Spring 2016

Performance Analysis of Secondary Users in Heterogeneous Cognitive Radio Network

Tanjil Amin

PERFORMANCE ANALYSIS OF SECONDARY USERS IN HETEROGENEOUS COGNITIVE RADIO NETWORK

by

TANJIL AMIN

(Under the Direction of Danda B. Rawat)

ABSTRACT

Continuous increase in wireless subscriptions and static allocation of wireless frequency bands to the primary users (PUs) are fueling the radio frequency (RF) shortage problem. Cognitive radio network (CRN) is regarded as a solution to this problem as it utilizes the scarce RF in an opportunistic manner to increase the spectrum efficiency. In CRN, secondary users (SUs) are allowed to access idle frequency bands opportunistically without causing harmful interference to the PUs. In CRN, the SUs determine the presence of PUs through spectrum sensing and access idle bands by means of dynamic spectrum access. Spectrum sensing techniques available in the literature do not consider mobility. One of the main objectives of this thesis is to include mobility of SUs in spectrum sensing. Furthermore, due to the physical characteristics of CRN where licensed RF bands can be dynamically accessed by various unknown wireless devices, security is a growing concern. This thesis also addresses the physical layer security issues in CRN. Performance of spectrum sensing is evaluated based on probability of misdetection and false alarm, and expected overlapping time, and performance of SUs in the presence of attackers is evaluated based on secrecy rates.

Index Words: Spectrum Sensing, Physical Layer Security, Cognitive Radio Networks.

PERFORMANCE ANALYSIS OF SECONDARY USERS IN HETEROGENEOUS COGNITIVE RADIO NETWORK

by

TANJIL AMIN

B.S., Bangladesh University of Engineering and Technology, Bangladesh, 2012

M.S., Georgia Southern University, 2016

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in Partial Fulfillment

of the Requirement for the Degree

MASTER OF SCIENCE

STATESBORO, GEORGIA

PERFORMANCE ANALYSIS OF SECONDARY USERS IN HETEROGENEOUS COGNITIVE RADIO NETWORK

by

TANJIL AMIN

Major Professor: Danda B. Rawat

Committee: Adel ElShahat

Mohammad Ahad

Electronic Version Approved:

May 2016

DEDICATION

This thesis is dedicated to my family

ACKNOWLEDGMENTS

First of all I wish to acknowledge the tireless help and suggestions of my research supervisor Dr. Danda B. Rawat. I am grateful to him for his continuous support and always providing me with the exact piece of words I am looking for. He not only encouraged me to understand the theoretical aspects of my research well but also helped me with the application of this knowledge into solving problems regarding my research. Besides guidance his patience and generous smile helped me a lot throughout my research. His words of advice always kept me thinking about the physics and real-world implications of my research.

I would like to thank the department of Electrical Engineering of Georgia Southern University to consider me as an eligible student for assistantship and helping me by funding my research partially.

I would also want to thank the U.S National Science Foundation (NSF) for their financial support throughout my research under CNS-1405670 grant. Any opinion, finding, and conclusions or recommendations expressed in this thesis do not necessarily reflect the views of NSF.

And lastly I will acknowledge the support of my family, specially my parents throughout my life.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. Almost all wireless communication signals need to travel through the air via radio frequency or spectrum band. Figure 1.1 shows that the useable radio frequency wave ranges from 30 kHz to 300 GHz. These full segments include VHF, UHF, and the low microwave frequencies from roughly 100 MHz to 4 GHz. That's where cell phones, broadcast TV, wireless local-area networks (LANs), and lots of popular short-range technologies like Bluetooth and Wi-Fi operate [1]. These frequency bands are used to be statically allocated to the licensed communication companies by regulatory agencies like Federal Communications Commission (FCC) in the USA.

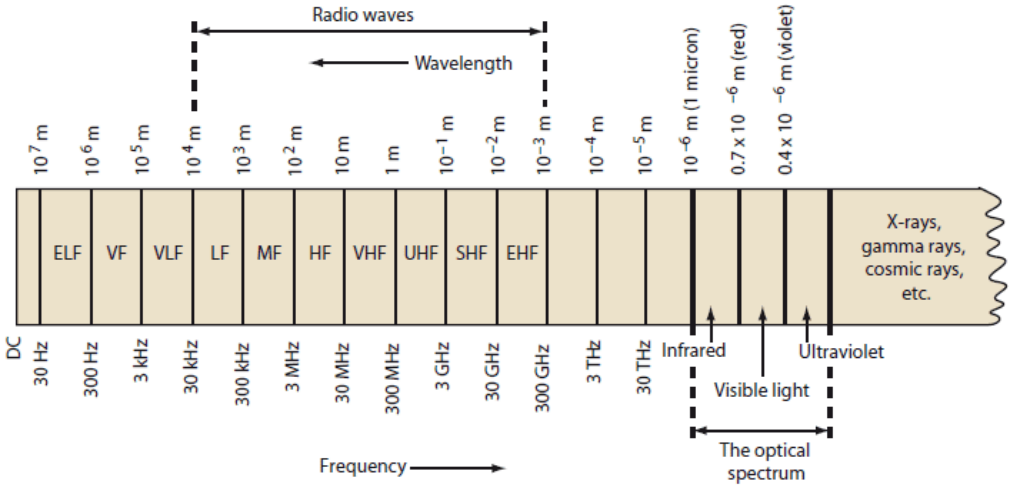


Figure 1.1: The electromagnetic frequency spectrum ranges from dc to light [1].

In the United States, the FCC regulates interstate and international communications by radio, television, wire, satellite and cable under a command-and-control model [5]. The FCC allocates frequency bands to be exclusively used for a particular service, within a given spatial region, and for a specified time duration. Figure 1.2 shows the National

Telecommunications and Information Administration's (NTIA) chart of spectrum allocation in the United States [2]. From the spectrum allocation chart it is evident that most of the usable frequencies are already allocated and that there is very little room for future innovative services. For example, in the U.S., the mobile communications spectrum (set between 0.7 and 2.6 GHz) has been completely allocated already. As a result, there is a large amount of chaos in the mobile world, with companies competing each other and panicking over the huge growth of smart-phone uses in the market. The Federal Communications Commission (FCC) has even declared a shortage of spectrum. On the other hand, Figure 1.3 shows spectrum utilization efficiency. The usage picture shows that only a small fraction (about 5%) of the spectrum is actually used. The inefficient use of spectrum due to the static and exclusive-use allocation model and continuous increase in wireless users have caused the frequency shortage problem.

The motivation of this thesis is directly related to this frequency spectrum shortage problem in wireless communication systems. It is clear from Figure 1.3 that there is a wastage in spectrum bands utilization and to prevent inefficient utilization of spectrum bands there is no better alternative to spectrum reuse. Therefore, new systems are expected to exploit the spectrum opportunities causing a minimum amount of interference to the licensed users [6]. CR networks include both licensed and unlicensed users in the system [7, 8]. The important components of the CR system concept are ability to measure, sense, learn, and be aware of the parameters related to the radio channel characteristics, availability of spectrum and power, radio's operating environment, user requirements and applications, available networks (infrastructures) and nodes, local policies and other operating restrictions. Spectrum sensing is the task of obtaining awareness about the spectrum usage and existence of primary users (PUs) in a geographical area. In CR system terminology, PUs can be defined as the users who have higher priority or legacy rights on the usage of a specific part of the spectrum. On the other hand, secondary users (SUs), which

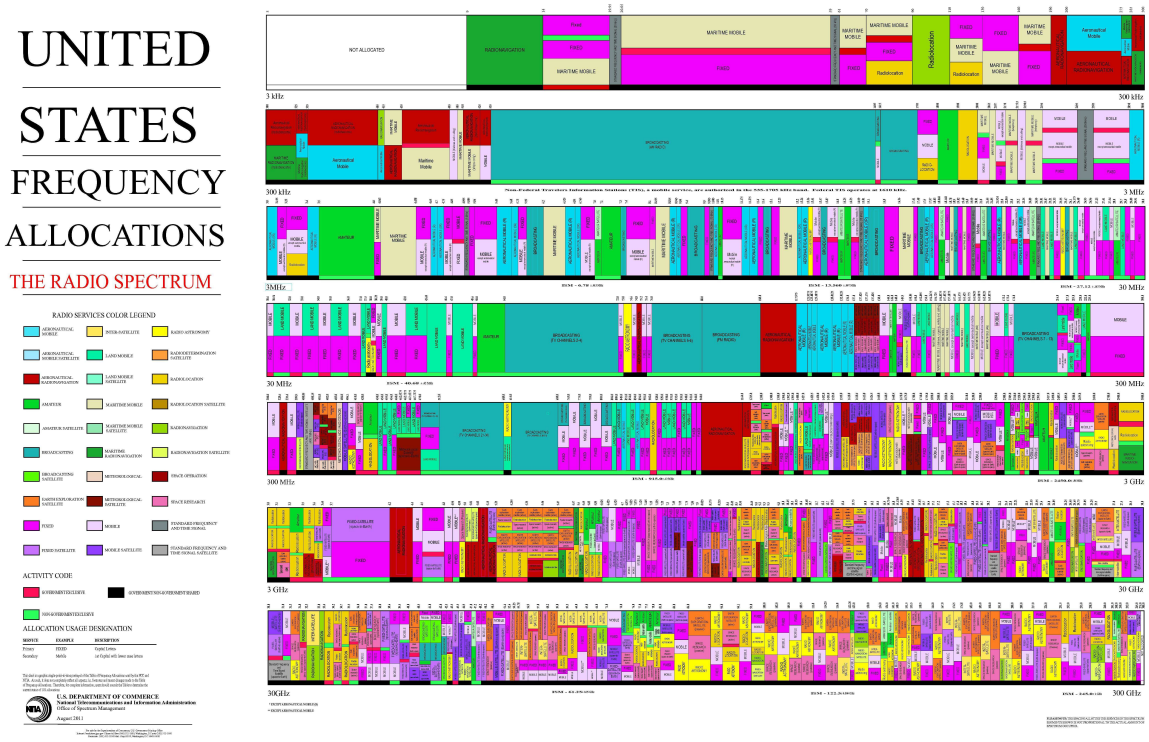


Figure 1.2: Spectrum Distribution of United States [2].

have lower priority, exploit this spectrum in such a way that they do not cause interference to PUs [9, 10]. Therefore, SUs need to have cognitive radio capabilities, such as sensing the spectrum reliably to check whether it is being used by a PU or not and to change the radio parameters to exploit the unused part of the spectrum. So whenever the unlicensed users or SUs in CR network try to set up a communication link on a particular frequency band or channel they have to make sure that no PUs are there on that channel by sensing the channel environment. Even if there are no PUs initially and the SUs have initiated the communication on that channel they have to continue sensing so that if PUs come back they can leave the channel without causing any trouble to the PUs. So it is safe to say that spectrum sensing is one of the major aspects of CR network as sensing enables the SUs to learn which channels are initially free, to sense the return of PUs on the channel later, and

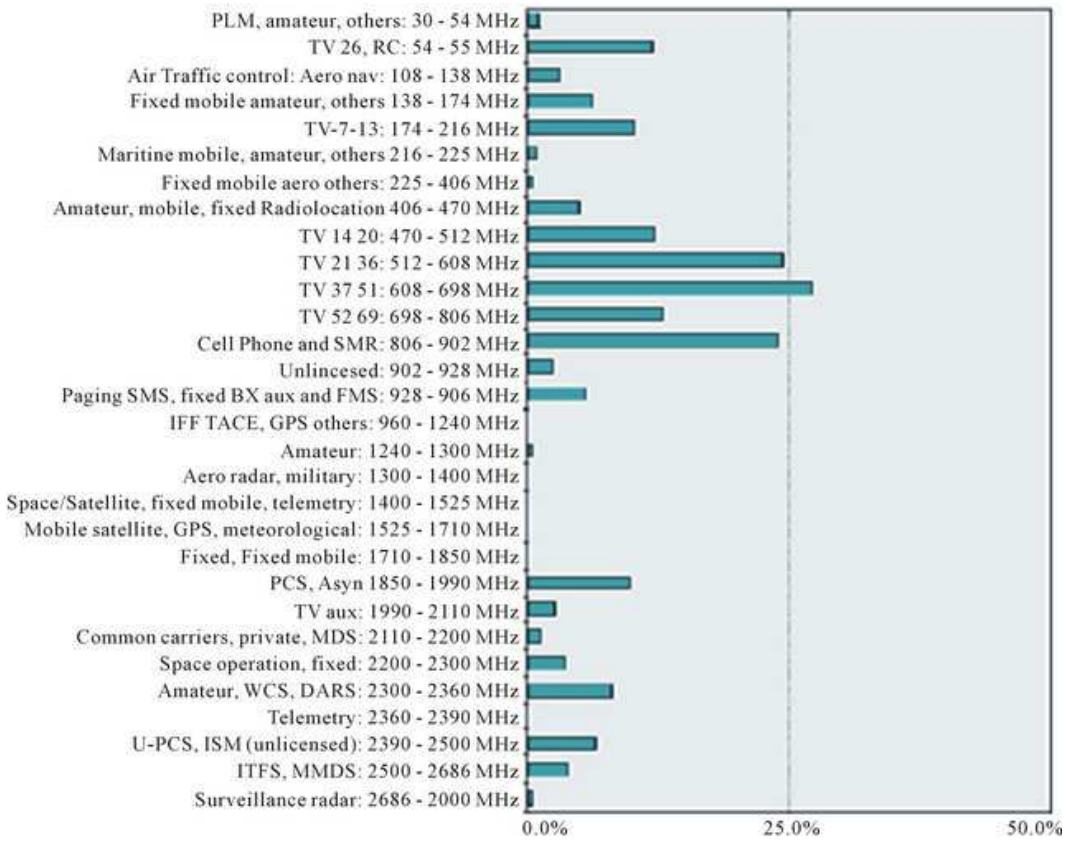


Figure 1.3: Spectrum Utilization Profile [3]

look for a new idle channel. It is important to locate a new idle channel as soon as possible so that when PUs return to a channel under SUs' utilization they can leave the channel immediately and resume their data transmission on a new channel with the least amount of interruption [11–15] to the PUs. Again mobility is one the major aspects of wireless communication system. As a result CR network needs to include mobile SUs and PUs to be truly wireless in nature. That being said, it is observed that the existing studies do not consider mobility of SUs or PUs in CR network while evaluating spectrum sensing. This motivated the research on considering SU mobility in spectrum sensing in this thesis. Another key technology used in CR network is dynamic spectrum access (DSA) which enables high utilization of the unused spectrum bands by allowing a variety of wireless subscribers

to use those under utilized bands. Undoubtedly this is the main advantage of CR network. Besides ensuring the most utilization of the under utilized bands DSA welcomes various unknown wireless devices which can in turn pose security threats to the entire network. To ensure secure communication in CR network this thesis also considers physical layer security issues in CR network. An overview of cognitive radio network is presented in the next section.

1.1 Overview of Cognitive Radio Network

The term 'Cognitive Radio' was first introduced by Joseph Mitola in an article published in 1999. There he described how a cognitive radio could increase the adaptability of personal wireless radio services through a new radio language called the radio knowledge representation language (RKRL) [8]. The idea of RKRL was further developed and advanced in Mitola's own doctoral dissertation, which was presented at the Royal Institute of Technology, Sweden, in May 2000 [7]. This dissertation presents a complete overview of CR system as an energizing multidisciplinary subject.

The FCC published a report in 2002, which was aimed at the adjustments in technology and the profound impact that those adjustments would have on spectrum policy [14]. That report set the platform for a workshop on CR system, which was held in Washington, DC, May 2003.

The depiction of CR by Mitola and Maguire in their seminal paper [7] concentrates on the radio knowledge representation language and how the CR system can upgrade the adaptability of personal wireless services. CR is formally defined by the FCC [16] as a radio that can change its transmitter parameters based on interaction with its environment. The ultimate objective of the CR system is to obtain the best available spectrum through cognitive capability and reconfigurability. Tasks required for adaptive operation are: Spectrum sensing, spectrum analysis, and spectrum decision [15, 17].

CR system [5] is defined as an intelligent wireless communication system that is aware of its surrounding environment in real-time with two primary objectives in mind: highly reliable communication whenever and wherever needed, and efficient utilization of the radio spectrum. A CR system can sense the communication environment (unused spectrum, neighboring Ad hoc wireless networks, service operators at the current location) and adapt its operating parameters (bandwidth, frequency of operation, power, modulation scheme, coding scheme). A wireless device which has cognitive radio capabilities, on the other hand, can sense the current network environment for available resources and best service offerings according to application's requirements and adapt its performance parameters according to policies and regulations [7] . For example, when a CR wireless device senses the presence of Wi-Fi and GSM systems in the surrounding along with spectrum holes in the frequency band of digital TV, it would download files from the Wi-Fi access point, perform a voice call through GSM network and communicate with other CR users using those spectrum holes. Another example of CR application is a military radio that can sense the urgency in the operator's voice and adjust QOS guarantees proportionally [18].

Two important components of CR network are the primary network and the secondary network. The primary network includes PUs and primary base station. PUs can be defined as the legal owners of certain spectrum bands and primary base station controls the access of PUs to the spectrum. The secondary network includes SUs, secondary base station and spectrum broker. SUs are the unlicensed users of spectrum bands. Secondary base station is a fixed infrastructure component with CR capabilities and provides single hop connection to SUs. Spectrum broker shares the spectrum resources among different CR networks [13, 18].

Dynamic spectrum access is the key technology in CR. It enables high utilization of the unused spectrum thereby accommodating the forthcoming wireless technologies in the radio spectrum band [8, 10]. Two key technologies for cognitive radio's success are:

Dynamic spectrum access and Software defined radio. While software defined radio caters the hardware challenges in CR system, dynamic spectrum access allows high utilization of unused spectrum thereby increasing spectral efficiency [19]. Software defined radio is a communication transceiver in which functionalities like modulation/demodulation, tuning, amplification and mixing are controlled by software. It has a reconfigurable hardware, and hence the entire system can be used for dynamic communication scenario [20].

Figure 1.4 shows the major blocks which make the radio system cognitive: Reasoning engine, Learning engine and Knowledge base. CR network performs better when it has an

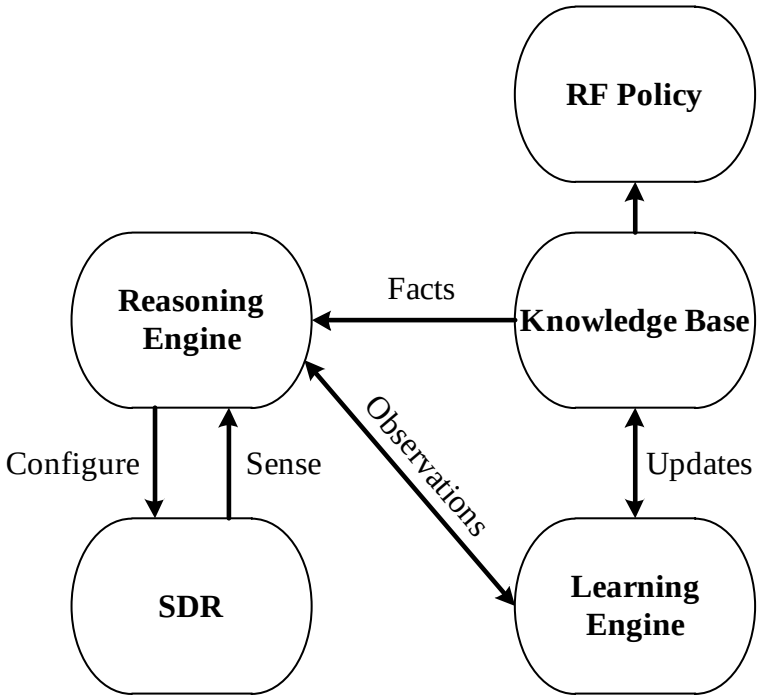


Figure 1.4: Cognitive Radio System

extensive knowledge base of the environment parameters, location and the network users [9]. This way, the network can associate the current situation to an earlier situation and react quicker. For example, knowledge of direction of motion of a CR system terminal can aid the CR network to pre-allocate resources for the upcoming cell handover thereby effectively

decreasing the time taken to perform handover. Knowledge of the terminal's availability in the network and the data rate received by it can help CR decide or predict how much time it would take to send a huge data file at any given time. Thus, having a huge knowledge base of user's history proves crucial in predicting future user behavior.

1.1.1 Interference Avoidance Approaches in CR network

The primary focus of CR network would be to mitigate or minimize the interference caused by the SUs to the PUs. Based on the available network information there are three approaches that can be taken [20] to mitigate interference.

1.1.1.1 Underlay Paradigm

The SUs maintain interference level below a certain threshold. Setting this threshold for spectrum sensing is a non-convex optimization process and the optimization should be such that the probability of error decreases. This method uses interference temperature model for measuring interference at the primary receiver caused by the SUs. For example one of the approaches used to mitigate the interference is to use wideband on which secondary transmission spread and de-spread at the secondary receiver (for example Ultra Wide Band (UWB)) which causes the interference to be spread across the whole spectrum there by reducing individual interference etc. This approach can be used to provide various class of service to different user.

