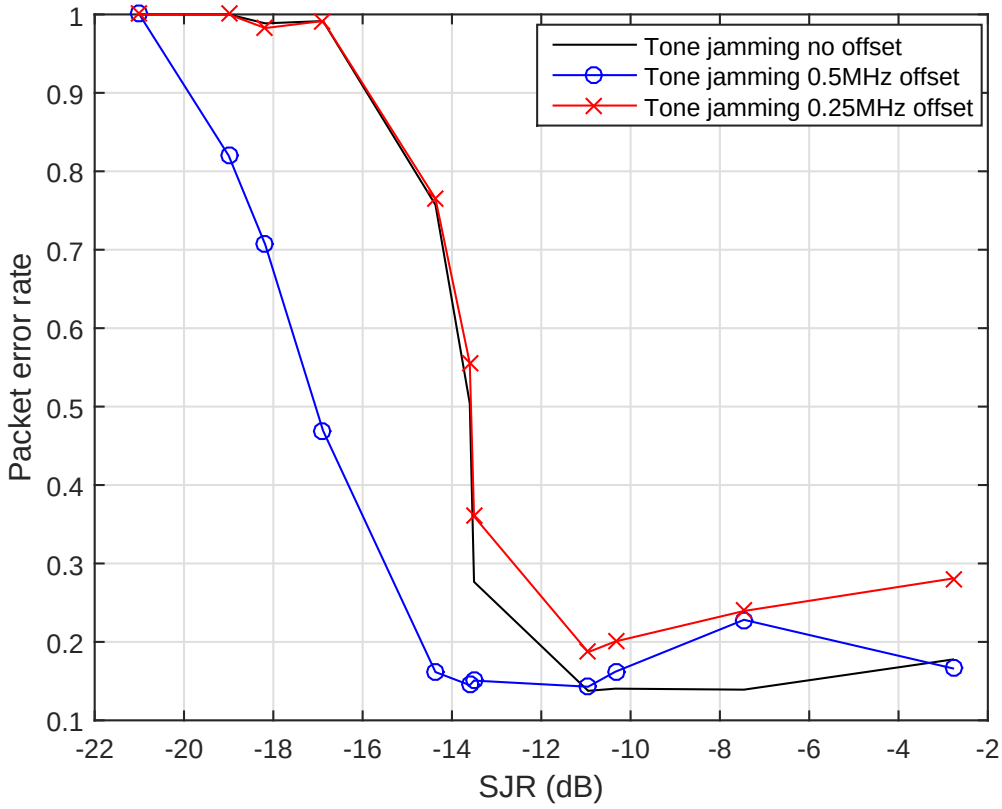


Figure 5.11: Influence of tone jamming signals with: 0 kHz, 0.25 kHz, and 0.5 kHz frequency offset

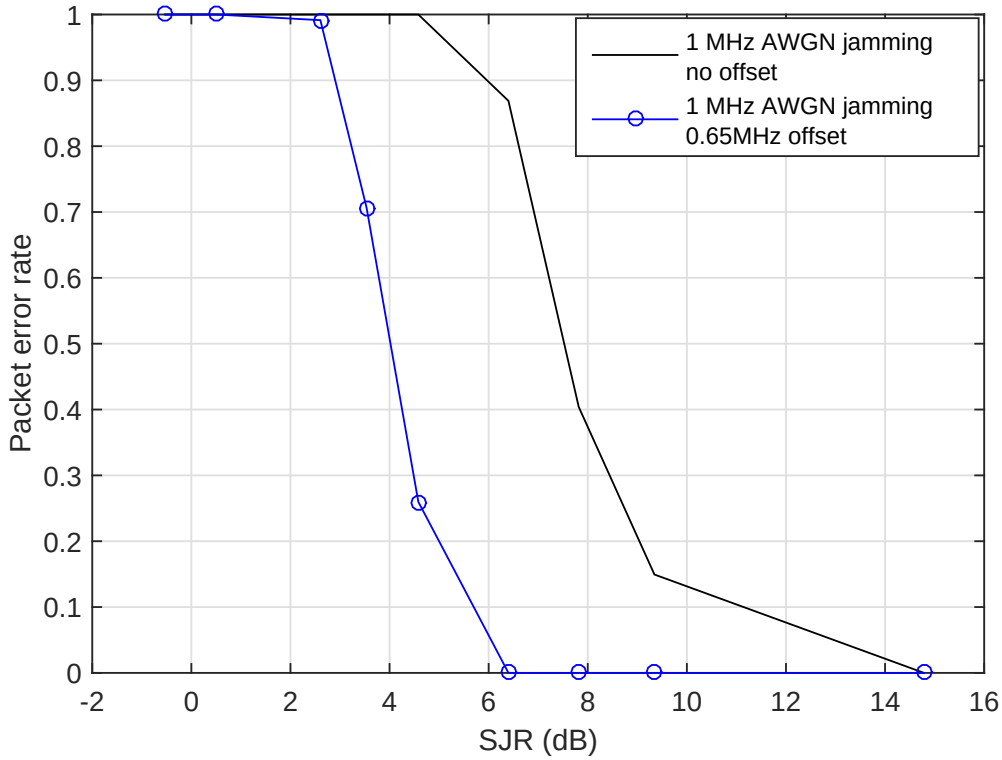


Figure 5.12: Influence of 1 MHz AWGN signal with and without frequency offset

by the targeted signal, but also to estimate the distribution of its energy over the occupied carriers.

The experiments were performed subsequently for narrowband noise jamming. Two cases are considered: i) the jammer is able to spread the noise around the center carrier frequency f_C of the targeted signal, and ii) the jammer spreads the noise around $f_C + 0.65$ MHz, i.e., it is able to target only half of the bandwidth of the SBW signal. The experiments are performed under the same conditions as for the tone jamming signals. The results are presented in Figure 5.12.

The jammer that is able to cover the full bandwidth used by the targeted signal (no frequency offset) is able to cause the same PER in approximately 4 dB higher SJR environments compared to the jammer that places the energy around the $f_C + 0.65$ frequency and effectively covers only half of the bandwidth.

Finally, we evaluate side-by-side efficiency of four different jamming tactics for the jammer with limited transmission power: i) tone jamming, ii) 1 MHz AWGN jamming, iii) 3 MHz AWGN jamming, and iv) 5 MHz AWGN jamming. The motivation for considering wideband noise jamming lies in the fact that the jammer may not be able to accurately predict the exact channel used by the targeted receiver. In that

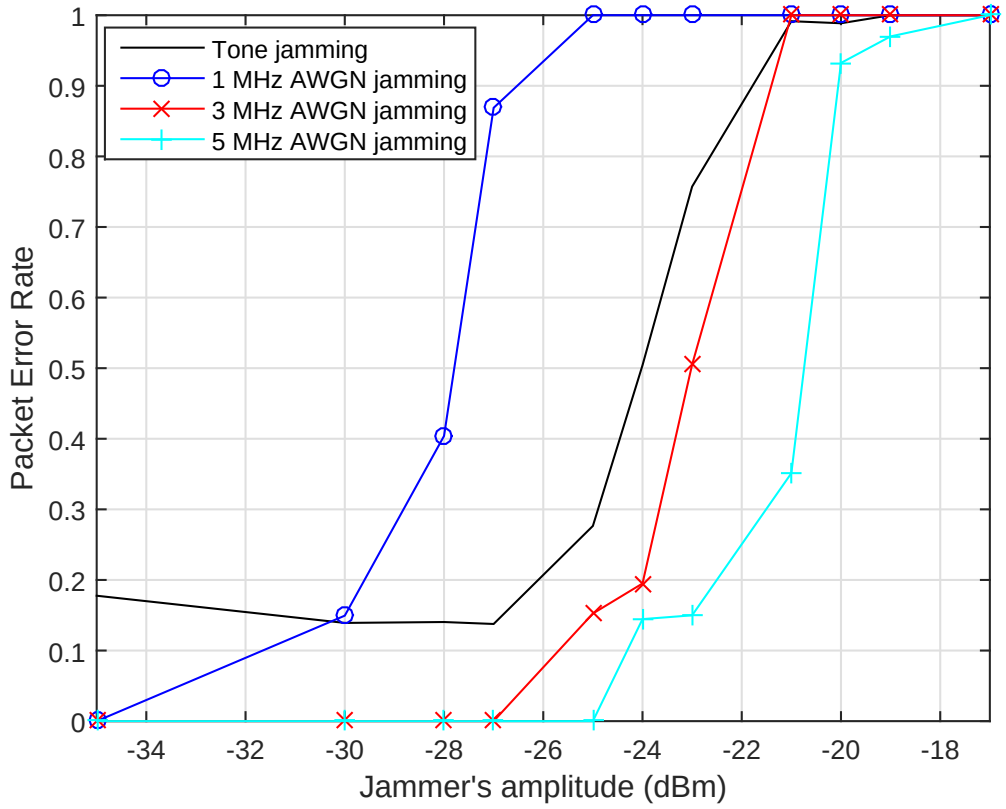


Figure 5.13: Jamming success of a jammer with fixed power in a low SJR environment

case, it could potentially increase its efficiency by spreading its energy over multiple consecutive channels.

We present the results of the analysis for the jammer that is able to accurately and consistently estimate and target the center carrier frequency of the system in Figure 5.13. Tone jamming proves somewhat successful in jamming the wideband waveform. However, in order to cause the same PER, a 1 MHz AWGN jammer would need to create a signal with approximately 4 dB lower amplitude compared to a tone jammer, 5 dB lower compared to a 3 MHz AWGN jammer, and 7 dB lower than a 5 MHz AWGN jammer. As such, narrowband noise jamming presents itself as an optimal choice for jamming wideband digital waveforms.

5.4 Conclusions

This chapter analyzed some of the most commonly deployed jamming and anti-jamming techniques using the legacy radio systems. Two basic jamming tactics,

narrowband noise jamming and tone jamming, were presented in more details. Their effects on the performance of communication systems deploying two most frequently used digital modulation techniques – BPSK and QPSK – were analyzed. Tone jamming was shown to be an efficient tactic against digital narrowband signals; however, its efficiency against PSK-modulated signals depends on its phase offset with respect to the targeted signal. The chapter has also described principles of the state-of-the-art anti-jamming solutions, namely emissions control and spread spectrum systems. In addition, the chapter provided experimental results showing the effects of different jamming signals on the Soldier Broadband Waveform – a digital QPSK-modulated wideband waveform used by the SWAVE HandHeld SDRs that were presented in Chapter 4. Narrowband noise jamming was shown to be the most efficient among the jamming tactics, provided that the jammer is able to correctly estimate the exact frequency used by the targeted transmitter–receiver pair.

Bibliography

[1] J.D. Andersen. A turbo tutorial. URL `http://www.coe.montana.edu/ee/rwolff/ee548/ee548-s06/turbocodes/turbotutorial.pdf`. [Accessed: 2015-02-06].

[2] R. Kohno, R. Meidan, and L.B. Milstein. Spread spectrum access methods for wireless communications. *Communications Magazine, IEEE*, 33(1):58–67, January 1995. doi: 10.1109/35.339882.

[3] B. Nguyen and R. Rom. Communication services under EMCON. *SIGCOMM Computer Communication Review*, 16(3):275–281, August 1986. doi: 10.1145/1013812.18203.

[4] R. Poisel. *Introduction to Communication Electronic Warfare Systems*. Artech House, Inc., Norwood, MA, USA, 2nd edition, 2008.

[5] R. Poisel. *Modern Communications Jamming: Principles and Techniques*. Artech House intelligence and information operations series. Artech House, 2011.

[6] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt. *Spread spectrum communications handbook*, volume 2. McGraw-Hill New York, 1994.

[7] I.R. Smith. Multiple binary independent mark-space as an improved form of M-ary FSK signaling. In *Military Communications Conference, 1985. MILCOM*

1985. IEEE, volume 2, pages 423–427, October 1985. doi: 10.1109/MILCOM.1985.4795062.

[8] K.C. Teh, A.C. Kot, and K.H. Li. Performance analysis of an FFH/BFSK product-combining receiver under multitone jamming. *Vehicular Technology, IEEE Transactions on*, 48(6):1946–1953, November 1999. doi: 10.1109/25.806787.

[9] Don J. Torrieri. *Principles of Secure Communication Systems*. Artech House, Inc., Norwood, MA, USA, 2nd edition, 1992.

[10] R. Viswanathan and K. Taghizadeh. Diversity combining in FH/BFSK systems to combat partial band jamming. *Communications, IEEE Transactions on*, 36 (9):1062–1069, September 1988. doi: 10.1109/26.7518.

Chapter 6

RF jamming and anti-jamming using Cognitive Radios

As opposed to the legacy radio systems, whose functionalities are for the most part restricted by the deployed hardware components, *Software Defined Radios (SDRs)* provide reconfigurability of most of their parameters through software changes run on the programmable processors: Field Programmable Gate Arrays (FPGAs) or Digital Signal Processors (DSPs). *Cognitive Radios* take the technological advances a step further by embodying the SDRs with the self-reconfigurability and learning prospectives.

This chapter focuses on some of the impacts that the SDR/Cognitive Radio technology brings to the *Communications Electronic Warfare (CEW)* domain. CEW systems [13] focus on intercepting or denying the communication on the targeted systems (*electronic attack*) [5], or taking actions aimed at preventing electronic attacks from successfully occurring (*electronic defense*). On-the-fly reconfiguration capabilities coupled with learning and self-adaptive potentials of Cognitive Radio technology may aid both the attacking and the defending side in multiple ways [3]. Deploying energy detection spectrum sensing may embody the attacker with the ability to monitor the target transmitter's transmission frequency, estimate the target receiver's signal strength and calculate the signal strength necessary to efficiently jam the communication. Performing feature detection spectrum sensing may allow the attacker to infer even more of the parameters of the target transmitter, such as deployed modulation type or coding mechanism. Subsequently, it may use these inferences to deploy jamming tactics with higher probability of success, e.g., by taking advantage of the fact that different modulation techniques are characterized by different levels of resilience to interference. Finally, the attacker may use learning techniques to observe and learn the transmitter's patterns, such as the deployed frequency hopping or power

allocation schemes. Analogously, similar benefits may be provided to the defending side.

The focus of the chapter is placed on the electronic defense part of the advanced CEW. We presents ideas, development and implementation aspects of the *Spectrum Intelligence algorithm for Radio Frequency (RF) Interference Mitigation*. The concept is built on the enabling technologies of spectrum sensing, waveform analysis, Temporal Frequency Maps[1], and self-reconfigurability potentials of the SDR/Cognitive Radio technology. Along the way, we acknowledge and address some of the challenges faced when porting the algorithms to the real-life SDR/Cognitive Radio platform, described in Chapter 4, and propose practical solutions for the identified problems.

6.1 Spectrum Intelligence for interference mitigation

The principal idea behind the Spectrum Intelligence algorithm [4] 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 reliable spectrum sensing mechanism, correct identification and extraction of the relevant parameters, and secure software unsubjected to tampering. The functional process of the Spectrum Intelligence algorithm can be represented in the form of the *Cognitive Cycle*, as shown in Figure 6.1.

6.1.1 Stages of the Cognitive Cycle

6.1.1.1 Sense

Sensing, i.e., 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.

6.1.1.2 Process

Then, *data processing* takes place. Parsed data is time aligned if needed, and transformed into frequency domain by performing the Fast Fourier Transform (FFT). Thresholding is then performed with the aim of discarding background noise, and

[1]We are intentionally creating a distinction between the Temporal Frequency Maps, and the similar but more advanced concept of Radio Environment Maps [16].

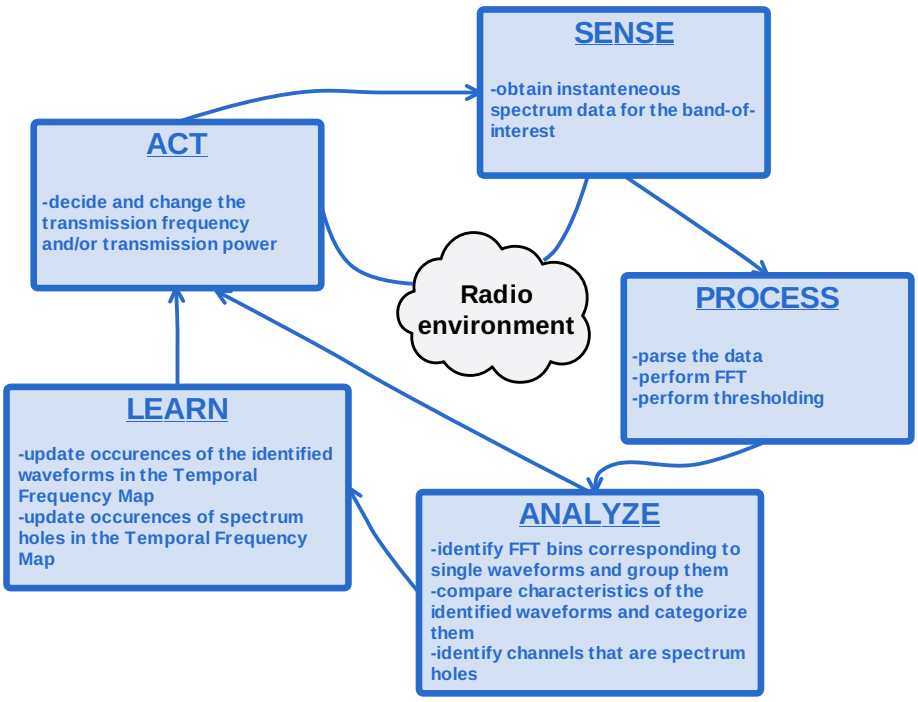


Figure 6.1: Cognitive cycle representing the Spectrum Intelligence algorithm

keeping only the FFT bins corresponding to actual signals. This corresponds to solving the decision problem between the following two hypotheses [6]:

$$Y(n) = \begin{cases} W(n) & H_0 \\ X(n) + W(n) & H_1 \end{cases} \tag{6.1}$$

where $Y(n)$, $X(n)$ and $W(n)$ are the received signals, transmitted signals and noise samples, respectively, H_0 is the hypothesis corresponding to the absence of the signal, and H_1 is the hypothesis corresponding to the presence of the signal.

Finding the appropriate threshold is the principal challenge of any energy detection scheme. The most common approaches 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, it should be noted that even in adaptive thresholding, presence of interference may confuse the energy detector [1].

In CEW domain, it is reasonable to assume a relatively low spectrum utilization – namely, there will typically be only a limited number of actual narrowband signals (either "friendly" or "potentially malicious") in the received wideband signal at any time instance. For this purpose, it is sufficient to implement a suboptimal thresholding

algorithm, where CFAR or CDR performance is not necessarily achieved. Practical experience has shown that threshold $\hat{\lambda}$ may be adaptively set based only on the mean value of the magnitudes of the scanned wideband signal, as:

$$\hat{\lambda} = 2 \cdot \frac{1}{n} \sum |Y(n)| \tag{6.2}$$

This step concludes the energy detection.

6.1.1.3 Analyze

Let us assume that as a result of the thresholding process, N frequency bins are identified. For a system where M actual signals ($N > M$) are present, $N - M$ frequency bins would incorrectly be classified as signals. Then, simple thresholding would result in the false alarm rate of $\frac{N-M}{N}$.

For this reason, frequency bins corresponding to the same signal need to be grouped together. For the ideal case (generic signals in high-SNR environments), the simplest approach consists of grouping consecutive samples together and classifying them as single waveforms. However, in most 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. For this purpose, the maximum acceptable distance (in Hz) between the two samples belonging to the same waveform is defined, and it is a function of the frequency resolution of the FFT as given by:

$$d_{MAX} = K \cdot d_f. \tag{6.3}$$

Here, K is the estimate of a number of consecutive samples that could be erroneously disregarded, and d_f is the frequency resolution of the FFT, defined as:

$$d_f = \frac{2 \cdot f_{max}}{N_S}, \tag{6.4}$$

where f_{max} is the maximum resolvable frequency (which in case of Nyquist sampling equals to half of the sampling frequency), and N_S is the number of samples acquired during the sampling process.

Then, grouped waveforms undergo smoothing, in order to alleviate impacts of the imperfect and erroneous sampling. For achieving this, a moving average filter has been implemented. For a waveform that consists of n_M grouped bins with magnitudes

$X_1, ..., X_{n_M}$, filtering with the window length K results in:

$$X_{filtered}(n_i) = \frac{1}{K} \sum_{j=i-K}^{i} X_j. \tag{6.5}$$

So, each element is an average of its preceding K points.

Figure 6.2 illustrates the difference between the original transmitted signal (a), sensed FFT bins (b), estimated signal after performing thresholding/bin grouping (c), and the same signal after the smoothing (d).

Next, the *waveform analysis* is performed, i.e., for each of the identified narrowband waveforms, relevant parameters are extracted. These parameters include waveforms' respective center frequencies, bandwidths, maximum values of their magnitudes, and variance of their magnitudes. It is assumed that the algorithm has an access to a database containing parameters of the "friendly" and/or "potentially malicious" waveforms in the system.

Spectrum intelligence relies on the Naive Bayes classification to distinguish between the types of waveforms currently occupying the spectrum. The Naive Bayes classification is a relatively simple, yet powerful classification method, based on Bayes rule. Bayes rule is given as:

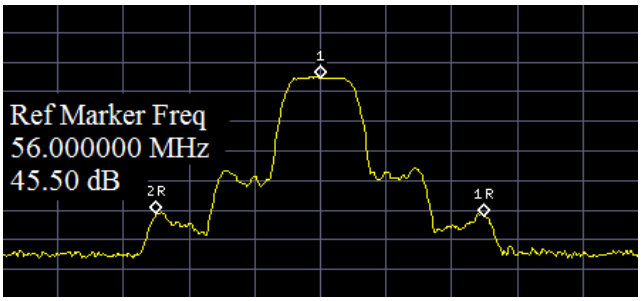
$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B|A)\Pr(A) + \Pr(B|\neg A)\Pr(\neg A)}, \tag{6.6}$$

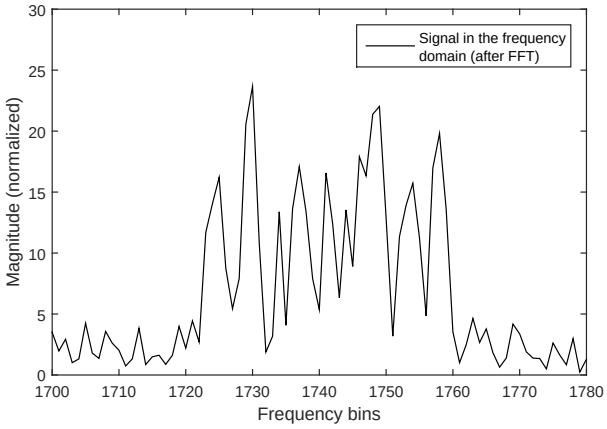
where $\Pr(A)$ is the prior probability, i.e., initial degree of belief in event A, $\Pr(\neg A)$ is the corresponding probability of the initial degree of belief against A, $\Pr(B|A)$ is the conditional probability of event B given that A is true, $\Pr(B|\neg A)$ is the conditional probability of event B given that A is not true, and $\Pr(A|B)$ is the posterior probability of A.

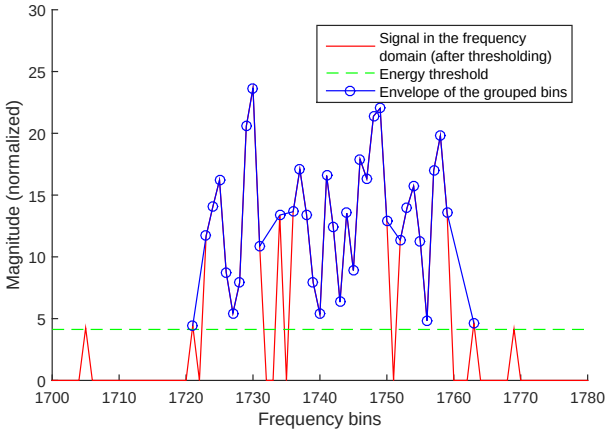
The Naive Bayes algorithm assumes that attributes are all conditionally independent of one another, however it typically performs well even when the independence assumption is not valid. The algorithm operates in two steps: training step, in which the training data is used to estimate the parameters of a probability distribution, and the prediction step, where posterior probability for every sample to belong to a certain class is calculated. The class with the highest probability is assigned to the tested sample.

A posterior probability that k is a result of the classification for an observation $(b_1, ..., b_p)$ is given as:

$$\Pr(A = k|b_1, ..., b_p) = \frac{\Pr(B_1, ...B_p|a = k)\pi(A = k)}{\Pr(B_1, ...B_p)}, \tag{6.7}$$







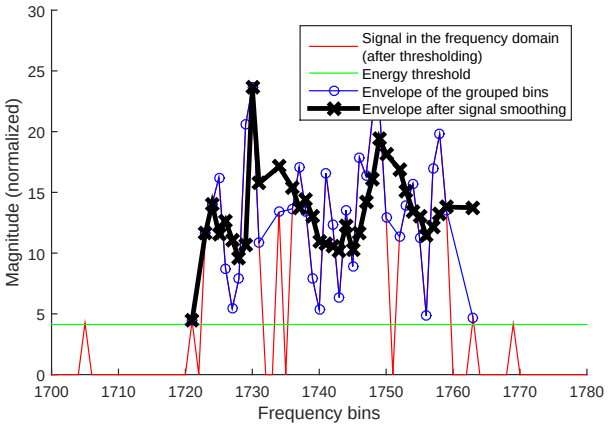


Figure 6.2: Signal: (a) transmitted – maximum hold, (b) sensed, (c) after thresholding and bin grouping, (d) after smoothing

where $\Pr(A = k|b_1, ..., b_p)$ is the conditional joint density of the predictors given that they are in class k, $\pi(A = k)$ is the class prior probability distribution, and $\Pr(B_1, ...B_p)$ is the joint density of the predictors.

Currently, the classification within the Spectrum Intelligence is binomial, however it may straightforwardly be extended to support multinomial classification (e.g., in order to account for different types of "friendly" waveforms). Result of the classification is a set of "potentially malicious" and/or "friendly" waveforms in each cycle of the algorithm. The reliable classification is of paramount importance to the successful functioning of the overall algorithm. However, the classification results are largely dependent on the features that the classifier is deploying. We consider a total of three features that may be extracted for each of the identified waveforms: their bandwidth, magnitude variance, and maximum value of the magnitude. In most communication systems, the latter will typically be available only in several special scenarios, such as when the cognitive receiver is able to correctly estimate the power of the friendly/potentially malicious transmitter by obtaining information of its real location and when there is no mobility nor significant changes in the direction of the radiation patterns of the antennas.

The implemented waveform analysis technique is lightweight, and performs well for systems with relatively low frequency resolution. Alternative, computationally more expensive waveform analysis techniques, include cross-correlation in time domain; more comprehensive Statistical Signal Characterization (SSC) methods [10]; and cyclostationary detectors [14]. These are not analyzed within this work, however they all impose themselves as viable future research topics.

Besides waveform identification and classification, the algorithm also recognizes instantaneous spectrum holes. We define a *spectrum hole* as the channel where the magnitudes of all of the corresponding FFT bins are below the energy threshold.

6.1.1.4 Learn

The algorithm then accesses the Temporal Frequency Map, where previous occurrences of spectrum activities are stored. The Temporal Frequency Map 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, as illustrated in Table 6.1.

In each cycle, previous values are updated with the newly acquired and processed information. This corresponds to the *learning* phase of the Cognitive cycle. Temporal

Table 6.1: Temporal Frequency Map

Spectrum activity/CHANNEL	1	2	...	n
Friendly	$m_{F/1}$	$m_{F/2}$		$m_{F/n}$
Potentially malicious	$m_{PM/1}$	$m_{PM/2}$		$m_{PM/n}$
Spectrum hole	$m_{SH/1}$	$m_{SH/2}$		$m_{SH/n}$

forgiveness is implemented within the algorithm, i.e., spectrum activities corresponding only to the last l 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.

6.1.1.5 Act

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

$$c_{t+1} \in (c_t = SH \mid (X(c_t) = min). \tag{6.8}$$

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:

$$X(c_t) = l^2 \cdot m_{PM/c_t} + (l+1) \cdot m_{F/c_t} - m_{SH/c_t}, \tag{6.9}$$

where m_{PM/c_t}, m_{F/c_t} and m_{SH/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.

The new transmission power is chosen according to:

$$P_{t+1} \in P \mid P_R > 10log_{10}\hat{\lambda} + 3dB. \tag{6.10}$$

Algorithm 1 provides the pseudocode of the Spectrum Intelligence algorithm.

Algorithm 1 Spectrum Intelligence – pseudocode

function SPECTRUM INTELLIGENCE
    Train the classifier with relevant parameters for "friendly" and "potentially malicious" waveforms
    Initialize all channel states to "free"
    Set the number of bursts to be acquired $\rightarrow k$
    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 $\rightarrow \frac{N_S}{2}\, frequency\, bins\, with\, magnitudes\, M$
    Calculate mean value of $M \rightarrow M_{mean}$
    Based on M_{mean}, set the energy threshold $\rightarrow \hat{\lambda}$
    for $i = 1\, to\, \frac{n_S}{2}$ **do** (for each frequency bin)
        if $M(i) > \hat{\lambda}$ **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
    Extract features of identified waveforms $\rightarrow$ *bandwidth*, *center frequency*, *maximum* M, *mean*
    Perform classification $\rightarrow$ *waveform is either* "*friendly*" *or* "*potentially malicious*"
    Update Radio Frequency Map
    If "potentially malicious" waveforms are near the current operating channel, choose new TX frequency/power
end function

6.1.2 Implementation on the Cognitive Radio test bed

The proposed algorithm is implemented on the SDR/Cognitive Radio test bed architecture described in Chapter 4.

The spectrum acquisition process is detailed as follows: HandHeld's (HH's) 14-bit Analog-to-Digital-Converter (ADC) performs sampling at 250 Msamples/s. When-

ever a `GET_SpectrumSnapshot` command is invoked, a burst of 8192 consecutive samples is buffered, and then outputted over the serial port at 115200 bauds to the System-on-Module (SoM), which is executing the Spectrum Intelligence algorithm. There, the samples, corresponding to 120 MHz around the center carrier frequency of the radio, are parsed, transformed into the frequency domain using the Fast Fourier Transform (FFT), and subsequently analyzed by the implemented energy detector. Alternatively, in order to increase the accuracy, several consecutive spectrum bursts can be FFT-ed, averaged and analyzed together. The spectrum sensing and the Spectrum Intelligence as a whole is a quiet process, i.e., the HH is able to transmit/receive data at all times. Controlled environment achieved by the coaxial implementation allows us to assume high coherence time of the analyzed frequency band, i.e., while performing the averaging of consecutive spectrum readouts, temporal variability of the channel may be disregarded. We acknowledge, however, that in case of the over-the-air transmission, nature of the wireless medium would not allow us to make such assumption. In order to obtain higher FFT frequency resolutions, necessary modifications to the equipment would include increasing the buffer size on the HH, and finding ways to transfer spectrum data at higher baud rate than is currently supported. Alternatively, appropriate techniques that estimate the temporal variability of the channel would need to be deployed.

The FFT-ed data is then further analyzed by the Spectrum Intelligence algorithm, as explained in Sections 6.1.1.2 – 6.1.1.5. The output of the algorithm is the transmission frequency and the transmission power to be deployed in the next cycle. These values are executed at the end of the Spectrum Intelligence cycle by issuing an appropriate SET command.

As explained in Section 4.2.1, HH provides support for reconfigurability of its transceiving parameters by means of the Simple Network Manager Protocol (SNMP) v3. The implementation is done in the following way: whenever the Spectrum Intelligence algorithm decides on a new transmission frequency/power, the algorithm running on the SoM invokes the appropriate SNMP command. Each SNMP command (`SET_RFchannel` or `SET_TXpower`) is characterized by the corresponding unique Object IDentifier (OID) and the new value of the parameter. OIDs and the respective values that each object can take are stored in the Management Information Base (MIB) on the HH. Once that the HH receives the SET request, it accesses the MIB, checks whether the requested value of the object is defined in MIB and, if so, changes the corresponding parameter. This finishes one cycle of the Spectrum Intelligence algorithm. Change of the transmission parameters occurs in every cycle in which the

Spectrum Intelligence has detected a "potentially malicious" waveform on a channel proximate to the one that HH currently uses for transmission.

The SNMP commands needed for successful execution of the Spectrum Intelligence algorithm are summarized in Figure 6.3.

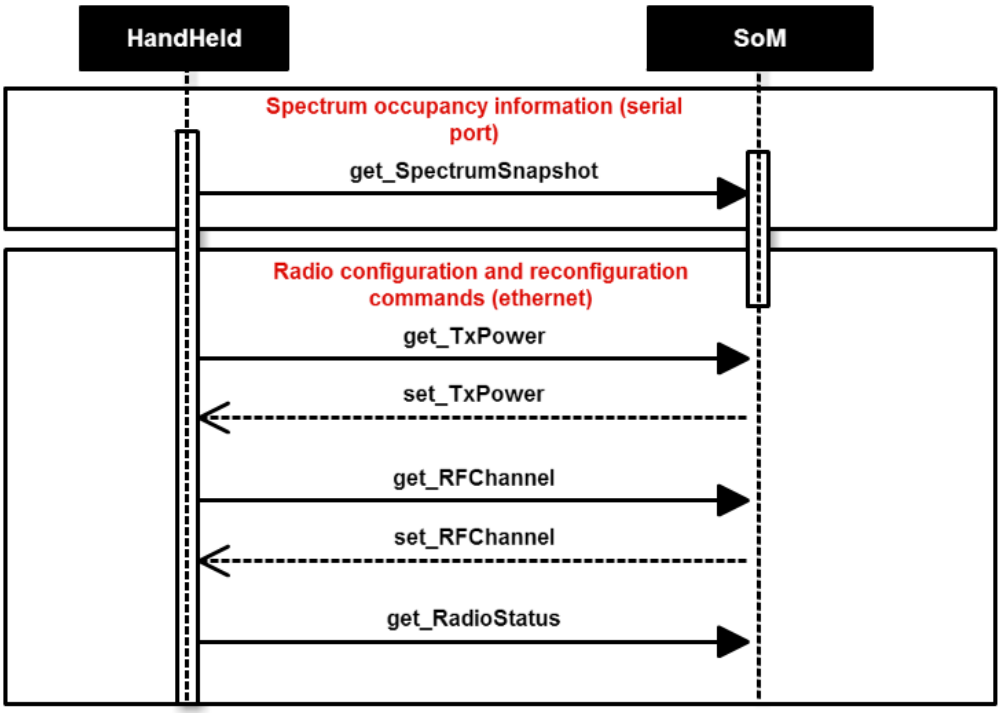


Figure 6.3: Relevant SNMP commands HandHeld–SoM for Spectrum Intelligence algorithm

6.2 Experimental results and major findings

Performance of the overall Spectrum Intelligence algorithm depends mainly on the accuracy of the energy detection and waveform classification phases. In order to evaluate the performance of these functionalities, a set of experiments is performed using the test bed architecture.

SelfNET Soldier Broadband Waveform (SBW), representing the "potentially malicious" waveform, is continuously transmitted on the fixed carrier frequency. SBW is a wideband digital waveform whose bandwidth was set to 1.25 MHz bandwidth, operable in VHF [30–88] MHz and UHF [256–512] MHz parts of the frequency band. When operating in VHF, a direct conversion principle is utilized, and the scanned frequency band always corresponds to the baseband, i.e., [0–120] MHz. When operating in UHF, superheterodyne principle is used, and the frequency band that is scanned

depends on the center carrier frequency f_c that the HH is operating on – namely, analyzed band corresponds to $[f_c - 35, f_c + 85]$ MHz. Vector signal generator is used to create and inject the "friendly" waveforms into the channel, emulating friendly communication. In addition, for the ease of analysis, all other sensed signals that do not correspond to the "potentially malicious" waveform are considered as "friendly". Hence, the task of the classifier is to successfully discriminate between the "potentially malicious" and "friendly" waveforms, based on the extracted features.

For the experiments, we utilize the VHF part of the transmission band where the radios are operable, meaning that the spectrum sensing is performed for the frequency band [0–120] MHz. SBW signal representing the "potentially malicious" waveform is transmitted at the center carrier frequency 51 MHz, for two varying transmission powers. The transmission power -7 dBm (100 spectrum bursts) represents the situation where the received power of the "potentially malicious" waveform is similar to the power of the "friendly" waveforms in the system. The transmission power -3 dBm (100 spectrum bursts) represents the case where the "potentially malicious" waveform has significantly higher power than the rest of the waveforms in the system. The goal is to quantify the potential discriminative quality of the expected received magnitude as a classification feature.

For each of the cases, the Naive Bayes classifier is trained with half of the overall data set (50 bursts for each transmission power), and the other half (50 bursts for each transmission power) is used for the testing. The idea is to observe how different combinations of the available features influence the performance of the classifier.

The first set of experiments corresponds to the transmission power of -7 dBm. Figures 6.4 and 6.5 shows scatter plots for all the combinations of the considered features.

The blue dots represent the samples of the "friendly" waveforms, and the red circles are the samples of the "potentially malicious" waveforms used for the training phase of the classifier. The green crosses represent all waveforms classified as "potentially malicious" in the testing phase, whereas the green squares correspond to the actual "potentially malicious" waveforms in the testing phase.

A more comprehensive insight into the results of the classification performance is given by the confusion matrices shown in Table 6.2.

Ideally, waveform analysis should classify only the SBW waveform as the "potentially malicious" waveform in every analysis cycle (true positives). However, as seen from the matrices, the analysis procedure will occasionally erroneously classify

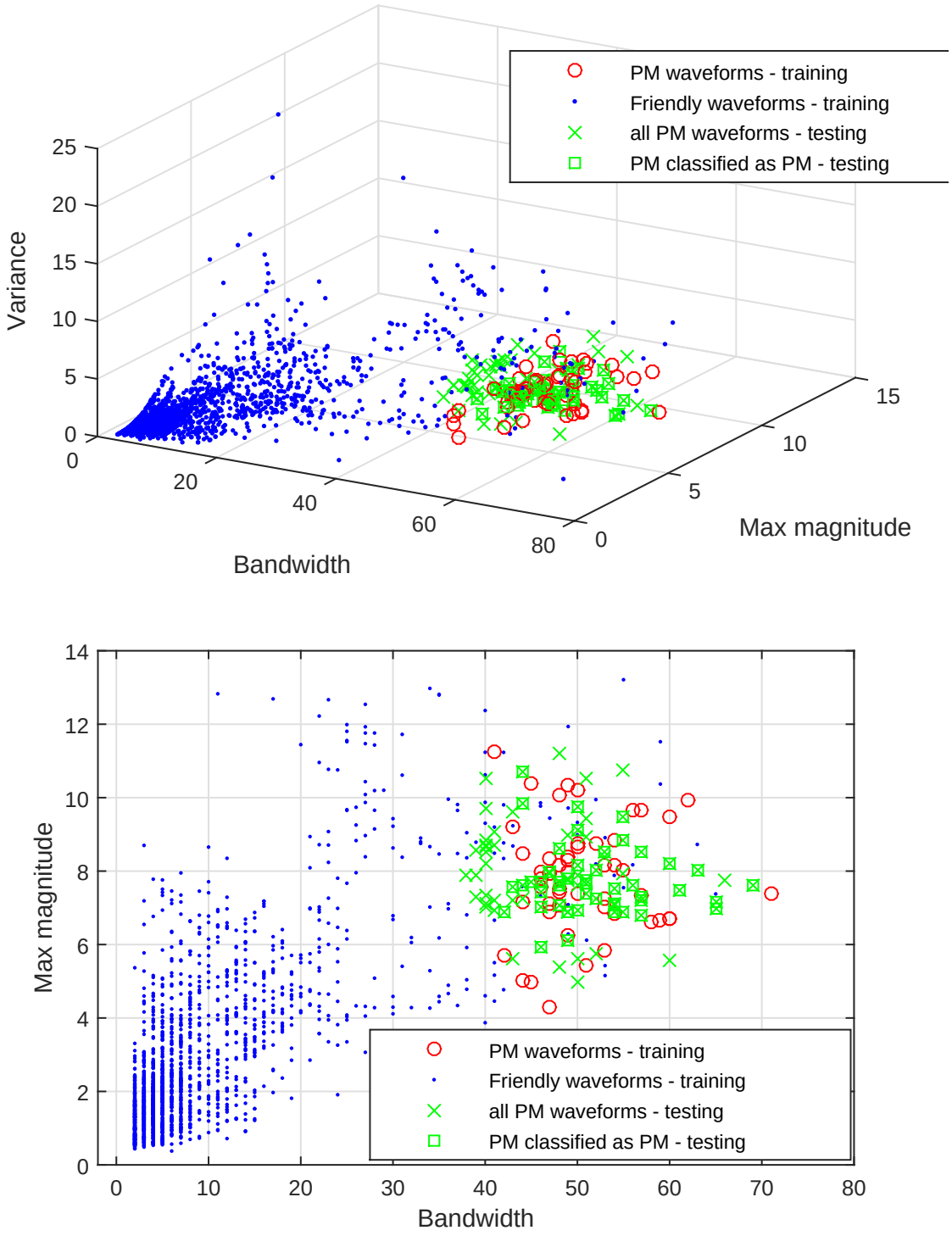


Figure 6.4: Scatter plots for −7 dBm transmission power: (a) Bandwidth + variance + magnitude, (b)Bandwidth + magnitude