1.1.1.2 Overlay Paradigm

In this approach the SUs need to know the channel used both between the secondary

transmitter and the primary receiver and between the primary transmitter and the secondary receiver. Based on this knowledge, it uses advanced algorithms and transmissions strategies so that the interference caused by the SUs can go down to minimum. This requires complicated architecture and protocols and is still an on going challenge.

1.1.1.3 Interweave Paradigm

Interweave approach is the basic idea [21] of CR system where the SUs strictly do not use the spectrum used by the PUs. Instead it senses the spectrum hole and uses this unused spectrum for communication. Once SUs detect any PU in that band they immediately leave that band and jump to other unused bands. The transceiver used for CR system consists of the same base band processor as used by the software defined radio along with a radio front end. The novel characteristics of a CR transceiver is radio front-end which has a wide range of sensing and adapting capabilities. This is achieved by having RF hardware technologies such as power amplifiers, adaptive filters and wideband antennas.

1.1.2 CR Environment Cycle

Figure 1.5, shows a typical CR duty cycle, that presents the major tasks that relate to cognitive capability and reconfigurability. The cognitive cycle consists of the following tasks:

- Opportunity: Detects unused spectrum and shares the spectrum without negatively interfering with other users.
- Analysis: Captures the best available spectrum to meet user communication requirements.

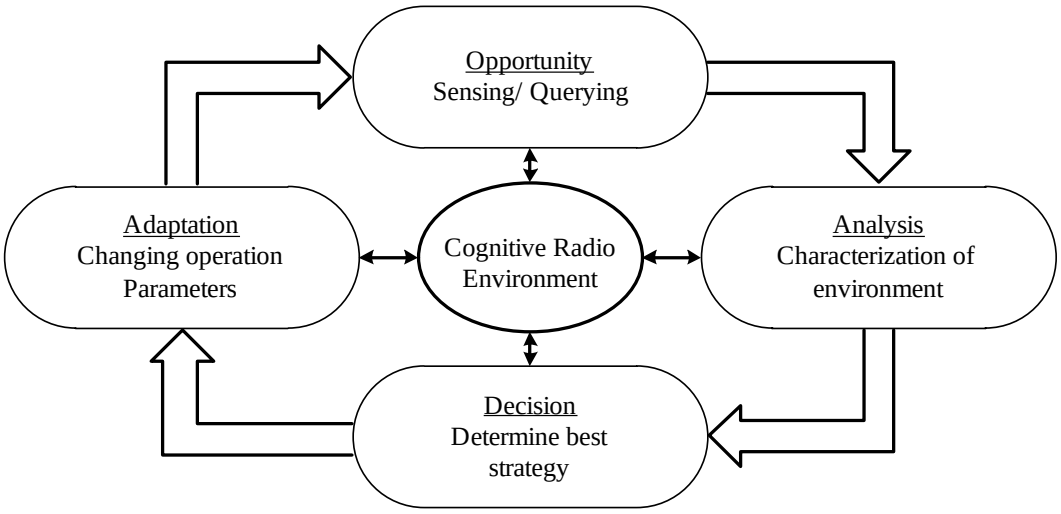


Figure 1.5: Radio Environment Cycle

- Decision: Enables SUs to choose the best frequency band and hop among multiple bands according to the time varying channel characteristics to meet the different Quality of Service (QoS) requirements [21].
- Adaptation: CR users adjust their transmission parameters (transmission power, modulation technique *etc.*) based on the information sensed from the environment.

In general, the dynamic use of the spectrum has a negative impact on the performance of conventional communication protocols that were designed for fixed frequency bands. It is important to consider this type of impact when designing CR systems.

1.1.3 CR network Functionalities

SUs in CR network have to execute four main functions: spectrum sensing, spectrum management, spectrum hopping and spectrum sharing. Figure 1.6 shows this CR network functionalities in different layer of communication. These functions will be discussed next.

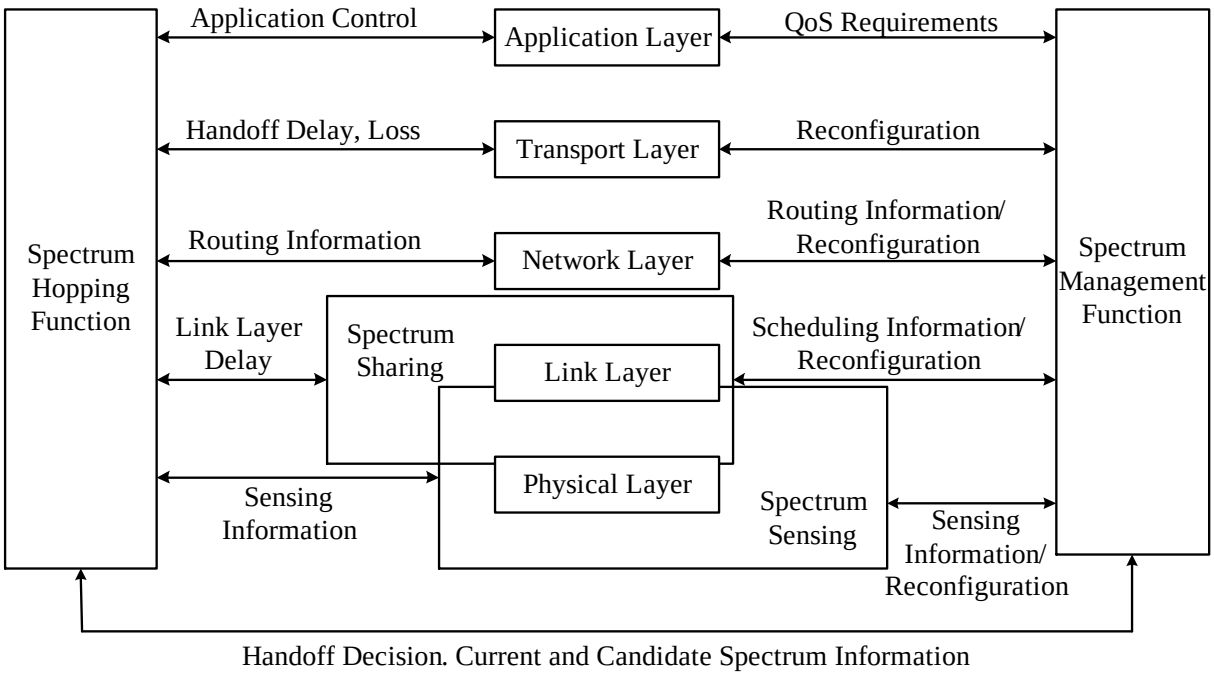


Figure 1.6: Functionalities of Cognitive Radio Networks

1.1.3.1 Spectrum Sensing

Spectrum sensing is one of the major tasks CR users need to execute continuously in CR network. In order to avoid interference the spectrum holes need to be sensed by the SUs. There are different types of techniques for spectrum sensing. Some of the popular techniques are primary transmitter detection, primary receiver detection, cooperative detection, interference temperature management, etc. Spectrum sensing will be discussed in more details in Chapter 2.

1.1.3.2 Spectrum Management

Spectrum management is important in CR network so that SUs can capture the best available spectrum to meet user communication requirements. CR users should decide on the best

spectrum band to meet the QoS requirements over all available spectrum bands. Spectrum management function can be classified as spectrum analysis and spectrum detection.

1.1.3.3 Spectrum Hopping

Spectrum hopping is a process where CR users change their frequency of operation. Two key factors act behind this spectrum hopping. One is return of the PU to the previous channel and another is degradation in QoS. As SUs need to follow the guideline of not interfering with PUs in a harmful manner, they will change their frequency of operation when PUs come back to the channel. Again SUs need to maintain a certain level of communication quality for that reason if QoS in a certain band drops SUs look for new idle bands to move to and set up communication in the new spectrum band.

1.1.3.4 Spectrum Sharing

Though SUs cannot access an occupied channel by PUs they can access the channels which are occupied by other SUs. For this reason SUs in a CR network follow a fair spectrum sharing and scheduling policy. Again in interference temperature management process SUs coexist with PUs. In this scenario the SUs also have to share the spectrum bands with PUs in fair manner without causing any trouble to the licensed users.

1.2 Problem Statement

The main objectives of this thesis are:

- To investigate the impact of SU mobility and PU activity on spectrum sensing performance

  - To incorporate the velocity of SUs while evaluating sensing performances of SUs
  - To incorporate the probability of PUs being active or idle in spectrum sensing in CR network
  - To investigate the impact of SUs' velocity and PUs' activity on probability of misdetection, probability of false alarm, and expected overlapping time

- To evaluate the performance of the SUs in the presence of eavesdroppers and jammers in CR network
  - To formulate utility functions for SUs and attackers
  - To apply game theory for performance evaluation of SUs in the presence of attackers
  - To evaluate SUs' performance with the help of utility functions of SUs

1.3 Outline

The outline of the remaining portion of this thesis is as follows,

Chapter 2 describes the background of CR network. Also PUs, SUs, spectrum sensing, different performance metrics of spectrum sensing are introduced. The chapter also describes necessary facts about physical layer security in CR network.

Chapter 3 presents a system model to imitate a scenario where the PUs are stationary and the SUs are mobile. This chapter formulates the velocity of SUs and activity of PUs. And finally evaluates the performance of spectrum sensing in CR network with the help of probability of misdetection, probability of false alarm, and expected overlapping time taking SUs' mobility and PUs' activity in account. Numerical outcomes are also presented in this chapter.

Chapter 4 presents another system model to replicate a CR network like environment where SUs and attackers coexist. Utility functions are developed in this chapter using the channel capacity of SUs and attackers. Finally, SUs' performance in the physical layer in the presence of jammers and eavesdroppers is evaluated here. Simulation results are also depicted in this chapter.

A conclusion of this whole thesis is drawn in Chapter 5. The effects and significance of the outcomes are discussed. Finally this chapter presents future work as an extension of this research study.

The findings presented in Chapter 3 are also published as a research article in 2015 IEEE INFOCOM Conference Smartcity Workshop titled as "The Impact of Secondary User Mobility and primary user Activity on Spectrum Sensing in Cognitive Vehicular Networks" [22]. The findings presented in Chapter 4 are also published as a research article in 2015 IEEE GLOBECOM Conference titled as "Performance Analysis of Secondary Users in the Presence of Attackers in Cognitive Radio Networks" [23].

CHAPTER 2

LITERATURE REVIEW

In this chapter fundamental ideas, definitions, institutionalization and administrative issues related to DSA, spectrum sensing, probability of misdetection, probability of false alarm and security issues in CR network will be clarified. Spectrum sensing has been identified as a key enabling functionality to ensure that cognitive radios would not interfere with PUs, by reliably detecting PU signals. In addition, reliable sensing plays a critical role on communication links of CR networks since it creates spectrum opportunities for SUs. In order to efficiently utilize the available opportunities, cognitive radios must sense its environment frequently while minimizing the time spent in sensing. Probability of misdetection refers to the probability by which SUs mistakenly considers a spectrum band to be idle though the spectrum band in question is actually occupied. Probability of false alarm refers to the probability by which SUs mistakenly considers a spectrum band to be occupied though the spectrum band in question is actually idle. These two are important performance metrics to evaluate spectrum sensing in CR network. Again it is very important to ensure secure communication link among the users in CR network. No matter how fast and stable setup a communication process may have, if it is not secure then eavesdroppers may secretly listen to classified information and jammers may transmit high power signals to prohibit the cognitive receivers from decoding the received signals appropriately. This thesis studies the impact of both eavesdroppers and jammers together. Combining the impact of both these attackers helps to understand the physical layer security concerns from a more practical viewpoint as it is very common for wireless communication networks to be under attack by both eavesdroppers and jammers.

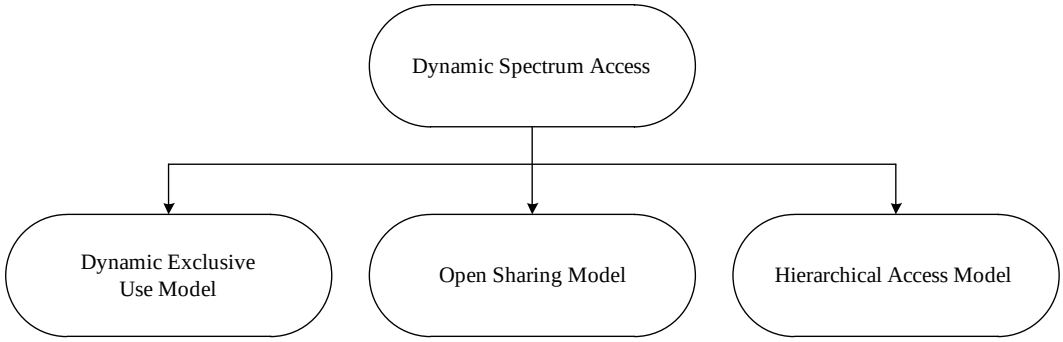


Figure 2.1: Different DSA Models

2.1 Dynamic Spectrum Access

The term dynamic spectrum access (DSA) has broad intentions that incorporate different ways to deal with spectrum reform from an opposing stand point of static spectrum management policy. The divers ideas exhibited at the first IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN) shaped the extent of this term. As represented in Figure 2.1, dynamic spectrum access techniques can be comprehensively arranged under three models.

2.1.1 Dynamic Exclusive Use Model

This model keeps up the fundamental structure of the present spectrum regulation approach: Spectrum bands are authorized to benefits for licensed use. The fundamental idea is to acquaint adaptability with enhanced spectrum effectiveness. Two methodologies have been proposed under this model: Spectrum property rights [22], [23] and dynamic spectrum allocation [24]. The former approach permits licensees to offer and exchange spectrum and to uninhibitedly choose technology. Economy and business sector will hence play a more vital part in heading toward the most beneficial utilization of this restricted asset. Note that despite the fact that licensees have the privilege to rent or share the spectrum for profit, such

sharing is not mandated by the regulation policy.

The second methodology, dynamic spectrum allocation, was delivered by the European DRiVE venture [24]. It means to enhance spectrum proficiency through dynamic spectrum assignment by exploiting the spatial and transient activity measurements of various administrations. At the end of the day, in a given region and at a given time, spectrum is allocated to services for restrictive use. This distribution, be that as it may, changes at a much faster scale than the present approach.

In light of an exclusive-use model, these methodologies cannot take out white space in spectrum coming about because of the uneven nature of wireless traffic.

2.1.2 Open Sharing Model

Additionally referred to as spectrum commons [25], [26], this model utilizes open sharing among peer users as the premise for dealing with a spectral region. Advocates of this model draw support from the marvelous accomplishment of wireless services working in the unlicensed industrial, scientific, and medical (ISM) radio band (e.g., WiFi). Centralized [27], [28] and dispersed [31] spectrum sharing systems have been initially examined to address technological difficulties under this spectrum management model.

2.1.3 Hierarchical Access Model

This model adopts a hierarchical access structure with PUs and SUs. The fundamental idea is to open licensed spectrum to SUs while restricting the interference perceived by PUs. Two approaches to deal with spectrum sharing between the PUs and SUs have been viewed as: Spectrum underlay and spectrum overlay.

The underlay approach forces serious imperatives on the transmission power of SUs so

they operate beneath the noise floor of PUs. By spreading transmitted signals over a wide frequency band (UWB), SUs can conceivably accomplish short-range high information rate with extremely low transmission power. In view of a worst case scenario that PUs transmit constantly, this approach does not depend on detection and exploitation of spectrum white space.

Spectrum overlay was initially envisioned by Mitola [32] under the term spectrum pooling and after that explored by the DARPA Next Generation (XG) program under the term opportunistic spectrum access. Contrasting from spectrum underlay, this approach does not necessarily impose extreme limitations on the transmission power of SUs, yet rather on when and where they may transmit. It straightforwardly focuses at spatial and transient spectrum white space by permitting SUs to recognize and exploit local and instantaneous spectrum availability in a non-intrusive way.

2.2 Spectrum Sensing

Spectrum sensing is the most important task in the cognitive cycle for the realization of cognitive radio. Since cognitive radios are considered lower priority or secondary users of spectrum allocated to a primary user, a fundamental requirement is to avoid interference to potential PUs in their vicinity. On the other hand, PU networks are not required to change their infrastructure for spectrum sharing with cognitive networks. Therefore, cognitive radios should be able to independently detect PU presence through spectrum sensing schemes. Although spectrum sensing is traditionally considered as measuring the spectral content or measuring the interference over the spectrum, when the ultimate cognitive radio is considered, it is a more general term that involves obtaining the spectrum usage characteristics across multiple dimensions such as time, space, frequency, and code [24, 25].

Spectrum sensing is defined as the task of finding spectrum holes by sensing the radio spectrum in the local neighborhood of the cognitive radio receiver in an unsupervised

manner. The term "spectrum holes" stands for those sub-bands of the radio spectrum that are underutilized (in part or in full) at a particular instant of time and specific geographic location [18,20]. To be specific, the task of spectrum sensing involves the following sub-tasks:

- detection of spectrum holes
- spectral resolution of each spectrum hole
- estimation of the spatial directions of incoming interference
- signal classification

In the next section different signal detection methods for spectrum sensing will be discussed.

2.2.1 Signal Detection Methods for Spectrum Sensing

The signal processing technique in spectrum sensing can be divided in two categories. They are the direct and indirect method. In direct method the estimation is executed directly from the signal over the frequency domain and in indirect method the estimation is executed using auto-correlation of the signal over the time domain. Another way of categorizing the spectrum estimation technique can be dividing it into two groups named model based parametric method and periodogram based non-parametric method [26,27,28].

In order to identify the PU signal in the system to exploit the spectrum opportunity, the received signal at CR receiver is considered in continuous time as

$$Y(t) = h.s(t) + w(t) \tag{2.1}$$

where $Y(t)$ is the received signal, h is the complex gain of the ideal channel between primary transmitter to CR receiver, $s(t)$ is the primary user's signal (to be detected), and $w(t)$ is the additive Gaussian white noise (AWGN).

So as to utilize the signal processing algorithm for spectrum sensing, the signal in the frequency band is considered with central frequency f_c and data transfer bandwidth B, and sample the received signal at a sampling rate f_s, where $f_s > B$, and $T_s = \frac{1}{f_s}$ is the sampling period. At that point the received signal samples can be defined as,

$$Y(n) = Y(nT_s) \tag{2.2}$$

the primary signal samples can be defined as,

$$s(n) = s(nT_s) \tag{2.3}$$

and the noise signal samples can be defined as,

$$w(n) = w(nT_s) \tag{2.4}$$

Then the sampled received signal can expressed as

$$Y(n) = h.s(n) + w(n) \tag{2.5}$$

If the channel gain is assumed to be 1, i.e., $h = 1$ (ideal case) between the transmitting and receiving nodes then (2.5) can be rewritten as,

$$Y(n) = s(n) + w(n) \tag{2.6}$$

Here two hypotheses can be considered for primary transmitter detection ($\mathcal{H}_0$ and $\mathcal{H}_1$). Hypothesis $\mathcal{H}_0$ represents that the channel is free of any PUs and SUs can access the channel given that SUs will keep sensing the channel to detect the return of any primary users as they have to avoid causing disturbance to the PUs. Hypothesis $\mathcal{H}_1$ represents that the channel is under use by other PUs and the SUs cannot access the channel right then. The sampled received signal under these hypotheses can be expressed as,

$$Y(n) = \begin{cases} w(n), & \mathcal{H}_0 \\ s(n) + w(n) \text{ or } h.s(n) + w(n), & \mathcal{H}_1 \end{cases} \tag{2.7}$$

Here, whether a primary signal is present or not depends on the value of $s(n)$. If the signal component $s(n) = 0$ then the particular frequency band is empty given that the detection is error free and if $s(n) \neq 0$ then the particular frequency band is under PU occupation and there is no spectrum band allocatable for that given time and location. Hypothesis $\mathcal{H}_0$ represents that the channel is free of any PUs and SUs can access the channel given that SUs will keep sensing the channel to detect the return of any primary users as they have to avoid causing disturbance to the PUs. Hypothesis $\mathcal{H}_1$ represents that the channel is under use by other PUs and the SUs cannot access the channel right then.

There are different signal detection methods such as matched filter based signal detection, covariance based signal detection, waveform-based detection, energy detection, cyclostationarity based detection, cooperative detection, etc. These are discussed here in detail.