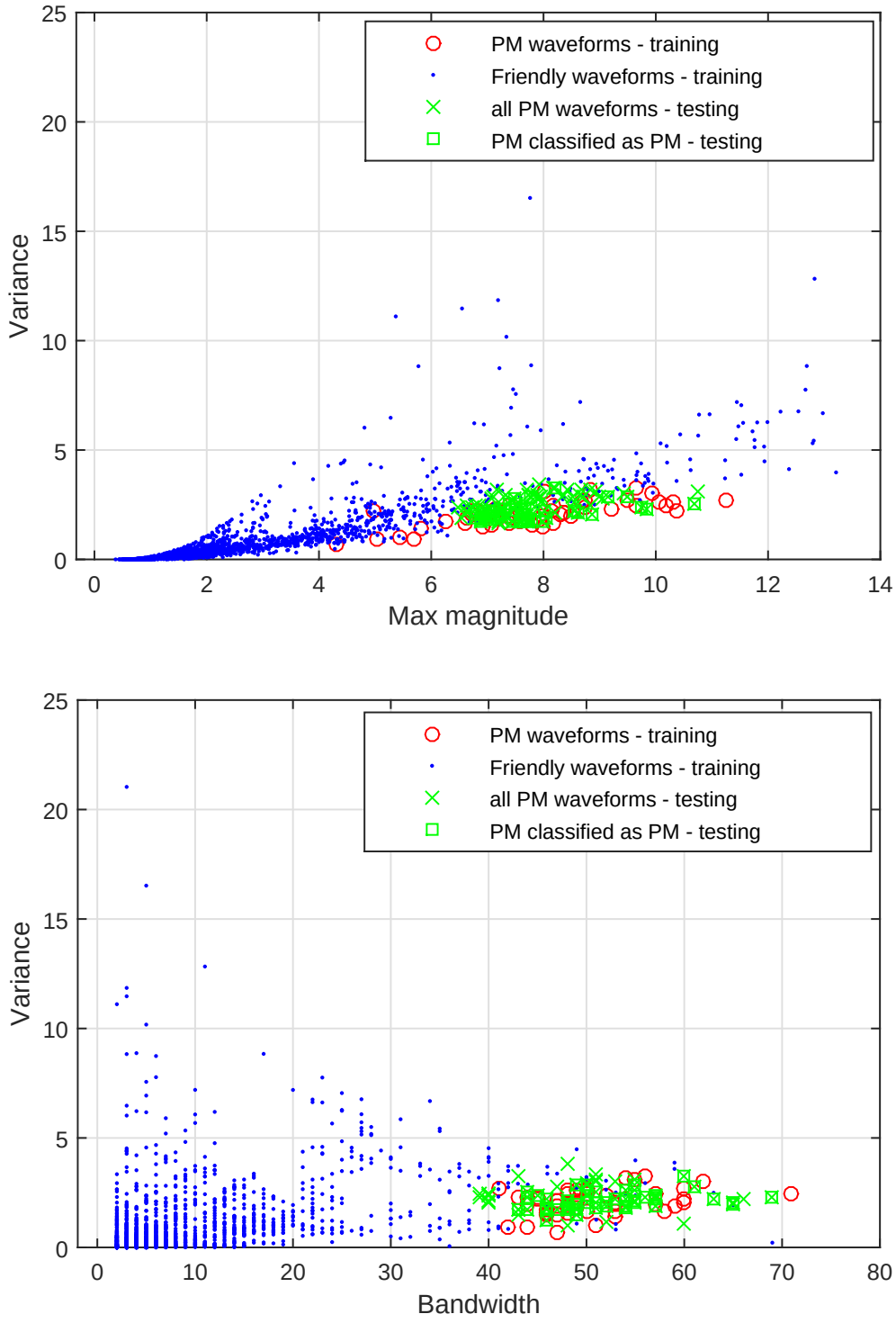


Figure 6.5: Scatter plots for −7 dBm transmission power: (a)Magnitude + variance, (b)Bandwidth + variance

Table 6.2: Confusion matrices for −7 dBm transmission power

	Pot. malicious	Friendly	
Pot. malicious	**46**	4	**Bandwidth + amplitude + variance**
Friendly	44	**1887**	
Pot. malicious	**47**	3	**Bandwidth + amplitude**
Friendly	40	**1897**	
Pot. malicious	**42**	8	**Amplitude + variance**
Friendly	55	**1876**	
Pot. malicious	**45**	5	**Bandwidth + variance**
Friendly	27	**1904**	

"friendly" waveforms as "potentially malicious", and vice versa. These classification results are directly dependent on the following factors:

- Energy detection threshold, $\hat{\lambda}$ – inappropriately low threshold may result in grouping too many of the adjacent bins (some of which actually correspond to noise) as single waveforms, consequently increasing the estimated bandwidths of these waveforms;
- Estimated number of consecutive samples that could be erroneously disregarded, K – overly low K may result in single waveforms being erroneously recognized as different waveforms on adjacent frequencies; overly high K may result in waveforms on adjacent frequencies being erroneously grouped as single waveforms;
- Similarity in the parameters between different waveforms present in the communication system that are subjected to classification;
- Discriminative values of the features used for classification;
- Number of training samples.

The first two points are defined according to Equations (6.2) and (6.3) respectively, with $K = 3$ heuristically shown to give the most satisfying performance. The number of training samples is fixed and is comprised of all the waveforms present in 50 spectrum bursts. In each training burst, there is one "potentially malicious" waveform injected on a known channel, and a varying number of other waveforms on other channels. Hence, it is interesting to focus the analysis on the discriminative

values of the used features. The best results are offered by the combination of the bandwidth and the amplitude of the signals. This is closely followed by analyzing all 3 features together. However, in many real-life systems, it is not reasonable to expect that the classifier has the information corresponding to the waveforms' received magnitudes, since this information will typically not be known a-priori and may be highly time-variant. For this reason, a good performance exhibited by the classifier that discriminates between the waveforms based on the bandwidth and the variance of the signal is of particular importance.

The experiments are then repeated for the case when the transmission power of the "potentially malicious" waveform equals to −3 dBm. Figures 6.6 and 6.7 and Table 6.3 show the results.

Table 6.3: Confusion matrices for −3 dBm transmission power

	Pot. malicious	**Friendly**	
Pot. malicious	**50**	0	**Bandwidth + amplitude + variance**
Friendly	17	**1862**	
Pot. malicious	**50**	0	**Bandwidth + amplitude**
Friendly	4	**1875**	
Pot. malicious	**48**	2	**Amplitude + variance**
Friendly	28	**1851**	
Pot. malicious	**50**	0	**Bandwidth + variance**
Friendly	17	**1862**	

The best performance both in the terms of the true positives rate and the false negatives rate for both classes is achieved by the classifier utilizing the combination of signal's bandwidth and amplitude as the classification features. As expected, in environments where one of the waveforms has a significantly higher received power, using the power/amplitude of the received signal is a particularly good classification feature.

Finally, we measure the execution time of the Spectrum Intelligence algorithm for a single cognitive cycle. The results are shown in Figure 6.8.

The full blue line shows the computational time of the Process–Compress–Analyze–Learn–Decide phase of the Spectrum Intelligence, corresponding to all the processes that are running on the SoM. Computational times of the whole cognitive cycle, including the sensing time and the time needed to deploy the appropriate SNMP command on the radio are represented by the dashed red line. Sensing time takes

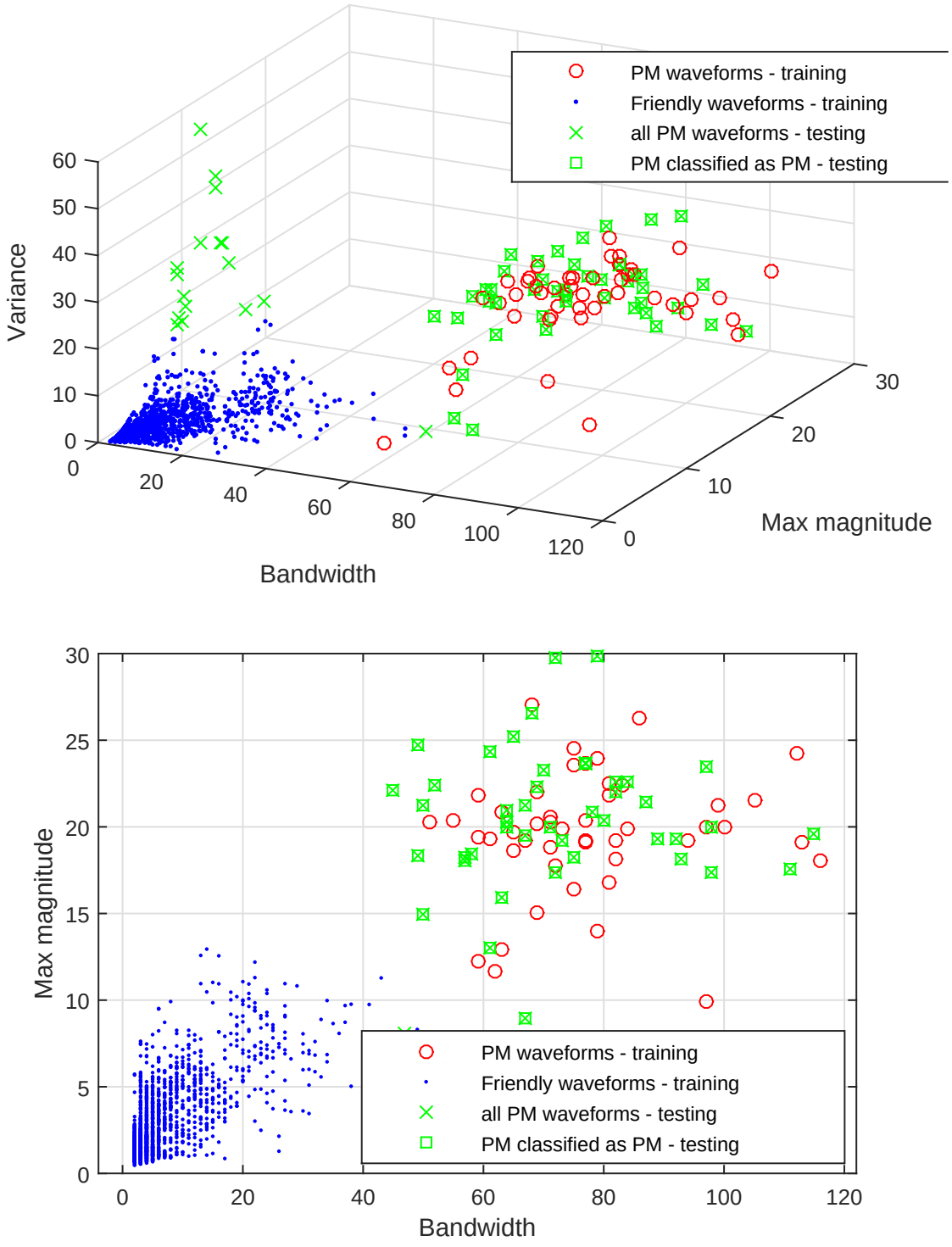


Figure 6.6: Scatter plots for −3 dBm transmission power: (a) Bandwidth + variance + magnitude, (b)Bandwidth + magnitude

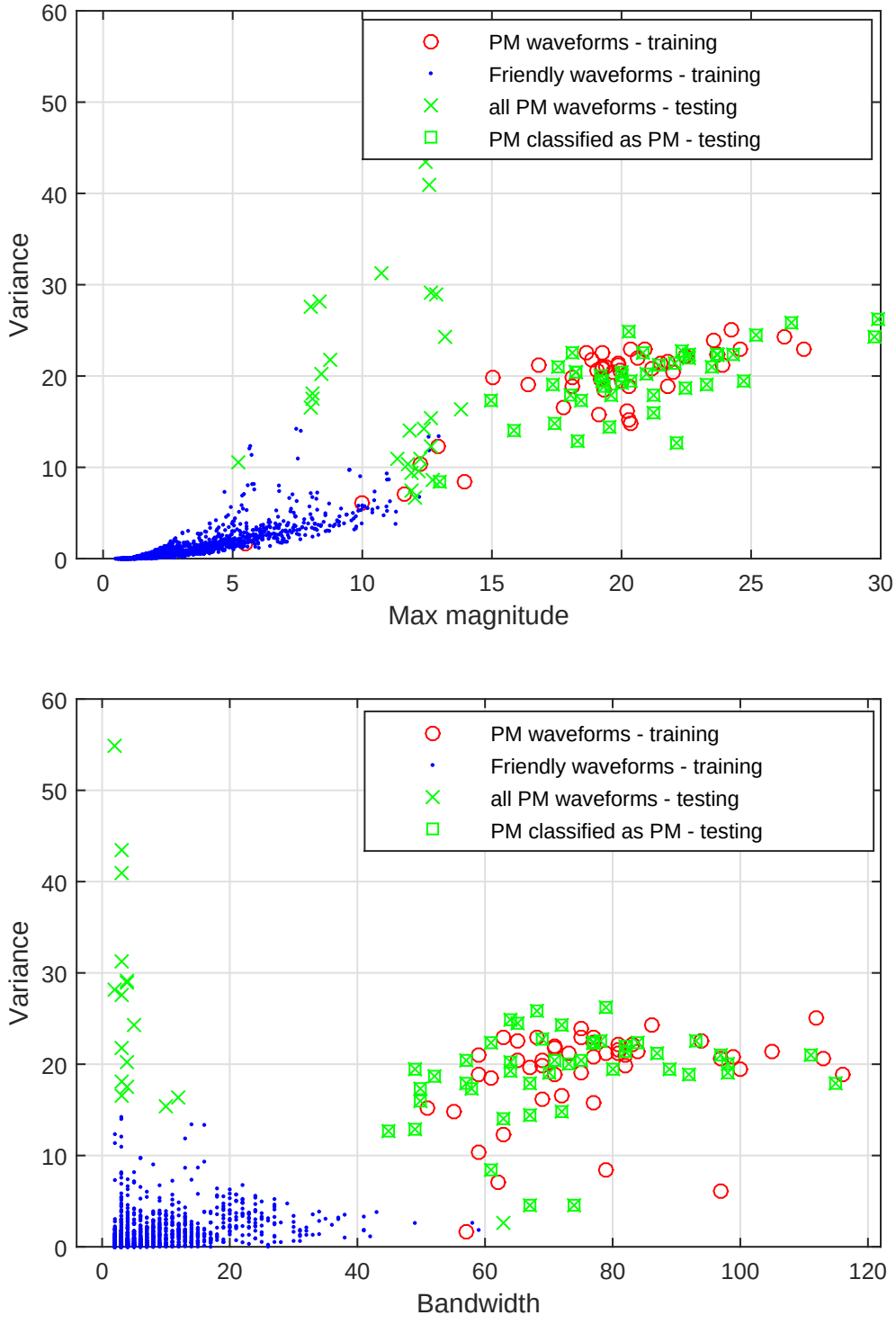
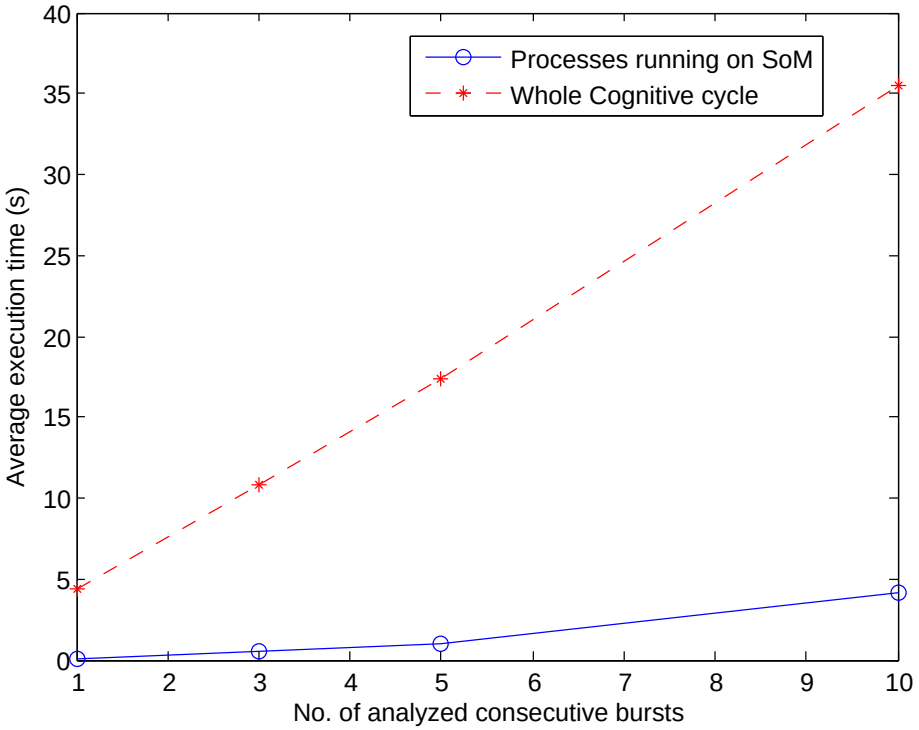


Figure 6.7: Scatter plots for −3 dBm transmission power: (a)Magnitude + variance, (b)Bandwidth + variance

Figure 6.8: Execution time of the Spectrum Intelligence algorithm



approximately 3 seconds per burst, whereas invoking and executing the SNMP command takes approximately 1.3 seconds. In case of channel surfing, additional frequency settling time of the HH is negligible, and corresponds to 40 microseconds. The measurements are performed for different number of bursts that are averaged and analyzed together. Whereas analyzing the average FFT values of multiple bursts may slightly improve the overall detection accuracy, it compromises real-time execution of the algorithm.

The performance of the Spectrum Intelligence algorithm as a whole depends primarily on the jamming tactics deployed by the adversaries, as well as on the system parameters, such as number of available channels for frequency hopping, and successful classification of these channels as spectrum holes depending on the occurrences of "friendly"/other waveforms in the system. Against naive narrowband jamming entities that change their transmission frequency slowly, Spectrum Intelligence proffers next to an infallible strategy for jamming evasion. However, against more advanced opponents that are able to adapt their tactics as fast as the Spectrum Intelligence algorithm, the performance still needs to be evaluated.

6.3 Further refinements to the Spectrum Intelligence algorithm

The Spectrum Intelligence is designed as a scalable algorithm that may relatively easily be embodied with new functionalities. In this section, we consider two of the refinements to the system that are currently in the implementation phase: compressed sensing and support for the human-in-the-loop.

Compressed sensing is currently implemented in the processing phase of the algorithm, i.e., running on the System-on-Module. However, the future intention is to implement it directly on the FPGA of the HH, prior to outputting the samples to the SoM.

A graphical user interface that enables the human operator to override decisions of the Spectrum Intelligence was developed. The ultimate goal is to embody the Spectrum Intelligence algorithm with the capabilities of cognitive refinement, i.e., the ability to incorporate decisions of the human operator in order to refine its reasoning mechanism.

6.3.1 Compressed Sensing

The major bottleneck of the current implementation of the Spectrum Intelligence is low frequency resolution, caused by the small buffer size on the HH's FPGA and the limited data rate supported by the serial transmission. This has led us to perform an analysis of the Compressed Sensing methods. The main idea is to increase the frequency resolution of the system by performing the Compressed Sensing directly on the HH's FPGA, filling the buffer with compressed samples, and then outputting them to the SoM for analysis.

Compressed Sensing (CS) [7] has become a popular research topic in the signal processing research community over the recent years. Contrary to the conventional methods that rely on Nyquist-or-above sampling rates, CS techniques show that it is possible to estimate the original signal even with sub-Nyquist rate sampling, provided that certain conditions are met. Namely, in order to be estimated or reconstructed in a satisfying manner, the signals subjected to CS need to be sparse. Since RF spectrum is by and large underutilized most of the time, sparsity is generally inherent to scanned wideband RF spectrum. The system model of the implemented CS technique, along with the preliminaries of CS along the lines of [18], [12], are given as follows.

The time-domain representation of the wideband signal received at the HH is given by:

$$r(t) = h(t) * s(t) + w(t), \tag{6.11}$$

where $h(t)$ is the channel coefficient between transmitting HH and receiving HH, $s(t)$ denotes the transmitted signal, $*$ denotes the convolution operation and $w(t)$ is the Additive White Gaussian Noise (AWGN) with zero mean and power spectral density σ_w^2.

In order to observe the frequency response of the received signal, an N-point FFT is taken on $r(t)$ to collect the frequency-domain samples into an $N_s \times 1$ vector r_f, as follows:

$$\mathbf{r}_f = \mathbf{D}_h \mathbf{s}_f + \mathbf{w}_f, \tag{6.12}$$

where $\mathbf{D}_h = diag(\mathbf{h}_f)$ is an $N_s \times N_s$ diagonal channel matrix, and $\mathbf{h}_f$, $\mathbf{s}_f$ and $\mathbf{w}_f$ are the discrete frequency-domain samples of $h(t)$, $s(t)$ and $w(t)$, respectively. In general form, this signal model can be expressed as:

$$\mathbf{r}_f = \mathbf{H}_f \bar{\mathbf{s}}_f + \mathbf{w}_f \tag{6.13}$$

From the above expression, we can observe that the spectrum sensing task requires to estimate $\bar{\mathbf{s}}_f$ in (6.13), provided that we have $\mathbf{H}_f$ and $r(t)$. Since we have a wideband signal at our disposition, we can take advantage of the CS theory to relieve high sampling rate (Nyquist rate or above) ADC requirements. Various computationally feasible algorithms, such as Basis Pursuit (BP) [2] and Orthogonal Matching Pursuit (OMP) [15], were developed to reliably estimate the received signal sampled at sub-Nyquist rate.

We start by collecting the compressed time-domain samples 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:

$$\mathbf{x}_t = \mathbf{S}_c \mathbf{r}_t, \tag{6.14}$$

where $\mathbf{r}_t$ is the $N_s \times 1$ vector of discrete-time representations of $r(t)$ at the Nyquist rate with $K \leq N_s$, and $\mathbf{S}_c$ is the $K \times N_s$ projection matrix. There are various designs introduced in the literature for compressive samplers, such as non-uniform samplers [9] and random samplers [17], [11].

Noting that $\mathbf{r}_t = \mathbf{F}_M^{-1} \mathbf{r}_f$, and given K compressed measurements, the frequency response $\bar{\mathbf{s}}_f$ from (6.13) can now be estimated as follows:

$$\mathbf{x}_t = \mathbf{S}_c^T \mathbf{F}_M^{-1} \mathbf{H}_f \bar{\mathbf{s}}_f + \tilde{\mathbf{w}}_f, \tag{6.15}$$

where $\tilde{\mathbf{w}}_f = \mathbf{S}_c^T \mathbf{F}_M^{-1} \mathbf{w}_f$ is the noise sample vector which is white gaussian. The sparsity of the signal vector $\mathbf{s}_f$ is measured by p-norm $||\bar{\mathbf{s}}_f||_p$, $p \in [0, 2)$, where $p = 0$ indicates exact sparsity.

Thus, equation (6.15) is a linear regression problem with signal $\bar{\mathbf{s}}_f$ being sparse. The signal $\bar{\mathbf{s}}_f$ can be reconstructed by solving the following linear convex optimization problem:

$$\min_{\bar{\mathbf{s}}_f} ||\bar{\mathbf{s}}_f||_1, \quad s.t. \quad \mathbf{x}_t = \mathbf{S}_c^T \mathbf{F}_M^{-1} \mathbf{H}_f \bar{\mathbf{s}}_f \tag{6.16}$$

There are several existing methods to solve this optimization problem, for example, by means of convex programming as in BP [2] method, or by using the greedy algorithms such as MP [8] and OMP [15].

We can assess performance of the considered CS algorithm on the data used in Section 6.2. The results for different levels of compression ratios, for the case when the transmission power of the "potentially malicious" waveform is -3 dBm and the classifier is able to use all 3 features, are shown in Table 6.4. As a reference, compression ratio of 75% means that the CS is performed on 75% of the original samples (sampled at 250 MSamples/s).

Table 6.4: Confusion matrices for -3 dBm transmission power: Compressed Sampling

	Pot. malicious	**Friendly**	**Compression ratio**
Pot. malicious	**50**	0	**75%**
Friendly	15	**1960**	
Pot. malicious	**50**	0	**50%**
Friendly	14	**2180**	
Pot. malicious	**48**	2	**25%**
Friendly	24	**3442**	
Pot. malicious	**46**	4	**10%**
Friendly	18	**1499**	
Pot. malicious	**25**	25	**5%**
Friendly	26	**487**	

Very good performance in the rate of true positives for the "potentially malicious" waveform is obtained even for low compression ratios, strengthening the motivation for further research on this topic. The true positives rate for the "friendly" waveforms should, however, be explained since, as can be seen from the table, the number varies significantly based on the compression ratio of the CS. As the compression ratio

starts to decrease, the number of friendly waveforms detected in the system increases, however at a certain level, this number starts decreasing drastically again. To explain this phenomenon, we show the reconstructed wideband spectrum for the compression ratios of 75% and 10% in Figure 6.9.

According to the theory of CS, when the signal is sparse, the random sampler tries to take more samples from the non-zero elements and less samples from the zero elements. For this reason, the waveforms with higher bandwidths, such as the injected SBW waveform, will be reconstructed in a better manner than the narrowband waveforms. Since the "friendly" waveforms in our system are typically narrowband signals (e.g. in the 98–105 MHz part of the band, they correspond to the FM radio transmission), their samples will often not be successfully reconstructed. For relatively high compression ratios, the system will in turn classify the same narrowband waveform split in multiple segments as multiple separate friendly waveforms, hence the initial increase in the true positives rate. For low compression ratios, magnitude values for most of these signals will be completely discarded, and simply treated as noise.

The additional computations introduced by the compressed sensing inherently prolong the execution time of the algorithm. Figure 6.10 presents the comparison of execution times for Spectrum Intelligence running CS with different compression ratios and the case when no compression is taking place, for analysis of single sensing burst.

6.3.2 Support for a human-in-the-loop

Another application of interest is the *support for a human operator* in the anti-jamming system. For this reason, a graphical user interface (GUI) was developed for the Spectrum Intelligence algorithm, which allows the human operator to overrule decisions of the algorithm. Screenshot of the interface is shown in Figure 6.11.

The interface is designed to continuously invoke `GET_Batterystatus` and `GET_Spectrumdata` over the predetermined port from the server (typically running on the SoM), automatically refreshing the display every time a command is executed. Three SET commands, namely `SET_RFchannel`, `SET_TXpower` and `SET_RFOn/Off` allow the human operator to change the operating frequency, transmission power, and turn the RF front-end on and off, respectively. The upper right part of the screen shows the status of the connection with other HH radios in the system. Whenever the HH running the GUI is not able to "ping" the other radios in the system, the "Remote link" status turns red, thus signaling to the human operator that the communication link is currently disabled.

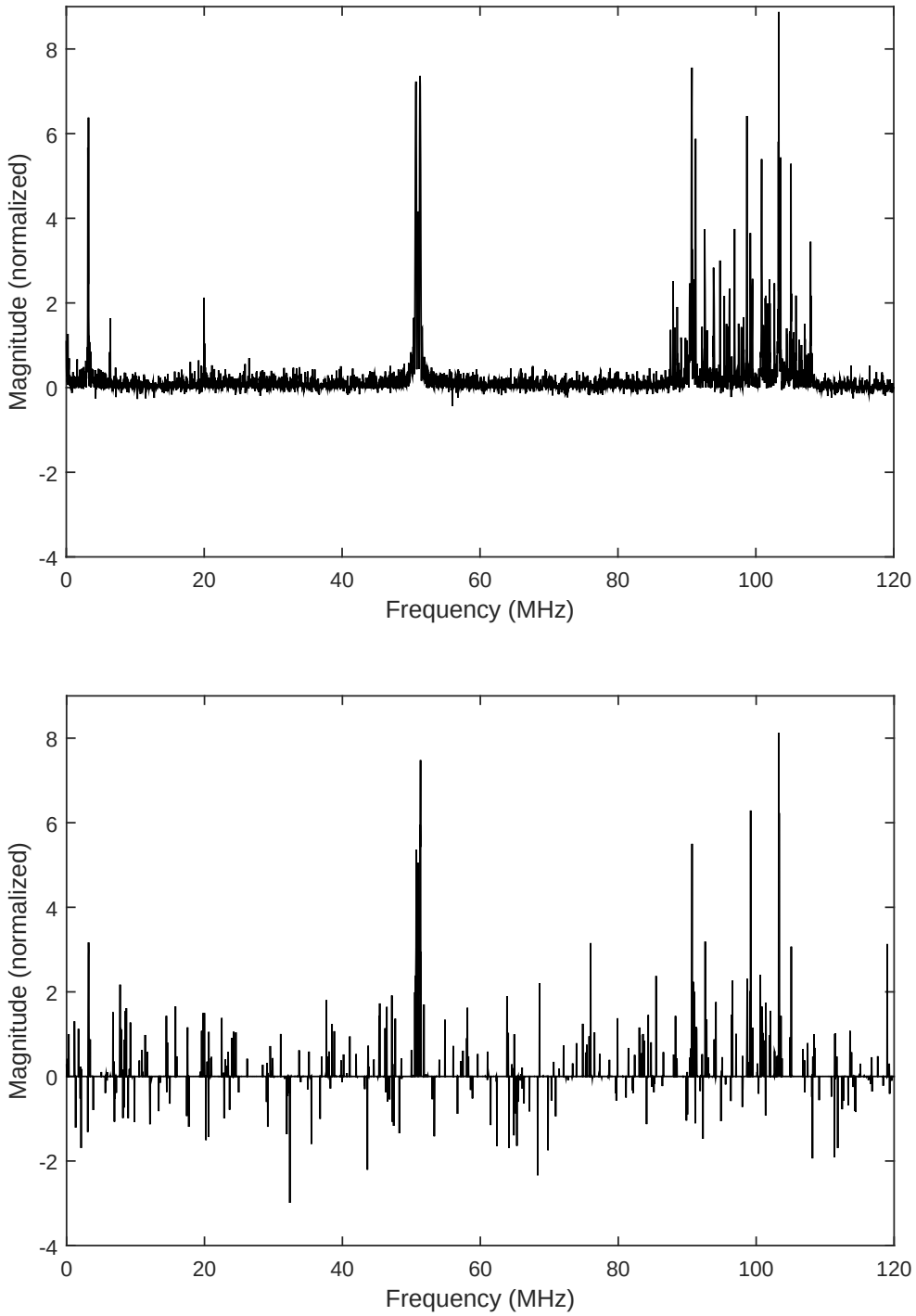
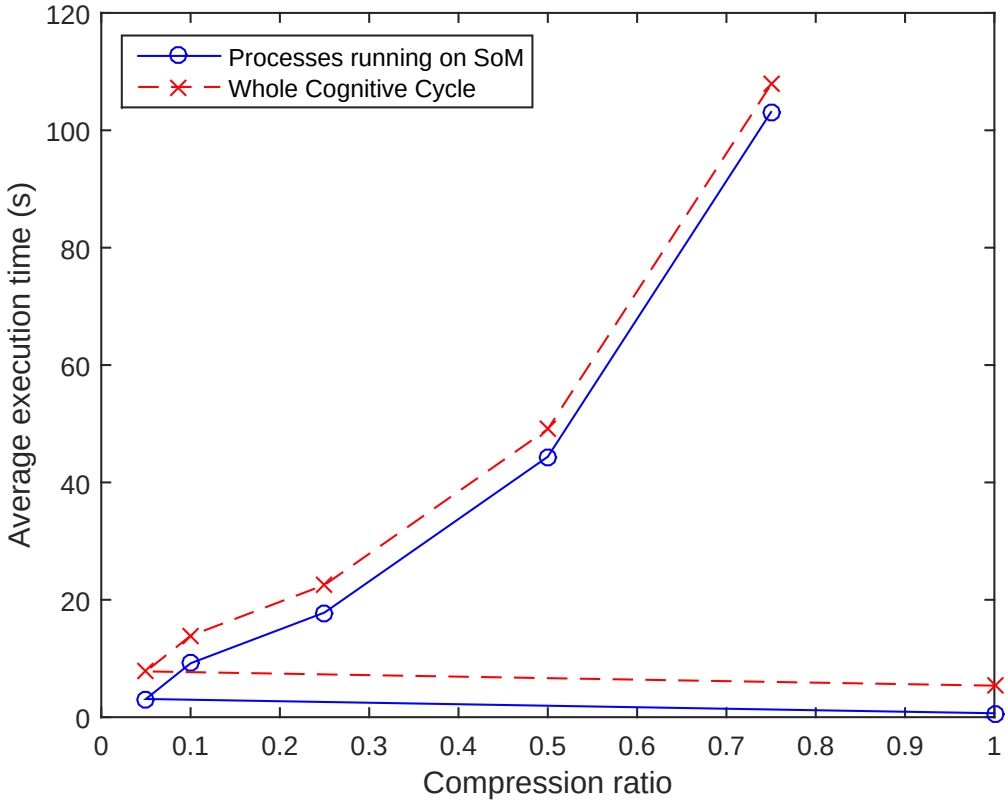


Figure 6.9: Reconstructed spectrum for compression ratios: (a)75%, (b)10%

Figure 6.10: Execution time of the Spectrum Intelligence algorithm with compressed sensing – 1 burst



As of now, the role of the developed GUI is to allow the human operator to take decisions irrespectively of the decisions of the Spectrum Intelligence algorithm. However, it also presents an interesting motivation for considering cognitive refinement principles, i.e., refining the policy-based reasoning behaviour of the algorithm by learning from the actions of the operator.

6.4 Conclusions

This chapter described some of the impacts that Cognitive Radio technology may have in designing advanced communications electronic warfare systems. The central focus of the chapter was on presenting the ideas, development and implementation aspects of the Spectrum Intelligence algorithm for Interference Mitigation. The algorithm is based on learning capabilities and on-the-fly reconfiguration of the transmission-related parameters characteristic to Cognitive Radio technology. Implementation of the algorithm was done on the SWAVE HandHeld – a military Software Defined Ra-

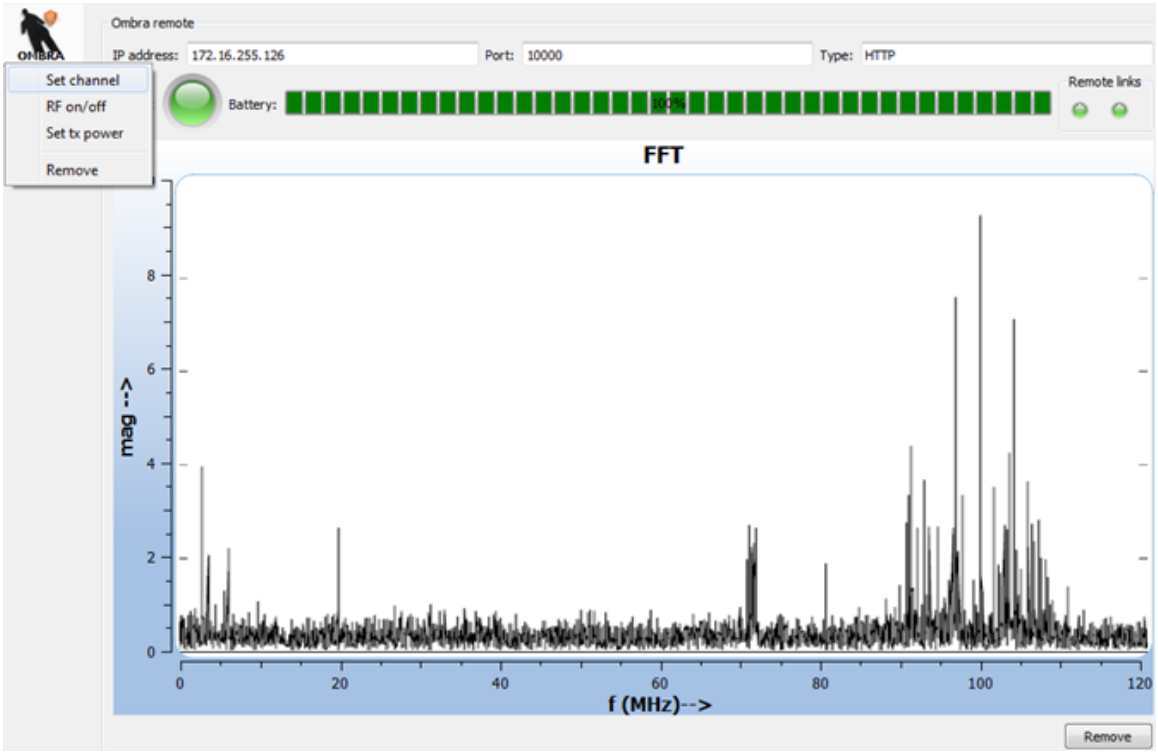


Figure 6.11: Screenshot of the Graphical User Interface

dio – interconnected with the computationally powerful System-on-Module. Performance of several crucial functionalities of the algorithm was evaluated and presented. Main identified challenges included: finding an optimal algorithm for adaptive energy detection thresholding; an optimal set of features for waveform classification, and achieving reasonable execution time. A sub-optimal thresholding approach was heuristically shown to give satisfactory results for the observed use cases. A Naive Bayes classifier is able to discriminate between the waveforms in the systems with high success rate, and the overall algorithm is able to be executed in real time.

Whereas Spectrum Intelligence can be considered a fully functional prototype in its present state, several interesting topics remain open for future research. These include deployment of Compressed Sensing in the pre-processing stage of the algorithm [12], support for the cooperation between multiple receivers running the Spectrum Intelligence, and support for cognitive refinement of the algorithm by learning from the human operator in the loop. Another interesting future research point involves combining the information obtained from spectrum sensing and analysis with the information available from local or global geolocation-based databases, in order to improve the spectrum awareness and increase the performance of the overall anti-jamming system.

Bibliography

[1] D. Cabric, S.M. Mishra, and R.W. Brodersen. Implementation issues in spectrum sensing for cognitive radios. In *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, volume 1, pages 772–776 Vol.1, November 2004. doi: 10.1109/ACSSC.2004.1399240.

[2] S. Chen, D.L. Donoho, and M.A. Saunders. Atomic decomposition by basis pursuit. *SIAM Journal on Scientific Computing*, 20(1):33–61, 1999.

[3] K. Dabcevic, A. Betancourt, C.S. Regazzoni, and L. Marcenaro. A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios. In *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pages 8208–8212, 2014.

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

[5] F. Delaveau, A. Evesti, J. Suomalainen, and N. Shapira. Active and passive eavesdropper threats within public and private civilian wireless-networks - existing and potential future countermeasures - a brief overview. In *Proceedings of SDR'13 -WinnComm-Europe*, pages 11–20, June 2013.

[6] F.F. Digham, M.-S. Alouini, and M.K. Simon. On the energy detection of unknown signals over fading channels. *IEEE Transactions on Communication*, 55 (1):21–25, 2007.

[7] D.L. Donoho. Compressed sensing. *IEEE Trans. on Information Theory*, 52(4): 1289–1306, April 2006.

[8] M.F. Duarte, M.B. Wakin, and R.G. Baraniuk. Fast reconstruction of piecewise smooth signals from random projections. In *SPARS*, 2005.

[9] P. Feng and Y. Bresler. Spectrum-blind minimum-rate sampling and reconstruction of multiband signals. In *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, volume 3, pages 1685–1691, May 1996.

[10] H.L. Hirsch. Statistical signal characterization - new help for real-time processing. In *Aerospace and Electronics Conference, 1992. NAECON 1992., Proceedings of the IEEE 1992 National*, pages 121–127 vol.1, May 1992. doi: 10.1109/NAECON.1992.220658.

[11] J. Laska, S. Kirolos, Y. Massoud, R. Baraniuk, A. Gilbert, M. Iwen, and M. Strauss. Random sampling for analog-to-information conversion of wideband signals. In *Proceedings of IEEE Dallas/CAS Workshop on Design, Applications, Integration and Software*, pages 119–122, 2006.

[12] M.O. Mughal, K.Dabcevic, G.Dura, L.Marcenaro, and C.S. 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)*, November 2014.

[13] R. Poisel. *Introduction to Communication Electronic Warfare Systems*. Artech House, Inc., Norwood, MA, USA, 2nd edition, 2008.

[14] A. Tkachenko, D. Cabric, and R.W. Brodersen. Cyclostationary feature detector experiments using reconfigurable bee2. In *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pages 216–219, April 2007. doi: 10.1109/DYSPAN.2007.36.

[15] 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, 2007.

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

[17] Z. Yu, S. Hoyos, and M. Sadler. Mixed-signal parallel compressed sensing and reception for cognitive radio. In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, pages 3861–3864, 2008.

[18] F. Zheng, 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.

Chapter 7

A game-theoretical approach to evaluating intelligent RF jamming/anti-jamming techniques

Radio Frequency (RF) jamming attacks may be defined as illicit transmissions of RF signals aimed at disrupting the normal communication on the targeted channels. Adversaries that utilize the Cognitive Radio learning mechanisms to improve their jamming capabilities are considered intelligent. Intuitively, being equipped with such learning mechanisms may also aid the legitimate users in improving their anti-jamming capabilities. The goals of legitimate transceivers and jammers are typically negatively correlated. This 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 problems. This chapter explores how game theory can be used to analyze the jamming/anti-jamming behaviour between Cognitive Radio systems. A non-zero-sum game with incomplete information on opponent's strategy and payoff is modelled as an extension of Markov Decision Process. Learning algorithms based on adaptive payoff play and fictitious play are considered. A combination of frequency hopping and power alteration is deployed as an anti-jamming scheme. The SDR/Cognitive Radio test bed architecture described in chapter 4 is used in order to perform measurements useful for quantifying the jamming impacts, as well as to infer relevant hardware-related properties. Results of these measurements are then used as parameters for the modelled jamming/anti-jamming game and are compared to the Nash equilibrium of the game [6].

7.1 Preliminaries of game theory

Prior to explaining the proposed game-theoretical framework, we briefly introduce the most important concepts related to game theory.

Game theory is a mathematical model that analyzes the strategic interactions between multiple rational agents. Its foundations were laid in the 1944 book *Theory of Games and Economic Behavior* by J. von Neumann and O. Morgenstern, which dealt with finding optimality criteria for particular cases of two-person zero-sum games. In 1951, J. Nash introduced the concept of Nash Equilibrium (NE), extending the previous discoveries to more general cases of non-zero-sum games. Since then, game theory continues to be an important tool for analysis of situations involving conflicts of interest in many different fields, including information systems.

Among several possible categorizations of game theory, one of the principal ones distinguishes cooperative vs. non-cooperative game theory. The former deals with finding optimal solutions of dividing the proceeds among members of coalitions, i.e., it considers games where the agents (players) can make binding mutual agreements. The latter, conversely, considers the games where the agents make their decisions and devise their strategies independently, and represents the branch of game theory that we are interested in.

Game is the formal model of an interactive situation, and it involves two or more *players*. The game is played in a sequence of *steps* where, at the end of each step, every player receives an immediate *payoff* and chooses an *action* for the next step. The number of actions that each player may take is limited. The set of actions that each player takes, depending on the previously received payoffs and/or the history of the actions of the opponent, comprise his *strategy*. The strategy can be *pure* or *mixed*. A central concept in game theory is represented by *Nash equilibrium* – a set of strategies of all the players involved in the game such that no player can directly benefit from unilaterally deviating from the Nash equilibrium strategy. Two important questions that are usually addressed when considering games is: i) "does the game have a Nash equilibrium?", and ii)"is the Nash equilibrium unique?". Nash equilibrium is formally introduced in Section 7.2.3.

7.2 A proposed game-theoretical approach

Most of the previous works in the literature on application of game theory to jamming problems, some of which were described in Section 2.2.3, consider either channel surf-

ing or power allocation as anti-jamming strategies. Furthermore, they are mutually differentiated mostly by the objective function subjected to optimization (Signal-to-Noise Ratio, Bit Error Rate, Shannon capacity); various forms of uncertainty (user types, physical presence, system parameters); game formulation (zero-sum vs. non-zero-sum, single-shot vs. dynamic), learning algorithms (Q-learning, SARSA, policy iteration), etc.