2.2.1.1 Matched Filtering Based Signal Detection

At the point when the transmitted signal is known at recipient, matched filtering (MF) is known as the ideal technique for detection of PUs [35] since it maximizes received signal-to-noise ratio (SNR), and the SNR relating to the mathematical statement in (2.6) is

$$\gamma = \frac{|s(n)^2|}{E[w^2(n)]} \tag{2.8}$$

Simple implementation of matched filter based detection is depicted in Figure 2.2, where a threshold value is set to estimate the signal. Authors in [21] use matched filter for pilot signal and matched filter-based detection where the method assumes that the primary user sends pilot signal along with data. The process is depicted in Figure 2.3. The performance of the matched filter based detection is the best when the receiver has prior knowledge about signaling features of the received signal [26]. Despite having best performance criterion set for MF, the MF has a greater number of disadvantages than its advantages. Firstly, MF

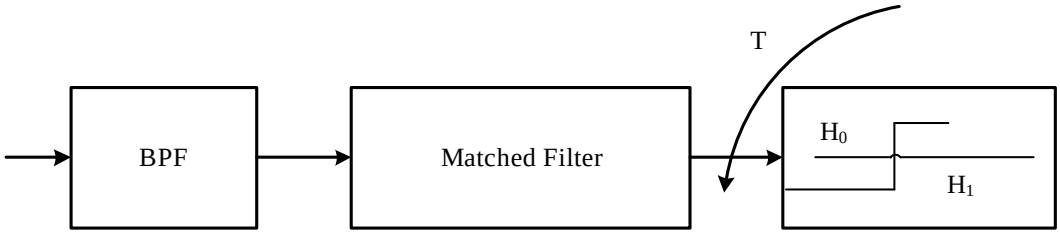


Figure 2.2: Matched filter for signal detection

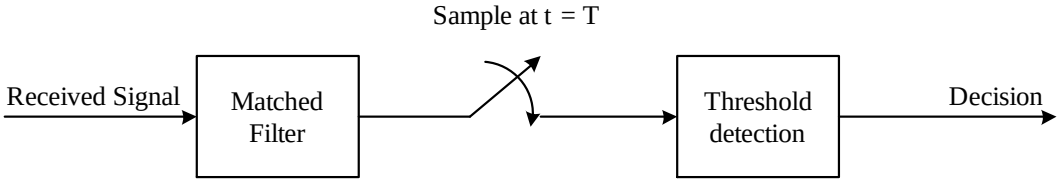


Figure 2.3: Pilot signal and matched filter based detection [21]

requires immaculate information of the PU signaling features, (for example- modulation type, operating frequency, and so on), which should be detected at cognitive radio. It is very common for cognitive radio to utilize wide band of spectrum wherever it finds the spectrum opportunities. Subsequently it is just about impossible to have MF executed in cognitive radio for a wide range of signals in wide band administration. Secondly, implementation of MF based detection unit in CR devices is highly complex [21] in light of the fact that CR system needs receivers for every sort of wide band signals. Lastly, huge amount of power will be consumed to execute such a detection processes for several times as CR system sense the wideband frequency bands. In this manner the inconveniences exceed the upsides of MF based detection. Note that MF based method might not be a decent choice for real CR system in view of its aforementioned disadvantages.

2.2.1.2 Covariance Based Signal Detection

This is another approach to distinguish the PU signal by CR users. Authors in [18] have proposed covariance based signal detection whose principle idea is that to utilize the covariance of signal and noise subsequent to the statistical covariance of signal and noise are typically distinctive. These covariance properties of signal and noise are utilized to separate signal from noise where the sample covariance matrix of the received signal is figured taking the receiving channel into account. The system model for received signal is considered as it appears in (2.5), and the received signal in a vector channel structure can be composed as [18]

$$\boldsymbol{Y} = \boldsymbol{A}.\boldsymbol{s} + \boldsymbol{w} \tag{2.9}$$

here $\boldsymbol{A}$ represents the channel matrix through which the transmitted signal travels. The covariance related to the sensed signal, the transmitted signal and the noise can be expressed as

$$cov(\boldsymbol{Y}) = E[\boldsymbol{Y}\boldsymbol{Y}^T] \tag{2.10}$$

$$cov(\boldsymbol{s}) = E[\boldsymbol{s}\boldsymbol{s}^T] \tag{2.11}$$

$$cov(\boldsymbol{w}) = E[\boldsymbol{w}\boldsymbol{w}^T] \tag{2.12}$$

where $E[.]$ stands for the expected value of [.]. In the event that there is no signal ($\boldsymbol{s} = 0$), then $cov(\boldsymbol{s}) = 0$ and subsequently the off-diagonal components of $cov(\boldsymbol{Y})$ are all zeros. On the off chance that there is signal ($\boldsymbol{s}0$) and the signal samples are correlated, then $cov(\boldsymbol{s})$ is no more a diagonal matrix. In this way, a portion of the off-diagonal components of $cov(\boldsymbol{Y})$ should not be zeros. Consequently, this technique distinguishes the presence of signals with the assistance of covariance matrix of the received signal. That is, if all the off diagonal estimations of the matrix $cov(\boldsymbol{Y})$ are zeros, then the PU is not utilizing the band around that time and location, and otherwise the band is occupied.

2.2.1.3 Waveform-Based Detection

This is another method for the detection of PU signal. In this method, the patterns relating to the signal, for example, preambles, mid-ambles, frequently transmitted pilot patterns, spreading sequences, and so forth, are generally utilized in wireless system to help synchronization or determine the presence of signal. At the point when a known pattern of the signal is available, the detection technique can be connected by associating the received signal with a known duplicate of itself [22] can be performed and the strategy is known as waveform-based detection. Authors in [22] has demonstrated that waveform-based detection is superior to energy based detection (introduced in the accompanying segment) in terms of unwavering quality and convergence time, furthermore has demonstrated that the performance of the algorithm improves as the length of the known signal pattern improves.

With a view to performing waveform-based signal detection, the system models is considered as it appears in 2.6 and the detection metric can be expressed as

$$\begin{aligned} M &= \mathrm{Re}\Big[\sum_{n=1}^{N} Y(n)s*(n)\Big] \\ &= \sum_{n=1}^{N} |s(n)|^2 + \mathrm{Re}\Big[\sum_{n=1}^{N} w(n)s*(n)\Big] \end{aligned} \tag{2.13}$$

where N represents length of known pattern. The sensing metric introduced (2.13) can be approximated as a Gaussian variable when N is large. It consists of two terms. $\sum_{n=1}^{N} |s(n)|^2$ in second equality stands for the first term and it is related to signal. $\mathrm{Re}\big[\sum_{n=1}^{N} w(n)s*(n)\big]$ in second equality stands for the second term and it is related to the noise component. Therefore, when there is no PU signal, the detection metric M will only have the second term of second equality in (2.13) which is only noise as $s(n) = 0$ but when there is presence of PU signal, the detection metric will have both the terms of second equality in (2.13). The detection metric value found in (2.13) can be compared with some threshold value λ for the sake of detecting the signal. It can be comprehended from the simulation results exhibited in [22] that waveform-based detection requires short estimations time, nonetheless, it is

vulnerable to synchronization errors.

2.2.1.4 Energy Detection

Another detection technique for PU detection for spectrum sensing is energy detection. This technique is viewed as the most well-known method for signal recognition as a result of its low computational and implementation complexities [21]. Whereas matched filter and other approaches require prior information about the PU for signal detection, energy detection does not require any kind of knowledge about the PU signals.

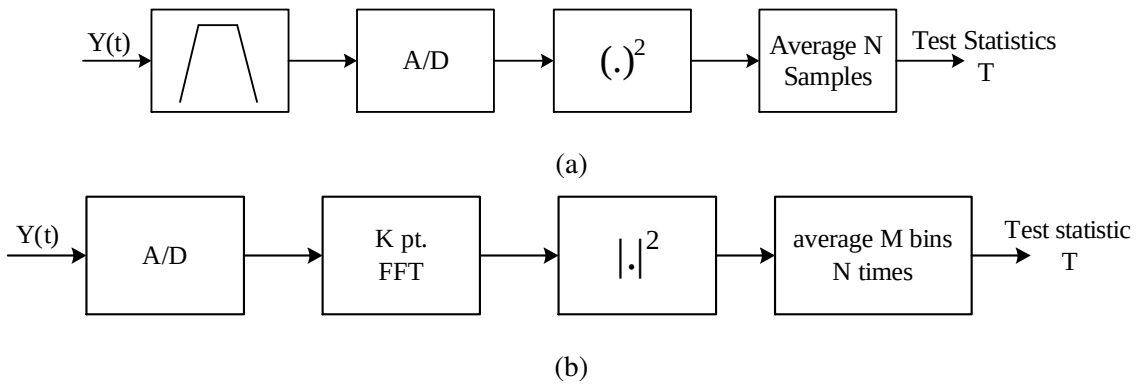


Figure 2.4: Digital implementation of energy detection (a) with periodogram: FFT magnitude squared and averages, (b) with analog pre-filter and square-law device [24].

In this technique, the signal detection is executed by contrasting the output of energy detector and a given threshold value [27] and the threshold value as in waveform based approach relies upon the noise variance and can be assessed in light of it. The Figure 2.4a and 2.4b demonstrate the digital implementation of energy detection. Figure 2.4a shows a conventional diagram for energy detection which is formed with a low pass filter to reject out band noise and adjacent signals, Nyquist sampling A/D converter to convert the signal to digital signal, square law device to get the test statistics. An alternative to this approach is depicted in Figure 2.4b which is devised using a periodogram approach to estimate the

spectrum. First of all the signal is converted to digital signal with the help of A/D converter then Fast Fourier Transform (FFT) is applied on the signal and then the output of the FFT process is squared and averaged to get the test statistics. In both of these approaches the computed test statistics are compared with given threshold value to determine the presence of PU signals.

For this energy detection method the detection metric can be formulated based on the system model from (2.6) in the following manner

$$M = \sum_{n=1}^{N} |Y(n)|^2 \tag{2.14}$$

Assuming that the detection metric M follows chi-square distribution with $2N$ degrees of freedom $(\chi_{2N})^2$ it can be modeled with the help of two hypotheses as

$$M = \begin{cases} \frac{\sigma_w^2}{2}\chi_{2N}^2, & \mathcal{H}_0 \\ \frac{\sigma_s^2 + \sigma_w^2}{2}\chi_{2N}^2, & \mathcal{H}_1 \end{cases} \tag{2.15}$$

The most important process that defines performance for energy detection is the selection of detection threshold. Fading due to distance or shadowing may reduce primary signal intensity perceived by secondary receiver, and considering a high threshold value, may cause that SU will never detect the presence of the primary transmitter, and possibly interfere with primary transmissions. On the other side, if the threshold value selected is too low, then detector will be very sensitive, and thus indicate the presence of PUs, even if they are not present. This may cause poor spectrum utilization by SUs, even when opportunities are present. Again it is noted that the strategy has a few more weaknesses, for example, poor performance under low Signal-to-Noise Ratio (SNR) value [27], and failure to separate between interference from PUs and noise that may restrain the performance of this methodology. Moreover, this methodology does not work ideally to detect spread spectrum such as CDMA signals [28].

2.2.1.5 Cyclostationarity Based Detection

The cyclostationarity based signal detection technique is also viewed as a decent contender for spectrum detecting in CR systems. This strategy exploits cyclostationarity properties of the received signals [23, 36] to distinguish PU transmissions. The digital implementation of this approach is delineated in Figure 2.5. The essential thought in this technique is to

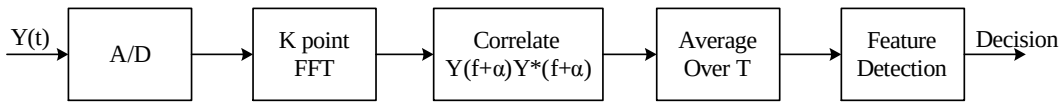


Figure 2.5: Pilot signal and matched filter based detection [23]

utilize the cyclostationarity components of the signals. In general, the transmitted signals are stationary random process. Moreover, the cyclostationarity features includes the periodicity in signal measurements, for example, mean and auto-correlation, are actuated in view of modulation of signals with sinusoid carriers, cyclic prefix in OFDM, and code sequence in CDMA. Then again, the noise is considered as Wide-Sense Stationary (WSS) with no connection to the signal whatsoever. Subsequently, this technique can separate PU signals from noise [24]. In this technique, cyclic spectral correlation function (SCF) is utilized for distinguishing signals present as a part of a given frequency band and the cyclic SCF of received signal in (2.6) can be calculated as [23, 36]

$$S_{YY}^{\alpha} = \sum_{\tau=-\infty}^{\infty} R_{YY}^{\alpha}(\tau) E^{-j2\pi f} \tag{2.16}$$

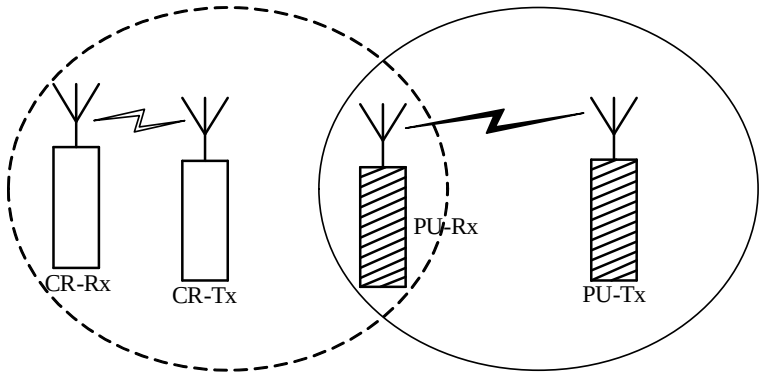
where $R_{YY}^{\alpha}(\tau)$ stands for the cyclic auto-correlation function which can be determined from the time varying auto-correlation function of $s(n)$, which is periodic in n, and the α is the cyclic frequency. It is worth of noting that the SCF turns into power spectral density when $\alpha = 0$. If PU signal is present at the network in the given frequency band, this cyclostationarity method gives the peak value in cyclic SCF which in turn means that the

primary user is present. If no such peak appears in the cyclic SCF then it should be assumed that the given frequency band is free of PUs at any given time and location. Based on this observation, CR users identify the status of PUs (absent or present) in the particular band in a given time and location.

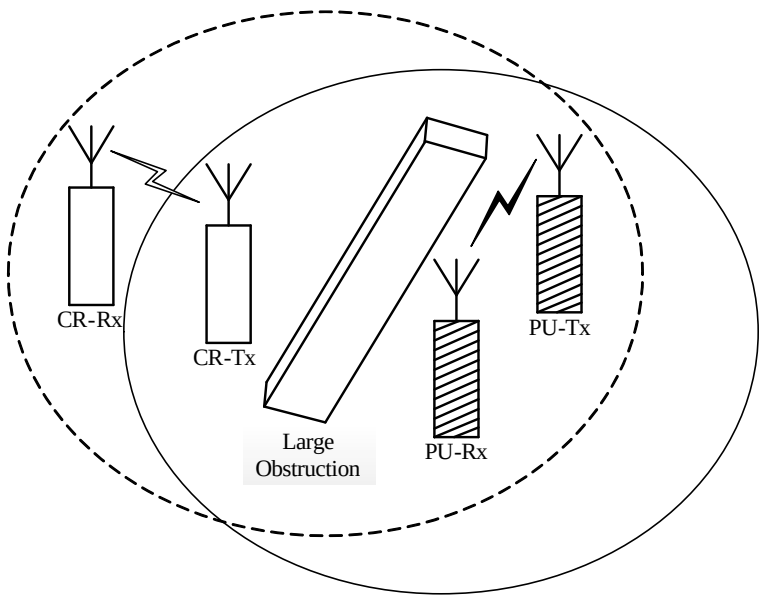
2.2.1.6 Cooperative Detection

In cooperative based signal detecting, CR users can utilize any suitable technique for primary spectrum detecting and work together for the detected data among partaking users keeping in mind the end goal to build the dependability of sensing. In cooperative detection, the spectrum estimation should be possible by associating or teaming up with different remote wireless users [19] to get reliable and exact data in regards to spectrum opportunities. In wireless system, there must be hidden terminal (PU) issue as appeared in Figure 2.6a due to path loss (or network coverage) and Figure 2.6b due to shadowing or hindering of transmission. This hidden terminal issue in recognizing PUs results in increasing false alarm, which is undesirable for signal detecting in cognitive radio systems. Therefore, keeping in mind the end goal to address this sort of issue and in addition to build the unwavering quality of sensed data, the CR users can coordinate or work together with other CR users and/or PUs to share the data. Along these lines, this strategy can fathom the hidden terminal (PU) issue [19]. Again this strategy takes care of numerous issues in spectrum estimation such as it reduces both probability misdetection and false alarms.

Among the detection techniques elaborated in this chapter energy detection requires short time for detection. Energy detection is also cost effective. Moreover energy detection does not require any prior knowledge about the PUs and it is less complex in nature [27]. Taking these characteristics in account energy detection is used in this thesis as the spectrum detection technique for SUs in CR network.



(a)



(b)

Figure 2.6: Hidden primary user problem because of (a) path loss and (b) shadowing/blocking

2.3 Probability of Misdetection and False Alarm for Spectrum Sensing

From (2.7) it is clear that $s(t)$ is the signal to be detected and $n(t)$ is the additive white Gaussian noise. Suppose the decision metric for spectrum sensing is considered to be M and the threshold value for the metric λ. If $M \geq \lambda$ then the band is occupied by a primary user and if $M < \lambda$ then the band is free of any primary user.

The performance of the detection algorithm can be summarized with two probabilities: probability of detection P_D and probability of false alarm P_F. P_D is the probability of detecting a signal on the considered frequency when it truly is present. Thus, a large detection probability is desired. It can be formulated as

$$P_D = Pr(M \geq \lambda | \mathcal{H}_1) \tag{2.17}$$

Probability of misdetection P_M is the opposite of probability of detection. It depicts the probability by which a cognitive radio mistakenly considers the band unoccupied though a primary user is present. It can be derived from (2.17) as

$$P_M = 1 - P_D \tag{2.18}$$

P_F is the probability that the detection algorithm incorrectly decides that the considered frequency is occupied when it actually is not, and it can be written as

$$P_F = Pr(M \geq \lambda | \mathcal{H}_0) \tag{2.19}$$

P_F should be kept as small as possible in order to prevent under utilization of transmission opportunities. The decision threshold λ can be selected for finding an optimum balance between P_M and P_F . However, this requires knowledge of noise and detected signal powers. The noise power can be estimated, but the signal power is difficult to estimate as it changes depending on ongoing transmission characteristics and the distance between the cognitive radio and primary user. In practice, the threshold is chosen to obtain a certain false alarm rate. Hence, knowledge of noise variance is sufficient for selection of a threshold.

2.4 Security in Cognitive Radio Networks

With the development of cognitive radio, extending to the level of network, the cognitive radio network can utilize idle licensed spectrum, thereby improving the utilization of spectrum resources to meet the demand for more spectrum for wireless users. Because of the physical characteristics of CR networks where various unknown wireless devices are allowed to opportunistically access the licensed spectrum, several types of attacks in CR networks has been attracting continuously growing attention. And it is necessary to take security measures to combat attacks launched by malicious attackers [35, 36].

Here some of the most common security threats for secondary users in cognitive radio networks are presented

2.4.1 Primary User Emulation Attack

The first is the primary user emulation (PUE) attack [28]. A PUE attacker may masquerade as a primary user by transmitting special signals in the licensed band, thus preventing other secondary users from accessing that band. In PUE attacks, the attacker only transmits on the channels that are not used by primary users. Therefore, the secondary users regard the attackers as primary users and do not try to access the channels that are not used by primary users. As pointed out in [29], there are several types of PUE attacks. In a selfish PUE attack, an attacker tries to make use of the unused spectrum. When a selfish PUE attacker detects an unused spectrum band, it transmits signals that emulate the signal characteristics of a primary user and prevent the secondary users from using it. Thus, the attacker can make use of the vacant channels that are not used by primary users. However, for a malicious PUE attack, the malicious attacker just tries to prevent the transmission of the secondary users without using it. There exist some more complicated PUE attacks. Some attackers can even attack only when the primary user is off, which means that attackers can save energy.

To defend against this threat, a transmitter verification scheme called localization-based defense (LocDef) was proposed in [30], which verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. In a practical case of cognitive radio networks, the primary users can mainly be composed of TV signal transmitters (i.e. TV broadcast towers) and receivers. Their locations are typically determined. If a malicious user wants to emulate the primary user and its location is almost the same as the primary user, secondary users would not receive the signal of the malicious user since the transmit power of the malicious node is much smaller than a TV tower. If the secondary users receive a high power signal from the malicious user, it means that the malicious user must be very close to the secondary user. Thus, the secondary user can determine whether a transmitter is a primary user or malicious user just by estimating the location of the transmitter. The transmitter verification scheme includes three steps: verification of signal characteristics, measurement of received signal energy level, and localization of the signal source. The first two steps have been investigated thoroughly. For the third step, there are many techniques that can be used to estimate the location of the transmitter, such as Time of Arrival (TOA), Time Difference Of Arrival (TDOA), Angle of Arrival (AOA), and Received Signal Strength (RSS). Take RSS as an example: there is a strong correlation between the distance of a wireless link and RSS. Therefore, if multiple secondary users take RSS measurements from a transmitter, the transmitter location can be estimated using the relationship between distance and RSS. Thus, the key to counter against PUE attack is to determine whether the transmitter is a primary user or a malicious user.