We summarize the contributions and novelties of our approach with respect to the state-of-the-art contributions on the application of game theory to intelligent jamming scenarios as follow:

- We present the ideas of learning algorithms that correspond to Cognitive Radios with and without spectrum sensing capabilities, comparing their performance.
- We compare the performance of the considered learning algorithms for the modeled game with the Nash equilibrium of the game.
- We consider an increased action space created by combining two anti-jamming tactics.
- We use real-life SDR/Cognitive Radio platform to infer parameters that allow modeling the game in a more realistic manner.

7.2.1 System model

Consider a simplistic two-way transmitter-receiver communication occurring over one of the n_f pre-defined channels and a malicious user (jammer) that is trying to disrupt the communication by creating narrowband interference. Transmitter and receiver are considered the primary users over all of the considered channels and are able to tune to the same channel at a given time instance. Without the loss of generality, all of the channels are modelled with the same parameters; however, it will become obvious that the proposed anti-jamming techniques would be able to indirectly infer different channel parameters and fit these inferences into their decision-making process.

Jammer is able to create narrowband interference on a single channel at a time, causing the deterioration of the Signal to Interference plus Noise Ratio (SINR) and subsequently increase of the Bit Error Rate (BER) on that channel. It is assumed that the jamming attack is the only possible reason for the deterioration of the channel quality, neglecting other possible sources of interference, as well as the time-varying nature of channels, including effects of the multipath propagation.

To mitigate the jamming effects and increase the SINR at the receiver side over the threshold needed for successful decoding, the transmitter may deploy a combination of channel hopping and increasing its transmission power (power alteration).

Both the transmitter and the jammer are able to make use of the on-the-fly reconfigurability as well as the learning prospectives of the Cognitive Radio technology. Under different studied scenarios, both the transmitter and the jammer may have different spectrum sensing capabilities. Following that, two different learning algorithms are studied: Payoff-Based Adaptive Play (PBAP), where players are not necessarily embodied with spectrum sensing, and fictitious play, where players are able to infer the actions of the opponent in each step as a result of the deployed spectrum sensing scheme. In addition, performance of the proposed jamming/anti-jamming schemes is evaluated against static, non-learning types of opponents.

Other assumptions and abstractions that were taken in order to take a game-theoretical approach to jamming/anti-jamming problem are given as follow:

- Considered channels are perfectly orthogonal, non-overlapping, with frequency spacing between them large enough to make any energy spillover negligible.
- A discrete number of transmission powers were considered for both the transmitter and the jammer.
- Following the previous assumption, occurrence of jamming is modelled as a discrete event, i.e., it always occurs with success or failure, disregarding the typical stochastic processing involved with the occurrence of jamming [1].
- Both the transmitter and the jammer are in continuous transmission mode, i.e., they always have packets ready to send.
- Jammer is able to create interference powerful enough to successfully jam communications when the transmitter is transmitting with its maximum transmission power (provided that they are both transmitting on the same channel at the time).
- All players maintain their relative positions as well as antenna orientations with respect to each other.

[1] This assumption may be built upon the existence of the threshold effect, characteristic for digital communication systems, where there is a certain SINR below which the BER significantly rises, and the communication systems perform poorly [15].

7.2.2 Game formulation

The attack and defense problem is modelled as a multi-stage proactive jamming/anti-jamming stochastic game. A *stochastic game* [10] is played in a sequence of steps, where at the end of each step, every player receives a payoff for the current step and chooses an action for the next step that is expected to maximize his payoff. A player's payoff in each step is determined not only by his action but also by the actions of all the other players in the game. Collection of all of the actions that a player can take comprise his (finite) action set. The distribution of player's choices of actions constitute his strategy. The strategy may be fixed or it may be updated according to the deployed learning algorithm.

The proposed game is an extension of *Markov Decision Process (MDP)*, whose state transition probabilities may be depicted as *finite Markov Chains*.

The modelled game consists of two players: Transmitter T and Jammer J. At the end of each step, every player observes his payoff for the given step and decides either to continue transmitting with the same power and at the same frequency or to change one of them, or both. The payoff consists of a summation of reward for the successful transmission (jamming), penalty for the unsuccessful transmission (jamming), and negative values related to cost of transmission (jamming) and cost of frequency hopping. Transmission (jamming) cost is related to the power spent by the user for transmitting (jamming) in a given step. Hopping cost may be explained by the fact that, after changing the channel of the transceiver pair (jammer), a certain time elapses before the communication may be resumed (interference created) due to the settling time of the radios or due to other hardware constraints.

A generalized payoff at the end of the step s for the transmitter T is expressed as (7.1). Here, R^T denotes the reward for successful transmission, X^T is the sustained fixed penalty for the unsuccessful transmission, H is the hopping cost, $g(C^T)$ is a function that expresses the transmitter's cost of transmission when power C^T ($C^T \leq T_{MAX}$) is used, f^T is the channel currently used by the transmitter–receiver pair, $\alpha = 1$ if transmission is successful and $\alpha = 0$ if not, and $\beta = 1$ if the transmitter decides to hop and $\beta = 0$ otherwise. In this notation, subindices are used to denote steps, and superindices to denote the players.

$$P_s^T(C_s^T, f_s^T, C_s^J, f_s^J) = R^T\alpha - X^T(1-\alpha) - H \cdot \beta - g(C_s^T) \tag{7.1}$$

Similarly, the jammer J's generalized payoff for the step s is given as (7.2). Here, R^J is the jammer's reward for successful jamming, X^J is the sustained fixed penalty

for the unsuccessful jamming, $g(C^J)$ is the jammer's cost of transmission when power C^J is used. Finally, $\gamma = 1$ if the jammer decides to hop and $\gamma = 0$ if it does not.

$$P_s^J(C_s^T, f_s^T, C_s^J, f_s^J) = R^J(1-\alpha) - X^J\alpha - H\gamma - g(C_s^J) \tag{7.2}$$

We next provide a motivation for our game formulation by first considering a naive deterministic game where the players are initially taking their decisions retroactively, and do not deploy any learning mechanism. In such an example, at the end of every step s, each player observes his current payoff, transmission power and transmission frequency. In case that the players were transmitting at the same frequency, the transmitter is also able to estimate the jammer's transmission power – presumably calculated from the SINR obtained at the receiver – whereas the jammer is always able to estimate the transmitter's power as well as transmission frequency using the spectrum sensing mechanism. Then, given these observations, each player devises an action that will maximize his payoff in the next state. It is easy to show that the problem comes down to a simple ternary decision. Each case denotes a simplified action set for the transmitter (7.3) and jammer (7.4) as (power, frequency): keep and stay (KS), restart and change (RC), increase and stay (IS). The magnitude of the power increase ΔC^T is the minimum increase that the transmitter needs to invest in order to get the SINR at the receiver side over the threshold that guarantees successful decoding. Correspondingly, increase of the power for the jammer relates to the minimum level of additional invested power required to ensure successful jamming on a given channel.

$$A_{s+1}^T = \begin{cases} \text{(KS)}, & \text{if } \alpha(s) = 1 \\ \text{(RC)}, & \text{if } \alpha = 0 \text{ and } (H < C_s^T + \Delta C^T \text{ or} \\ & \qquad C_s^T + \Delta C^T > T_{MAX}) \\ \text{(IS)}, & \text{if } \alpha = 0 \text{ and } (H \geq C_s^T + \Delta C^T \text{ and} \\ & \qquad C_s^T + \Delta C^T \leq T_{MAX}) \end{cases} \tag{7.3}$$

$$A_{s+1}^J = \begin{cases} \text{(KS)}, & \text{if } \alpha = 0 \\ \text{(RC)}, & \text{if } \alpha = 1 \text{ and } f_s^T \neq f_s^J \\ \text{(IS)}, & \text{if } \alpha = 1 \text{ and } f_s^T = f_s^J \end{cases} \tag{7.4}$$

However, deploying the simple learning mechanisms on either (or both) of the sides would allow the players to take more advanced decisions, thus exploiting the decisions of the opponent. Illustratory example of gradual evolution of the game when

such an arms race is present is shown in Figure 7.1. In order to simplify analysis, only two hopping channels are considered, and are denoted by $f1$ and $f2$.

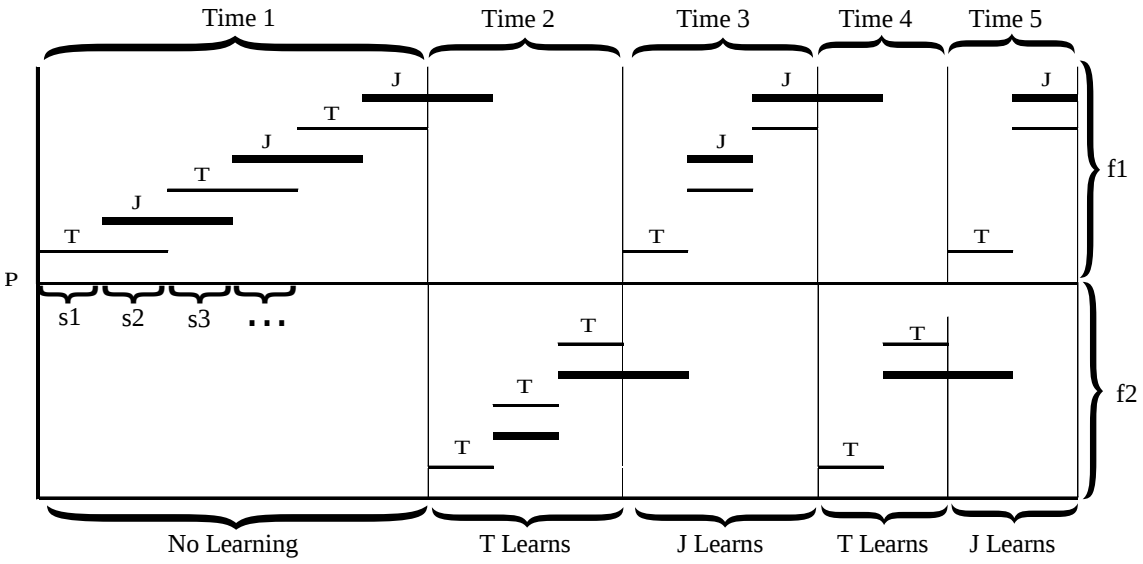


Figure 7.1: Illustration of the arms race of the players' learning mechanisms.

In time 1, both players observe whether their action in the given step brought them positive payoff. If so, they choose the action (KS) for the following step, otherwise they keep increasing their transmission powers by ΔC^T (transmitter) or ΔC^J (jammer). This is repeated for as long as $C^T_{s+1} < H$ and $C^T_{s+1} \leq T_{MAX}$. State of the system is illustrated as T when transmission is successful and J when jamming is successful. Then, at time 2, the transmitter decides to switch to another frequency. However, by observing the jammer's behaviour in time 1, it also realizes that better result would be yielded by proactively increasing its transmission power by two discrete increments in every step. When cost of the transmission has once more risen above the cost of hopping, the transmitter will hop back to frequency 1. In time 3, the jammer will observe this pattern and will decide to increase the probability of successful jamming by proactively increasing its transmission power in each step by 3 increments. Intuitively, the game will eventually evolve towards proactive hopping and transmitting with maximum power in every step. However, the players can achieve even better payoffs by observing the overall history of their previously obtained payoffs for any given action, and/or the history of the actions of the opponent, and incorporating these observations into their decision-making process. This corresponds to players deploying one of the learning algorithms explained in Section 7.2.4.

7.2.3 Equilibrium analysis of the game

Nash equilibrium is inarguably the central concept in game theory, representing the most common notion of rationality between the players involved in the game. It is defined as the set of distributions of players' strategies designed in a way that no player has an incentive to unilaterally deviate from its strategy distribution.

Let n_f be a discrete number of channels available to both players for channel hopping, and let n_{C^T} and n_{C^J} be the discrete number of transmission power for the transmitter and the jammer, respectively. For the game with $n_f \cdot n_{C^T}$ ($n_{C^T} = n_{C^J}$) pure strategies available to each player, we define S^T as the set of pure strategies of the transmitter and S^J as the set of pure strategies of the jammer. Then, $x \in \mathbb{R}^{S^T}$ and $y \in \mathbb{R}^{S^J}$ represent the mixed strategies of the transmitter and jammer, respectively. By denoting the payoff matrices of the transmitter and the jammer as A and B, respectively, a best response to the mixed strategy y of the jammer is mixed strategy x^* of the transmitter that maximizes its expected payoff $x^{*\intercal}Ay$. Similarly, the jammer's best response y^* to the transmitter's mixed strategy x is the one that maximizes $x^\intercal By^*$. A pair (x^*, y^*) that are best responses to each other is a Nash equilibrium of the bimatrix game, i.e., for any other combination of mixed strategies (x,y) the following equations hold true:

$$xAy^{*\intercal} \leq x^*Ay^{*\intercal}, \tag{7.5}$$

$$x^*By^\intercal \leq x^*By^{*\intercal}. \tag{7.6}$$

In 1951, Nash proved that all finite non-cooperative games have at least one mixed Nash equilibrium [12]. Particularization of this proof for bimatrix games may be given as follows [14]:

Let x and y be arbitrary pairs of mixed strategies for the bimatrix game (A,B), and $A_{i\cdot}$ and $B_{\cdot j}$ represent the i-th column and the j-th row of the matrices A and B, respectively. Then,

$$c_i = max\left\{A_{i\cdot}y^\intercal - xAy^\intercal, 0\right\}, \tag{7.7}$$

$$d_j = max\left\{xB_{\cdot j} - xBy^\intercal, 0\right\}, \tag{7.8}$$

$$x'_i = \frac{x_i + c_i}{1 + \sum_k c_k}, \tag{7.9}$$

$$y'_j = \frac{y_j + d_j}{1 + \sum_k d_k}. \tag{7.10}$$

Since $T(x,y)=(x',y')$ is continuous and x' and y' are mixed strategies, it can be shown that $(x',y')=(x,y)$ if and only if (x,y) is an equilibrium pair. Furthermore, if (x,y) is an equilibrium pair, then for all i:

$$A_{i\cdot}y^{\intercal} \leq xAy^{\intercal}, \tag{7.11}$$

hence $c_i=0$ (and similarly $d_j=0$ for all j), meaning that $x'=x$ and $y'=y$. Assume now that (x,y) is not an equilibrium pair, i.e., there either exists $\overline{x}$ such that $\overline{x}Ay^{\intercal} > xAy^{\intercal}$, or there exists $\overline{y}$ such that $xB\overline{y}^{\intercal} > xBy^{\intercal}$. Assuming the first case, as $\overline{x}Ay^{\intercal}$ is a weighted average of $A_{i\cdot}y^{\intercal}$, there must exist i for which $A_{i\cdot}y^{\intercal} > xAy^{\intercal}$, and hence some $c_i > 0$, with $\sum_k c_k > 0$. As $xAy^{\intercal}$ is a weighted average of $A_{i\cdot}y^{\intercal}$, there must exist $A_{i\cdot}y^{\intercal} \leq xAy^{\intercal}$ for some i such that $x_i > 0$. For this i, $c_i = 0$, hence:

$$x'_i = \frac{x_i + c_i}{1 + \sum_k c_k} < x_i, \tag{7.12}$$

and so $x' \neq x$. In the same way, it can be shown that $y' \neq y$, leading to the conclusion that $(x', y') = (x, y)$ if and only if (x, y) is an equilibrium. As the transformation $T(x, y) = (x', y')$ is continuous, it must have a fixed point, and so by applying Brouwer's fixed point theorem [2], it follows that this fixed point indeed represents an equilibrium point. This concludes the proof of the existence of mixed-strategy equilibrium points in a bimatrix game.

However, efficient computation of equilibria points, as well as proving uniqueness of an equilibrium, remains an open question for many classes of games. Lemke-Howson (LH) [18] is the most well-known algorithm for the computation of Nash equilibria for bimatrix games and is our algorithm of choice for finding the Nash equilibrium strategies. A bimatrix game requires the game to be fully defined by two payoff matrices (one for each player). Since in our case the immediate payoff of every player in each step depends not only on his own action and the action of the opponent but also on the previous state of the player (influence of the hopping cost), our game as a whole cannot be represented by two deterministic payoff matrices. For this reason, we divide the game into $n_f \cdot n_{C^T}$ subgames, where each subgame corresponds to a unique combination of possible states of the transmitter and the jammer. Since each subgame can be treated as the separate game in a bimatrix form, we proceed to apply the LH method to find mixed strategy Nash equilibriums (one per subgame). Hence, in each step, every player plays an equilibrium strategy corresponding to that step. A union of equilibria strategies of all the $n_f \cdot n_{C^T}$ combinations of the states within the game represents the Nash equilibrium of the game.

Gambit [9], an open-source collection of tools for solving computational problems in game theory, was used for finding equilibrium points using the LH method. For details on the implementation of the LH algorithm, an interested reader is referred to [19].

Each of the subgames (A_{ij}, B_{ij}) where $i = 1 \dots n_f$ and $j = 1 \dots n_{C^T}$ is a nondegenerate bimatrix game. Then, following Shapley's proof from [18], we may conclude that there exists an odd number of equilibria for each subgame. In [22], the upper bound on the number of equilibria in $d \times d$ bimatrix games was shown to be equal to $\frac{2.41^d}{d^{1/2}}$; however, the uniqueness of Nash equilibrium may still be proven only for several special classes of bimatrix games. Here, we provide conditions that the bimatrix game has to satisfy in order to have a unique completely mixed Nash equilibrium. Completely mixed Nash equilibrium is an equilibrium in which the supports of each of the mixed equilibrium strategies are equal to the number of available pure strategies (i.e., each strategy from a mixed strategy set is played with a non-zero probability). As shown by Milchtaich and Ostrowski [11], whose proof we re-state, a bimatrix game (A, B) whose matrices A and B are square, has a unique completely mixed Nash equilibrium if $det(A, \mathbf{e}) \neq 0$ and $det(B, \mathbf{e}) \neq 0$, i.e.:

$$det(A, \mathbf{e}) \cdot det(B, \mathbf{e}) \neq 0, \tag{7.13}$$

where $\mathbf{e}$ is a column vector with all entries 1.

The saddle point matrix $(A, \mathbf{e})$ is given by:

$$(A, \mathbf{e}) = \begin{bmatrix} A & \mathbf{e} \\ \mathbf{e}^\intercal & 0 \end{bmatrix}. \tag{7.14}$$

Then, the equilibrium strategies of the players are given as:

$$x^*{}_i = -\frac{detB^i}{det(B, \mathbf{e})}, \tag{7.15}$$

$$y^*{}_i = -\frac{detA_i}{det(A, \mathbf{e})}, \tag{7.16}$$

where B^i (A_i) is the matrix of B (A) with all entries of the i-th column (row) replaced by 1.

Let us now suppose that (x^*, y^*) is an equilibrium point of the bimatrix game (A,B), where x^* is completely mixed. Then, every pure strategy would give that player the same payoff P against the opponent's strategy y^*, i.e.:

$$Ay^* = P\mathbf{e}. \tag{7.17}$$

Since y^* is a vector of probabilities,

$$\mathbf{e}^\intercal y^* = 1. \tag{7.18}$$

Or, in matrix form:

$$\begin{bmatrix} A & \mathbf{e} \\ \mathbf{e}^\intercal & 0 \end{bmatrix} \begin{bmatrix} y^* \\ -P \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{7.19}$$

Following the assumption $det(A, \mathbf{e}) \neq 0$ and by applying Cramer's rule, it follows from (7.19) that (7.16) is true for $(i = 1, 2, ..., n)$ (in our case, $n = n_{C^T} \cdot n_f$). Similarly, the same holds for ${x^*}_i$. As shown by Milchtaich and Ostrowski [11]:

$$det(A_i, \mathbf{e}) = det(A_i - \mathbf{e}\mathbf{e}^\intercal) - det(A_i) = -detA_i, \tag{7.20}$$

hence (7.15) and (7.16) are shown to be true. This concludes the proof of the uniqueness of the completely mixed equilibrium.

It may be computationally shown that all of the $n_f \cdot n_{C^T}$ subgames constructed within the considered game satisfy (7.13). Furthermore, by observing the Markov state chains corresponding to the equilibrium points found by the LH method, it may indeed be observed that $supp(x^*) = supp(y^*) = n_f \cdot n_{C^T}$, i.e., the equilibriums are completely mixed. Trying to find multiple equilibria for each subgame using other computational methods available within [9] has also resulted in a single (completely mixed) equilibrium for each subgame: empirical evaluation of these results, based on the algorithms to find all possible equilibrium points of the bimatrix game, further points to the existence of a unique Nash equilibrium for each subgame.

One of the common criticisms of using computational algorithms such as LH for finding Nash equilibria is that they fail to realistically capture the way that the players involved in the game may reach the equilibrium point. For this reason, it is useful to discuss the payoff performance and the convergence properties to Nash equilibrium of the algorithms realistically used for learning in games. This discussion is done for two multi-agent learning algorithms: fictitious play in Section 7.2.4.1 and payoff-based adaptive play in Section 7.2.4.2.