2.4.2 Objective Function Attack

Another attack on cognitive radio networks is the objective function attack (OFA) [31]. This attack mainly targets the learning engine of cognitive radios. In cognitive radios, a

cognitive engine has the ability to tune many parameters to maximize its objective function. These objective functions take as variables high transmission data rate, low power consumption, low delay, and high security level. Such parameters might include bandwidth, power, modulation type, coding methods, MAC protocol, routing schemes, and encryption mechanisms [29]. Among those variables of the objective function, high transmission rate and low delay are related to the channel, while low power consumption and high security level are directly determined by the inputs of the users. So for an objective function attack, whenever the user wants to raise the security level, the malicious nodes may use some ways to increase the delay of the user. Thus, the user may connect high delay with high security level and not want to use high security level at all. Thus, it will become more susceptible to security attacks. It is necessary to remark that the OFA performance is related to which optimization method is used in the cognitive radio network [31]. Some cognitive radios perform optimization instantly after getting the input of the environment. On the other hand, other cognitive radios observe the environment just once, then search for an optimized result, and the decision will not be changed by the input of the environment. In this case, the type of cognitive radio is not affected by OFAs. However, cognitive radio devices generally have high sensing ability and perform optimization frequently. Therefore, a cognitive radio network is susceptible to OFA attacks.

In order to combat an objective function attack, a simple suggestion has been made in [28]. It is to define threshold values whenever the radio parameters need to be updated. If the detected parameters do not meet the predefined thresholds, the secondary user will not collect that information. Moreover, a good intrusion detection system can be used to strengthen the countermeasure. However, using an intrusion detection system is a general countermeasure that may not perform well in defending against objective function attacks [29].

2.4.3 Learning Attack

In a learning attack (LA) [31] the adversary provides false sensory input for the learning radio in cognitive radios. If a learning radio learns some wrong ideas about the transmission schemes, it will be used all the way until it can learn the correct ideas. Generally, a learning attack is combined with other types of attacks. For example, an attacker can conduct a PUE attack or an OFA attack whenever a cognitive radio tries to use the best transmission scheme. Thus, the learning radio might decide that the best transmission scheme will not be optimal and it will take sub-optimal transmission schemes as the optimal transmission schemes, which leads to lower performance.

Several methods have been proposed to combat learning attacks [31]. First, the learning results must always be reevaluated over time. For example, the activities of the primary users in a cognitive radio network should be constantly recomputed so that the previously learned statistical process of activities of the primary users that may be incorrect will be abandoned. Second, there should be a truly controlled environment during the learning phases, which means no malicious signals are present during the learning phase. Third, if the learned action breaks some basic theoretic results, then this action should not be used. Fourth, cognitive radios can make use of group learning instead of individual learning. Several secondary users can form a group to learn the environment, and thus the attacker cannot conduct a learning attack so easily.

2.4.4 Spectrum Sensing Data Falsification

Spectrum Sensing Data Falsification (SSDF) is discussed in [29]. Also known as the Byzantine Attack, it is a popular attack in cognitive radio networks. An attacker sends false local spectrum sensing results to its neighbors or to the fusion center, causing the receiver

to receive the wrong sensing information and make a wrong spectrum access decision. This attack can target the fusion center or just one secondary user. If it attacks the secondary user and sends wrong sensing information to just one secondary user, the secondary user may not have the ability to tell the real sensing information from the wrong sensing information and then make wrong decisions. While the attack targets the fusion center, the fusion center can collect sensing information from many other users, either legitimate secondary users or malicious users. If most of the sensing information is from legitimate users, the fusion center will have a high probability to make a right decision to determine which information would be real.

A two-level defense is required to counter SSDF attacks effectively [32]. At the first level, the data fusion center needs to authenticate all local spectrum sensing results since there might be malicious users who will eavesdrop the spectrum sensing results and then launch replay attacks or inject false data. The second level of defense is to implement an effective data fusion scheme that can determine which sensing information is real. There are several ways to improve existing data fusion schemes to counter SSDF attacks. One way is the Sequential Probability Ratio Test (SPRT). SPRT can support a large number of spectrum sensing results and combine them together. In this way, SPRT can have a higher probability to guarantee the spectrum sensing correctness. Another way is to use a reputation-based scheme in the Distributed Spectrum Sensing (DSS) process. This scheme can make a long time record of the sensing results and rate the users according to the correctness of their sensing results. Those who are always right can get a high reputation, and their results would be adopted. However, the malicious nodes would be low rated and would not be believed.

2.4.5 Jamming Attack

Another attack on cognitive radio networks is the jamming attack, which can be classified as a single-channel jamming attack or a multi-channel jamming attack [33]. In a single channel jamming attack the malicious node continuously transmits high-power signals on one channel. Therefore, all transmissions on this channel will be jammed. However, this type of jamming is not so effective, since the malicious node should transmit continuously, which consumes much energy. Moreover, the high power interfering signal can be easily detected. Another more effective way of jamming is to jam multiple channels simultaneously. The traditional way is to transmit interfering signals on all the channels at the same time. However, this still consumes too much energy, especially when the number of channels is large. An improved way is to use cognitive radio technology so that the attacker can switch from one channel to another according to the activities of the primary users. Since cognitive radios can significantly reduce channel switching delay, attackers can jam the channel more effectively in this way.

To counter jamming attacks, secondary users first need to detect that a jamming attack really exists. One way to detect a jamming attack is to collect enough data of the noise in the network and build a statistical model [34]. Thus, when an attacker tries to jam the secondary user and transmits large power interference, the secondary user can have the ability to differentiate the interference of an attacker from normal noise. The second step to counter a jamming attack is to defend against it, mainly in two ways [29]. One is to use frequency hopping. Whenever the secondary users find the jamming attack, they will use their high switching ability to switch to other channels that are not jammed. Another way is to do spatial retreat. The secondary users may escape from the location where jamming happens to where there is no jammer. Thus, the interfering signals transmitted by the jammer will not be received by the secondary users. The disadvantage of this method is that spatial retreat may make the secondary user lose communication with the users it is now communicating with.

2.4.6 Eavesdropping

The last security threat described here is eavesdropping, which means that a malicious node would listen to the transmission of the legitimate users. In [35] the authors considered a network model in which the secondary users use multiple input multiple output (MIMO) transmission, the primary users use a single antenna, and the eavesdroppers can use either multiple antennas or a single antenna. The authors studied the achievable rates of the MIMO secrecy rate between secondary users and formed a non-convex max-min problem to maximize secrecy capacity without interfering with the primary users. The maximum achievable secrecy rate can be obtained by optimizing the transmit covariance matrix in the case of Gaussian input. Algorithms were proposed to compute the maximum achievable secrecy rate for the case of single-antenna eavesdroppers, and bounds on the achievable secrecy rate were obtained for general cases with multi-antenna secrecy and eavesdropper receivers. Here the key idea behind [35] is using power control algorithms in order to increase the rate between the legitimate users while decreasing the rate to the eavesdroppers. Thus, secrecy rate can be improved.

Among the security attacks described here eavesdropping and jamming are taken into consideration while evaluating performance of SUs in CR network.

2.5 Chapter Summary

In this chapter literature review related this thesis is presented. Dynamic spectrum access is described in Section 2.1. Besides the main theme of DSA, three models are also presented in this section to categorize DSA. Spectrum sensing is broadly described in Section 2.2. Spectrum sensing is the task of looking for spectrum holes in CR network. There are different techniques of signal detection such as primary transmitter detection, primary

receiver detection, cooperative detection and interference temperature management. The key terms in investigating spectrum sensing performance in CR network like probability of misdetection and probability of false alarm are discussed in Section 2.3. Probability of the event where a channel in CR network is actually occupied by PUs but is detected as idle by SUs is called probability of misdetection. Again probability of the event where a channel in CR network is actually idle but is detected as occupied by SUs is called probability of false alarm. Section 2.4 shows the common security threats towards cognitive radio networks such as eavesdropping, jamming, primary user emulation attack, objective function attack, learning attack, and spectrum sensing data falsification.

CHAPTER 3

EFFECTS OF SECONDARY USER MOBILITY IN SPECTRUM SENSING

Spectrum sensing is one of key technologies of CRN. Spectrum sensing refers to the ability of a cognitive radio to measure the electromagnetic activities due to the ongoing radio transmissions over different spectrum bands and to capture the parameters related to such bands (e.g., cumulative power levels, user activities, etc.).The performance study of existing spectrum sensing algorithms often overlooks the impact of secondary user mobility. Many of them assume secondary users stationary or with low mobility. As an addition to the wireless communication technology CRS should consider mobility in spectrum. In this chapter, the joint impact of secondary user mobility and primary user activity on spectrum sensing for highly dynamic cognitive vehicular networks is investigated. It is assumed that each vehicle is equipped with a cognitive radio for spectrum sensing. Mathematical models of probability of misdetection and expected overlapping time duration for spectrum sensing are investigated in this chapter. The proposed method incorporates velocity of secondary user, activity of primary user, initial distance between primary and secondary users and their transmission ranges. In ordered to corroborate the analysis, numerical results obtained from simulations are presented. It is noted that the speed of the vehicular secondary user and the activity of primary user have significant impact on misdetection probability, but not on false alarm probability. Furthermore, transmission range, velocity and initial separation distance have huge impact on expected overlapping time duration.

3.1 Background

With exponential growth of hand-held devices and huge number of wireless subscriptions, wireless service providers are experiencing exponential growth in wireless traffic that results in huge demand of RF spectrum [12,36,37]. Vehicular networks are expected to be a major contributing factor in spectrum scarcity in the near future [38–41]. Opportunistic spectrum

access is emerging to improve spectrum efficiency in wireless networks where unlicensed secondary users (SUs) sense channels to find idle bands and use those bands without creating any harmful interference to primary users (PUs) [12, 37]. In vehicular networks, there are seven dedicated channels in IEEE 802.11p based vehicular communications to help reduce accidents, traffic jams, and cost associated with fuel consumption and lost productivity, to help many commercial applications, and to help improve traffic management. However, these reserved seven channels could be easily congested when the vehicle density is high such as in urban areas. Thus, spectrum sensing and access in cognitive vehicular networks have been introduced to fully exploit the underutilized licensed spectrum opportunistically to provide efficient vehicular communications. The spectrum sensing is one of the major steps not to interfere with PUs in cognitive vehicular networks [37, 42] where users are highly mobile in dynamic network topology.

A variety of sensing methods have been proposed in the literature [37,43–48]. In most of these works, SUs are assumed to be stationary and PUs are assumed to be idle during SU transmissions. Mobility of SUs is considered in [45] for sensors on the performance of spectrum sensing and scheduling framework. Impact of mobility in cooperative spectrum sensing is presented in [47] whereas impact of PU mobility in spectrum sensing is studied in [46]. Effect of mobility of SUs using random way point model is presented in [48] where PUs are stationary. None of these methods consider the joint effect of velocity of vehicles, PUs' activities, transmission range of PUs, and sensing range of SUs to evaluate the performance of spectrum sensing in cognitive radio enabled vehicular networks.

In this chapter, the combined impact of PU activity and mobility of SUs on the performance of spectrum sensing in cognitive vehicular networks is investigated. Note that the performance of spectrum sensing also depends on transmission range of PUs and sensing range of SUs. This chapter considers joint effect of all of these parameters while developing mathematical models for both misdetection probability and expected overlapping

time duration in cognitive radio enabled vehicular networks.

Each vehicle has a sensing range to sense channels and a transmission range to communicate opportunistically using spectrum opportunities in vehicular networks. Note that the transmission range of SUs should be shorter than or equal to sensing range in order not to interfere with PUs. PUs have protected range where SUs are not allowed to use PUs' licensed bands at any cost [37, 49]. Note that if the sensing range of SU is enough (not enough) to cover protected region of PU, the SU and PU will (will not) be reachable wirelessly. When an SU and a PU are within the range of each other, the given SU will be able to sense PU's signals. If a PU is outside the sensing range of the SU, the SU may not be able

Sample scenario with a road segment containing TV/WiMAX residential roadside users as stationary PUs with their protection ranges r and a mobile SU with its sensing range s in cognitive vehicular network. to notice the existence of PU around it. If the SU and PU are not mobile, the scenario is static and straightforward in a sense that the distance between the SU and PU is not changing with respect to time. When the SU is mobile, the PU may fall within (outside) the sensing range of SU or fall outside (inside) the sensing range after certain observation/travel time. Speed and direction of an SU in vehicular networks also determine whether or how long the SU can fall within the PUs' range. Furthermore, the PU's activities also has significant impact on the sensing performance. In a typical vehicular network, unlike other mobile ad-hoc networks, SUs in vehicular networks move in same direction or opposite directions based on the road structure. The distance between SUs and PUs is a critical parameter for spectrum sensing because distance determines whether a PU is inside the sensing range of SU or not. This distance depends on the relative speed of SU and PU. Note that in case of intersection, relative speed is determined using speed times the cosine of the angle [50]. Based on the speed of SU, the probability that the sensing range covers PU or PU lies outside the sensing range is derived. In this chapter, analytical

expressions of the probability of misdetection and the expected overlapping time duration based on velocity of SUs are developed, transmission range of PU, sensing range of SU and transmission activities of PU.

The rest of the chapter is organized as follows. the system model is presented in Section 3.2. In Section 3.3, joint impact of SU mobility and PU activity on the performance of spectrum sensing in cognitive vehicular networks is presented in terms of probability of misdetection. Section 3.4 introduces the impact of SU speed on the expected overlapping time duration between PU and SU. The numerical results obtained from simulations are presented in Section 3.5. And finally, the concluding remarks are presented in Section 3.6.

3.2 System Model and Problem Statement

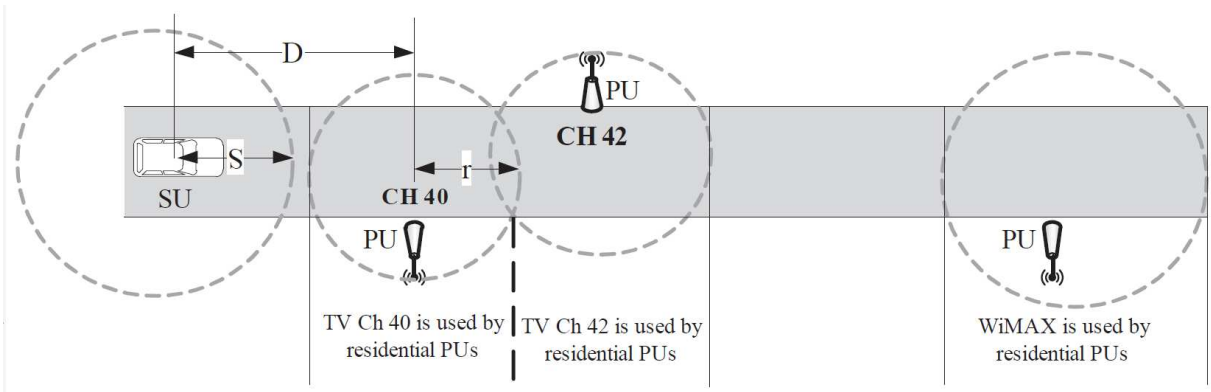


Figure 3.1: Sample scenario with a road segment containing TV/WiMAX residential roadside users as stationary PUs with their protection ranges r and a mobile SU with its sensing range s in cognitive vehicular network.

The system model used in this chapter is shown in Figure 3.1. This typical scenario has one vehicle representing SU and multiple PUs with their protected regions/radii. SU has sensing range s. For analysis purpose, it is considered that the residential TV/WiMAX network users are PUs and transmission range r of their base-stations/access points gives

the protection range for PUs as shown in Figure 3.1. it is assumed that sensing range of SU is longer than the protection range of PU. To illustrate the scenario clearly, a single SU and stationary PUs are considered in the system model

as shown in Figure 3.1, however, the analysis presented in this chapter is applicable to multiple SUs. According to the system model, the relative speed between mobile SU and stationary PU is equal to the speed of the SU as the PU is stationary. The distance between PU and SU depends on their initial distance between them and their relative speed. The overlap duration between PU and SU depends on their speed and direction, transmission range of PU and sensing range of SU. When an SU moves towards a PU, they begin being withing the communication range of each other for some time and when the SU moves away from the PU, they get disconnected after some time. The received signal $s_r(t)$ at a given mobile SU can be just noise or signal from PU plus the noise that corrupts the received signal. Note that the PU channel activity can be demonstrated by two state birth-death process [11]. Thus, for spectrum sensing, received signal at SU can be detected using two possible hypotheses as

$$s_r(t) = \begin{cases} n(t), & \mathcal{H}_0 \\ g.s(t) + n(t), & \mathcal{H}_1 \end{cases} \tag{3.1}$$

where $s(t)$ is the signal coming from PU, g is the channel gain between given PU and SU, $n(t)$ is the additive white Gaussian noise, and hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, represent that the PU signal is either absent or present in the received signal $s_r(t)$ in (3.1). The test statistics for distinguishing between two hypotheses using energy detection is given as

$$R_E = \frac{1}{W} \sum_{j=0}^{W-1} |s_r(j)|^2 \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \lambda \tag{3.2}$$

where W is the sensing window length and λ is a decision threshold [51]. The process of threshold selection for energy detection is addressed by the Constant False Alarm Rate (CFAR) method and selection is carried out considering present conditions of noise levels.

The misdetection and false alarm probabilities depend on the threshold λ, and hence it is necessary to choose an appropriate value based on the requirements.

When there is no overlap between the transmission range of a PU and the sensing range of an SU, the SU perceives that there is no PU active. In this case, the received signal is just a noise for both $\mathcal{H}_0$ and $\mathcal{H}_1$ and thus the PU 'absent' event is defined as the event A. Similarly, when an SU senses the channel and it detects that there is PU signal in a given channel (that is, hypothesis $\mathcal{H}_1$), this 'busy' event is denoted as the event B.

So, the main target of this study is to formulate the velocity of secondary users, determining the probability of event "A" and "B" and the PU activity, inspecting the impact of the velocity of SUs and the activity of PUs on the performance of spectrum sensing of SUs in CRN.

3.3 Impact of SU Mobility and PU Activity on Spectrum Sensing

In this section, the effect of mobility on spectrum sensing for vehicular network users is investigated by considering the probability of misdetection and the expected overlapping time duration.

3.3.1 Probability of presence or absence of PU

First of all it is assumed that the event A represents PU is absent in a given channel i.e., the channel is idle and the event B represents PU is present in a given channel i.e., the channel busy. The probability of the event A and B depends on the distribution function of separation distance between a fixed PU and a mobile SU. Note that the vehicles' mobility is predefined by the road structure and typically they travel in a linear track. As discussed, the radius r is the protected radius/region for PUs which implies that no SUs can use channels used by PUs in the protected region of road segment of length $2r$ as shown in Figure 3.1.

Let us start with static scenario first. The probability distribution of existence of a link (so that an SU can sense the channel) between two vehicles separated by a distance d is log-normal and is given by [52]

$$F_R(d = r) = \int_{-\infty}^{r} \frac{1}{\sigma_z\sqrt{2\pi}} \exp\frac{(z-\mu_z)^2}{2\sigma_z^2} dz = \frac{1}{2}[1 + \text{erf}(\frac{r-\mu_r}{\sigma_r\sqrt{2}})] \tag{3.3}$$

where $er\,f(.)$ is an error function, μ_z and σ_z are, respectively, the average and standard deviation values of the transmission range of PU.

Similarly, for a sensing range of the SU, it can be written that

$$F_S(s) = \frac{1}{2}[1 + \text{erf}(\frac{s-\mu_s}{\sigma_s\sqrt{2}})] \tag{3.4}$$

where μ_s and σ_s are, respectively, the average and standard deviation values of the sensing range of SU.

When the separation distance between a PU and an SU is D, the condition for the PU being inside the sensing range of SU is $r < D \leq S$. Then, the probability for the event B, that is, $Pr(B)$, the probability that the PU is inside the sensing range of SU can be computed as

$$P_r(B) = P_r(r < D \leq S) = F_S(s)F_R(r) = \frac{1}{2}[\text{erf}(\frac{s-\mu_s}{\sigma_s\sqrt{2}}) - \text{erf}(\frac{r-\mu_r}{\sigma_r\sqrt{2}})] \tag{3.5}$$

Then, the probability for the event A, $P_r(A)$, that is, the probability that the PU is outside the sensing range can be computed as

$$Pr(A) = 1 - 2Pr(B) \tag{3.6}$$

Note that the $P_r(B)$ in (3.5) gives the probability that the SU's sensing range covers the PU and it detects that the PU is present in a given channel. However, it does not consider SU's mobility which is discussed as below.

Note that the speed of different vehicles in free flow state is a Gaussian distribution [53], and for $v_{min} = \mu_v 3\sigma_v$ and $v_{max} = \mu_v + 3\sigma_v$ as minimum and maximum level of the vehicle

speed, the probability density function (PDF) is given by [52]

$$g_V(v) = \frac{f_V(v)}{\int_{v_{min}}^{v_{max}} f_V(v)dv} \tag{3.7}$$

where

$$f_V(v) = \frac{1}{\sigma_v\sqrt{2\pi}} \exp\left(\frac{-(v-\mu_v)^2}{2{\mu_v}^2}\right) \tag{3.8}$$

is the Gaussian PDF with a average speed μ_v and standard deviation σ_v. Then, $g_V(v)$ can be written as

$$g_v(v) = \frac{2f_V(v)}{erf\left(\frac{v_{max}-\mu_v}{\mu_v\sqrt{2}}\right) - erf\left(\frac{v_{min}-\mu_v}{\mu_v\sqrt{2}}\right)} \tag{3.9}$$

Then, the expected value of speed can be computed as

$$E[V] = \bar{v} = \int_{v_{min}}^{v_{max}} v g_V(v)dv \tag{3.10}$$

Whether a PU and an SU are reachable or not after certain time t can be checked by using SU's initial speed, its acceleration and time interval. For a given vehicle with its initial speed $\bar{v}(0)$, the instantaneous speed $v(t)$ at time t can be computed as

$$v(t) = \bar{v}(0) + \int_0^t a(y)dy \tag{3.11}$$

where $a(y)$ is the acceleration of a vehicle at time y. Using (3.11), the distance traveled by a given vehicle for a given time interval $[0, t]$ is defined as

$$D_{su}(t) = \int_0^t v(y)dy \tag{3.12}$$

Thus, using (3.12), each vehicle can compute its distance traveled in time period t. Then, the distance between the mobile SU and stationary PU for the interval $[0, t]$, where the SU is approaching PU and initial separation distance between them was D, is computed as

$$D_e = |I(su)D_su(t) + D| \tag{3.13}$$

where $I(su) \in \{1, 1\}$, i.e., if SU is approaching PU, then $I(su) = 1$, and if the SU is moving away from PU, then I(su) = 1.

The PDF of the random variable time $T = t$ can be easily derived as

$$f_T(t) = \int_0^{\bar{v}} v\, f_D(|I(su)xS_{su}(t) + D|)\, f_V(v)dv \tag{3.14}$$

Then, the probability of event B, $P_r(B)$, with respect to SU's velocity v can be further derived as

$$\begin{aligned} Pr(B) = Pr(r < (|I(su)xS_{su}(t) + D|) \leq S) &= \int_{\frac{r-D}{\bar{v}}}^{\frac{S-D}{\bar{v}}} f_T(t)dt \\ &= \int_{\frac{r-D}{\bar{v}}}^{\frac{S-D}{\bar{v}}} \int_0^{\bar{v}} v \frac{1}{\sqrt{2\pi}\sigma_v} [\exp\{-\frac{(v-\mu_v)^2}{2\sigma_v^2}\}]^2 dv dt \end{aligned} \tag{3.15}$$

Then, the probability of event A can be calculated as

$$Pr(A) = 1 - Pr(B) \tag{3.16}$$

From (3.15), it can be seen that $Pr(B)$ depends on sensing range of SU, velocity of SU and initial distance between the PU and SU, and protected radius of PU.

3.3.2 Probabilities of PU Activities

In wireless networks, the nodes being active and idle are exponentially distributed with parameters α and β respectively [54]. Then the probabilities of PU being present/active and absent/idle are, respectively, represented by p_p and p_a and are given as

$$p_p = \frac{\alpha}{\alpha + \beta} \tag{3.17}$$

and

$$p_a = \frac{\beta}{\alpha + \beta} \tag{3.18}$$

With this information, if a given channel was not used by a PU during previous sensing period and the probability of a given channel being used by the PU in current sensing period

is given by

$$Pr_{(OFF \rightarrow ON)} = p_p - p_p.\exp\{-(\alpha + \beta)t\} \tag{3.19}$$

where the probability $Pr(OFF \rightarrow ON)$ represents that the channel will be used by a PU during current sensing period t, which was idle during previous sensing period.

Similarly, in the previous sensing period, a channel was used by a PU and the probability of this channel being used by the PU again in current sensing period is given by

$$Pr_{(ON \rightarrow ON)} = p_p - p_a.\exp\{-(\alpha + \beta)t\} \tag{3.20}$$

where the probability $Pr(ON \rightarrow ON)$ represents that the channel will be used by the PU during current sensing period t which was active during previous sensing period.

3.3.3. Effect of SU Mobility and PU Activity on Probability of misdetection

In this section, impact of SU mobility and PU activity on spectrum sensing is investigated through the probability of misdetection, which is the probability that an SU detects no PU signal (i.e., wrong decision about the presence of PUs) when a PU is actually present. The probability of misdetection, $Pr(miss)$, can be expressed as follows

$$\begin{aligned} Pr(miss) = {} & Pr(R_E \leq \lambda | \mathcal{H}_1, B) Pr(B) Pr_{(ON \rightarrow ON)} \\ & + Pr(\lambda \leq R_E | \mathcal{H}_0, A) Pr(A) Pr_{(OFF \rightarrow ON)} \end{aligned} \tag{3.21}$$

where R_E is the energy of the received signal at SU in (3.2), λ is the threshold, and $Pr(B)$ and $Pr(A)$ are, respectively probabilities of PU being inside and outside the sensing range of SU. The probabilities $Pr(R_E \leq \lambda | \mathcal{H}_1, B)$ and $Pr(\lambda \leq R_E | \mathcal{H}_0, A)$ represent the conditional probability of misdetection for the event B and event A respectively. To find these conditional probabilities $Pr(R_E \leq \lambda | \mathcal{H}_1, B)$ and $Pr(\lambda \leq R_E | \mathcal{H}_0, A)$, energy detection given in (3.2) is used to find whether there is PU signal present or not [11, 51]. The energy of the signal is compared against the threshold and decision is made based on (3.2).

For a given SU with the event B, the conditional probability $Pr(R_E \leq \lambda|\mathcal{H}_1, B)$ can be written using $Q(.)$ function as follows

$$Pr(R_E \leq \lambda|\mathcal{H}_1, B) = 1 - Pr(R_E > \lambda|\mathcal{H}_1, B) = 1 - Q(\frac{\lambda - E(R_E|\mathcal{H}_1, B)}{\sqrt{Var(R_E|\mathcal{H}_1, B)}}) \tag{3.22}$$

where $E(R_E|\mathcal{H}_1, B) = n(\sigma_{noi}^2 + \sigma_{sig}^2)^2$ with $n = 2$ degree of freedom in vehicular network and $Var(R_E|\mathcal{H}_1, B) = 2n(\sigma_{noi}^2 + \sigma_{sig}^2)^2$ for noise variance σ_{noi} and received signal variance σ_{sig} [48]. Similarly, for the event A, the conditional probability $Pr(\lambda \leq R_E|\mathcal{H}_0, A)$ can be written as follows

$$Pr(\lambda \leq R_E|\mathcal{H}_0, A) = 1 - Pr(\lambda > R_E|\mathcal{H}_0, A) = 1 - Q(\frac{\lambda - E(R_E|\mathcal{H}_0, A)}{\sqrt{Var(R_E|\mathcal{H}_0, A)}}) \tag{3.23}$$

where $E(R_E|\mathcal{H}_0, A) = n(\sigma_{noi}^2)^2$ and $Var(R_E|\mathcal{H}_0, A) = 2n(\sigma_{noi}^2)^2$.

By substituting (3.15), (3.16), (3.19), (3.20), (3.22) and (3.23) into (3.21), the probability of misdetection Pr(miss) for a given SU where sensing range of SU, protection range of PU, velocity of SU and threshold in energy detection will influence the sensing performance can be computed. Once the probability of miss detection (3.21) is computed, the probability of successful detection as $Pr(success) = 1 - Pr(miss)$ can also be computed.

Note that the impact of speed of vehicular secondary user and activity of primary user have no significant impact on false alarm probability.

3.4 Expected Overlap Time Duration Between Stationary PU and Mobile SU

For the expected velocity $E(v)$ and PU's sensing range s, the expected value of overlapping time duration T available between stationary PU and mobile SU can be computed as

$$E[T] = \frac{s}{E(V)} \tag{3.24}$$

Eq. (3.24) does not consider the impact of initial distance between PU and SU, and assumes that the PU and SU are within the communication range of each other at the beginning.

However, the expected time duration depends jointly on the sensing range of SU, the initial distance between PU and SU, and the speed of SU. Thus, the overlapping time duration T is a random variable with a PDF in (3.14) and its expected value can be computed as

$$E[T] = \int_0^t t f_T(t) dt \tag{3.25}$$

By substituting (3.14) into (3.25), the expected overlapping time duration can be computed as

$$E[T] = \int_0^t x \int_0^{\bar{v}} v \frac{1}{\sqrt{2\pi}\sigma_v} [\exp\{-\frac{(v-\mu_v)^2}{2\sigma_v^2}\}]^2 dv dx \tag{3.26}$$

where $t = (S - D)/\bar{v}$.

Note that in order for a mobile SU to be able to sense the PU signal correctly, the value of $E(T)$ in (3.26) should be greater than or equal to sensing time W in (3.2), that is, $E(T) \geq W$. Otherwise, the SU would not have enough time to collect sufficient signal samples to make a correct decision.

3.5 Numerical Analysis

In this section, different scenarios are simulated to corroborate the theoretical analysis presented in previous sections. It is considered that the SU is mobile and has its sensing range, and the PU is stationary (residential base station or access point) and has its protection range where SUs are not allowed to use its licensed channels.

To corroborate mathematical analysis, a simulation scenario with a network area of 100m radius is considered where SUs, eavesdropper and jammer are located and $M = 5$ channels are assumed to be available in that region for the users. The transmission power of SUs is varied between 0.01mW and 30mW. It is assumed that the variance of Gaussian noise is $\sigma^2 = 120$dBm, the path loss exponent is set to $\mu = 4$ and $w_m = 1$. All the gathered results are averaged over random positions of the SUs, eavesdroppers and jammers, channel

gains, and the channel availability P_x.

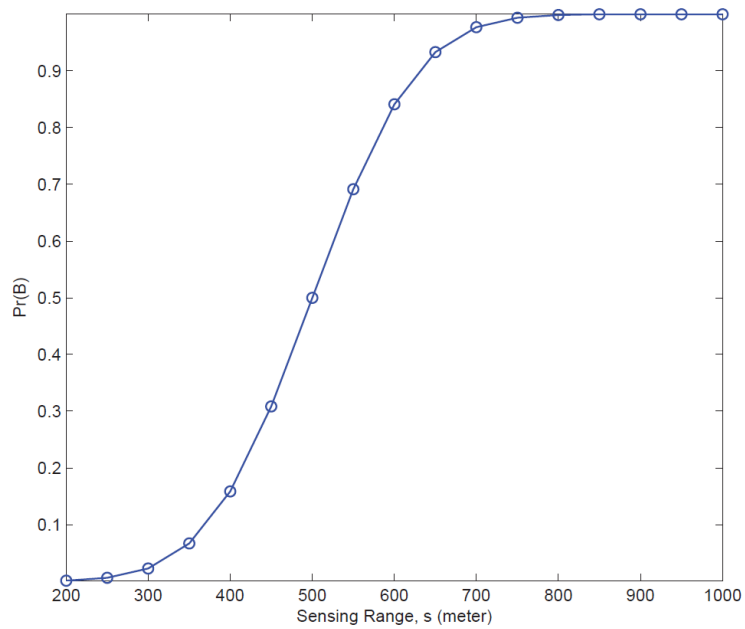


Figure 3.2: Variation of probability of PU being inside the SU's sensing range, i.e., $Pr(B)$, versus variable sensing ranges for protection range of PU $r = 100$ meter.

First, the variation of probability of PU being inside the SU's sensing range, $Pr(B)$, with different sensing range values using (3.15) is plotted as shown in Figure 3.2. The maximum sensing range of SU is considered as 1000 meter (this is the maximum range in 802.11p DSRC standard for vehicular networks). It is observed that when sensing range increases from 200 meter to 1000 meter, as expected, the probability of PU being within the sensing range of SU ($Pr(B)$) increases as shown in Figure 3.2. From the figure it is clear that probability of PU being inside the sensing range drastically increases for sensing range from 400 meters to 700 meters. At 500 meters the probability is almost 50%. Here the considered protection range for PUs is 100 m. For this protection range probability of PU being inside the SU's sensing range does not experience much change after the sensing range is increased further from 750 m.

Second, the variation of probability of misdetection $Pr(miss)$ versus the speed of

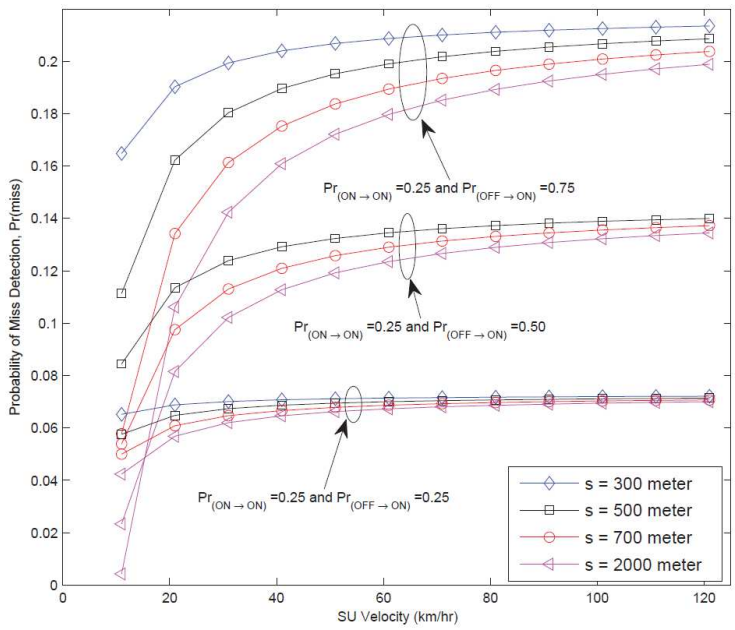


Figure 3.3: Variation of probability of misdetection for PU activities versus the velocity with different sensing ranges of a SU and $PU_{(OFF \rightarrow ON)} = 0.25$.

mobile SU where a given PU's protection range $r = 100$ meter, initial separation distance between PU and SU $D = 200$ meters and SU's sensing ranges ($s = 300, 500, 700$ and 1000 meter) using (3.21) is plotted as shown in Figure 3.3. In this case, the probability $PU_{(OFF \rightarrow ON)}$ is also varied from 0.25 to 0.50 to 0.75 to see how PU's $OFF \rightarrow ON$ activity impacts the performance of misdetection. In Figure 3.3, it is observed that the probability of misdetection, $Pr(miss)$, decreases when sensing range of SU increases for a given $PU_{(OFF \rightarrow ON)}$ value. However, the probability of misdetection increases when speed of the mobile SU increases for a given $PU_{(OFF \rightarrow ON)}$ value. In other words, a faster speed results in a higher probability of misdetection as faster speed makes PU to be outside of the SU's sensing range quickly resulting in higher chance of miss detection of PUs signal. It is also observed that when the probability of PU being active during sensing period (when it was idle in previous sensing period) increases from 0.25 to 0.50 and again from 0.50 to

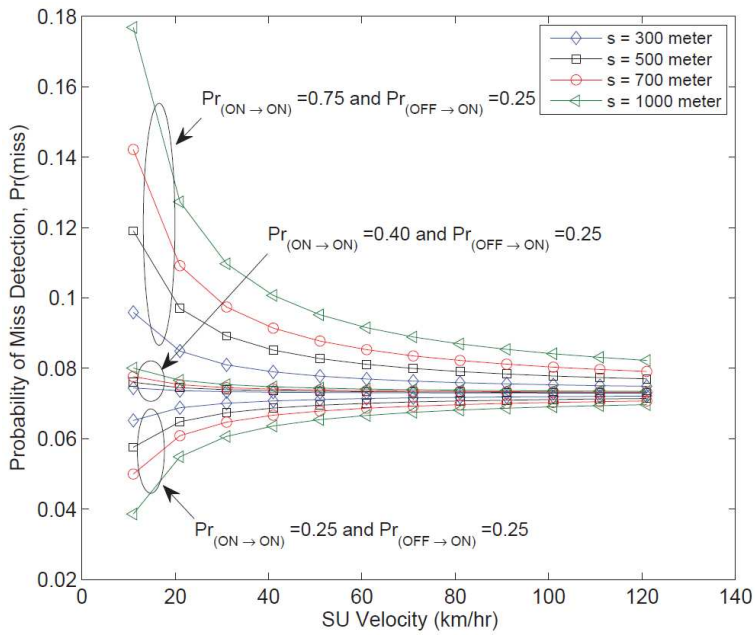


Figure 3.4: Variation of probability of misdetection for different $PU_{(ON \rightarrow ON)}$ values versus the velocity with different sensing ranges of a SU and $PU_{(OFF \rightarrow ON)} = 0.25$.

0.75, the probability of misdetection increases by approximately 6% in each case with SU's speed being higher than 45 km/hr as shown in Figure 3.3. This happens since PU was idle in previous sensing period and it is expected to be idle during current sensing period with given probability but it is not which results in higher misdetection probability for a given sensing range. If a closer look is given upon Figure 3.3 it is seen that when the probability of PU being ON in the current sensing period is 25% if PU is ON in the previous sensing period and 75% if the PU is OFF in the previous sensing period the probability of misdetection is highest. With increasing value of sensing range the probability of misdetection decreases as the PU stays inside the sensing range with higher probability and even with mobile SUs the chance of PU being inside the sensing range is higher.

Next, different values of $PU_{(ON \rightarrow ON)}$ are considered and the variation of probability of misdetection versus the velocity of SU is plotted where a given PU's protection range

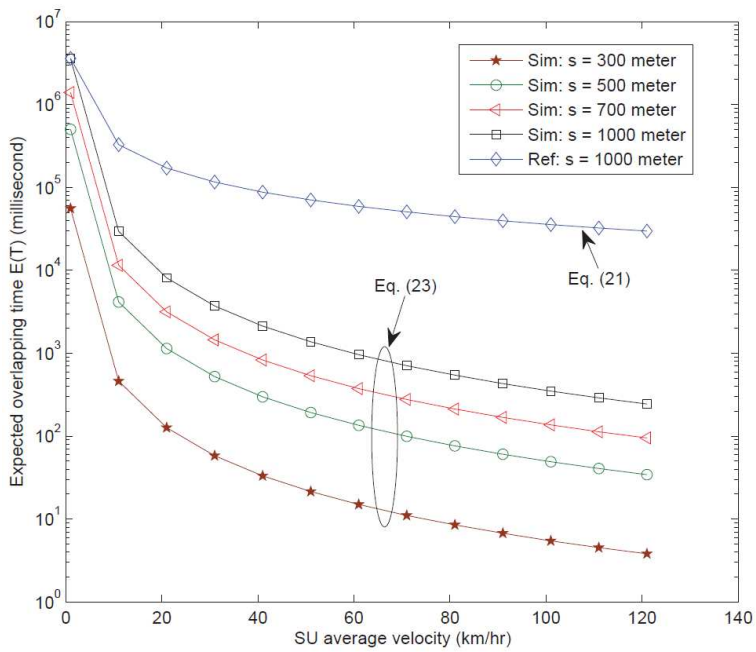


Figure 3.5: Expected value of overlapping time per epoch versus the SU velocity where protection range of PU $r = 100$ meter and initial separation distance between PU and SU $D = 200$ meter.

$r = 100$ meter, initial separation distance between PU and SU $D = 200$ meters and SU's sensing ranges ($s = 300, 500, 700$ and 1000 meter) using (3.21) is plotted as shown in Figure 3.4. In this case, the probability $PU_{(ON \to ON)}$ is varied from 0.75 to 0.40 to 0.25 to see how PU's $ON \to ON$ activity impacts the performance of misdetection. It is seen from Figure 3.4 that the misdetection probability decreases for a given velocity if $PU_{(ON \to ON)}$ also decreases. But for a fixed value of $PU_{(ON \to ON)}$ probability of misdetection does not behave in the same manner. When $PU_{(ON \to ON)}$ is greater than $PU_{(OFF \to ON)}$, the misdetection probability starts decreasing for increasing velocity of the SU and When $PU_{(ON \to ON)}$ is lower than $PU_{(OFF \to ON)}$, the misdetection probability starts increasing for increasing velocity of the SU as shown in Figure 3.4.

Furthermore, from both Figure 3.3 and Figure 3.4, it is observed that when probability

$PU_{(OFF \rightarrow ON)}$ is greater than or equal to the probability $PU_{(ON \rightarrow ON)}$, the probability of miss detection increases.

Finally, using (3.24) and (3.26), the variation of expected overlapping duration per epoch versus the SU's velocity is plotted as shown in Figure 3.5. In this scenario, the protection range of PU $r = 100$ meter, an initial separation distance between PU and SU $D = 200$ meter, and SU's sensing range $s = 1000$ meter are considered for reference plot in Figure 3.5. The SU's sensing range is varied as $s = 300, 500, 700$ and 1000 meter and is used in (3.26). In Figure 3.5, it is observed that the expected overlapping duration per epoch decreases with increasing velocity for given sensing range and it increases with increasing sensing range of SU. This can be interpreted as, for higher sensing range, the PU has a higher possibility to fall into the SU's sensing range for longer overlapping duration and for lower sensing range, the PU has a lower possibility to fall into the SU's sensing range for shorter overlapping duration. Furthermore, from Figure 3.5, it is observed that the expected overlapping time using (3.24) is highest since it assumes that initial separation distance between PU and SU is equal to the sensing range of SU, and PU and SU are assumed to be within the communication range of each other at the beginning.