7.2.4 Learning algorithms

Learning algorithms for MDPs have been extensively studied in the past [17, 20]. Based on their spectrum occupancy inference capabilities, an illustrating example of the corresponding learning algorithms for the considered game and the dimensionality of the action space is given in Figure 7.2

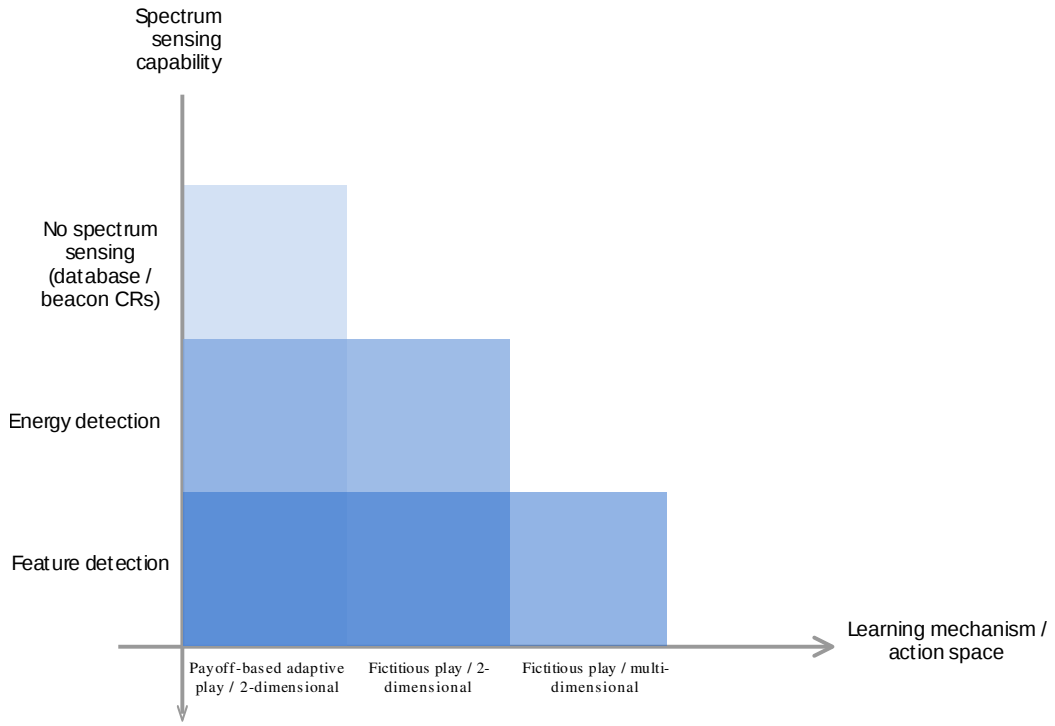


Figure 7.2: Spectrum sensing capability vs. learning mechanism and action space

For Cognitive Radios that are not equipped with spectrum sensing capabilities (gelocation/database-driven Cognitive Radios and Cognitive Radios utilizing beacon rays), payoff-based reinforcement algorithms impose themselves as the optimal viable learning algorithms. In these cases, each player is able to evaluate the payoff received in every step and modify its strategy accordingly.

Cognitive Radios that are able to perform energy detection spectrum sensing, in addition, also have the possibility of observing their opponents' actions in each step (influenced possibly by the accuracy of the deployed spectrum sensing mechanism). By incorporating these observations into their future decision-making process, the players may build and update a belief regarding the opponents' strategy distribution. This learning mechanism is called fictitious play.

Finally, Cognitive Radios that are able to perform feature detection spectrum sensing may recognize important parameters of the opponent's signal and use these observations to their advantage. Since various waveforms exhibit different jamming and anti-jamming properties, depending mainly on their modulation and employed coding (see, for example, results by Poisel [15]), increased action space could consist of switching between multiple modulation types or coding techniques.

In this chapter, we focus our analysis on the first two cases. Algorithm 2 illustrates the general formulation of the game. It can be seen how, in every step, each player takes a decision d_s for his next action based on their expected utility $\overline{P_s} = E[P_s|P_{1:s-1}]$ under PBAP or $\overline{P_s} = E[P_s|P_{1:s-1}, ss_{1:s-1}]$ under fictitious play. Received payoffs P_s are calculated for each player using (7.1) and (7.2). Thereafter, spectrum sensing is performed and the expected payoff is updated with the new information available. To simplify explanation of the learning strategies and Algorithm 2, it is assumed that both players perform the spectrum sensing step; however, the result of this step is used only under fictitious play framework. For the players with perfect spectrum sensing capabilities, $ss_s^T = d_s^T$ and $ss_s^J = d_s^J$.

Algorithm 2 Game pseudocode

```
1:  function TRANSMITTER JAMMER GAME
2:      nSteps ← Number of steps
3:      R^T, R^J ← Rewards
4:      C^T, C^J ← Cost of hopping
5:
6:      Initialize the expected utilities
7:      s ← 0
8:      while s < nSteps do
9:          d_s^T ← Decide Transmitter                    ▷ Section 7.2.5
10:         d_s^J ← Decide Jammer                         ▷ Section 7.2.5
11:         P_s^T ← Transmitter utility                   ▷ Equation (7.1)
12:         P_s^J ← Jammer utility                        ▷ Equation (7.2)
13:         ssd_s^J ← Transmitter Spectrum Sensing
14:         ssd_s^T ← Jammer Spectrum Sensing
15:         Transmitter.learn(P_s^T, ssd_s^J)             ▷ Section 7.2.4
16:         Jammer.learn(P_s^J, ssd_s^T)                  ▷ Section 7.2.4
17:         s ← s + 1
18:     end while
19: end function
```

Note from the pseudocode that the game consists of two main parts: the learning algorithm, in charge of updating the expected payoffs, and the decisioning policy, which uses the available observations to decide upon the future actions.

Let us assume that in step s the transmitter was transmitting with power C_s^T on the frequency f_s^T. Using one of the decisioning policies described in Section 7.2.5, its action in the next step constitutes of transmitting with power C_{s+1}^T on frequency f_{s+1}^T. We denote this action as a list of 4 elements $d_s^T = [C_s^T, f_s^T, C_{s+1}^T, f_{s+1}^T]$ for the transmitter and the equivalent values $d_s^J = [C_s^J, f_s^J, C_{s+1}^J, f_{s+1}^J]$ for the jammer.

7.2.4.1 Fictitious play

Fictitious play [16] is an iterative learning algorithm where, at every step, each player updates his belief about the stochastic distributions of the strategies of the other players in the game. The application of a learning mechanism based on fictitious play to the modelled game is constructed under the assumption that the player is necessarily endowed with the spectrum sensing capabilities, allowing him to infer the actions of the other player. A payoff of a particular action given the player's current state and the opponent's action is deterministic and may be calculated using (7.1) and (7.2) for the transmitter and the jammer, respectively. If the player has the information regarding the opponents' action in each step, then it is possible to calculate the expected utility more precisely, by accessing the history of the opponents' actions. This is particularly true for the jammer because of the higher number of non-jammed states compared to the states of successful jamming. Hence, learning the transmitter's pattern as soon and with as much precision as possible makes a significant difference to the overall payoff. This updating process is denoted in Algorithm 3.

Algorithm 3 Expected utility update under fictitious play

```
1:  function FictiousExpectedUtilityUpdate
2:      powers ← Available powers
3:      freqs ← Available frequencies
4:      SS ← Opponent's state [Spectrum Sensing]
5:      flist ← Opponent's previous states
6:      ---------------------------------------------------------
7:      flist.append(SS)
8:      for d ∈ possible actions do
9:          sum ← 0
10:         for C, f ∈ powers, freqs do
11:             N ← count (C, f) in flist
12:             sum ← sum + N · P(d[3], d[4], C, f)
13:         end for
14:         P^T_{s+1}(d) = sum / s
15:     end for
16: end function
```

It is known that the convergence of the fictitious play to Nash equilibrium is guaranteed only for several special cases, such as zero-sum games, non-degenerate $2\times n$ games with generic payoffs, games solvable by iterated strict dominance and weighted potential games. For other types of games, including the game considered

presented in this chapter, convergence to Nash equilibrium is not guaranteed, and even when it converges, the time needed to run the algorithm to convergence may be very long due to the problem being polynomial parity arguments on directed graphs (PPAD)-complete [7]. This has led to the introduction of the concept of approximate Nash Equilibrium (ϵ-equilibrium). Here, ϵ is a small positive quantity representing the maximum increase in payoff that a player could gain by choosing to follow a different strategy.

Conitzer [4] has shown that fictitious play achieves the worst-case guarantee of $\epsilon = (r+1)/(2r)$ (where r is the number of fictitious play iterations) and in reality provides even better approximation results. Furthermore, as recently shown by Ostrovski and van Strien [13], fictitious play may in some cases outperform any actual Nash equilibrium – for this reason, it is useful to study the performance of the fictitious play algorithm in terms of average and final payoff compared to the Nash equilibrium.

7.2.4.2 Payoff-based adaptive play

Payoff-based adaptive play [3] is a type of reinforcement learning algorithm, where it is assumed that the player does not have access to the information about the state of the other player and relies on the history of his own previous payoffs. The expected utility of d_s given previous payoffs is given by Equation (7.21).

$$\overline{P_{s+1}(d_s)} = E[P_s(d_s)|P_{1:s-1}(d_s)] = \frac{\overline{P_s(d_s)} \cdot s + P_s(d_s)}{s+1} \tag{7.21}$$

PBAP has been shown to converge to Nash equilibrium for zero-sum games [8]. For general finite 2-player games, it was shown to converge to close-to-optimal solutions in polynomial time [1].

In addition to comparing the performance of the PBAP to the computed Nash equilibrium strategy from Section 7.2.3, of particular interest to this work is the comparison to the performance of the fictitious play. This comparison should reflect the benefit that each player gains by being equipped with the spectrum sensing algorithm (fictitious play) over not being equipped with it (PBAP).

7.2.5 Decisioning policies

Decisioning policy of the learning algorithm corresponds to the set of rules that the player uses to select his future actions.

7.2.5.1 Greedy decisioning policy

The most intuitive decisioning policy consists of always choosing the action that is expected to yield the highest possible value based on the current estimates – the so-called greedy decisioning policy [23]. However, a greedy method is overly biased and may easily lead the learning algorithm to "get stuck" in local optimal solutions. An example of this is given in Figure 7.3, where both players are employing the greedy decisioning policy. Here, each player fairly quickly learns the "best response" to an opponent's action and starts relying on using it. Then, a significant amount of time has to pass before his expected payoff for the given action drops enough that other action starts being considered as "best response", where in the meantime significant payoff losses are sustained. This could partially be mitigated by introducing temporal forgiveness into the learning algorithm.

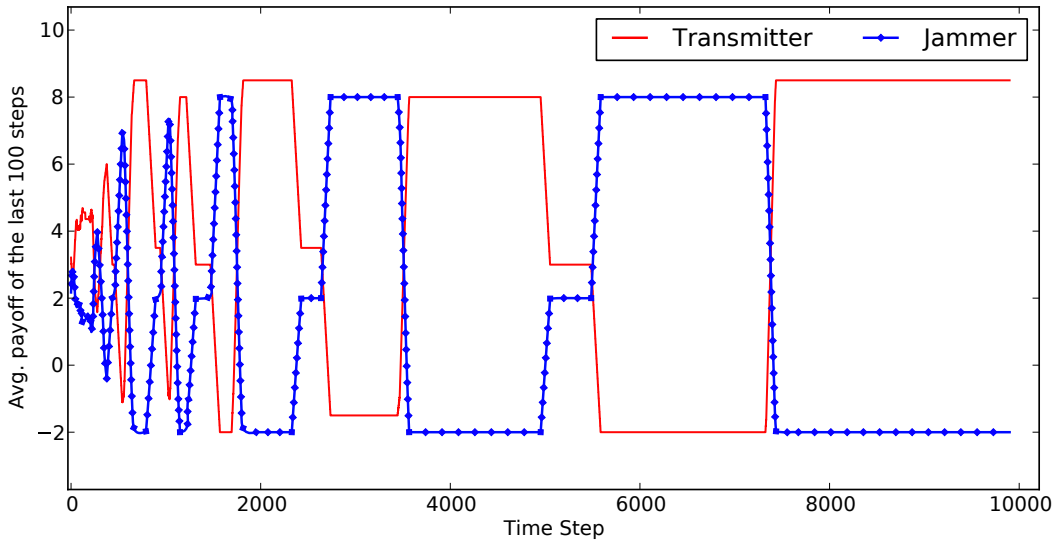


Figure 7.3: Expected payoff over time for the greedy decisioning policy and payoff-based adaptive play learning algorithm.

7.2.5.2 Stochastically sampled decisioning policy

Another common approach to this issue is choosing a stochastically sampled policy (also known as ϵ-greedy policy, [21]) where, at each step, a randomly sampled action is taken with a probability p. We propose a variation of the stochastically sampled policy where sampling is performed by scaling the expected payoff value of each action to the minimum possible payoff for the game. For a minimum payoff $PMIN$ and n

actions with expected payoffs $\overline{P(1)} \ldots \overline{P(n)}$, the probability of choosing an action d is given by (7.22):

$$p(d) = \frac{\overline{P(d)} - PMIN}{\sum_{k=1}^{n} \overline{P(k)} - PMIN} \tag{7.22}$$

7.2.6 Experimental setup

In order to infer the parameters related to the occurrence of jamming, and to be able to extract the physical parameters relevant for the game, a set of experiments using the test bed architecture described in Chapter 4 is performed.

The measurements and parameters relevant for the constructed game are:

- Impact of interference on the quality of communication link;
- Transmission powers;
- Battery life of the HHs for varying transmission powers;
- Number of considered channels;
- Time needed to perform frequency hopping;
- Spectrum sensing time;
- Spectrum sensing detection accuracy.

The connection between the HandHelds (HHs) is established using the Soldier Broadband Waveform (SBW). The waveform's bandwidth is 1.3 MHz, and channel spacing is 2 MHz – large enough to disregard the influence of potential energy spillover between adjacent channels. Experiments are done at 300 MHz central carrier frequency.

Interference is created by injecting a single-tone signal onto the central carrier frequency of the HHs. To measure the impact of interference, a set of Bit Error Rate (BER) tests was performed for varying levels of transmission power and different levels of interference. Results for three discrete values of transmission power: -12 dBW, 4 dBW and 7 dBW respectively, are presented in Figure 7.4. By setting the threshold for the communication failure at BER=10^{-1}, corresponding interference powers needed to achieve the target BER for the observed values of transmission powers are found, equaling to: 1, 6, and 9 dBW, respectively.

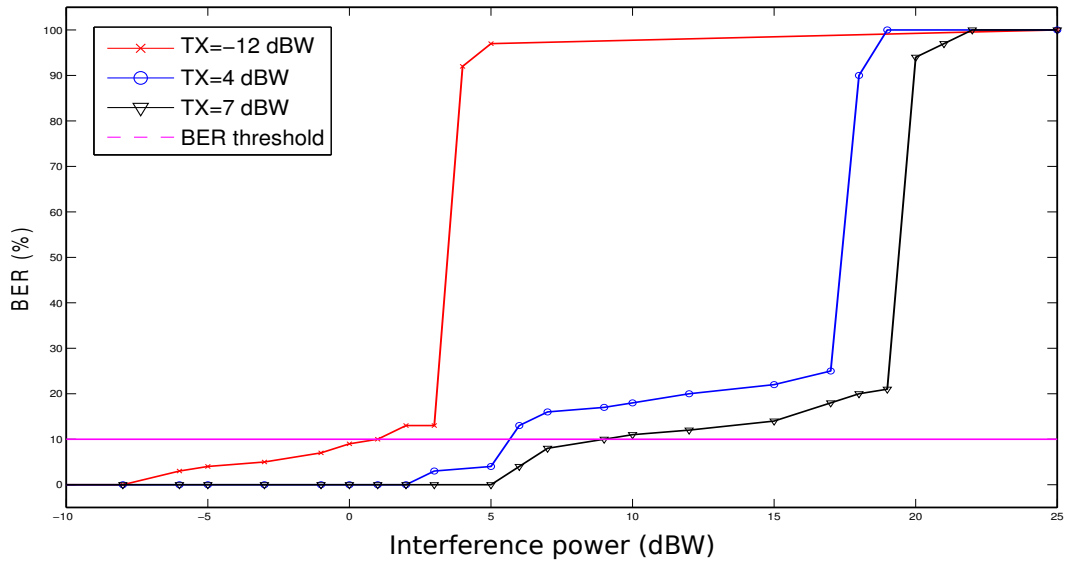


Figure 7.4: SINR vs BER

Details on the implementation of the spectrum sensing are given in Chapter 4, whereas details regarding all the data processing are presented in Chapter 6. In summary, the whole data processing part currently lasts around 0.2s, making the whole spectrum sensing cycle last approximately 1.3s.

HH's battery time for states of continuous packet data stream (packets are generated by the BER test function) are measured for the identified relevant values of the transmission power of -12, 4, and 7 dBW, equaling to 120, 94, and 90 min, respectively. The results for the relevant transmission powers of the supposed jammer were then linearly interpolated from the aforementioned, equaling to 99, 92, and 87 min, respectively.

The relevant parameters are summarized in Table 7.1.

Table 7.1: Overview of the inferred parameters relevant for the game

	Transmitter	**Jammer**
Considered frequencies [MHz]	(300, 302.65, 305.3)	(300, 302.65, 305.3)
Transmitting powers [dBW]	(-12, 4, 7)	(1, 6, 9)
Battery life for TX powers [min]	(120, 94, 90)	(99, 92, 87)
Spectrum sensing time [s]	1.3	1.3
Frequency hopping time [s]	0.3	0.3
Signal detection accuracy [%]	(50,70,90,100)	(50,70,90,100)

7.3 Results and major findings

Starting from the general expressions for the payoffs of the transmitter and the jammer given in Equations (7.1) and (7.2), a short discussion is offered on the interpretation of the parameters measured in the previous section and the feasibility of their application to the proposed game. The discussion is followed by the simulation results.

7.3.1 Adaptation of the measured parameters to the proposed game

One of the principal problems with introducing the experimental parameters in the theoretical model is the method of aligning the parameters with different units (namely, Watts and seconds), used in the equations (7.1) and (7.2). The first and the second term represent the transmission (jamming) reward and penalty, which may be defined arbitrarily. For the simulation purposes, we define them as $R = 1$ and $X = -R$ respectively.

Hopping cost, the third term of the equation, can be expressed as a function of the reward. If the hopping is performed and the transmission is successful, the final utility is decreased by the hopping cost, denoted as $Rh\alpha\beta$. Here, $h = \frac{0,3}{1,3}$ is the proportion of the time step where the transmission is not taking place due to the hopping process. An increase of the transmission power, conversely, directly influences battery life. For this purpose, transmission cost may be described as a function of battery life of the radio, as denoted in (7.23). Maximum battery life corresponds to the minimum transmission power of $-12dBW$, and equals to $Bmax = 120$ minutes. Transmission costs of higher transmission powers are then scaled with respect to this value.

$$g(C) = R\left(1 - \frac{B(C)}{Bmax}\right) \tag{7.23}$$

Finally, for each step s, expression (7.1) may be re-written as (7.24) and expression (7.2) as (7.25) for the transmitter and the jammer, respectively.

$$\begin{aligned} P^T &= R^T\alpha - R^T(1-\alpha) - R^T h\alpha\beta - R\left(1 - \frac{B(C_s^T)}{Bmax}\right) \\ &= R^T\left(\alpha(2 - H\beta) + \frac{B(C_s^T)}{Bmax} - 2\right) \end{aligned} \tag{7.24}$$

$$
\begin{aligned}
P^J &= R^J(1-\alpha) + R^J\alpha - R^J h\gamma(1-\alpha) - R^J\left(1 - \frac{B(C_s^J)}{Bmax}\right) \\
&= R^J\left(H\gamma(\alpha-1) + \frac{B(C_s^J)}{Bmax}\right) \qquad (7.25)
\end{aligned}
$$

Following the experiments denoted in Figure 7.4, the occurrence of jamming in step s for the three couplets of transmission powers $C^T = (-12, 4, 7)$ and $C^J = (1, 6, 9)$ can be defined as (7.26). An overview of the adapted parameters is given in Table 7.2.

$$
\alpha = \begin{cases} 1 & \text{if } T_s > J_s \text{ or } f_s^T \neq f_s^J \\ 0 & \text{if } T_s \leq J_s \text{ and } f_s^T = f_s^J. \end{cases} \qquad (7.26)
$$

Table 7.2: Overview of the parameters adapted to the game

	Transmitter	**Jammer**
R	1	1
h	$\frac{0.3}{1.3}$	$\frac{0.3}{1.3}$
g(C)	$0, \frac{94}{120}, \frac{90}{120}$	$\frac{99}{120}, \frac{92}{120}, \frac{87}{120}$
Default prob. of misdetection [%]	0	0

7.3.2 Simulation results

In this section, we analyze the performance of the considered learning algorithms under the proposed game and compare it to the computed Nash equilibrium. All the games are constructed using the parameters denoted in Table 7.2, unless indicated otherwise. Default number of simulation steps is 10,000. Each simulation is repeated 100 times, and the points are averaged. It has been verified that each pair of the constructed payoff matrices satisfy condition (7.15), guaranteeing uniqueness of a completely mixed Nash equilibrium. In several games, a comparison with the player whose strategy is fully randomized, i.e., whose taken actions are irrespective of his observations, is performed.

Figure 7.5 shows the percentage of occurrences of successful jamming for different dimensions of the players' action sets, from games with one channel and one transmission power, to four channels and three transmission powers. In all games, the transmitter is deploying fictitious play learning, whereas the jammer is alternating

between fictitious play (full lines) and random strategy (dashed lines). Benefit of having the learning algorithm for the jammer is particularly prominent for the low-dimensional games, where the transmitter is able to adapt to any static strategy of the jammer (including fully randomized) and start exploiting it significantly.

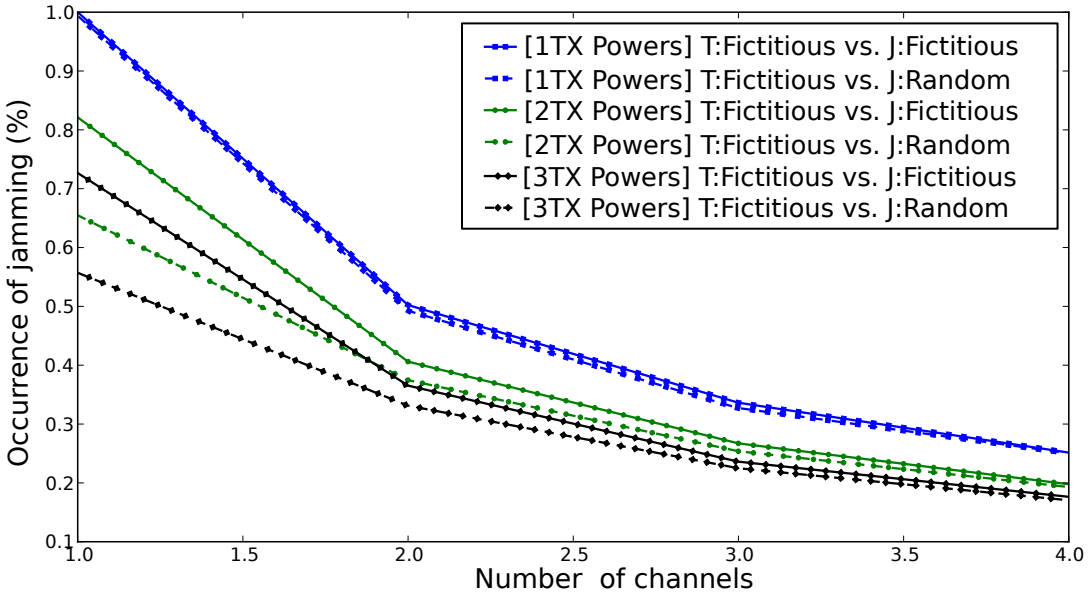


Figure 7.5: Number of jamming occurrences while the number of channels increases

To verify the importance of spectrum sensing capabilities corresponding to the fictitious play learning algorithm, we propose the analysis of the overall utility of each player when the opponent is utilizing payoff-based adaptive play. Furthermore, in order to understand how the spectrum sensing accuracy affects the performance, we consider a spectrum sensing mechanism with a certain probability of misdetection. For the simplicity of analysis, we disregard the fact that the misdetection probability realistically depends on the instantaneous Signal to Interference and Noise Ratio (SINR). Figures 7.6 and 7.7 show the results of these simulations for the transmitter and the jammer, respectively. In the left side of the figures, the overall payoff obtained during the game for each player is shown. For the visualization purposes, a trend is removed in the right side of the figures.

From Figure 7.6, it is evident that the compared schemes perform almost equally – regardless of the misdetection probability – for the transmitter. This points to the conclusion that the optimal strategy of the transmitter under the considered game when the jammer is endowed with the learning algorithm is not too far from "random". Conversely, Figure 7.7 demonstrates once again the significance of the

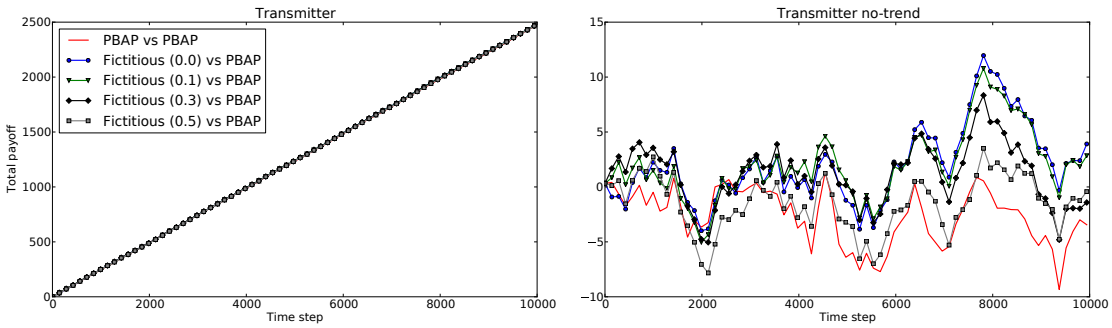


Figure 7.6: Overall payoff of the transmitter with different probabilities of misdetection

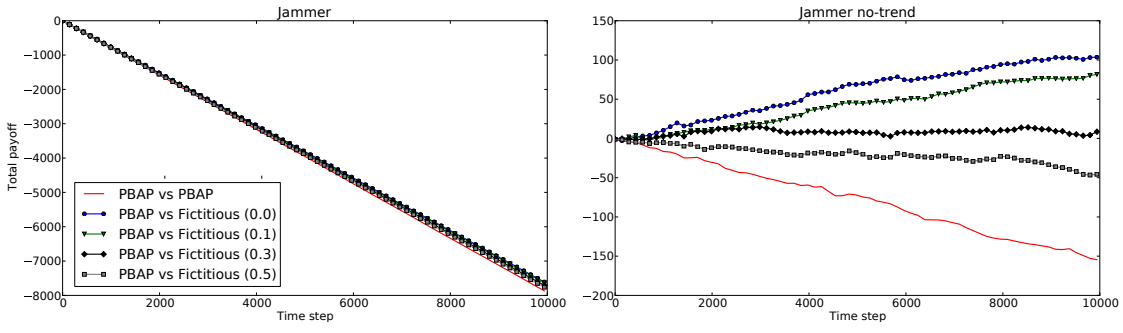


Figure 7.7: Overall payoff of the jammer with different probabilities of misdetection

spectrum sensing for the jammer side, as its overall payoff is significantly higher when utilizing fictitious play, compared to payoff-based adaptive play, even for sub-optimal spectrum sensing mechanisms (mechanisms with higher probabilities of misdetection).

In order to study this occurrence in more detail and in order to facilitate the comparison, we next present these results in the forms of normal distributions. Figure 7.8 shows performance of the transmitter using PBAP learning algorithm in the upper part and fictitious play in the bottom part, for different learning algorithms of the jammer. Similarly, Figure 7.9 shows performance of the jammer employing PBAP learning algorithm in the upper part and fictitious play in the bottom part, for different learning algorithms of the transmitter. The title of each subplot denotes the learning algorithm utilized by the observed player while colors of the lines are used to differentiate between the learning strategies of the opponent.

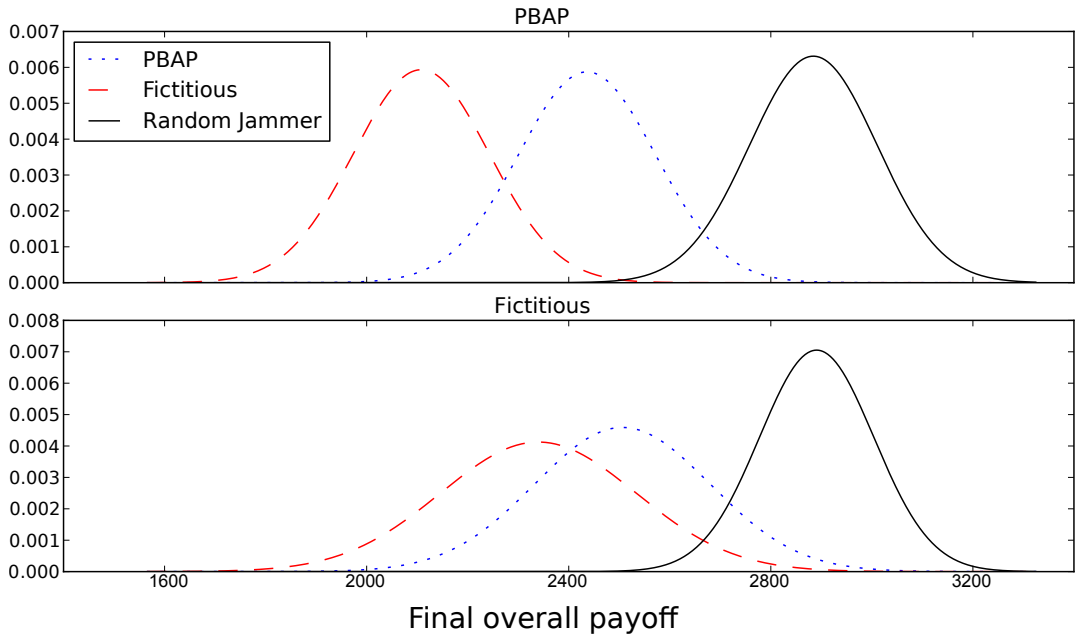


Figure 7.8: Difference in the overall payoff for the transmitter under different learning policies.

The results verify that the performance of the transmitter is very similar while using PBAP (top part) and fictitious play (bottom part). The exception is the case when the jammer employs fictitious learning. In this case, transmitter will benefit slightly more by also deploying fictitious play in order to infer the jammer's strategy as soon as possible. The results for the jammer confirm our intuition - significantly better results for both cases are obtained using fictitious play.

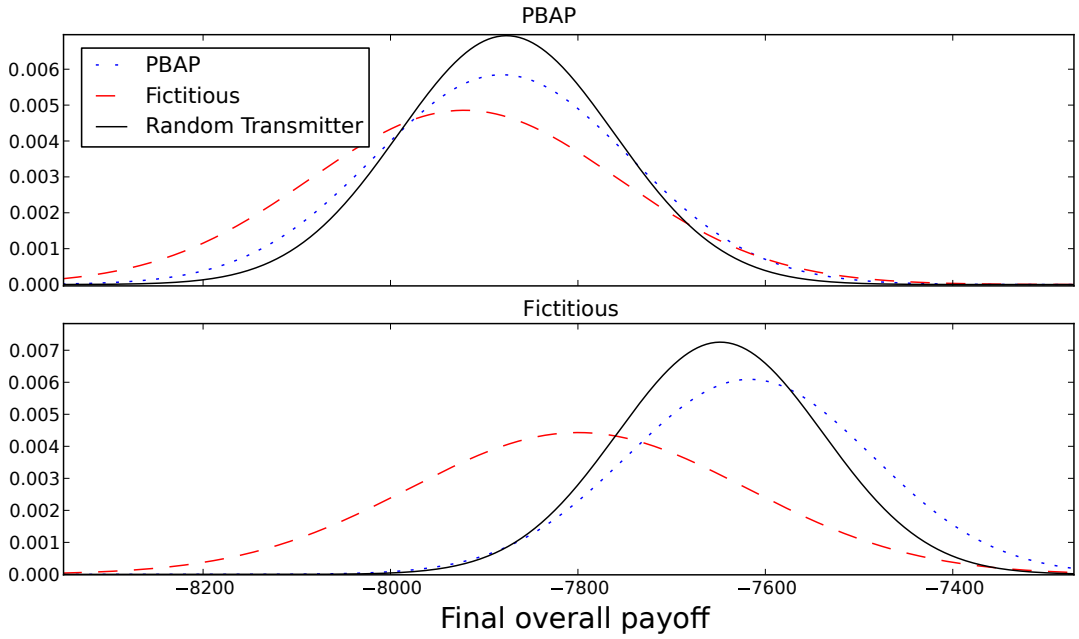
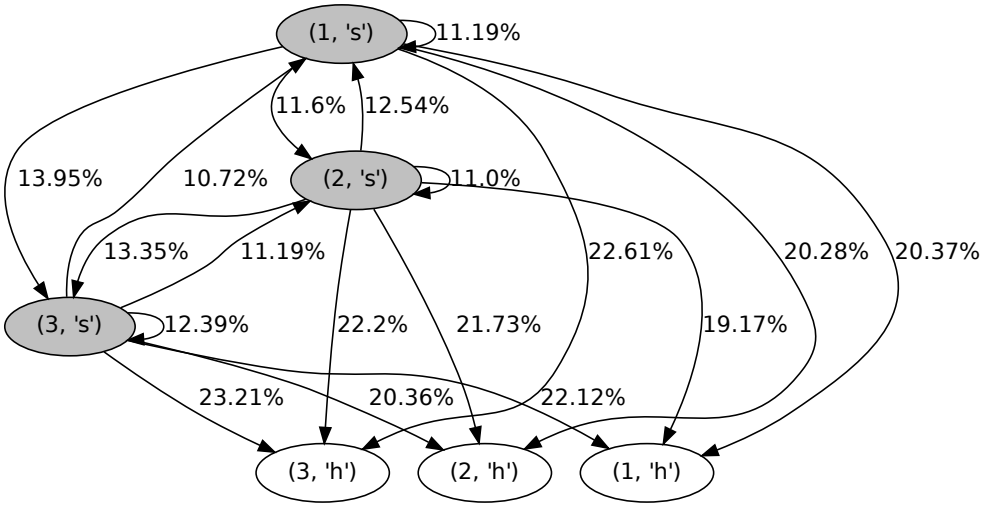


Figure 7.9: Difference in the overall payoff for the jammer under different learning policies.

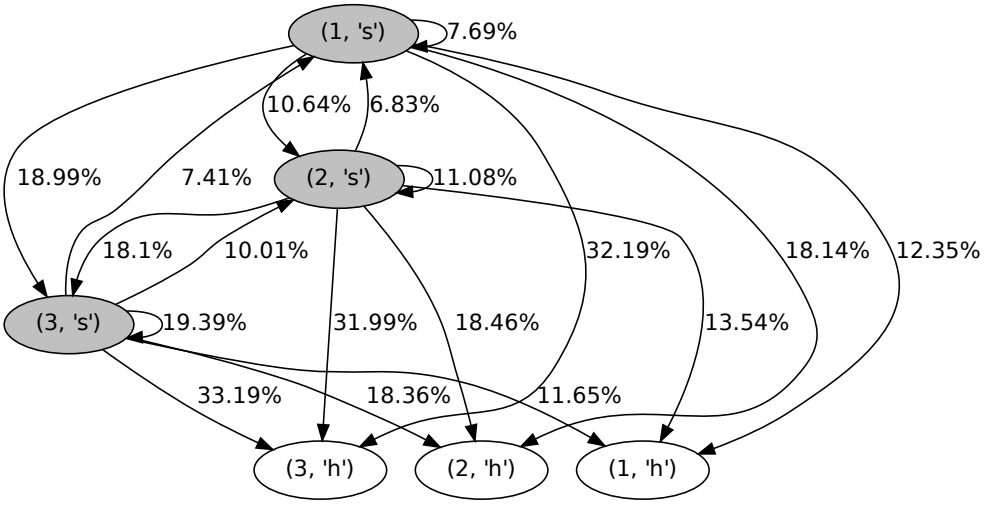
Next, we aim to show how evolution of the game is influenced when the parameters of the game are modified. As explained previously, the state/action space of the players can be depicted by Markov chains, where each Markov state represents the current state of the player, and each edge the probability of taking an action leading to the new state. A graphical representation of the Markov transition probabilities is difficult to interpret for the full set of states of high-action-space games (higher than 2×2). Some examples of the full Markov chains for small action spaces were presented by Dabcevic et al. [5]. This problem can partially be alleviated by creating state-grouped Markov chains, as shown in Figure 7.10a,b. Here, the number refers to the ordinal number of transmission power (i.e., '1'=−12 dBW for the transmitter, '1'=1 dBW for the jammer, etc.). Actions pertaining to frequency hopping are grouped and marked as 'h', while actions of staying on the same frequency are marked as 's'.

Then, the simulations are done for two extreme values of the hopping cost: 0.01 and 1.3, while keeping all other parameters the same. Figure7.11a,b shows the differences in final stochastic distributions of the transmitter's strategies. As expected, evident trend of the learning algorithm focuses on placing more importance on action 's' as the hopping cost increases.

Stochastic distributions of the mixed strategy Nash equilibrium for the transmitter and the jammer under the default game parameters may be shown in the form of the

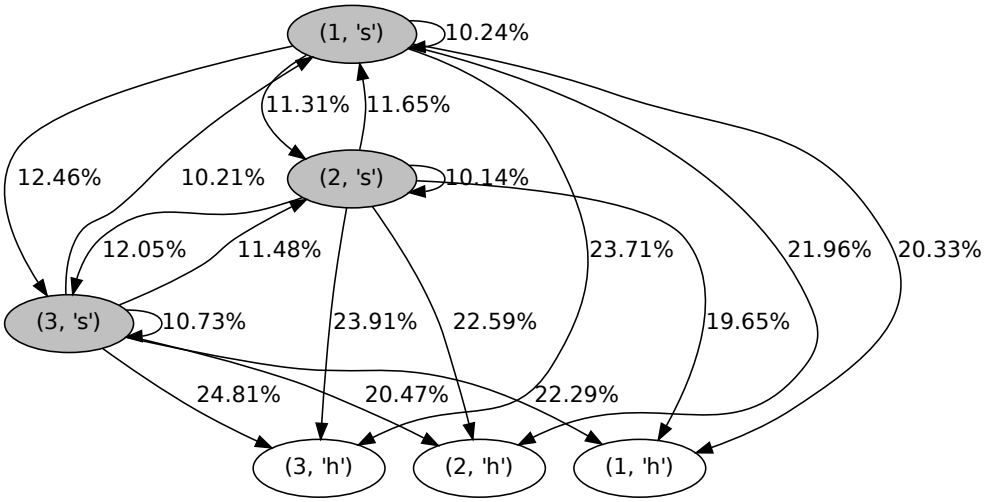


(a) PBAP - Transmitter

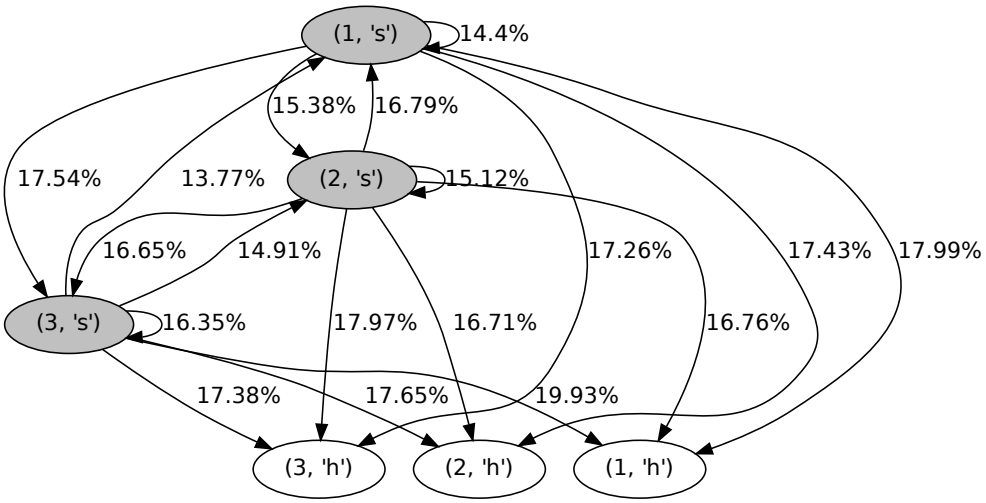


(b) Fictitious - Jammer

Figure 7.10: State-grouped Markov chain with the default parameters.



(a) PBAP - Transmitter (0.01 cost of hopping)



(b) PBAP - Transmitter (1.3 cost of hopping)

Figure 7.11: State-grouped Markov chain for different hopping cost

state-grouped Markov chains as well, as done in Figure 7.12a,b.

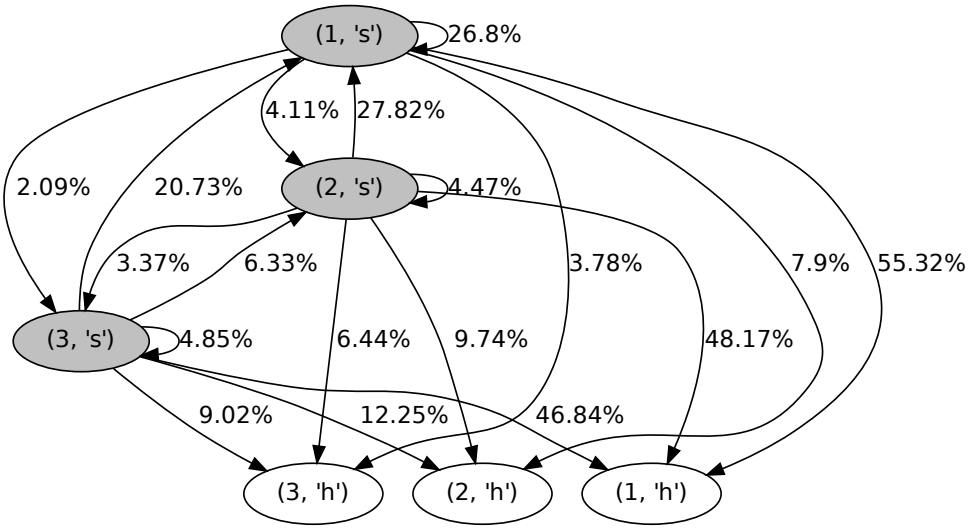
Finally, we perform the evaluation of the convergence to Nash equilibrium in terms of overall payoff for the considered learning algorithms.