3.6 Chapter Summary

In this chapter performance of spectrum sensing of the secondary users taking secondary users' mobility and primary users' activity into consideration is evaluated with the help of probability of misdetection and expected value of overlapping time. First a system model is developed to depict the real like scenario for a vehicle working as secondary user and residential TV/WiMAX network users working as primary users. Two hypotheses are then introduced to present the two spectrum state scenarios the cognitive radio network can experience. The fist one is $\mathcal{H}_0$ representing that the primary user is either absent or inactive and the second one is $\mathcal{H}_1$ representing that the primary user is present and

currently engaging the spectrum bands into use. Probability of the primary user being inside the sensing range of the secondary user is determined with the help expected value of secondary user's velocity, initial and instantaneous distance. The expected velocity of the secondary users is determined with the help of average velocity and variation in velocity found from Gaussian distribution of the free flow state of vehicles. Primary user's activity is determined based on whether the primary user is turning into 'ON' mode in the current sensing period from 'ON' mode or 'OFF' mode in the previous sensing period. Later both of the secondary user mobility and primary user activity are used to determine the probability of misdetection and expected value of overlapping time.

The numerical analysis is presented in Section 3.5. It is observed from the numerical analysis that the probability of misdetection shows proportional behavior with respect to velocity of secondary users. With increase in velocity of the secondary users the probability of misdetection decreases and with decrease in velocity of the secondary users the probability of misdetection increases. Expected value of overlapping time shows different behavior than that of the probability of misdetection. It decreases with increase in velocity of secondary users and increase with decrease in velocity of secondary users.

CHAPTER 4

PHYSICAL LAYER SECURITY IN COGNITIVE RADIO NETWORKS

Cognitive radio network is regarded as an emerging technology to solve 'spectrum scarcity' through dynamic spectrum access to support exponentially increasing wireless subscriptions. However, spectrum sensing and dynamic spectrum sharing in cognitive radio network invite more security attacks making security as one of the main concerns [36, 37]. In this chapter, the performance of the secondary users in terms of physical-layer security in the presence of both eavesdroppers and jammers is analyzed in cognitive radio networks. In this case, secondary users not only have to compete against eavesdroppers and jammers (who are trying to reduce the secrecy rates of secondary users) but also have to compete with other secondary users to gain access to idle channels to gain high secrecy rates. In this chapter a game theoretical model is investigated to maximize utility of secondary users in the presence of eavesdroppers and jammers. The proposed approach can be particularized to a scenario with eavesdroppers only or jammers only while evaluating the performance of secondary user physical layer security. Performance of the proposed approach is evaluated with the help of numerical results obtained from simulations and the proposed approach outperforms other existing methods. Furthermore, there is sever impact on utilities (secrecy rates) of secondary users when both eavesdroppers and jammers are active in the network.

4.1 Background

Cognitive radio (CR) is regarded as an emerging technology that can relieve wireless communication system from the pressure of spectrum shortage. CR technology allows unlicensed users aka secondary users (SUs) to access under utilized spectrum bands of the licensed primary users (PUs) opportunistically without causing harmful interference to PUs. CR technology helps SU devices learn from their operating wireless environment and helps them to adapt dynamically according to their wireless environment by changing

their transmit parameters such as channels, transmit power/rate, modulations, etc. Due to the capability of spectrum sensing and sharing idle bands, CR system is highly dynamic and reconfigurable which enables SUs to change channels immediately from one to another when PU is detected in the current channel and change SUs' transmit parameters accordingly [55–57]. Although, dynamic spectrum access is one of the most efficient approaches to solve spectrum scarcity problem in wireless communications, it introduces various types of security threats and challenges to users in the network because of its openness to the environment and sharing nature to other SUs [42, 58–61]. Therefore security of wireless users is one of the most important traits of cognitive radio networks. There are several kinds of attacks in cognitive radio networks including eavesdropping (aka passive attack) and jamming (aka active attack) [42, 62].

Recent studies related to security in cognitive radio networks include [4, 42, 63–69]. The power control based approach for SUs when there are smart jammers present in the network has been studied using Stackelberg game in [66]. The jammers are capable of adjusting their transmission power according to the change in the transmission power of the users to magnify the harmful impact on the users. In [63], it was shown that improving the quality of the cognitive channel with respect to the eavesdropper's channel, the secrecy throughput of the system can be improved to a limited extent but after some point the throughput reaches saturation. In [64], the authors have proposed to characterize secrecy capacity in the presence of multiple colluding eavesdroppers. The authors in [4] have analyzed the interactions between SUs and eavesdroppers in a cognitive radio network in the presence of multiple primary users. Similarly, in [65], a framework for cross-layer detection of stealthy jammers in multi-hop CR network was proposed. The cross layer framework is capable of detecting the distribution changes of the jammers at different layers with minimum delay. In [67], the authors derived a simple closed-form expression of cognitive radio throughput in a simplified jamming with the help of Markov model. In [68],

the authors proposed a game theoretic model which shows how SUs and malicious attackers can obtain the maximum utility simultaneously using the history of the previous attacks. However, none of these method consider combined impact of eavesdroppers and jammers on the performance of SUs' utility in cognitive radio networks.

In this chapter, the joint impact of eavesdroppers and jammers on SUs' physical layer security is investigated by using game theory. The goal of the eavesdroppers is to overhear the channel for the information passively to reduce secrecy rates of legitimate SUs. Furthermore, the objective of the jammers is to inject high power signal to jam legitimate channels or to deteriorate the signal-to-interference-plus-noise ratio (SINR) at legitimate SU receiver with an aim to reduce the secrecy rates of legitimate SUs. In this work, jammers and eavesdroppers are called attackers and assumed to be independent and work without cooperation to provide threat to cognitive radio networks. The rest of the chapter is organized as follows. The system model considered in this chapter is presented in Section 4.2 followed by the game formulation in Section 4.3. Numerical results obtained from simulations are presented in Section 4.4. And finally, conclusions are drawn in Section 4.5.

4.2 System Model and Problem Statement

The system model considered in this chapter is shown in Figure 4.1 where P unlicensed SU transmitter and receiver pairs access idle channels dynamically for peer-to-peer communications on equal priority basis in the presence of multiple eavesdroppers and jammers. It is assumed that the probability of any channel being available to the SUs is P_x. The combination of a set of Q eavesdroppers and a set of R jammers is considered as attackers. d_s, d_j, and d_e, respectively, represent the distance between transmitter and receiver of legitimate SU link, distance between jammer j and receiver of p-th link of SU, and distance between eavesdropper q and transmitter of p-th SU link.

It is assumed that the channel (if available) follows Rayleigh fading where the channel gain for a given SU link p in channel m is given by ${g^S}_{p,m} = \alpha_m.d_s^{-\mu}$, where μ is path loss exponent, α_m is Rayleigh fading amplitude in channel m, The channel gain for the eavesdropper for the signal received from SU's pth link in chanel m is ${g^E}_{q,m} = \alpha_m.d_e^{-\mu}$. Channel gain in m-th channel for p-th SU receiver and jammer is ${g^J}_{r,m} = \alpha_m.d_j^{-\mu}$.

The objective of SUs is to look for idle channels to access them opportunistically and choose the one that provides the highest transmission rate. In cognitive radio network, SU p has to share the channels with other SUs. Thus, there will be transmission from some different SUs on the same channel m resulting in interference from other SUs. At the same time, jammers will also try to block the communication signals between the communicating SUs or deteriorate the SINR of SUs to reduce their rates. When there are no attackers, the

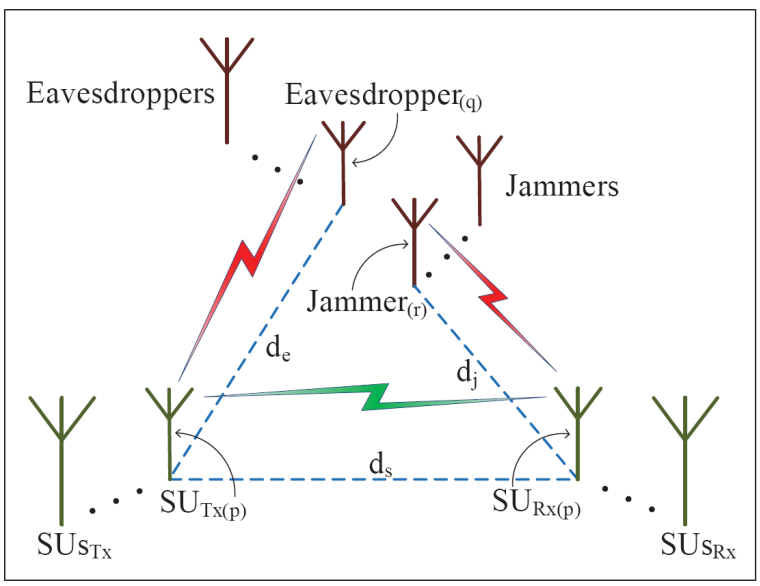


Figure 4.1: System model showing the secondary users and attackers and their corresponding distances

SINR at the SU receiver p in m-th channel is given by

$$\gamma_{p,m} = \frac{g^S{}_{p,m}.P^S{}_{p,m}}{\sum\limits_{p' \in \mathbb{P}, p' \neq p} g^S{}_{p',m}.P^S{}_{p',m} + \sigma^2} \tag{4.1}$$

where $P^S{}_{p,m}$ is the transmit power of the p-th SU in channel m. The achievable rate (capacity) of SU in a given channel m with bandwidth w_m can be calculated as,

$$C_p^m = \beta_m[w_m \log(1 + \gamma_{p,m})] \tag{4.2}$$

where $\beta_m \in 0, 1$, i.e., if channel m is available for the SUs, $\beta = 1$. Otherwise, $\beta = 0$.

If channel m is not available for SUs, the value of C_p^m is zero. The goal of the SU link is to maximize the achievable rate in (4.2) by choosing suitable channels. However, in the presence of attackers (eavesdroppers and jammers), the SUs responsibility become a little complex. Instead of limiting themselves in maximizing the channel capacity, the SUs try to choose a suitable channel that can help them to set up a secure communication link. In this scenario the objective of each SU turns into selecting such a channel from the available ones which can provide the highest secrecy rate at a minimum transmission cost for per unit power. This brings the SUs in a competitive environment not only because they have to compete against the attackers but also because they have to compete with each other to gain access to the available channels so that they can maintain the maximum secrecy rate. On the other hand the attackers try to reduce the secrecy rate of the whole cognitive radio network or at least a subset of SUs on the price of high transmission cost per unit power, by choosing their optimal channels. To calculate the channel capacity of the attackers the signal strength (i.e., SINR) of p-th SU in m-th channel at the eavesdroppers and signal strength of jammers at a given p-th SU receiver separately are measured. For eavesdroppers, the received signal strength (SINR) from p-th SU and interference from jammers in m-th channel can be expressed as

$$\gamma_{q,m} = \frac{g^E{}_{q,m}.P^S{}_{p,m}}{\sum\limits_{p' \in \mathbb{P}, p' \neq p} g^E{}_{q,m}.P^S{}_{p',m} + \sum\limits_{r \in \mathbb{R}} g^J{}_{r,m}.P^J{}_{r,m} + \sigma^2} \tag{4.3}$$

Thus, the channel capacity between p-th SU transmitter and q-th eavesdropper on channel m is expressed as

$$C_{p,q}^{m} = \begin{cases} w_m \log(1 + \gamma_{q,m}), & \text{if } \gamma_{q,m} \geq \bar{\gamma}_{q,m} \\ 0, & \text{otherwise} \end{cases} \tag{4.4}$$

where $\bar{\gamma}_{q,m}$ is the minimum SINR that eavesdropper needs to decode the SU signal. If $\gamma_{q,m} < \bar{\gamma}_{q,m}$, eavesdropper cannot decode the signal.

Furthermore, the jammers objective is to deteriorate the SINR of the SU receiver by transmitting a signal towards receiver of the SU link. Due to the transmit power of the jammer, the signal strength (SINR) from jammer r to p-th SU receiver in channel m is expressed as

$$\gamma_{r,m} = \frac{{g^J}_{r,m}.{P^J}_{r,m}}{\sum\limits_{p\in\mathbb{P}} {g^S}_{p,m}.{P^S}_{p,m} + \sum\limits_{r'\in\mathbb{R},r'\neq r} {g^J}_{r',m}.{P^J}_{r',m} + \sigma^2} \tag{4.5}$$

Thus the channel capacity for the link between jammer and p-th receiver on channel m can be expressed as

$$C_{r,p}^{m} = w_m \log(1 + \gamma_{r,m}) \tag{4.6}$$

Along the line of [70], the secrecy rate achieved by SUs in the presence of both eavesdroppers and jammers for SU link p in channel m can be expressed as

$$\widetilde{C}_{p}^{m} = [C_{p}^{m} - \max_{q\in\mathbb{Q}} C_{p,q}^{m} - \sum_{r=1}^{R} C_{r,p}^{m}]^{+} \tag{4.7}$$

where $[x]+ := \max(x, 0)$. Thus, the channel congestion (because of multiple SUs), eavesdropping and jamming are working together to decrease the overall secrecy rate of SUs. The next thing comes into consideration is how an SU trades between the presence of channel congestion and attackers. While the SUs try to maximize their secrecy rate, there is obviously a trade-off between going for a tightly congested channel with better rate of secrecy (less attackers) against a lightly congested channel with worse secrecy rate (more attackers).

So the main objective of this study in this chapter is to formulate utility functions for all the users (secondary users, eavesdroppers, and jammers) in the CRN so that an optimization point can be attained using the utility functions in a non-cooperative selfish game.

4.3 Game Formulation and Solution

The system model formulated here is made of selfish players such as the SUs and the attackers. Their main concern is to maximize their utility function. The structure of non-cooperative game theory is employed to evaluate the selfish interaction between the SUs and the attackers [71–74].

Let us assume that the set of SUs $\mathbb{P}$ and the set of eavesdroppers $\mathbb{Q}$ and set of Jammers $\mathbb{R}$ contribute as the combined set of players in the network and express it by $\mathbb{H} = \mathbb{P}, \mathbb{Q}, \mathbb{R}$. Players from set $\mathbb{H}$ select their actions from the same action space $\mathbb{M}_e = \mathbb{M}\ \forall e \in \mathbb{H}$ of size M (total number of channels available in the system). The action of the SU p, $m_p \in \mathbb{M}_p$ stands for the channel that SU p selects for transmission. The action of the eavesdropper q as $m'_q \in \mathbb{M}_q$ and action of the jammer r, $m'_r \in \mathbb{M}_r$ respectively represent eavesdropper q and jammer r select the channel for eavesdropping or jamming respectively. Therefore, the secrecy rates can be defined as function of the channels the SUs or attackers relying on.

The transmission cost per unit power of the SUs and the jammer is considered as T_S and T_J respectively. Then the transmission costs of SUs and jammers are $P^S_{p,m}.T_S$ and $P^J_{r,m}.T_J$ respectively. Based on PUs' activity on the channel, the secrecy rate on the channel and the total transmission cost, the utility function of a SU $p \in \mathbb{P}$ which selects an action $m_p \in \mathbb{M}p$ can be expressed as,

$$U_{SU}(m_p, \boldsymbol{m_{-p}}, m'_{q,r}) = P_x[C^m_p(m_p) - \max_{q\in\mathbb{Q}} C^m_{p,q}(m'_q) - \sum_{r=1}^{R} C^m_{r,p}(m'_r)]^+ - P^S{}_{p,m}.T_S \quad (4.8)$$

Here, m represents all the actions taken by all the SUs on channel m and m' represents all the actions taken by the attackers. Each SU targets to maximize the utility function and m_{-p}

represents all the actions taken by SUs except the SU on link p and the utility function of the eavesdroppers q on channel m for $q \in Q$ can be expressed as

$$U_{EV}(m, m'_q) = -P_x[C_p^m(m_p) - \max_{q \in \mathbb{Q}} C_{p,q}^m(m'_q)]^+ \tag{4.9}$$

and the utility function of the jammers r on channel m for $r \in \mathbb{R}$ can be expressed as,

$$U_{JM}(m, m'_r) = P_x[\sum_{r=1}^{R} C_{r,p}^m(m'_r)]^+ - P^J{}_{r,m}.T_J \tag{4.10}$$

Now suppose, $a_e \in \mathbb{M}_e$ be the action of all players such that $e \in \mathbb{H}$ where $a_e = m_e$ if $e \in \mathbb{P}$ and $a_e = m'_e$ if $e \in \mathbb{U}$, where $\mathbb{U} = \mathbb{Q} \cup \mathbb{R}$. Now combining (4.8), (4.9), and (4.10), the general utility function can be defined as follows,

$$U_e(a_e, \boldsymbol{a_{-e}}) = \begin{cases} U_{SU}(m_e, \boldsymbol{m_{-e}}, m'), & \text{if } e \in \mathbb{P} \\ U_{EV}(m, m'_e), & \text{if } e \in \mathbb{Q} \\ U_{JM}(m, m'_e), & \text{if } e \in \mathbb{R} \end{cases} \tag{4.11}$$

It is clear from (4.9) and (4.10) that the attackers are mainly competing against the SUs, not against themselves thus maximizing their utility in order to decrease the secrecy rate of the SUs. Thus, instead of calculating different utility functions for the eavesdroppers and jammers their utility functions are combined into a single utility function as the utility function of attackers. The combined utility function can be represented as,

$$U_{AC}(m, m') = -P_x[C_p^m(m_p) - \max_{q \in \mathbb{Q}} C_{p,q}^m(m'_q) - \sum_{r=1}^{R} C_{r,p}^m(m'_r)]^+ - P^J{}_{r,m}.T_J \tag{4.12}$$

Using (4.12) and (4.11) the general utility function for all the players can be re-written as,

$$U(a_e, \boldsymbol{a_{-e}}) = \begin{cases} U_{SU}(m_e, \boldsymbol{m_{-e}}, m'), & \text{if } e \in \mathbb{P} \\ U_{AC}(m, m'), & \text{if } e \in \mathbb{U} \end{cases} \tag{4.13}$$

It is assumed that $g_e = [g_e^1, g_e^2, g_e^3, \cdots, g_e^M] \in \Lambda_m$ is the mixed strategy of any player e $\forall e \in \mathbb{H}$ where player e consists of SUs, jammers and eavesdroppers. Each component g_e^m represents how frequently player e uses channel m for transmission (if the player is SU) or

how frequently player e eavesdrops or jams channel m (if the player is an attacker). So, g_e^m represents the space of all possible mixed strategies for player e. Then, the expected utility function of player e can be expressed as,

$$\begin{aligned}\bar{U}_e(g_e, \boldsymbol{g_{-e}}) &= \mathbb{E}_g[U_e(a_e, \boldsymbol{a_{-e}})] \\ &= \sum_{a_1 \in \mathbb{M}_1} \cdots \sum_{a_\phi \in \mathbb{M}_\phi} U_e(a_1, \cdots, a_\phi) \prod_{k=1}^{\phi} g_k^{a_k}\end{aligned} \tag{4.14}$$

where $\phi = P + Q + R$.

Among P SUs, Q eavesdroppers, and R jammers, based on (4.14), a non-cooperative game can be formulated as

$$\mathcal{G} = \{\mathbb{H}, \Lambda_m, \bar{U}_e(.)\} \tag{4.15}$$

where

- $\mathbb{H}$ is the set of players that are active users (SUs, eavesdroppers, and jammers) in the network.
- Λ_m is the set of strategies for the players. For SUs Λ_m represents how frequently they uses channel m and for attackers Λ_m represents how frequently they eavesdrop or jam channel m.
- $\bar{U}_e(.)$ is the utility (aka payoff) that is the outcome based on the strategies chosen by the player.

Individual players (SUs and attackers) in the non-cooperative game $\mathcal{G}$ chooses their strategies form their strategy space and reach to the optimal point that is known as the Nash equilibrium (NE) [75]. It is assumed that the position of all players is known to each other [76] through cognitive radio and ranging technology as this assumptions is common to physical layer security (e.g., [77–79]) in cognitive radio networks. However, localization of players is beyond the scope of this chapter but interested reader could refer to the literature (e.g., [80, 81]).

In the proposed game, it is considered that players redesign their convictions about their adversaries by observing their actions. Since these actions are time dependent, $a_e(n_t)$ is characterized to be the channel selected by player e at any time n_t. Let ${g^{a_e}}_e(n_t)$, $a_e \in \mathbb{M}_e$, $e \in \mathbb{H}$, be the empirical frequency, which means that ${g^{a_e}}_e(n_t)$ is the frequency with which a player e chooses action a_e until time n_t. At current time n_t, player e has the information of the past incidents. Thus, at time n_t, when a given player e follows the actions of all other players for time n_{t-1} and n_{t-2}, it can update its knowledge of the frequencies using the recurrence, that is

$$g_e^{a_e}(n_t) = \frac{1}{n_t - 1} + \frac{n_t - 2}{n_t}.g_e^{a_e}(n_t - 1) + \frac{n_t - 2}{n_t(n_t - 1)}.g_e^{a_e}(n_t - 2) \tag{4.16}$$

When each player reached NE in the game with mixed strategy g_e^*, the expected utility function $\bar{U}_e(g_e, \boldsymbol{g}^*_{-e})$ is maximized.

$$a_e(n_t) = arg \max_{a_e \in \mathbb{M}_e} \bar{U}_e(a_e, \boldsymbol{g}_{-e}(n_t)) \tag{4.17}$$

where, $\bar{U}_e(a_e, \boldsymbol{g}_{-e}(n_t))$ represents the expected utility at the current time n_t, and is expressed as,

$$\bar{U}_e(a_e, \boldsymbol{g}_{-e}(n_t)) = \sum_{a_{-e} \in \mathbb{M}_{-e}} U_e(a_e, \boldsymbol{a}_{-e}) \prod_{a_{q/r} \in a_{-e}} g_{q/r}^{a_{q/r}}(n_t) \tag{4.18}$$

Based on the observation of the SUs, the players sequentially update their empirical frequencies using (4.16), and then select their actions according to (4.17). Note that at Nash equilibrium, strategy of each player is an optimal response to the strategies, no player could increase its utility by deviating their strategy unilaterally [75, 82, 83]. Thus, no SUs in considered system model is capable of generating a higher secrecy rate. Similarly, there is no way available for the attackers to lower the secrecy rate of the SUs by changing their strategies in a unilateral manner. For a mixed strategy profile $g^* = (g_e^*, \boldsymbol{g}^*_e)$, at Nash equilibrium, the following set of inequality for a given player $e \in \mathbb{H}$ is satisfied

$$\bar{U}_p(g_e^*, \boldsymbol{g}^*_{-e}) \geq \bar{U}_p(g_e, \boldsymbol{g}^*_{-e}), \qquad \forall g_e^* \in \Lambda_e \tag{4.19}$$

The proposed game has finite number of players and strategies to choose finite number of channels. Thus, there exists a Nash equilibrium in mixed strategies for the proposed finite non-cooperative game [75].

4.4 Numerical Analysis

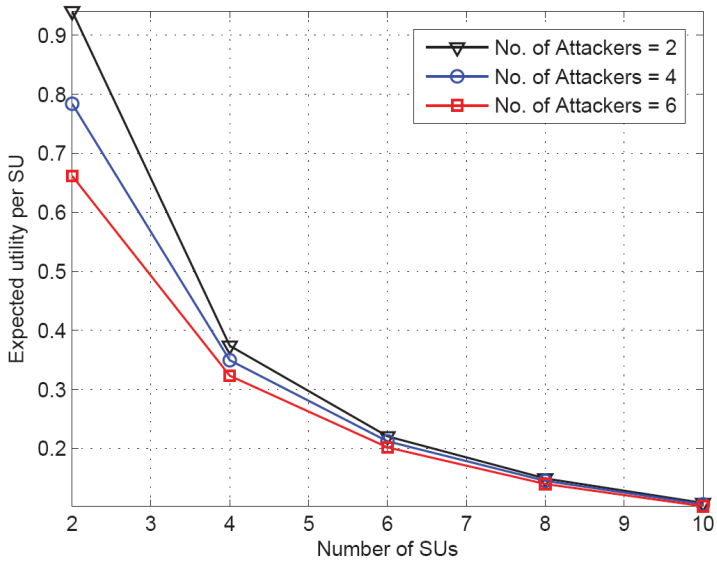


Figure 4.2: Variation of expected utility per SU vs. the total number of SUs in the network.

First, the variation of expected utility per SU against the number of active SUs for given number of attackers in the network is plotted as shown in Figure 4.2. It is observed that the increase in number of SUs in the network results in decrease in expected utility function for SUs since more SUs interfere with each other while contending for the channel access and avoiding attackers in the network. Furthermore, for a given number of SUs, as expected, increase in number of attackers results in decrease in expected utility function per SU since more attackers cause more harm to SUs as shown in Figure 4.2. The SUs experience maximum utility when the number of attackers and SUs is the minimum (only 2 attackers and 2 SUs are present). The reasoning behind that is simple. With less attackers

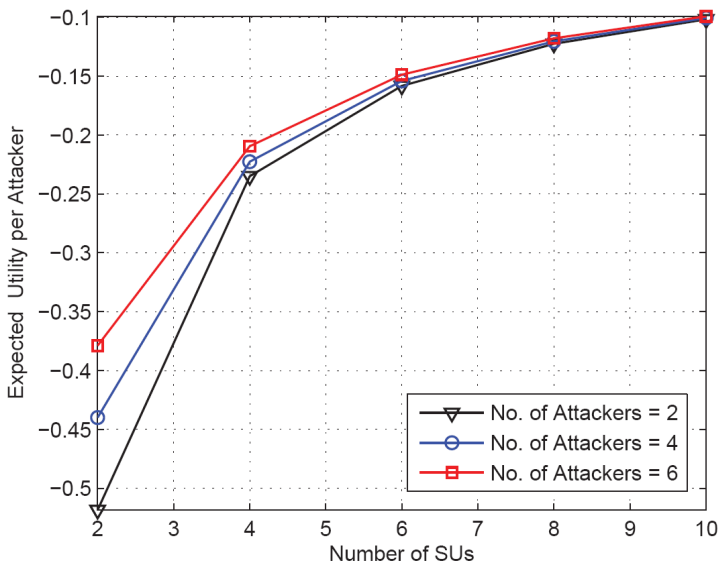


Figure 4.3: Variation of expected utility per attacker vs. the total number of SUs in the network.

SUs have less utility to loose and with less SUs the competition among the SUs to increase their channel capacity is less. When number of attackers is 2 in CR network, for 2 SUs the expected utility per SU is around 0.94, for 4 SUs the expected utility per SU is around 0.38, for 6 SUs the expected utility per SU is around 0.23, for 8 SUs the expected utility per SU is around 0.16, and for 10 SUs the expected utility per SU is around 0.1. When number of attackers is 4 in CR network, for 2 SUs the expected utility per SU is around 0.79, for 4 SUs the expected utility per SU is around 0.35, for 6 SUs the expected utility per SU is around 0.22, for 8 SUs the expected utility per SU is around 0.15, and for 10 SUs the expected utility per SU is around 0.1. When number of attackers is 6 in CR network, for 2 SUs the expected utility per SU is around 0.67, for 4 SUs the expected utility per SU is around 0.32, for 6 SUs the expected utility per SU is around 0.21, for 8 SUs the expected utility per SU is around 0.14, and for 10 SUs the expected utility per SU is around 0.1. Then, in Figure 4.3 the variation of expected utility for attackers against the number of SUs present in the

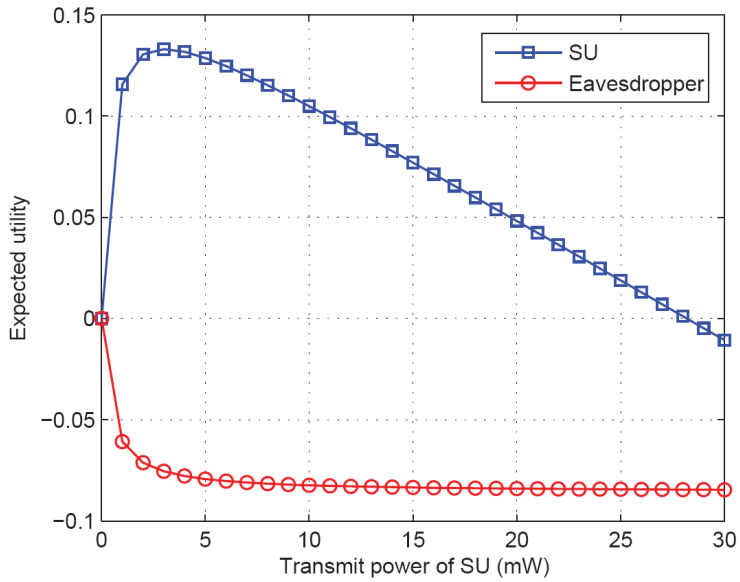


Figure 4.4: Variation of expected utilities of SU and eavesdropper vs. transmit power of SU.

network is plotted. As expected, it is observed that with increase in number of SUs, the expected utility per attacker increases as shown in Figure 4.3 since more users are harmed by given number of attackers. Furthermore, for a given number of attackers, when number of attackers increases, the utility for attackers increases since more number of attackers could harm SUs more severely as shown in Figure 4.3. The attackers experience maximum utility when the number of attackers and SUs is the maximum (6 attackers and 10 SUs are present). The reasoning behind that is very simple. As more attackers are present in the network it results into less utility for SUs which in turn ensures more utility for attackers. And also more SUs mean there is more competition present in the network among the SUs. This results in less utility for SUs which in turn means that the attackers have more utility. When number of attackers is 2 in CR network, for 2 SUs the expected utility per attacker is around -0.53, for 4 SUs the expected utility per attacker is around -0.24, for 6 SUs the expected utility per attacker is around -0.17, for 8 SUs the expected utility per attacker is

around −0.13, and for 10 SUs the expected utility per SU is around −0.1. When number of attackers is 4 in CR network, for 2 SUs the expected utility per attacker is around −0.44, for 4 SUs the expected utility per attacker is around −0.23, for 6 SUs the expected utility per attacker is around −0.16, for 8 SUs the expected utility per attacker is around −0.125, and for 10 SUs the expected utility per SU is around −0.1. When number of attackers is 6 in CR network, for 2 SUs the expected utility per attacker is around −0.38, for 4 SUs the expected utility per attacker is around −0.22, for 6 SUs the expected utility per attacker is around −0.15, for 8 SUs the expected utility per attacker is around −0.12, and for 10 SUs the expected utility per SU is around −0.1.

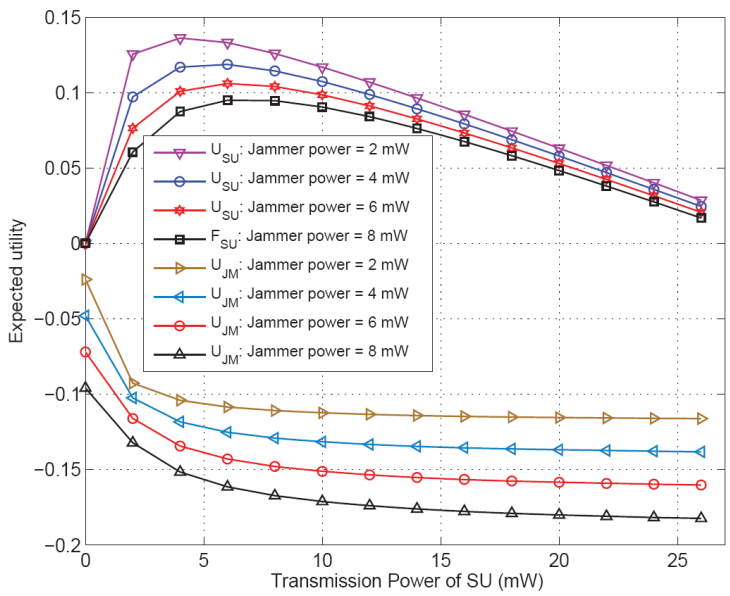


Figure 4.5: Variation of expected utilities of SUs and jammers (with different transmit powers) vs. transmission power of SUs.

Second, it is considered that there are SUs and eavesdroppers present in the network but no jammers are there (i.e., there is no transmissions from attackers). In Figure 4.4, the variation of expected utility function of both SUs and eavesdroppers vs. the transmission power of SUs is plotted. For a given scenario, expected utility increases for a while for SUs

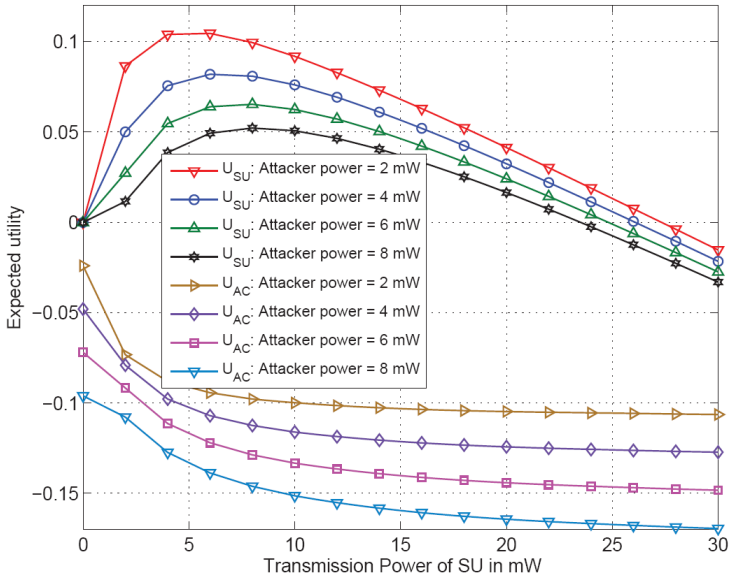


Figure 4.6: Variation of expected utility of the SUs and the attackers vs. transmit power of SU for different jamming powers.

and decreases for eavesdroppers however, it starts decreasing for SUs after the transmission power of SUs crosses 3 mW as shown in Figure 4.4. It is observed that the gap in expected utility of SUs and eavesdropper is the highest for 3 mW transmit power for SUs. This represents the best desired case for the game for a given scenario. After crossing 3 mW transmission power the utility of SUs starts decreasing and keeps behaving the same way for the remaining portion of the simulated scenario.

Then, it is considered that there are only SUs and jammers are present in the network (i.e., there is no eavesdropping from attackers). The variation of expected utility function for both SUs and jammers vs. the transmission power of SU is plotted as shown in Figure 4.5. It is considered that jammers are transmitting jamming signals with transmit power 2 to 8 mW to deteriorate the SINR of legitimate SUs. They use low power as they do not like to be detected while deteriorating SINRs of SUs. The SUs' expected utility function is increasing and then decreasing for given scenario as shown in Figure 4.4. In this case,

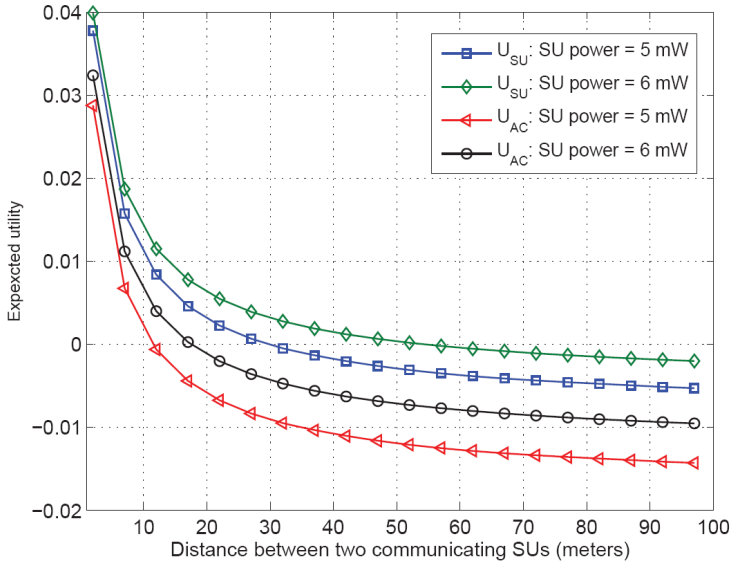


Figure 4.7: Variation of expected utility of the SUs and the attackers vs. distance between the SUs with different transmit power.

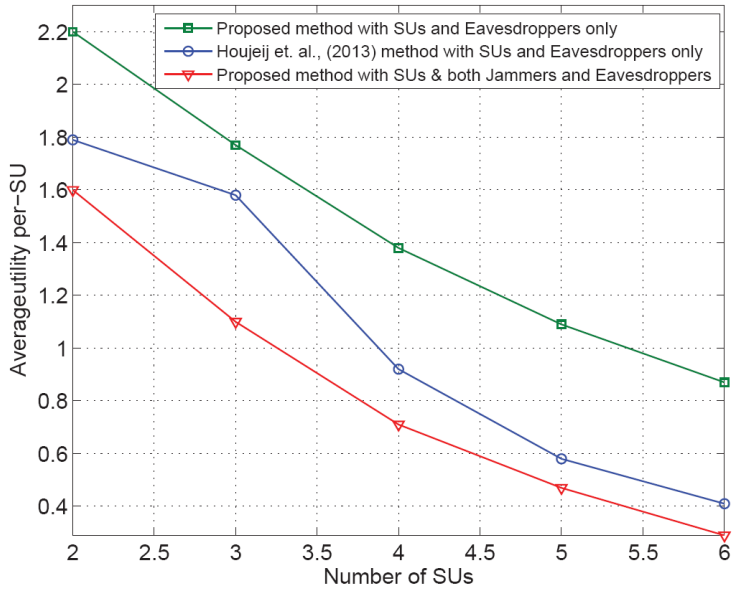


Figure 4.8: Comparison of expected utility per SU between proposed approach and the method in [4] for a given number of SUs.

the expected utility for SUs is the highest at around 5 mW transmission power of SU and 2 mW transmission power of the jammer. The SUs' transmit power for the highest expected utility increases from previous case since jammers are injecting signal which in turn forces SUs to transmit with higher powers to maintain the signal quality. When the jammers are transmitting with 2 mW power the maximum difference between the utility of SUs and jammers is achieved with transmission power of 4 mW for SUs. And the difference is around 0.25. When the jammers are transmitting with 4 mW power the maximum difference between the utility of SUs and jammers is achieved with transmission power of 5 mW for SUs. And the difference is around 0.24. When the jammers are transmitting with 6 mW power the maximum difference between the utility of SUs and jammers is achieved with transmission power of 6 mW for SUs. And the difference is around 0.23. When the jammers are transmitting with 8 mW power the maximum difference between the utility of SUs and jammers is achieved with transmission power of 7 mW for SUs. And the difference is around 0.22.

Then, it is assumed that there are SUs as well as both eavesdroppers and jammers are present in the network. The expected utility function of both SUs and attackers (joint eavesdroppers and jammers effect) are plotted for different transmit powers of SUs in Figure 4.6. Transmit power of the jammers is also varied as shown in Figure 4.6. In this case, since there is joint impact of both eavesdroppers and jammers in the network, the expected utility function is lower (in Figure 4.6) than the case with the eavesdroppers only (in Figure 4.4) or jammers only case (in Figure 4.5). When the jammers are transmitting with 2 mW power the maximum difference between the utility of SUs and attackers is achieved with transmission power of 4 mW for SUs. And the difference is around 0.19. When the jammers are transmitting with 4 mW power the maximum difference between the utility of SUs and attackers is achieved with transmission power of 6 mW for SUs. And the difference is around 0.18. When the jammers are transmitting with 6 mW power the

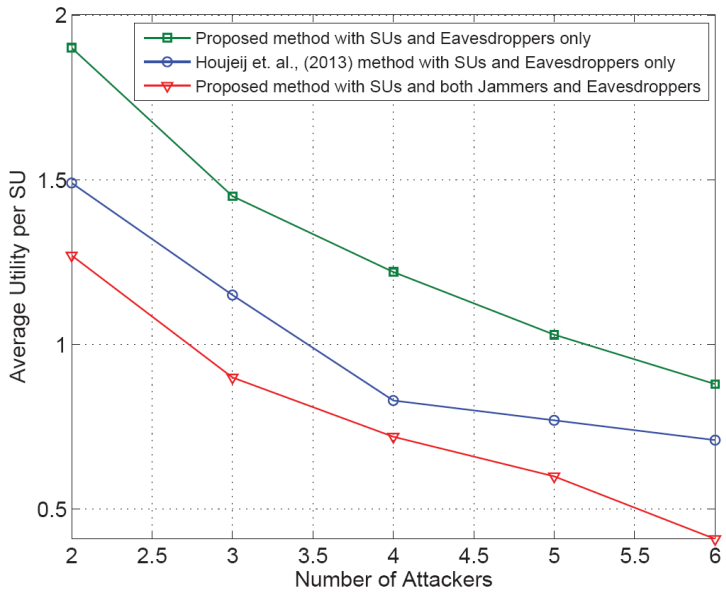


Figure 4.9: Comparison of expected utility per SU between proposed approach and the method in [4] for a given number of attackers.

maximum difference between the utility of SUs and attackers is achieved with transmission power of 8 mW for SUs. And the difference is around 0.17. When the jammers are transmitting with 8 mW power the maximum difference between the utility of SUs and attackers is achieved with transmission power of 9 mW for SUs. And the difference is around 0.16.

Next, in Figure 4.7, the expected utility function of the SUs and the attackers vs. the distance between SU transmitter and receiver pairs as well as SU receivers and jammers is plotted. As expected, increase in distance between transmitter and receiver pair results in decrease in expected utility function of both the SUs and the attackers as shown in Figure 4.7. With a transmission power of 5 mW for SUs and a distance of 22 m between two communicating SUs the expected utility for SUs is around 0.002. With a transmission power of 6 mW for SUs and a distance of 22 m between two communicating SUs the expected utility for SUs is around 0.008. With a transmission power of 5 mW for SUs

and a distance of 22 m between two communicating SUs the expected utility for attackers is around -0.008. With a transmission power of 6 mW for SUs and a distance of 22 m between two communicating SUs the expected utility for attackers is around -0.002.

Finally, identical scenarios are considered to compare the proposed approach with the method in the literature [4]. Note that the work in [4] considers the impact of eavesdroppers only. When it is considered that the jammers are not present in the network, the approach mentioned in this chapter becomes identical to that of [4]. In this scenario, multiple experiments are conducted to find average of expected utility for a given number of SUs (six SUs) and plotted its variation against the number of SUs as shown in Figure 4.8 and the variation of expected utility against the number of attackers as shown in Figure4.9.