Figure 7.13 shows the convergence to Nash equilibrium in terms of payoff for fictitious play. Here, the red line shows the payoff obtained when both players are playing Nash equilibrium strategies. Blue line shows the case when the transmitter is playing the Nash strategy, and the jammer is deploying fictitious play. As can be seen for the jammer in the bottom part of the figure, fictitious play is able to obtain performance nearly as good as the strategy played in Nash equilibrium, when the opponent is playing according to Nash strategy. Similar conclusions, although once again less prominent, may be drawn from the upper part of the figure for the transmitter playing fictitious play, and the jammer playing according to Nash equilibrium. The results are compared to the flow of the game when both players are playing according to fictitious play (black line). The results are in line with those presented by Conitzer [4]: fictitious play indeed seems to converge in payoff to ϵ-equilibrium.

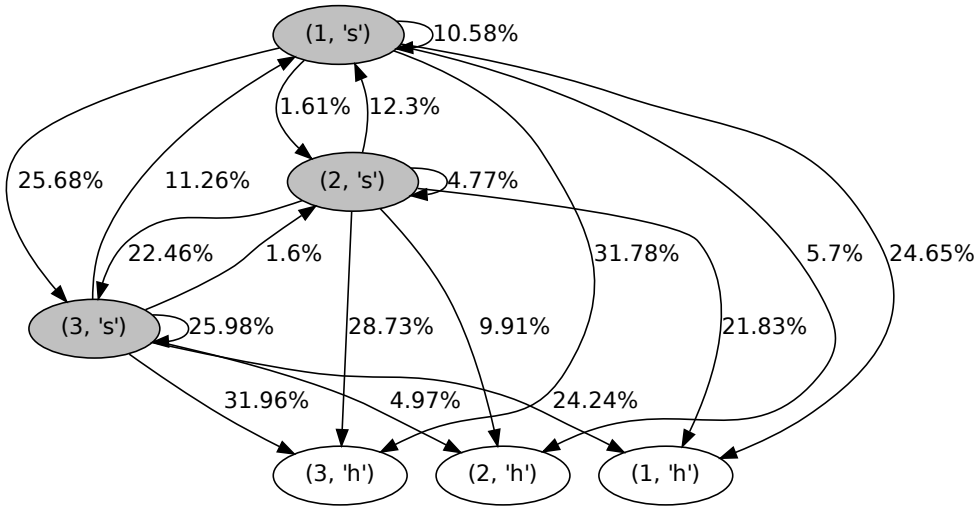
Similar results are obtained for the PBAP when faced against the Nash strategy. Figure 7.14 shows the convergence comparison for the jammer.

7.4 Conclusions

This chapter has introduced game theory as a tool for analyzing jamming/anti-jamming problems between intelligent entities. A Cognitive Radio stochastic jamming/ anti-jamming game between two players was modelled. Increased action space of the anti-jamming algorithm was created by combining power alteration and channel hopping. Two learning algorithms were considered: payoff-based adaptive learning corresponding to radios without spectrum sensing capabilities and fictitious play which may be utilized by the spectrum sensing radios. In addition to their performance, their convergence properties to Nash equilibrium in terms of overall payoff and empirical distributions of the strategies were studied. In order to narrow the gap between the theoretical constraints inherent to game theory and practical aspects of the communication systems, relevant parameters for the game were inferred by performing a set of experiments using the real-life Software Defined Radio test bed. The major finding is the importance of the spectrum sensing endowment for the jamming side, compared to relatively insignificant benefits for the transmitting side in proactive anti-jamming games. In addition, evolution dynamics for different game parameters were presented.



(a) Nash - Transmitter



(b) Nash - Jammer

Figure 7.12: State-grouped Markov chain for transmitter and jammer playing Nash equilibrium strategies

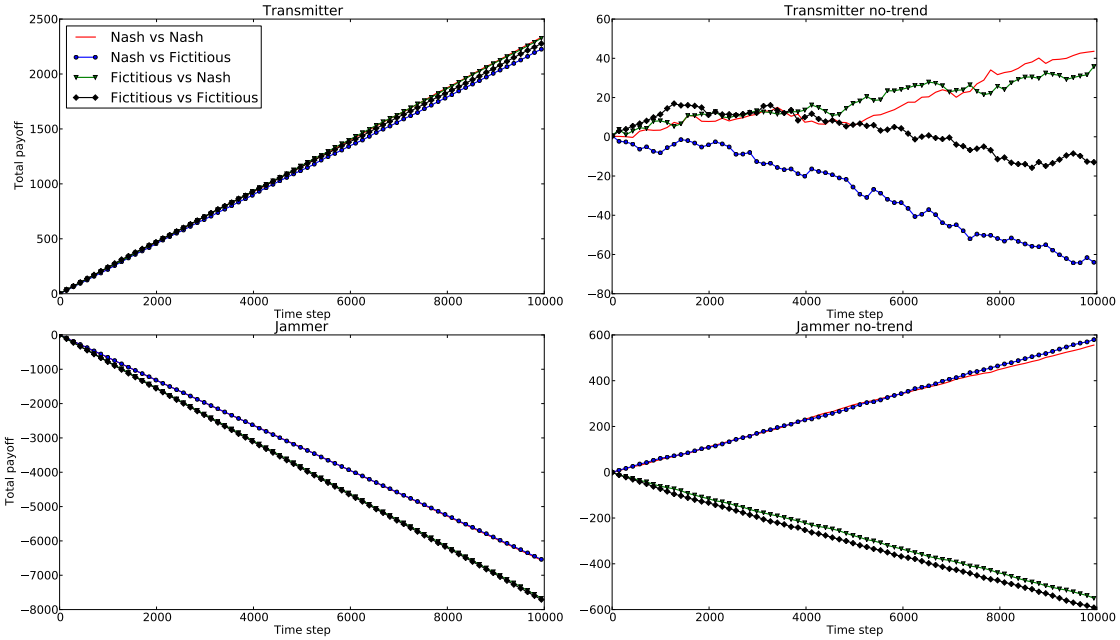


Figure 7.13: Comparison of fictitious play to Nash equilibrium strategy.

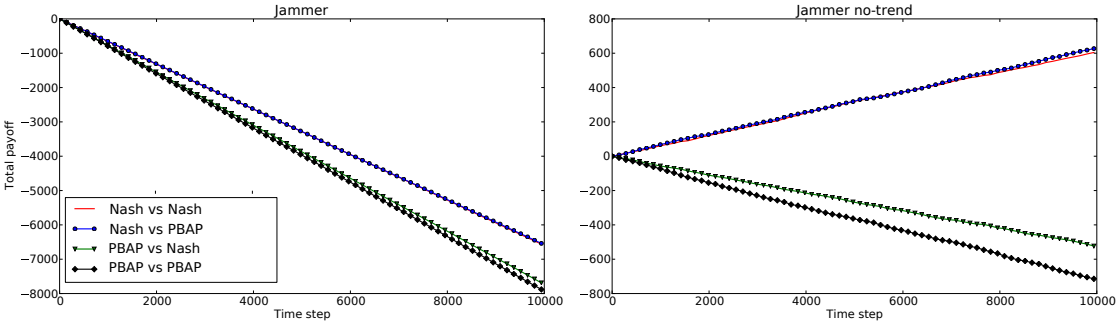


Figure 7.14: Comparison of PBAP to Nash equilibrium strategy.

Deployment of feature detectors is a logical next step in the arms race between the narrowband jammers and the anti-jamming systems. However, introduction of the additional parameters under the currently proposed framework would increase the action space to the point of infeasibility for analysis. For this purpose, future work will focus on finding ways for clusterizing overly complex action spaces and further optimizing their graphical representations by the means of state-grouped Markov chains.

Bibliography

[1] B. Banerjee and J. Peng. Efficient no-regret multiagent learning. In *Proceedings of the 20th National Conference on Artificial Intelligence - Volume 1*, AAAI'05, pages 41–46, Pittsburgh, Pennsylvania, 2005. AAAI Press.

[2] L.E.J. Brouwer. Über abbildung von mannigfaltigkeiten. *Mathematische Annalen*, 71(1):97–115, 1911.

[3] R. Cominetti, E. Melo, and S. Sorin. A payoff-based learning procedure and its application to traffic games. *Games and Economic Behavior*, 70(1):71 – 83, 2010. doi: http://dx.doi.org/10.1016/j.geb.2008.11.012. Special Issue In Honor of Ehud Kalai.

[4] V. Conitzer. Approximation guarantees for fictitious play. In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing*, Allerton'09, pages 636–643, Piscataway, NJ, USA, 2009. IEEE Press.

[5] K. Dabcevic, A. Betancourt, L. Marcenaro, and C.S. Regazzoni. A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios. In *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pages 8158–8162, May 2014. doi: 10.1109/ICASSP.2014.6855191.

[6] K. Dabcevic, A. Betancourt, L. Marcenaro, and C.S. Regazzoni. Intelligent cognitive radio jamming - a game-theoretical approach. *EURASIP Journal on Advances in Signal Processing*, 2014. doi: 10.1186/1687-6180-2014-171.

[7] C. Daskalakis, P.W. Goldberg, and C.H. Papadimitriou. The complexity of computing a nash equilibrium. In *Proceedings of the Thirty-eighth Annual ACM*

Symposium on Theory of Computing, STOC '06, pages 71–78, New York, NY, USA, 2006. ACM. doi: 10.1145/1132516.1132527.

[8] C. Daskalakis, R. Frongillo, C.H. Papadimitriou, G. Pierrakos, and G. Valiant. On learning algorithms for nash equilibria. In *Proceedings of the Third International Conference on Algorithmic Game Theory*, SAGT'10, pages 114–125, Berlin, Heidelberg, 2010. Springer-Verlag.

[9] R.D. McKelvey, A.M. McLennan, and T. L. Turocy. Gambit: Software tools for game theory, version 13.1.2. `http://www.gambit-project.org`, 2014.

[10] J.F. Mertens and A. Neyman. Stochastic games. *International Journal of Game Theory*, 10(2):53–66, 1981. doi: 10.1007/BF01769259.

[11] I. Milchtaich and T. Ostrowski. On some saddle point matrices and applications to completely mixed equilibrium in bimatrix games. *International Journal of Mathematics, Algebra and Game Theory*, 18(2), 2008.

[12] J. Nash. Non-cooperative games. *Annals of Mathematics*, 54(2):pp. 286–295, 1951.

[13] G. Ostrovski and S. van Strien. Payoff performance of fictitious play. *Journal of Dynamics and Games*, 1(4):621–638, 2014. doi: 10.3934/jdg.2014.1.621.

[14] G. Owen. *Game Theory*. Academic Press, San Diego, CA, USA, 3rd edition, 1995.

[15] R. Poisel. *Modern Communications Jamming: Principles and Techniques*. Artech House intelligence and information operations series. Artech House, Norwood, 2011.

[16] J. Robinson. An iterative method of solving a game. *Annals of Mathematics*, 54 (2):pp. 296–301, 1951.

[17] J.S. Shamma and G. Arslan. Dynamic fictitious play, dynamic gradient play, and distributed convergence to nash equilibria. *Automatic Control, IEEE Transactions on*, 50(3):312–327, March 2005. doi: 10.1109/TAC.2005.843878.

[18] L.S. Shapley. A note on the lemke-howson algorithm. In M.L. Balinski, editor, *Pivoting and Extension*, volume 1 of *Mathematical Programming Studies*, pages 175–189. Springer, Springer Berlin Heidelberg, 1974. doi: 10.1007/BFb0121248.

[19] B. Von Stengel. Chapter 45 computing equilibria for two-person games. In R. Aumann and S. Hart, editors, *Handbook of Game Theory with Economic Applications*, volume 3, pages 1723–1759. Elsevier, 2002. doi: http://dx.doi.org/10.1016/S1574-0005(02)03008-4.

[20] R.S. Sutton and A.G. Barto. *Introduction to Reinforcement Learning*. MIT Press, Cambridge, MA, USA, 1st edition, 1998.

[21] M. Tokic. Adaptive ϵ -greedy exploration in reinforcement learning based on value differences. In R Dillmann, J Beyerer, U Hanebeck, and T Schultz, editors, *KI 2010: Advances in Artificial Intelligence*, volume 6359, pages 203–210. Springer Berlin Heidelberg, Karlsruhe, 2010. Lecture Notes in Computer Science.

[22] B. Von Stengel. New maximal numbers of equilibria in bimatrix games. *Discrete & Computational Geometry*, 21(4):557–568, 1999.

[23] K. Wang, Q. Liu, and L. Chen. Optimality of greedy policy for a class of standard reward function of restless multi-armed bandit problem. *Signal Processing, IET*, 6(6):584–593, 2012. doi: 10.1049/iet-spr.2011.0185.

Chapter 8

Conclusions and future developments

Radio Frequency (RF) jamming is defined as illicit RF transmission aimed at disabling the communication on the targeted system. Cognitive Radio is a radio that is RF-aware, and is able to autonomously reconfigure its transmission parameters in order to improve its efficiency. When Cognitive Radios are used in the domain of the jamming and anti-jamming systems, such systems are considered intelligent. This thesis has studied the impact of Cognitive Radios in the domain of the intelligent jamming and anti-jamming solutions. It has presented practical solutions and concrete ideas to help move the current tactical battlefield solutions beyond the state of the art.

8.1 Summary of contributions and major findings

Main contributions of the thesis are summarized as follows:

- A comprehensive overview of the main security issues related to Cognitive Radios was presented. Main identified threats to Cognitive Radio systems were Primary User Emulation attacks, Byzantine attacks, Objective Function attacks, and intelligent jamming attacks. In addition, Cognitive Radios that are built on a Software Defined Radio (SDR) architecture inherit the corresponding security issues related to SDR technology. Furthermore, they are susceptible to many of the threats associated with legacy radio systems, which mainly stem out from the open nature of the wireless medium.

- An SDR/Cognitive Radio test bed architecture able to operate in VHF and UHF parts of the frequency band was implemented. The architecture was comprised of military SDRs, computationally powerful embedded systems in charge of

signal processing, and several off-the-shelf components and auxiliaries. The architecture was designed to allow for real-time testing and validating of all relevant developed algorithms.

- An intelligent self-reconfigurable system for jamming mitigation was proposed. The system was deployed and tested on the aforementioned SDR/Cognitive Radio architecture. The algorithm exhibited high level of accuracy in recognizing relevant RF spectrum activities, and was able to execute itself in real time.

- A game-theoretical approach to formalizing intelligent jamming and anti-jamming problems was proposed. Major results included the analysis of importance of spectrum sensing endowment for jamming and anti-jamming Cognitive Radio systems.

8.2 Future developments

The work presented in this thesis opened several interesting future research topics. The most important ones are summarized as follows:

- One of the bottlenecks of the Spectrum Intelligence for Interference Mitigation algorithm is low spectrum resolution. Performed analysis of the compressed spectrum sensing techniques indicated that sub-Nyquist sampling could be a remedy for this problem. Compressed spectrum sensing is currently deployed in the processing stage of the algorithm, however future modifications will see it deployed in the pre-processing stage, i.e., prior to buffering and outputting the spectrum samples to the external module in charge of signal processing.

- One of the security issues of all self-reconfigurable entities that rely on machine learning mechanisms is the possibility that the entity gets deceived into learning incorrect patterns. In the Cognitive Radio domain, this is know as the Objective Function attack. Furthermore, the system could make erroneous assumptions due to the imperfections related to its sensors, or the software flaws of the learning system itself. As a result, system may take sub-optimal actions that may seriously degrade overall performance. This introduces the motivation for cognitive refinement of the mechanism by learning from the human operator in the loop. For the Spectrum Intelligence algorithm, a graphical user interface that allows the human operator to override the decisions of the algorithm was developed. Future work will focus on finding methods that would allow the

algorithm to refine its reasoning process by learning from the actions of the human operator.

- The proposed game-theoretical approach is modeled using the parameters obtained experimentally from the assembled test bed architecture. Future work will include testing the proposed game-theoretical scheme using the developed test bed architecture in real-time, and comparing the results with those obtained from the simulations.

Abbreviations

AD Analog-to-Digital
ADC Analog-to-Digital Converter
AES Advanced Encryption Standard
AKA Authentication and Key Agreement
AM Amplitude Modulation
ANN Artificial Neural Network
AWGN Additive White Gaussian Noise
BEE2 Berkeley Emulation Engine
BER Bit Error Rate
BP Basis Pursuit
BPSK Binary Phase Shift Keying
BS Base Station
CCC Common Control Channel
CODEC Coder-Decoder
CS Compressed Sensing
DAC Digital-to-Analog Converter
DC Direct Current
DoS Denial of Service
DSA Dynamic Spectrum Access
DSP Digital Signal Processor
DSS Dynamic Spectrum Sharing
EAP Extensible Authentication Protocol
EMCON Emissions Control
FM Frequency Modulation
FPGA Field Programmable Gate Array
FSK Frequency Shift Keying
GPP General Purpose Processor
GPRS General Packet Radio Service
GPS Global Positioning System
GSM Global System for Mobile Communications
GTK Group Temporal Key
GUI Graphical User Interface
HH Handheld
ICNIA Integrated Communications, Navigation, and Identification Architecture
IEEE Institute of Electrical & Electronic Engineers
IF Intermediate Frequency
IMSI International Mobile Subscriber Identity
ISM Industrial, Scientific and Medical
ITU International Telecommunication Union
IV Initialization Vector
JSR Jamming to Signal Ratio
JTRS Joint Tactical Radio System
LH Lemke-Howson
LPD Low Probability of Detection
LPI Low Probability of Interception
LTE Long Term Evolution
MAC Media Access Control
MANET Mobile Ad-hoc NETwork
MDP Markov Decision Process

MIB Management Information Base
MIMO Multiple Input Multiple Output
MP Matched Pursuit
MS Mobile Station
NE Nash Equilibrium
NSA National Security Agency
OFA Objective Function Attack
OID Object IDentifier
OMP Orthogonal Matched Pursuit
PBAP Payoff-Based Adaptive Play
PDF Probability Density Function
PKI Public Key Infrastructure
PSK Pre-Shared Key
PSK Phase Shift Keying
PTT Push-To-Talk
PU Primary User
PUEA Primary User Emulation Attack
QoS Quality of Service
QPSK Quaternary Phase Shift Keying
RA Radio Applications
REM Radio Environment Map
RF Radio Frequency
ROE Radio Operating Environment
RSNA Robust Security Network Association
RSS Received Signal Strength
SBW Soldier Broadband Waveform
SCA Software Communications Architecture
SDR Software Defined Radio
SER Symbol Error Rate
SINR Signal to Interference plus Noise Ratio
SNMP Simple Network Management Protocol
SNR Signal to Noise Ratio
SoM System-on-Module
SPA Service Provider Applications
SRM Secure Radio Middleware
SSL Secure Socket Layer
SU Secondary User
SWAVE HH Secure Wideband Multi-role - Single-Channel Handheld
TCP Transmission Control Protocol
TKIP Temporal Key Integrity Protocol
UA User Applications
UHF Ultra High Frequency
USB Universal Serial Bus
USRP Universal Software Radio Peripheral
VGA Video Graphics Array
VHF Very High Frequency
VULOS VHF/UHF Line Of Sight
WEP Wired Equivalent Privacy
WLAN Wireless Local Area Network
WMB Wireless Microphone Beam
WPA Wi-fi Protected Access
WPA-PSK Wi-fi Protected Access Pre-Shared Key
WRAN Wireless Regional Area Network

Publications

Journal papers

- K. Dabcevic, M.O. Mughal, L. Marcenaro, and C.S. Regazzoni. Cognitive Radio as the Facilitator for Advanced Communications Electronic Warfare Solutions. Under review, *Springer Journal of Signal Processing Systems.*

- K. Dabcevic, A. Betancourt, L. Marcenaro, and C.S. Regazzoni. Intelligent Cognitive Radio Jamming – a Game-theoretical Approach. *EURASIP Journal on Advances in Signal Processing*, 2014

Conference and workshop papers

- K. Dabcevic, A. Betancourt, L. Marcenaro, and C.S. Regazzoni. A Fictitious Play-based Game-theoretical Approach to Alleviating Jamming Attacks for Cognitive Radios. *2014 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2014

- K. Dabcevic, M.O. Mughal, L. Marcenaro, and C.S. Regazzoni. Spectrum Intelligence for Interference Mitigation for Cognitive Radio Terminals. *2014 Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (WInnComm-Europe 2014)*, 2014

- M.O. Mughal, K. Dabcevic, G. Dura, L. Marcenaro, and C.S. Regazzoni. Experimental Study of Spectrum Estimation and Reconstruction based on Compressive Sampling for Cognitive Radios. *2014 Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (WInnComm-Europe 2014)*, 2014

- K. Dabcevic, L. Marcenaro, and C.S. Regazzoni. SPD-driven Smart Transmission Layer Based on a Software Defined Radio Test Bed Architecture. *Measurable security for Embedded Computing and Communication Systems (MeSeCCS 2014), within the International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014)*, 2014

- K. Dabcevic, A. Betancourt, M.O. Mughal, L. Marcenaro, and C.S. Regazzoni. A Game-theoretical Analysis of Intelligent Cognitive Radio Jamming. *Riunione Annuale 2014 dell'Associazione Gruppo nazionale Telecomunicazioni e Tecnologie dell'Informazione*, 2014

- P. Morerio, K. Dabcevic, L. Marcenaro, and C.S. Regazzoni. Distributed Cognitive Radio Architecture with Automatic Frequency Switching. *2012 IEEE Workshop on Complexity in Engineering (COMPENG2012)*, 2012

Book chapters

- K. Dabcevic, L. Marcenaro, and C.S. Regazzoni. Security in Cognitive Radio Networks. In T.D. Lagkas, P. Sarigiannidis, M. Louta and P. Chatzimisios eds., *Evolution of Cognitive Networks and Self-Adaptive Communication Systems, IGI Global*, 2013