In Figure 4.8 the proposed method provides average utility of 2.2, 1.78, 1.39, 1.1 and 0.88 per SU for the number of SUs being 2, 3, 4, 5 and 6 respectively when only eavesdroppers are present in the network besides SUs. But the method described in [4] provides average utility of 1.8, 1.6, 0.92, 0.6 and 0.4 per SU for the number of SUs being 2, 3, 4, 5 and 6 respectively when only eavesdroppers are present in the network besides SUs. All of these utility values in [4] are less than the utility values of the proposed method of this thesis. The proposed method provides average utility of 1.6, 1.1, 0.71, 0.43 and 0.28 per SU for the number of SUs being 2, 3, 4, 5 and 6 respectively when both jammers and eavesdroppers are present in the network besides SUs. This time the utility of the proposed method in this thesis is less than the method mentioned in [4].

In Figure 4.9 the proposed method provides average utility of 1.9, 1.45, 1.25, 1.05 and 0.8 per SU for the number of attackers being 2, 3, 4, 5 and 6 respectively when only eavesdroppers are present in the network besides SUs. But the method described in [4] provides average utility of 1.5, 1.2, 0.8, 0.7 and 0.6 per SU for the number of attackers being 2, 3, 4, 5 and 6 respectively when only eavesdroppers are present in the network besides SUs. All of these utility values in [4] are less than the utility values of the proposed

method of this thesis. The proposed method provides average utility of 1.25, 0.85, 0.72, 0.65 and 0.4 per SU for the number of attackers being 2, 3, 4, 5 and 6 respectively when both jammers and eavesdroppers are present in the network besides SUs. This time the utility of the proposed method in this thesis is less than the method mentioned in [4].

It is observed that when there are only eavesdroppers, the proposed approach gives higher utility than that in [4] as the model in this chapter compares the impact of eavesdropper's instantaneous SINR with its minimum target SINR while decoding the information by the eavesdropper. Note that when instantaneous SINR at eavesdropper is less than its minimum target SINR, the given eavesdropper can not decode the message and can not get any information resulting in zero loss in secrecy rate of SUs. However, when both eavesdroppers and (four) jammers are considered, the expected utility is lower than that in [4]. This happens since jammers are not considered in [4] which inject jamming power to deteriorate the SUs' SINRs which results in decrease in expected utility. It is observed that the expected utility of SU is higher (when number of SUs are increased in the network for a given number of jammers as shown in Figure 4.8) than that of when the number of attackers are increased in the network for a given number of SUs as shown in Figure 4.9.

4.5 Chapter Summary

In this chapter the performance of the secondary users in the physical layer of cognitive radio networks is evaluated when attackers (eavesdroppers and jammers) are also present. First a system model is developed depicting the the distance between transmitter and receiver of legitimate SU link, distance between jammer and receiver of the SU link, and distance between eavesdropper and transmitter of the SU link. Based on that system model $SINR$ of the secondary users, eavesdroppers and jammers is determined. Then the channel capacity is determined based on the $SINR$ values. To formulate the game it is necessary to formulate utility function of the players. First of all in this chapter secondary users, eavesdroppers and

jammers are considered as the players. Then their utility functions are formulated based on their rate of secrecy and transmission cost if there is any. The strategy used by the secondary users in this chapter is how many times they use a particular channel for transmission and the strategy used by the attackers is how many times they use that particular channel to either eavesdrop (if the attacker is eavesdropper) or jam (if the attacker is jammer) on secondary users. A Nash equilibrium position is later reached in this game which results into maximum attainable rate of secrecy for the secondary users.

The numerical analysis is presented in Section 4.4. It is observed from the numerical analysis that secondary users provide better performance in an order of when there is no attackers in the network, when there are only eavesdroppers present in the network, when there are only jammers present in the network, and when there are both eavesdroppers and jammers present in the network. It is also observed that the proposed approach outperforms other existing methods in terms of expected utility only when eavesdroppers are present in the network as attackers.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion and Discussion

Cognitive radio has become an major enabling technology to exploit the idle or inactive licensed bands. CR has to first scan the channel and if it senses that no PU is currently using the channel it will occupy the idle channel and keep sensing the channel to sense the return of the eligible owner or licensed user of the channel. Whenever it senses that PU is back it has leave the channel immediately and start looking for a new idle channel. Therefore, the concept of spectrum sensing is very important in CR. Again tremendous increase in demand for CR devices may make it vulnerable to major security threats. To ensure the secrecy of classified or personal information and to make the receiving end comfortable in getting and decoding information CR networks must introduce strict security against eavesdroppers and jammers.

Chapter 2 describes about the theoretical background of this thesis. CR can be defined as as a radio that can change its transmitter parameters based on interaction with its environment. The ultimate objective of the CR is to obtain the best available spectrum through cognitive capability and reconfigurability. Since CR is considered lower priority compared to the PUs, a fundamental requirement is to avoid interference to potential PUs in their vicinity and for this reason spectrum sensing is very important feature of CR. In spectrum sensing the probability by which a CR mistakenly considers the band unoccupied though a PU is present is called probability of misdetection and the probability by which the detection algorithm incorrectly decides that the considered frequency is occupied when it actually is not is called probability of false alarm.

Chapter 3 mainly focuses on investigating the joint impact of SU mobility and PU activity on spectrum sensing in CR enabled vehicular networks. Analytical model is derived

for the probability of misdetection for spectrum sensing and expected value of overlapping time duration per epoch for mobile SUs. The theoretical analysis and analytical results are validated and confirmed by numerical results obtained from simulations. It is observed that when speed of the vehicles increases, the probability of misdetection increases (but no significant impact on false alarm) and the expected overlapping time duration per epoch (between mobile SU and stationary PU) decreases.

Chapter 4 on the physical layer security concerns of CR. Here the performance of physical layer security of SUs in the presence of both eavesdroppers and jammers in CR networks is analyzed using game theory. In the proposed game, SUs choose their strategies to maximize their utilities (secrecy rates) while eavesdroppers and jammers choose their actions to minimize the same. A generalized form is proposed which can be particularized to a scenario with only eavesdroppers or only jammers or both eavesdroppers and jammers are present in the physical layer of the CR networks while calculating the secrecy rates of SU. Numerical results obtained from simulations support theoretical analysis. It is also observed that there is sever impact on secrecy rates of SUs when both eavesdroppers and jammers are active in the network. Furthermore, it is observed that the proposed approach outperforms the other existing methods in terms of expected utility when only eavesdroppers are considered to be present as attackers in the network.

5.2 Future Work

This thesis provides extensive evaluation of spectrum sensing performance of SUs in CR networks and on performance evaluation of SUs in the presence of physical layer security threats of CR networks when eavesdroppers and jammers act as attackers. Future works include investigation of spectrum sensing performance by incorporating velocity of both PUs and SUs. That will enable us to study the change of distance between PUs and SUs in any direction and to learn its impact on spectrum sensing. Besides that impact of non-

linear movement from both SUs and PUs on spectrum sensing could also be investigated. Again this thesis focuses on preventing eavesdroppers from secretly listening to classified or personal information and jammers from jamming the channel to to degrade the signal quality in the receiver's end. But besides eavesdroppers and jammers there are some more threats to the physical layer security of CR networks such as PU emulation attack, objective function attack, learning attack, spectrum sensing data falsification attack. In future study, the horizon of the research will be broaden to include mobility of both SUs and PUs in spectrum sensing and other types of physical layer security threats. In future study, the system models could be tested using experiments with the help of NI-USRP devices.

REFERENCES

[1] L. Frenzel, *Understanding Solutions For The Crowded Electromagnetic Frequency Spectrum*, 2012. [Online]. Available: http://electronicdesign.com/communications/understanding-solutions-crowded-electromagnetic-frequency-spectrum

[2] NTIA, *United States Frequency Allocation Chart*, 2003. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

[3] M. Subhedar and G. Birajdar, "Spectrum sensing techniques in cognitive radio networks: a survey," *International Journal of Next-Generation Networks*, vol. 3, no. 5, pp. 37–51, 2011.

[4] A. Houjeij, W. Saad, and T. Bascar, "A game-theoretic view on the physical layer security of cognitive radio networks," *in Proceedings of 2013 IEEE International Conference on Communications (ICC)*, pp. 2095–2099, 2013.

[5] R. H. Coase, "The federal communications commission," *The Journal of Law & Economics*, vol. 2, no. 5, pp. 1–40, 1959.

[6] R. Saruthirathanaworakun and J. M. Peha, "Dynamic primary-secondary spectrum sharing with cellular systems," *in Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks & Communications (CROWNCOM)*, pp. 1–6, 2010.

[7] J. Mitola, "Cognitive radio-an integrated agent architecture for software defined radio," *in Proceedings of IEEE Personal Communications*, 2000.

[8] J. Mitola III and G. Q. Maguire Jr, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[9] B. Wang and K. Liu, "Advances in cognitive radio networks: A survey," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 5, pp. 5–23, 2011.

[10] J. L. Mauri, K. Z. Ghafoor, D. B. Rawat, and J. M. A. Perez, *Cognitive Networks: Applications and Deployments*. CRC Press, 2014.

[11] W.-Y. Lee and I. F. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3845–3857, 2008.

[12] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *IEEE Transaction on Spectrum Sensing*, vol. 50, no. 13, pp. 2127–2159, 2006.

[13] G. Staple and K. Werbach, "The end of spectrum scarcity [spectrum allocation and utilization]," *IEEE Transaction on Spectrum Sensing*, vol. 41, no. 3, pp. 48–52, 2004.

[14] P. Kolodzy and I. Avoidance, "Spectrum policy task force," *IEEE transaction on Digital Signal Processing*, vol. 41, no. 3, pp. 48–52, 2002.

[15] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *IEEE Communications Magazine*, vol. 46, no. 5, pp. 32–39, 2008.

[16] F. C. Commission *et al.*, "Notice of Proposed Rulemaking, in the matter of unlicensed operation in the TV broadcast bands (ET Docket No. 04-186) and additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band (ET Docket No. 02-380), FCC 04-113," 2004.

[17] S. Haykin, D. J. Thomson, and J. H. Reed, "Spectrum sensing for cognitive radio," *in Proceedings ofIEEE Signal Processing Conference*, pp. 849–877, 2009.

[18] D. B. Rawat, J. J. Rodrigues, and I. Stojmenovic, *Cyber-Physical Systems: From Theory to Practice*. CRC Press, 2015.

[19] D. B. Rawat, B. B. Bista, G. Yan, and S. Shetty, "Waiting probability analysis for opportunistic spectrum access," *International Journal of Adaptive and Innovative Systems 7*, vol. 2, no. 1, pp. 15–28, 2014.

[20] D. B. Rawat and D. C. Popescu, "Precoder adaptation and power control for cognitive radios in dynamic spectrum access environments," *IET Communications Journal*, vol. 6, no. 8, pp. 836–844, 2012.

[21] Y. Gongjun, D. Rawat, and B. Bista, "Provisioning vehicular ad hoc networks with QoS," *Int. Conf. on Broadband, Wireless Computing, Communic. and Applications (BWCCA)*, pp. 102–107, 2010.

[22] D. B. Rawat, T. Amin, and M. Song, "The impact of secondary user mobility and primary user activity on spectrum sensing in cognitive vehicular networks," *in Proceedings of 2015 IEEE INFOCOM Conference Smartcity Workshop*, pp. 588–593, 2015.

[23] T. Amin, D. B. Rawat, and M. Song, "Performance Analysis of Secondary Users in the Presence of Attackers in Cognitive Radio Networks," *in Proceedings of IEEE GLOBECOM Conference*, pp. 101–108, 2015.

[24] H. Arslan, *Cognitive radio, software defined radio, and adaptive wireless systems*. Springer, 2007, vol. 10.

[25] D. B. Rawat and G. Yan, "Spectrum sensing methods and dynamic spectrum sharing in cognitive radio networks: A survey," *International Journal of Research and Reviews in Wireless Sensor Networks*, vol. 1, no. 1, pp. 1–13, 2011.

[26] D. B. Rawat, S. Shetty, and K. Raza, "Geolocation-aware resource management in cloud computing-based cognitive radio networks," *International Journal of cloud computing*, vol. 3, no. 3, pp. 267–287, 2014.

[27] A. Singh, "Review article digital change detection techniques using remotely-sensed data," *International Journal of Remote Sensing*, vol. 10, no. 6, pp. 989–1003, 1989.

[28] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing cognitive radio networks," *International journal of communication systems*, vol. 23, no. 5, pp. 633–652, 2010.

[29] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," *Journal of Internet Technology*, vol. 12, no. 2, pp. 181–198, 2011.

[30] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[31] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," *in Proceedings of 3rd IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pp. 1–8, 2008.

[32] R. Chen, J.-M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *in Proceedings of 3rd International Conference on Digital Signal Processing*, pp. 50–55, 2008.

[33] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, "Multi-channel jamming attacks using cognitive radios," *in Proceedings of 16th International Conference on Computer Communications and Networks*, pp. 352–357, 2007.

[34] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," *in Proceedings of the 3rd ACM Workshop on Wireless Security*, pp. 80–89, 2004.

[35] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Transactions on Communications*, vol. 58, no. 6, pp. 1877–1886, 2010.

[36] D. Goldman, "Sorry, America: Your wireless airwaves are full," *CNN Money Tech*, vol. 55, no. 4, pp. 523–531, 2012.

[37] D. B. Rawat, M. Song, and S. Shetty, "Resource Allocation in Spectrum Underlay Cognitive Radio Networks," in *Dynamic Spectrum Access for Wireless Networks*, 2015, vol. 55, no. 4, pp. 523–531.

[38] D. B. Rawat, B. B. Bista, G. Yan, and S. Olariu, "Vehicle-to-Vehicle Connectivity and Communication Framework for Vehicular Ad-Hoc Networks," *in Proceedings of 2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, pp. 44–49, 2014.

[39] D. B. Rawat, S. Reddy, N. Sharma, and S. Shetty, "Cloud-assisted dynamic spectrum access for VANET in transportation cyber-physical systems," *in Proceedings of 2014 IEEE International Performance Computing and Communications Conference (IPCCC)*, pp. 1–2, 2014.

[40] D. B. Rawat, S. Reddy, N. Sharma, B. B. Bista, and S. Shetty, "Cloud-assisted GPS-driven dynamic spectrum access in cognitive radio vehicular networks for transportation cyber physical systems," *in Proceedings of 2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1942–1947, 2015.

[41] D. B. Rawat, D. C. Popescu, G. Yan, and S. Olariu, "Enhancing VANET performance by joint adaptation of transmission power and contention window size," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 9, pp. 1528–1535, 2011.

[42] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

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

[44] Y. Zhao, M. Song, and C. Xin, "A weighted cooperative spectrum sensing framework for infrastructure-based cognitive radio networks," *IEEE Computer Communications*, vol. 34, no. 12, pp. 1510–1517, 2011.

[45] A. W. Min and K. G. Shin, "Impact of mobility on spectrum sensing in cognitive radio networks," *in Proceedings of ACM workshop on Cognitive radio networks*, pp. 13–18, 2009.

[46] A. S. Cacciapuoti, I. F. Akyildiz, and L. Paura, "Primary-user mobility impact on spectrum sensing in cognitive radio networks," *in Proceedings of IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pp. 451–456, 2011.

[47] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication Journal*, vol. 4, no. 5, pp. 40–62, 2011.

[48] Y. Zhao, P. Paul, C. Xin, and M. Song, "Performance analysis of spectrum sensing with mobile sus in cognitive radio networks," *in Proceedings of IEEE International Conference on Communications (ICC)*, pp. 2761–2766, 2014.

[49] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," *in Proceedings of New Frontiers in Dynamic Spectrum, 2010*, pp. 1–12, 2010.

[50] G. Yan, D. B. Rawat, and B. B. Bista, "Provisioning vehicular ad hoc networks with quality of service," *International Journal of Space-Based and Situated Computing*, vol. 2, no. 2, pp. 104–111, 2012.

[51] H. Urkowitz, "Energy detection of unknown deterministic signals," *IEEE Intelligent Vehicles Symposium*, vol. 55, no. 4, pp. 523–531, 2014.

[52] D. B. Rawat and S. Shetty, "Enhancing connectivity for spectrum-agile vehicular ad hoc networks in fading channels," *in Proceedings of IEEE Intelligent Vehicles Symposium*, pp. 957–962, 2014.

[53] S. Yousefi, E. Altman, R. El-Azouzi, and M. Fathy, "Improving connectivity in vehicular ad hoc networks: An analytical study," *IEEE Transaction on Computer communications, 2008*, vol. 31, no. 9, pp. 1653–1659, 2008.

[54] S. Song, K. Hamdi, and K. B. Letaief, "Spectrum sensing with active cognitive systems," *IEEE Transactions on wireless communications*, vol. 9, no. 6, pp. 1849–1854, 2010.

[55] R. C. Qiu, Z. Hu, H. Li, and M. C. Wicks, *Cognitive radio communication and networking: Principles and practice*. John Wiley & Sons, 2012.

[56] D. B. Rawat, M. Song, and S. Shetty, *Dynamic Spectrum Access for Wireless Networks*. Springer, 2015.

[57] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust On the Security of Wireless Vehicular Ad-hoc Networking," *Ad Hoc & Sensor Wireless Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.

[58] S. Alrabaee, A. Agarwal, D. Anand, and M. Khasawneh, "Game theory for security in cognitive radio networks," *in Proceedings of IEEE International Conference on Advances in Mobile Network, Communication and Its Applications (MNCAPPS)*, pp. 60–63, 2012.

[59] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," *in Proceedings of 3rd IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pp. 1–7, 2008.

[60] C. Xin and M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern," *IEEE Transactions on Mobile Computing*, vol. 13, no. 5, pp. 1022–1034, 2014.

[61] O. Cepheli and G. Karabulut Kurt, "Physical layer security in cognitive radio networks: A beamforming approach," *in Proceedings of First International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 233–237, 2013.

[62] D. B. Rawat, G. Yan, B. B. Bista, and V. Chandra, "wireless network security: an overview," *Building Next-Generation Converged Networks: Theory and Practice*, 2012.

[63] S. Maleki, A. Kalantari, S. Chatzinotas, and B. Ottersten, "Power allocation for energy-constrained cognitive radios in the presence of an eavesdropper," *in Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 5695–5699, 2014.

[64] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," *in Proceedings of IEEE Military Communications Conference*, pp. 1501–1506, 2005.

[65] L. Qian, X. Li, and S. Wei, "Cross-layer detection of stealthy jammers in multi-hop cognitive radio networks," *in Proceedings of IEEE International Conference on Computing, Networking and Communications (ICNC)*, pp. 1026–1030, 2013.

[66] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A stackelberg game approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 8, pp. 4038–4047, 2013.

[67] W. Cadeau and X. Li, "Jamming probabilities and throughput of cognitive radio communications against a wideband jammer," *in Proceedings of 47th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, 2013.

[68] E. Meamari, K. Afhamisisi, and H. S. Shahhoseini, "An analysis on interactions among secondary user and unknown jammer in cognitive radio systems by fictitious play," *in Proceedings of 10th International ISC Conference on Information Security and Cryptology (ISCISC)*, pp. 1–6, 2013.

[69] C. Chen, M. Song, and C. Xin, "A density based scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks," *in Proceedings of 2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 623–628, 2013.

[70] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[71] J. C. Harsanyi, R. Selten *et al.*, "A general theory of equilibrium selection in games," *MIT Press Books*, vol. 1, no. 10, pp. 4687–4698, 1988.

[72] D. B. Rawat, C. Bajracharya, G. Yan, and V. Rangel-Licea, "Game Theory for Resource Allocation in Wireless Networks," *in Proceedings of Emerging Technologies in Wireless Ad-hoc Networks: Applications and Future Development*, p. 335, 2010.

[73] D. B. Rawat and S. Shetty, "Game Theoretic Approach to Dynamic Spectrum Access with Multi-radio and QoS Requirements," *in Proceedings of 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 1150–1153, 2013.

[74] D. B. Rawat, B. B. Bista, and G. Yan, "CoR-VANETs: Game theoretic approach for channel and rate selection in cognitive radio VANETs," *in Proceedings of 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*, pp. 94–99, 2012.

[75] T. Basar, G. J. Olsder, G. Clsder, T. Basar, T. Baser, and G. J. Olsder, *Dynamic noncooperative game theory*. Springer, 1995, vol. 200.

[76] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, 2009.

[77] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[78] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," *in Proceedings of International Symposium on Information Theory*, pp. 2152–2155, 2005.

[79] H. Yamamoto, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Transactions on Information Theory*, vol. 37, no. 3, pp. 634–638, 1991.

[80] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[81] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," *in Proceedings of 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1132–1138, 2008.

[82] S. Azhar, A. McLennan, and H. Reif, "Computation of equilibria in noncooperative games," *in Proceedings of International Conference on Computer networks*, pp. 56–61, 1991.

[83] P. J. Reny, "Non-Cooperative Games: Equilibrium Existence," *The New Palgrave Dictionary of Economics*, 2005.